

A
C
A
D
E
M
I
C

T
R
A
C
K

4th Annual Symposium on Information Assurance



>> ASIA '09

conference proceedings

4th Annual Symposium on Information Assurance (ASIA '09)

Symposium Chair:

Sanjay Goel

Information Technology Management, School of Business
University at Albany, State University of New York

Academic Track of 12th Annual NYS Cyber Security Conference
Empire State Plaza Albany, NY, USA
June 3-4, 2009

**Proceedings of the 4th Annual Symposium on Information Assurance
Academic track of the 12th Annual 2009 NYS Cyber Security Conference
June 3-4, 2009, New York, USA.**

Symposium Chairs

Sanjay Goel, Chair

Director of Research, NYS Center for Information Forensics and Assurance (CIFA)
Associate Professor, Information Technology Management, School of Business, University at Albany, SUNY

Laura Iwan, Co-Chair

State ISO, NYS Office of Cyber Security and Critical Infrastructure Coordination (CSCIC)

Program Committee

Alexey Salnikov, Moscow State University, Russia
Arun Lakhota, University of Louisiana at Lafayette
Anil B. Somayaji, Carleton University, Canada
George Berg, University at Albany, SUNY
Gurpreet Dhillon, Virginia Commonwealth University
Hong C. Li, Intel Corporation
Martin Loeb, University of Maryland
Michael Sobolewski, Texas Tech University
R. Sekar, Stony Brook University, SUNY
Robert Bangert-Drowns, University at Albany, SUNY
S. S. Ravi, University at Albany, SUNY
Raj Sharman, University at Buffalo, SUNY
Stelios Sidiroglou-Douskos, MIT

Daniel O. Rice, Technology Solutions Experts, Inc.
M.P. Gupta, Indian Institute of Technology, Delhi
Dipankar Dasgupta, University of Memphis
Shiu-Kai Chin, Syracuse University
Ronald Dodge, USMA West Point
Rahul Singh, University of North Carolina, Greensboro
Melissa Dark, Purdue University
Nasir Memon, Brooklyn Polytechnic
Raghu T. Santanam, Arizona State University
Stephen F. Bush, GE Global Research Center
Boleslaw Szymanski, Rensselaer Polytechnic Institute
Shambhu J. Upadhyaya, University at Buffalo, SUNY
Saeed Abu-Nimeh, Websense Inc.

External Reviewers

Scott Buffett, National Research Council Canada, Institute for Information Technology
Suresh N. Chari, Secure Software and Development, IBM T.J. Watson Research Center
Ingrid Fisher, Accounting, School of Business, University at Albany, SUNY
Saggi Nevo, Information Technology Mgt., School of Business, University at Albany, SUNY
Prahalad Rangan, College of Computing and Information, University at Albany, SUNY
Scarlet Schwiderski-Grosche, Information Security Group, Royal Holloway, University of London

Submissions Chair

Damira Pon, University at Albany, SUNY

Note of Thanks

We would like to express our appreciation to all of the sponsors which supported the symposium.

SYMPOSIUM DINNER SPONSOR



CONFERENCE KILOBYTE SPONSOR



This volume is published as a collective work. Rights to individual papers remain with the author or the author's employer. Permission is granted for the noncommercial reproduction of the complete work for educational research purposes.

A
C
A
D
E
M
I
C

T
R
A
C
K

4th Annual Symposium on Information Assurance



>> ASIA '09

conference proceedings

4th Annual Symposium on Information Assurance (ASIA '09)

Symposium Chair:

Sanjay Goel

Information Technology Management, School of Business
University at Albany, State University of New York

Academic Track of 12th Annual NYS Cyber Security Conference
Empire State Plaza Albany, NY, USA
June 3-4, 2009

MESSAGE FROM SYMPOSIUM CHAIRS

Welcome to the 4th Annual Symposium on Information Assurance (ASIA'09)! This symposium complements the NYS Cyber Security Conference as its academic track with a goal of increasing interaction among practitioners and researchers to foster infusion of academic research into practice. For the last two years, this symposium has been a great success with excellent papers and participation from academia, industry, and government and highly attended sessions. This year, we again have an excellent set of papers, invited talks, and keynote addresses.

Our keynote speakers this year are Philip Reiting, Deputy Undersecretary of the National Protection and Programs Directorate, U.S. Department of Homeland Security and Raphael Perl, Head, Action Against Terrorism Unit, Office of Security Cooperation in Europe. The symposium has papers in multiple areas of security, including web/email security, distributed security management, nanosensor security, security governance, application security, and internet security. We hope to include selected papers from this symposium in a journal special issue. We have also included the roundtable discussion on forensics training and education to the program that we held last year based on strong participant interest.

We would like to thank the talented program committee that has supported the review process of the symposium. In most cases, the papers were assigned to at least three reviewers who were either members of the program committee or experts outside the committee. We ensured that there was no conflict of interest and that each program committee member was not assigned to review more than two papers. We also personally read the papers and the reviews and concurred with the assessment of the reviewers. For this year's symposium, we have 8 refereed papers and two invited papers. Our goal is to keep the quality of submissions high as the symposium matures. The program committee serves a critical role in the success of the symposium and we are thankful for the participation of each member.

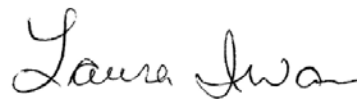
We were fortunate to have extremely dedicated partners in the NYS Office for Cyber Security and Critical Infrastructure Coordination (CSCIC) and the University at Albany, State University of New York (UAlbany). Our partners have managed the logistics for the conference, allowing us to focus on the program management. We would like to thank the University at Albany's School of Business and Symantec for providing financial support for the symposium.

We hope that you enjoy the symposium and continue to participate in the future. In each of the subsequent years, we plan to have different themes in security-related areas. Next year, the symposium will be held on June 9-10, 2010. If you would like to propose a track, please let us know. The call for papers for next year's symposium will be distributed in the fall and we hope to see you again in 2010.



Sanjay Goel

Director of Research, CIFA
Associate Professor, School of Business



Laura Iwan

NYS ISO, Office of Cyber Security and Critical
Infrastructure Coordination (CSCIC)

SYMPOSIUM ON INFORMATION ASSURANCE AGENDA

DAY 1: Wednesday, June 3 2009

REGISTRATION – Base of the Egg (7:00am – 4:00pm)

VISIT THE EXHIBITORS / IA GAMES – Base of the Egg (7:00am – 9:00am)

CONFERENCE MORNING SESSION – Egg Swyer Theater (9:00am – 10:30am)

Welcome Address: William Pelgrin, *Director, CSCIC* & George Philip, *President, UAlbany*

Plenary Session

Talk – Cyber Warfare: The New Frontier of International Conflict: Sanjay Goel

Hacking Demo – X-Men: Hacking Underworld: Sanjay Goel & Damira Pon, *School of Business and NYS Center for Information Forensics and Assurance at the University at Albany, SUNY*

MORNING BREAK & VISIT EXHIBITORS / IA GAMES (10:30 – 11:45)

SYMPOSIUM SESSION 1: Invited Talk - Mtg. Rm. 7 (10:45am – 11:45am)

Chair: George Berg, *University at Albany, SUNY*

Russian Cyber Warfare and the Magic of Misdirection

Jeff Carr, *Greylogic*

LUNCH / VISIT EXHIBITORS / IA GAMES – Base of the Egg (11:45am – 12:30pm)

CONFERENCE OPENING TALKS – Egg Swyer Theater (12:30am – 1:30pm)

Introduction: Will Pelgrin, *Director, CSCIC*

Keynote: Philip Reiting, *Deputy Undersecretary of the National Protection and Programs Directorate, U.S. Department of Homeland Security*

SYMPOSIUM SESSION 2: Security Management (1:40pm – 2:40pm)

Chair: Raj Sharman, *University at Buffalo, SUNY*

Behavior Targeting and the Modeling of Economic Compensation for Accessing Private User Behavior Information

Daniel O. Rice, *Technology Solutions Experts, Inc.*

Organizational Power and Information Security Implementation

Jon Blue, *University of Delaware* & Gurpreet Dhillon, *Virginia Commonwealth University*

COFFEE BREAK / VISIT THE EXHIBITORS / IA GAMES (2:40pm – 3:00pm)
– Base of the Egg

SYMPOSIUM SESSION 3: Distributed Security (3:00 – 4:00)

Chair: Arun Lakhotia, *University of Louisiana at Lafayette*

Federated Role-based Access Control in Exertion-Oriented Programming

Satish Vellanki & Michael Sobolewski, *Texas Tech University*

IDKEYMAN: An Identity-Based Key Management Scheme for Wireless Ad Hoc Body Area Network

Sriram Sankaran, Mohammad Iftekhar Husain & Ramlingam Sridhar, *University at Buffalo, SUNY*

SYMPOSIUM ON INFORMATION ASSURANCE AGENDA, CONT'D.

DAY 2: Thursday, June 4 2009

REGISTRATION - Base of the Egg and VISIT EXHIBITORS – Convention Hall
(7:30am – 3:50 pm)

VISIT THE EXHIBITORS / IA GAMES – Base of the Egg (7:00am – 9:00am)

ASIA Keynote & Best Paper Award – Mtg. Rm. 6 (9:15am – 10:00am)

Introduction: Sanjay Goel, *Symposium Chair*

Welcome Address: Donald Siegel, *Dean, School of Business, UAlbany*

Reflections on Emerging Cyber Threats and 7 International Cooperative Responses

Raphael Perl, *Head, Action Against Terrorism Unit, Office of Security Cooperation in Europe*

Best Paper Award Presentation: Laura Iwan, *Symposium Co-Chair*

SYMPOSIUM SESSION 4: Information Assurance – Mtg. Rm. 7 (10:15 – 11:15am)

Chair: Boleslaw Szymanski, *Rensselaer Polytechnic Institute*

On Optimal AV System Strategies against Obfuscated Malware

Anshuman Singh¹, Bin Mai², Arun Lakhota¹ & Andrew Walenstein¹

¹*University of Louisiana at Lafayette*

²*Northwestern State University, Natchitoches*

A Brief Letter on Reasoning about Information Assurance using the Semantic Web

Stephen F. Bush, *GE Global Research Center*

SYMPOSIUM SESSION 5: Invited Talk (11:30 – 12:30pm)

Chair: Daniel O. Rice, *Technology Solutions Experts, Inc.*

Social and Behavioral Approaches to Information Assurance

H.R. Rao, *University at Buffalo, SUNY*

SYMPOSIUM SESSION 6: Authentication (1:30pm – 2:30pm)

Chair: Shobha Chengalur-Smith, *University at Albany, SUNY*

Re-evaluating Single Sign-On System Design Risks: An Activity Theoretic Approach

Manish Gupta, Kranti Banala & Raj Sharman, *University at Buffalo, SUNY*

Bridging Research and Practice: Secure Date Management in the Classroom

Richard Savacool & Rajendra K. Raj, *Rochester Institute of Technology*

AFTERNOON BREAK / VISIT THE EXHIBITORS / IA GAMES (2:30pm – 3:50pm)
– Base of the Egg

SYMPOSIUM SESSION 7: Roundtable: Forensic Education (2:50pm – 3:50pm)

Panelists: Fabio Auffant, *NY State Police*, Christian Balan, *Champlain College*, and Sean Smith, *NY Prosecutors Training Institute*

CLOSING REMARKS (3:50pm – 4:00pm)

Sanjay Goel, *Symposium Chair*

TABLE OF CONTENTS

| | |
|--|-----------|
| Session 1: Invited Talk | |
| Russian Cyber Warfare and the Magic of Misdirection..... | 1 |
| Jeff Carr, <i>Greylogic</i> | |
| Session 2: Security Management | |
| Behavior Targeting and the Modeling of Economic Compensation for Accessing Private User Behavior Information | 2 |
| Daniel O. Rice, <i>Technology Solutions Experts, Inc.</i> | |
| Organizational Power and Information Security Implementation | 7 |
| John Blue, <i>University of Delaware & Gurpreet Dhillon, Virginia Commonwealth University</i> | |
| Session 3: Distributed Security | |
| Federated Role-based Access Control in Exertion-Oriented Programming..... | 16 |
| Satish Vellanki & Michael Sobolewski, <i>Texas Tech University</i> | |
| IDKEYMAN: An Identity-Based Key Management Scheme for Wireless Ad Hoc Body Area Network | 23 |
| Sriram Sankaran, Mohammad Iftexhar Husain & Ramlingam Sridhar, <i>University at Buffalo</i> | |
| Symposium Keynote Address | |
| Reflections on Emerging Cyber Threats and International Cooperative Responses..... | 29 |
| Raphael Perl, <i>Head, Action Against Terrorism Unit, Office of Security Cooperation in Europe</i> | |
| Session 4: Information Assurance | |
| On Optimal AV System Strategies against Obfuscated Malware..... | 30 |
| Anshuman Singh*, Bin Mai†, Arun Lakhotia* and Andrew Walenstein*, <i>*University of Louisiana at Lafayette, LA, USA; †Northwestern State University, Natchitoches, LA, USA</i> | |
| A Brief Letter on Reasoning about Information Assurance using the Semantic Web.... | 36 |
| Stephen F. Bush, <i>GE Global Research Center</i> | |
| Session 5: Invited Talk | |
| Social and Behavioral Approaches to Information Assurance..... | 39 |
| H.R. Rao, <i>University at Buffalo, SUNY</i> | |
| SESSION 6: Authentication | |
| Re-evaluating Single Sign-On System Design Risks: An Activity Theoretic Approach... | 40 |
| Manish Gupta, Kranti Banala and Raj Sharman, <i>University at Buffalo, SUNY</i> | |
| Bridging Research and Practice: Secure Date Management in the Classroom..... | 50 |
| Richard Savacool and Rajendra K. Raj, <i>Rochester Institute of Technology</i> | |
| SESSION 7: Roundtable: Forensic Education..... | |
| Panelist: Fabio Auffant, <i>NY State Police</i> , Christian Balan, <i>Champlain College</i> , Sean Smith, <i>NY Prosecutors Training Institute</i> | 56 |
| Author Biographies..... | 57 |
| Index of Authors | 65 |

Invited Talk: Russian Cyber Warfare and the Magic of Misdirection

Jeffrey Carr, Founder & Principal
Greylogic

THE way that the Kremlin conducts its cyber warfare operations is akin to the way a magician fools his audience - through the use of misdirection. When Lee Siegel was researching his book *Net of Magic* in India, he noted in his field notes a frequent exchange that occurred with the locals: "I'm writing a book on magic," I explain, and I'm asked, "Real magic?" By real magic people mean miracles, thaumaturgical acts, and supernatural powers. "No," I answer: "Conjuring tricks, not real magic." Real magic, in other words, refers to the magic that is not real, while the magic that is real, that can actually be done, is not real magic." (Siegel, *Net of Magic*, Univ of Chicago Press, 1991, p. 425)

This upside-down illustration of what is perceived as 'real' and what isn't, lays the groundwork for one of the most important principles in magic and military operations – the art of misdirection. It also happens to be the key to the Russian Federation's strategy in conducting Information warfare, otherwise known as International Information Security. We know it as 'Cyber Warfare'. This presentation will include a survey of Russian military doctrine (A. Burutin, P. Koayesov, I. N. Dylevsky, S. A. Komov, S. V. Korotkov, S. N. Rodionov, and A. V. Fedorov) related to information warfare including a Russian Colonel's recounting of the Georgian cyber campaign of 2008. It will particularly examine the careful use of words as a tool of misdirection and compare it with the same technique used in "The Tuned Deck" as described in Daniel Dennett's paper "The Magic of Consciousness" (*Journal of Cultural and Evolutionary Psychology*, 1(2003)1, 7.19).

This presentation will also explore the misdirection of a free Russian Internet with the reality of an aggressive anti-Kremlin counter-research operation whose remit from Moscow is to "Ensure the domination of pro-Kremlin view on the Internet" and how that policy is enforced through the enlistment of Russian youth organizations; the same organization that was involved in the Estonia and Georgia cyber conflicts. Finally, this presentation will detail how one anti-Georgia Web forum was deliberately designed to obfuscate GRU/FSB involvement through the use of blacklisted hosts and Spam servers. The success of Russia's use of misdirection continues today as many Western security experts struggle to attribute the work of Russian hackers back to the Kremlin.

Behavior Targeting and the Modeling of Economic Compensation for Accessing Private User Behavior Information.

Daniel O. Rice

Technology Solutions Experts, Inc.

Abstract— Behavioral targeting uses web technologies to gather web browsing information that when analyzed is used to tailor direct marketing efforts at specific potential customers or groups of customers. The use of 3rd party cookies in this manner, however, has been called “behavioral targeting” and many believe that it is an invasion of personal privacy. Organizations and businesses who engage in behavior targeting usually do it surreptitiously, without the individuals’ permission, and with the cooperation of the users’ Internet Service Providers (ISPs). This ongoing research proposes a simple solution that will allow informed users to participate in the collection and reselling of their own personal information including compensation to users for allowing their browsing behavior and personal information to be tracked. The market premise is that there is extreme value created by firms who track, analyze, and sell Internet users’ browsing activity. Businesses, such as marketing firms like DoubleClick, will be willing to pay for that information supporting compensation to users and ISPs. The technologies and economic foundations exist to support the functioning of an information market sustained by existing demand as well as the voluntary individual and ISP participation.

Index Terms— Behavioral targeting, behavioral advertising, direct marketing, 3rd party cookies, personal privacy

I. INTRODUCTION

BEHAVIOR targeting is a recent version of customer profiling which is becoming popular with some online advertising firms through cooperative efforts with internet service providers (ISPs). This sometimes furtive advertising method uses 3rd party cookies to collect information about users as they browse the internet and click through hyperlinks¹. The intended use of 1st party cookies, small files created and stored by the web browsers, was to allow functionality enhancing the browsing or commerce experience of browser users. More recently, 3rd party cookies have been used by web advertising companies, such as DoubleClick, to track behavior on the internet – these 3rd party cookies were simple to implement by inserting a graphics image (often a one by one clear pixel) on a webpage. The image links to a server controlled by a 3rd party advertising company that would serve up the graphics image

¹ 3rd party cookies are small files recorded by the web browser pursuant to the visiting of a website, the original intention of cookies was that cookies would allow the browser to identify a returning user and ‘remember’ certain user characteristics and enable certain functions such as shopping carts that remember what is in the cart as a user goes from page to page in an online shopping environment).

and add or update the associated cookie file in the web browsers cookie folder whenever the image is retrieved.

Behavior targeting entails the cooperation of the ISP; in some cases the ISP even allows a 3rd party to intercept and alter web traffic to users. Early tests of this practice, some rather alarming, have been pursued as early as 2006 in the United Kingdom when British Telephone allowed a 3rd party ISP to install equipment for the interception of their users’ web traffic without informing their users. [3] [4]

Informed individuals often provide personal information in the course of routine interactions with various organizations in order to conduct business or to receive service. [16] The exchange of such information is vitally important for most organizations, especially advertisers, and it also may have some significant benefits for individuals as well. Naturally, an organization may require information in the course of providing goods and services to individuals and these individuals may receive better service by truthfully revealing personal information. For instance, a patient may be asked by a doctor to report the average number of alcoholic beverages they consume in a week. The doctor then has information that may allow her to make a better diagnosis. However, through this process individuals may also expose themselves to threats of abuse of their personal information. An abuse of particular interest is the release and use of personal data for purposes other than the original intended purpose (i.e. suppose the doctor provides the above information to a beverage company or even to the patient’s insurance provider). Individuals’ perceptions about the threat of abuse are significant, in fact a large percentage of the population are concerned and believe that they have lost all control of their personal information. [7]

II. RIGHT TARGETING FOR ONLINE MARKETING

Behavior targeting provides a solution to a very important set of marketing problems; namely these problems involve the narrowing down of a population into a target list of individuals whom are most likely to respond to target marketing. Solving this problem often will reduce the cost of advertising in direct marketing because the individuals are likely to be more responsive to the advertising, reduce the social cost of bombarding individuals who are unlikely to purchase products and services with advertisements, and increase the benefit by getting the right information to those who are interested and likely to buy (most of us don’t mind when Amazon.com is able to give a good book recommendation, or a special offer on something that interests us).

The two essential elements of direct marketing on the Internet are (1) finding the right target market segment, and (2) getting the right advertisement to that segment. Behavior profiling helps in both of these arenas. There are a few typical information elements about users that online advertising firms would like to and usually do quite easily track online. [8] These include:

- visitor profiles gathered from site registration, age, gender, income, business data, etc. ;
- area of content a visitor is viewing starting with the first visit, systems automatically start learning about each site visitor's individual interests and tastes, they keep learning more with each repeat visit;
- Internet-based registration domain type, browser type, ISP, platform, time of day, day. of the week;
- key-word or key-phrase searches;
- demographic data IP address, high-level and specific domain;
- geographic data country, state, zip code, area. code;
- IP address and cookie information for ad or page;
- cumulative history of exposures to all ads in a campaign.

When online advertisers are not able to get these key pieces of information, they may resort to other means. Behavior targeting is one of these that necessarily involves the corporation of the internet service providers (ISPs) and is often done without the knowledge of the ISP user. Behavioral targeting of this type involves the surreptitious collection and analysis of personal information. Privacy advocates, watch guard groups, and now federal regulating bodies like the Federal Trade Commission (FTC) are becoming alarmed to this practice. [1] Some of these privacy concerns are discussed further in the following section.

III. PRIVACY CONCERNS

The concern over privacy has so alarmed public advocacy groups that they have even made requests to the president that he should appoint a privacy czar. The White House responded by at least calling privacy a "top priority." [5] The federal government has been investigating various options to ensure the preservation of the privacy rights of its citizens in the information age. For example, the U.S Department of Commerce has issued several reports on privacy. [10][11][16] Still, the federal government is reluctant to become too involved in the regulation of information markets dealing in individuals' personal information. Regulation would be costly and may overly restrict the free exchange of information that is necessary for market efficiencies. Discussions of self-regulation of markets that deal in personal information are on the forefront of the debate. [11] Still, recent surveys reveal that little has changed over the past several years and the majority of individuals are still very concerned about their privacy. [6][7][13] "Online trust issues continue to impact consumer behavior on the Internet", states Fran Meier executive director and president of TRUSTe, when referring to a recent survey concerning online privacy by

TRUSTe/TNS. Meier goes on to add "high profile privacy breaches this year have exacerbated consumer concern." Still, it appears that little has been done by organizations, including the U.S. government, to safeguard citizens' privacy. [13]

IV. A SIMPLE SOLUTION - COMPENSATING USERS THROUGH A BEHAVIOR TARGETING INFORMATION MARKET

One simple step in improving privacy is for third party advertisers or the ISPs to compensate users for voluntarily allowing behavioral profiling. The same mechanisms that enable third party cookies and the tracking of individuals on the Internet could be used to enable the compensation to individual users. The economic foundations for self-regulating the buying and selling personal information using a market mechanism have been developing over the past several years. [9][16]

As an example of how this market might function, consider the collection of a user's web browsing behavior when visiting an internet site for creation of actionable marketing information and analysis. Quite fortunately, the architects of the internet have created the perfect protocol this type of web browsing behavior and information tracking with the Hypertext Transfer Protocol (HTTP)² which enables the explicit tracking of this type of information using the Uniform Resource Locator (URL). The Web uses URLs to provide unique addressing so that a user's web browser can retrieve files from locations such as the URL;

<http://www.getstuffforless.net>

which, when typed into a web browser's address line will retrieve the associated document from the server that resides at that URL. The fact that an individual is looking at the Get Stuff for Less website has value to several parties including 3rd party marketers and perhaps the Get Stuff for Less retailer. It is likely that information of additional value could be derived from a 3rd party knowing exactly what topics, articles, and information that user accesses information at the Get Stuff for Less website.

For instance, knowing that a user has clicked through to more detailed URL, such as,

<http://www.getstuffforless.net/watches/>

on the Get Stuff for Less website, is much more revealing and perhaps very valuable. In fact, marketing and advertising firms conduct extensive data analysis on exactly that type of information to leverage the knowledge that users visiting URLs like, <http://www.getstuffforless.net/watches/>, may just be interested in watches.

More detailed URL information such as,

² HTTP is an application-level protocol "for distributed, collaborative, hypermedia information systems." HTTP has been in use enabling the World Wide Web (WWW) global information initiative since 1990 (please see <http://www.w3.org/> for more information on the subject)

<http://www.getstuffforless.net/watches/designer/gold>

shows that a user has accessed even more specific information and may reveal more specific preference information about that user's interests; that is, that they are not only interested in watches, but in "high end" gold designer watches. The more specific the information about what users are looking for online the more the more valuable it is likely to be to a 3rd party online marketing firm or retailer.

Ideally, the mechanism would provide increased levels of compensation for increases in the revelation of information (that is, the information that a user visits the Get Stuff for Less website requires lower compensation than the additional information that the user looked at gold designer watches on the site). Ideally, a variable pricing mechanism could accomplish this. A simple compensation mechanism would provide an initial compensation for allowing knowledge of visiting a particular web site on the "home" level, and then could provide more compensation for each additional level where the "level" is the depth of the web browsing,

for example, http://home/level_1/level_2/.../level_N.

Each individual then could choose whether or not they'd like to participate where participating users could receive compensation perhaps in the form of a flat price reduction in their cost of internet access (from the ISP). Next, they could determine if and to what level of detail the 3rd party should be allowed to track them which would result in a variable compensation depending on how much information the 3rd party is allowed to glean from users' web activity.

V. INCENTIVES FOR MARKET PARTICIPATION

The goal of economic compensation model is to design a system that captures the value a 3rd party online marketing firm would place on this type of web browsing information and then design a mechanism for 3rd party to compensation to the individual users producing the data. A successful mechanism in the online marketing environment will require that: (1) the 3rd party marketing firm deriving value from collecting browsing information; (2) the users are willing to allow for this practice for compensation; and (3) the compensation mechanism is fair and secure.

The compensation model is only viable if sufficient market incentive exists to ensure market participation. It's been shown, and is generally accepted, that with appropriate compensation and assurance that personal information will not be abused, many individuals are willing to allow their personal information to be used for marketing purposes. [2] However, implementation of the compensation model should be careful not to reinforce the tendency some individuals may have to cheat or "game" the system by prolific strategic browsing simply to increase personal revenue. One possibility to govern cheating behavior would be setting a compensation limit, either daily or monthly, based on the normal or expected usage rate.

Although this simple solution may not eliminate cheating, it should at least mitigate the impact of intentional abuse by

cheaters and will avoid the problem of wildly overcompensating cheaters. More elaborate anti-cheating devices may also be employed such as anomaly detection technologies that can be used to ensure that browsing data collected is reasonable (discussion of these technologies are beyond the scope of this paper). Then if cheating is detected, the data derived from obvious abuse can be removed, and the user can be removed from the market. Ultimately we should realize that some of the information collected by 3rd parties may not be an entirely accurate representation of genuine browsing behavior. This is true of much of the real marketing behavior data collected using various devices including surveys, registrations, and other techniques. In this case the analysts may have to rely on analytics, statistical analysis, and data-mining tools to help sift through good and bad data. Also, in cases when a user does not want to be tracked they should have the option to turn off the tracking (a luxury currently not afforded by the behavior targeting techniques). Finally, we are optimistic that most users will be incentivized to trade their genuine browsing behavior for compensation.

Next, both the internet service providers (ISPs) and the 3rd party marketing information firms have economic and legal pressure to participate in the self-regulation of behavioral targeting based marketing. [11][13] The economic incentive to participate in the collection and sale of behavior marketing information is clear – there is a strong demand for these products and participation can add significant revenue to both ISPs and 3rd parties. The incentive to self-regulate is strong and getting stronger. Recently "the F.T.C. revised its suggestions for behavioral advertising rules for the industry, proposing, among other measures, that sites disclose when they are participating in behavioral advertising and obtain consumers' permission to do so." In fact, in the same article it is reported that the FTC commissioner, Jon Leibowitz, warned that "if the industry did not respond, intervention would be next." As has been the case in the past, it is likely that the marketing industry will enthusiastically find ways to self-regulate in order to avoid forced regulation. [1]

VI. THE ECONOMICS OF BUYING AND SELLING PERSONAL INFORMATION

The rise of Internet commerce has greatly changed the application of economics to business commerce and part of this involves the economics of information privacy. Historically, information systems and computer science research have taken a rather technical view of privacy where privacy is reduced to a security issue. On the other hand, many modern economists have taken a different view of privacy. These economists view privacy as the voluntary exchange of individuals' personal information between parties. For instance, Hal Varian gives a simple example that shows how personal information could be used in economic transactions and points out that there are advantages to making personal information available. [14][15][16] It is mutually advantageous for sellers and buyers if the sellers are allowed to know some personal information about buyers such as what the buyer intends to buy. The benefit of this flow of information is most obviously the seller's discovery of

information enabling for the delivery of an appropriate product.

However, if a seller decides to pass the private information on to a 3rd party negative externalities may exist. The perceived invasion of privacy has a cost. Therefore, Varian suggests that a contractual agreement between individuals and the 3rd party. He illustrates this agreement using a simple example where an individual is offered a contract from the information seeker at the point of data collection such as "Check here if you would like your name distributed to other parties who will provide you with information about computer peripherals until 12/31/98. After that, name and address information will be destroyed. In exchange you will be paid \$5.00 for each list to whom your name and address is distributed." [12] [16]

Contractual agreements like this show an economic transaction which stipulates the right to use personal information and compensation to the individual each time the information is sold. Laudon develops this concept further in his National Information Market (NIM) concept. [9] The NIM illustrates a market where personal information is bought and sold by institutions. Businesses collect and process personal information reselling as an information product. Purchasers of the information may use it for commercial purposes over a defined period of time. Contributors of personal information are compensated each time the information is used or sold. This market functions much as the banking industry. The marketplace allows for a complete computer-based audit trail mitigating the risk of information abuse.

Laudon's NIM is a hypothetical market that illustrates how personal information could be bought and sold in a market setting. One important factor to consider when considering the trade of personal information goods is the pricing. Information goods cost structure is very different than many other products. There are typically large setup and collection costs and then each additional item costs comparatively very little. Varian explains the pricing these goods on cost makes little sense, and recommends pricing information goods based on value. [14] This would also support situations where different consumers have different values for the information product. [14] The issue of pricing these products would be of concern for the 3rd party firms collecting and reselling behavioral profiles. An overall market solution should consider all of these cost and pricing issues and will be the topic of future work in this area.

VII. A COMPENSATION MODEL FOR 3RD PARTY COMPENSATION TO ISPS AND INTERNET USERS

A compensation model is used to incentivize (1) 3rd parties who are willing to pay for better web browsing information; (2) ISPs who are willing to sell user/individuals web browsing information; and (3) users/individuals who are willing to be compensated for the collection and sale of web browsing information. This compensation model illustrates the concept of how ISPs and users would be compensated by a 3rd party. The 3rd party total compensation, C_t , which is the total amount of payment they will make to the ISP and individuals who are providing personal information is:

$$C_t = C_{ISP} + C_{user} = C_{ISP} + W \sum_{u \in U} \sum_{s \in S} d_{us} t_s$$

where;

C_{ISP}

- is the compensation the 3rd party makes to the ISP

$u \in U$

- represents a user u who is a member of the set of all internet users, U , who visit internet sites through the ISP

$\sum_{u \in U} \sum_{s \in S} d_{us} t_s$

- is the sum over all users, a cost of compensation for a compensation base of d_{us} , the compensation coefficient for user u visiting site s , and t_s the compensation for revealing that the user retrieved the level t of site s .

W

- is a scaling factor

The above formulation shows an approach to begin modeling the compensation of users and the ISPs for access to personal information related to web browsing activity. Continuing research will include the application of this model in simulation by applying existing data sets about user web browsing behavior.

VIII. CONCLUSION AND ONGOING RESEARCH

Behavioral targeting is a recent phenomenon that takes advantage of web technologies in order to better tailor direct marketing efforts increasing the cost efficiency of online marketing methods. However, many consider the use of 3rd party cookies for behavioral targeting as an invasion of personal privacy because the agencies engaged in this practice are doing it surreptitiously and with the cooperation of the users' ISP, but without the knowledge of the users. A simple solution is to inform the users and allow them to participate in the collection and reselling of their own personal information by compensating them. Obviously, enough value is created through this activity to support this type of compensation and the technology exists to enable a functioning information market.

Future research in this area will delve into the details an information market and compensation mechanism for behavioral targeting. The next opportunity in this research lies in the specification of a market mechanism and the analytical study of the market mechanism that demonstrate conditions under which social welfare is increased. This future research may be accomplished in several ways including either a designed economic experiment, quasi-experiment, or through simulation and numerical experience.

REFERENCES

- [1] P. Boutin. (2009, Mar. 18). Survey: Online privacy is your problem, not DoubleClick's. *The Industry Standard* [Online]. Available: <http://www.itworld.com/internet/64534/survey-online-privacy-your-problem-not-doubleclicks>
- [2] A.-N. Chang, P.K. Kannan, and A.B. Whinston. "The economics of freebies in exchange for consumer information on the Internet: an exploratory study," *International Journal of Electronic Commerce*, vol. 4, no. 1, pp. 85-102, Sept. 1999.
- [3] M. Kassner. (2008, Jul. 31). Behavior targeting: What You Need to Know. *Tech Republic* [Online]. Available: <http://blogs.techrepublic.com.com/networking/?p=612>
- [4] S. Gibson and L. LaPorte. (2008, Jul. 3). Security Now Podcast Episode #151, Phracking Phorm. *Gibson Research Corporation* [Online]. Available: <http://www.grc.com/sn/sn-151.txt>, August 25, 2008.
- [5] P. Greenberg. (2001, May 8). Internet Privacy: Back to Basics. *E-Commerce Times* [Online]. Available: <http://www.ecommercetimes.com/story/9473.html>.
- [6] Louis Harris and Associates and A. Westin. "Consumer Privacy Survey," Harris-Equifax, Atlanta, GA, 1995.
- [7] Harris Interactive Poll, Privacy On and Off the Internet: What Consumers Want, <http://www.harrisinteractive.com/news>, February 20, 2002.
- [8] G.G. Karuga, A.M. Khraban, S.K. Nair, and D.O. Rice. "AdPalette: an algorithm for customizing online advertisements on the fly," *Decision Support Systems*, vol. 32, no. 2, pp. 85-106, Dec. 2001.
- [9] K. Laudon. "Markets and privacy," *Communications of the ACM*, vol. 39, no. 9, pp. 92-104, Sept. 1996.
- [10] "Privacy and the NII: Safeguarding Telecommunications-Related Personal Information," *U.S. Department of Commerce*, Oct. 1995. Available: <http://www.ntia.doc.gov/ntiahome/privwhitepaper.html>
- [1] "Privacy and Self-regulation in the Information Age," *U.S. Department of Commerce*. Available: http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm
- [2] H.R. Varian. "Pricing Information Goods," presented at the Research Libraries Group Symposium Symposium on "Scholarship in the New Information Environment" held at Harvard Law School, Cambridge, MA, 1995. Available: <http://www.sims.berkeley.edu/~hal/Papers/price-info-goods.pdf>
- [3] "Consumers Have False Sense of Security About Online Privacy – Actions Inconsistent with Attitudes," *TRUSTe/TNS Privacy Survey*, Dec. 2006. Available: http://www.truste.org/about/press_release/12_06_06.php
- [4] H.R. Varian. "Versioning Information Goods," Digital Information and Intellectual Property, Harvard University, Cambridge, MA, 1997. Available: <http://www.sims.berkeley.edu/~hal/Papers/version.pdf>
- [5] H.R. Varian. "Differential Pricing and Efficiency," *First Monday* [Online], vol. 1, no. 2, 1996. Available: <http://131.193.153.231/www/issues/issue2/different/>
- [6] H.R. Varian. "Economic Aspects of Personal Privacy," *Privacy and Self-Regulation in the Information Age*, Department of Commerce. Available: http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm

Organizational Power and Information Security Implementation

Jon Blue¹ and Gurpreet Dhillon²

¹University of Delaware

²Virginia Commonwealth University

Abstract—This purpose of this paper is to show how the implementation of information systems security policies in an organization can be improved by applying a power exercise model. It argues that stakeholders' awareness of the power being exercised by the policy enforcers, affects the success of the policy implementation. The model is developed by adapting, and extending, a power exercise framework presented by Markus and Bjørn-Andersen [20]. The information systems security policy model is applied to the introduction and compliance of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) at HealthCo Systems, a non-profit health care organization in a major United States city.

Index Terms—Organizational Power, Power Exercise, IS Security Policy, Policy Implementation, Compliance, HIPAA

I. INTRODUCTION

THIS paper shows how the awareness of the power brokers in an organization can assist management in successfully implementing information systems security policies. There continues to be a high level of attention on the successful development and implementation of information systems security policies. While most organizations have developed a security policy, many have now turned their attention to successfully implementing these policies. In this context, success equates to employee compliance. Compliance has become a greater concern, not just because of potential threats to an organization's information, but also because over the past few years there has been an influx of regulatory and compliance mandates by the United States government. Some of these mandates, such as the Financial Modernization Act of 1999¹ (known as the Graham-Leach-Bliley Act), applies to all corporations. Others, such as the Health Insurance Portability and Accountability Act of 1996² (HIPAA), are applicable to certain industries [29]. Executives' concerns of compliance are warranted because employee non-compliance to information systems security policies can be fiscally devastating.

¹ Includes provisions to protect consumers' personal financial information held by financial institutions. There are three principal parts to the privacy requirements: the Financial Privacy Rule, Safeguards Rule and pretexting provisions.

² Administered by the U.S. Department of Health and Human Services, a set of national standards for the use and disclosure of individuals' health information as well as standards for individuals' privacy rights to understand and control how their health information is used [23].

It is believed that the successful implementation of information systems security policies will increase with an awareness and appreciation by all stakeholders of the use of power and politics in organizations. These stakeholders consist of employees, who are directed to follow policy, and management, who are responsible for enforcing compliance. Actually, management usually empowers their *agents* to act on their behalf to ensure employees adherence to organizational policies. It is imperative to view the failed implementations of security policies from a power perspective because power assists in realizing change [7] – which is needed when the institutionalization of security policy compliance is desired. It is unfortunate that power is still viewed as negative by many [19], as oppose to how power is presented in this paper – as a phenomenon to be aware of by all stakeholders in order to obtain the most beneficial result. In this case, the positive output is the successful implementation of information systems security policy, which is employee compliance.

While it may be equally important to look at the development of information systems security policy from a power perspective, the purpose of this study is to show how the implementation of information systems security policies can be improved. This work takes for granted that the security policy is in existence. Markus and Bjørn-Andersen [20] present a framework that specifically looks at the exercise of power by IS professionals over systems users. This paper adapts the Markus and Bjørn-Andersen framework in order to model the exercise of power by information systems security agents over employees and its impact on successful policy implementations.

II. LITERATURE REVIEW

A. Power and Information Systems

The term power is used quite interchangeably in the literature to represent differing conceptualizations of power: power, politics, authority, legitimacy [2][5][9][12][19][24][32]. Hall [14] capsulated power by stating that “power has to do with relationships between two or more actors in which the behavior of one is affected by the behavior of the other.”

Given these diverse definitions, there have been numerous attempts to define and measure the theoretical construct of “power” in organizations. Unfortunately, this has been done in different ways, which has led to varying results. One reason for this difficulty is that power not only has visible characteristics, but there are also many invisible characteristics [32]. Another reason for this difficulty is that

many disciplines (e.g., management, sociology, marketing, political science) have been used as referenced disciplines to describe the interaction between power and information technology [17]– which has resulted in definitions that have been discipline specific and inconsistent.

Over many years, there have been multiple suggestions by researchers on how organizations can, and should be viewed, to explain and describe organizational phenomenon. Jaspersen et al. [17] use four power lenses to view the role of power/organizational politics and different information technology outcomes. These views are rational, pluralist, interpretive, and radical. The Jaspersen et al. lenses are projected from Bradshaw-Camball and Murray [6] who specifically use a trifocal lens of functionalist, interpretive and radical. Both views are adapted from Burrell and Morgan [8]. Rational power is defined as structural power which is focused on information, authority, and expertise as bases of power. This is where power is viewed as an objective reality. The pluralist lens of power assumes an objective definition where conflict is normal. In this view, the development, prioritization, and execution of goals are political and involve negotiation based on the control of information and resources. When power is based on the ability to control access to, and direct the construction of organizational realities, then the interpretive lens is being used. Similar to other interpretive views, power is socially constructed and the stakeholders exert influence by constructing the meanings of others. Lastly, the radical view looks at power and politics as the result of social structures (e.g., class, gender, institutional structures, race) that are exogenous to the organization. Bradshaw-Camball and Murray [6] say that political activity (broadly defined) involves either maintaining or undermining (and ultimately overthrowing) the current power structures [17].

An additional theory that describes power's use in organizational teams such as information systems is the "strategic contingencies theory" [16]. If a team is in a central part of the workflow of an organization, then what they do is very important. This gives them many opportunities to be noticed. It also means that they are on the critical path to success, such that if they are not involved, the whole show stops -- again creating attention and giving them bargaining power. Finally, if they are difficult to replace (e.g., because of their knowledge or skill level), then enemies that are made up the hierarchy cannot just move the powerful team out, or sideways.

Organizations that are responsible for information systems security policy implementation and compliance are often housed in the information systems department. The strategic contingency theory suggests that these agents are in the teams that are quite powerful in organizations and have power that is described by the theory. As stated, Markus and Bjørn-Andersen [20] point out that testing has shown that other departments do not consider information systems departments as having power. However, Clegg [9] described a specific form of power as a set of capabilities and purported that having power does not mean you have to use it. This being said, it is quite possible that employees do not necessarily see power used by information systems professionals and therefore equate this to them not having said power.

... some social actors, who might be potentially powerful, may not recognize the [sources of power] or the fact that they possess them.... Even if power positions are recognized, organizational actors may choose not to employ their power [20].

While power is a very significant base in our proposed model, as important is information systems security policy.

B. Information Systems Security Policy

Information Systems security policy can be fractioned into the development, and implementation (rollout and enforcement). While there is wide standing agreement that a good information systems security policy begins an organization's information security, there is little work on the development [3], and implementation of good security policies.

As presented by Baskerville and Siponen [3], definitions of security policies, fall into two camps: non-technical/security management and technical/computer security. In defining the non-technical/security management, Wood [33] states that 'policies' are statements that come from high management and mid-level management enforce 'standards' that are more specific and often direct technological standards that conform to high level management policies. He reserves the term 'procedure' for the actual method of how the policies are implemented. Dhillon [11] differentiates strategy, policy, and operating procedures and purports that instead of developing policies, organizations should develop an information security vision and strategy at the apex of the organization.

In defining the technical/computer security, security policy is viewed by some, on one end of the continuum, to be from security architectures of operating systems [3][31]. Other researchers present security policy on the opposite end of the spectrum: controlling the access to systems by rules [26]. As presented by Sterne [30], a different perspective is presented that is between these two extremes and presents three security policies. These policies are objective (protects an identified resource from unauthorized use), organizational (description of how to achieve security policy objectives), and automated (how a computer systems protects computer resources according to an organization's security policy) [3]. Abrams and Bailey [1] offer an additional technical view. They distinguish three views of security policy: top management's view, users' view, and the designer's view.

C. Power and Information Systems Security Policy

Where there is literature present in each of the domains of power and of information systems security policy, as presented above, absent is literature that views these policies through a power lens. Given the different views of organizational power as stated earlier, there can be as many different ways to explain the failure of these implementation attempts.

A possible research stream for power's affect on information systems security policy compliance would be to view it from the lens as suggested by Jaspersen et al. [17], which as stated above, is a model adapted from Bradshaw-Camball and Murray [6]. This would allow researchers to

view power from the four different perspectives of rational, pluralist, interpretive, and radical views. As suggested by Bradshaw-Camball and Murray, each view would uncover different explanations and descriptions. Used in various combinations, these views could assist researchers in an expansion in their knowledge on how information systems security policy implementations could become more successful.

The remainder of this paper is organized as follows. First presented is an overview of the power exercise conceptual framework as presented by Markus and Bjørn-Andersen [20]. This framework is then be used to create a model of the exercise of power by information systems security policy agents over employees. Subsequent to this, the model is applied to HealthCo to show how the stakeholders' awareness of power exercise can assist in improving the success of information systems security policy implementations. In the discussion section, the agent-employee dyad results are described with the model's assistance. Lastly, in conclusion, the model's applicability to both the practitioner and academic environments, is given.

III. IS PROFESSIONALS POWER EXERCISE CONCEPTUAL FRAMEWORK

Markus and Bjørn-Andersen [20] focus on the use of power in the user/information systems professional dyad. While intuitively one would think that information systems professionals have power over users because information technology is a resource that many people value, it has been purported that this is not necessarily the case [18][27][28]. These rewards (information technology) can be extracted from those who depend on it [24]. This power theory is "resource dependence" [25].

In their paper, Markus and Bjørn-Andersen [20] discuss the power of IS professionals over systems users and view this situation from a Jaspersen et al. [17] interpretive power perspective. These authors purport that if both professionals and users can increase their awareness of the different types of power exercise, the quality of systems developed and the outcomes of their use, will be significantly enhanced. The framework they present looks at both the context of power exercise (specific development project or information systems management policy) and target of power exercise (issues of fact or issues of values). This framework is a matrix that gives the four types of power exercise: technical, structural, conceptual, and symbolic).

A technical exercise of power occurs when system designers select system design features to which users explicitly object, at least initially. A structural exercise of power occurs outside any specific systems development effort. A conceptual exercise of power, as well as symbolic exercise of power, deals with the users' values about, and attitudes towards, the issues of fact as the design features of systems and the distribution of access to computing equipment and services. The conceptual exercise of power links closely with the methods used to analyze organizational situations prior to

developing system design features. Information systems professionals exert power symbolically by shaping user's desires and values outside the context of an individual systems development effort.

Additionally, Markus and Bjørn-Andersen [20] looked at information systems professionals' and employees' awareness of power exercise. They suggest that having and using power are different. Power is often exercised without the knowledge of the actor or the receiver. This unawareness of power exercise occurs because people "seem to evaluate 'having power' differently from 'using power'" [20].

This awareness of power exercise results in four possible outcomes: 1) if both are aware then there is mutual negotiation, 2) if both are unaware then unintended influence occurs, 3) if the information systems professional is the only one aware, then professional manipulation occurs, and 4) with the reverse awareness level, user resistance occurs.

The exercise of power is not defined in the terms of intentions or the perceived legitimacy of outcomes; it is defined in terms of behavioral outcomes. The result of such a definition is that when information systems professionals have exercised power over the users then this is to say that the users behave differently than they would have if not for the professionals. This power over end-users can be collective or individual.

Hardy [15] and Lukes [19] use a similar definition of power exercise. However, there is some disagreement with this definition. A common alternate definition of the exercise of power, as that of Meyer [21], occurs only when the powerless individual views the powerful individual's behavior as illegitimate, or when the powerless does not accept their behavior. Additionally, Dahl [10] and Pfeffer [25] believe that the exercise of power only exists when the parties involved are not in agreement about a decision and where it is possible to view the powerful actor's behavioral attempts to influence the outcome of decisions. Both of these two alternatives are more restrictive and assume that the exercise of power is an intended action by individuals.

IV. INFORMATION SYSTEMS SECURITY POLICY POWER EXERCISE MODEL

This paper addresses the policy agent-employee dyad and specifically the power exercise of information systems security policy agents over the employees. It is suggested that with the mutual awareness of the different types of power exercise, the successful implementation of information systems security policy in organizations will improve. As stated, a successful implementation is defined as employee policy compliance.

An adaptation of the Markus and Bjørn-Andersen [20] framework of information systems professional power exercise to information systems security policy agents can be seen in Table I. So, in bridging from the Markus and Bjørn-Andersen framework, it is necessary to look at the target of power exercise (issues of fact or issues of values) and the

context of power exercise (information systems security policy).

A. Target

Information Systems security power exercise can be directed at issues of fact and tangible resources. For instance, this may entail specific directives of the implementation plan like ‘all employees must attend a security 101 course’ or ‘each department will allocate \$300.00 per employee for physical

TABLE I
TYPES OF POWER EXERCISE

| | | Target of Power Exercise | |
|---------------------------|--------------------------------------|--------------------------|------------------|
| | | Issues of Fact | Issues of Values |
| Context of Power Exercise | Specific IS Security Policy Category | Technical | Conceptual |
| | IS Management Policy | Structural | Symbolic |

Adapted from Markus and Bjørn-Andersen [20]

security apparatuses such as locks.’ Additionally, an individual’s values may be taken into account. This may be values such as an individual’s acceptance of the objectives/reasons of a particular item in the implementation plan, the assessment of a policy’s success, the individual benefits of particular policies, cultural definitions of sound policy, or workplace institutionalizations [4].

B. Context

An information systems security agent’s ‘power exercise’ can also occur contextually. This can happen during activities such as when developing the implementation plan. In addition, power exercise can occur in the management policy environment around specific implementation specifics such as password use, password expiration, the mandated use of certain security applications like virus scan software, or the monies charged to departments to pay for information systems security policy classes.

As shown in Table I, the intersection of these two dimensions of target and context, produce four different ‘power exercises.’ These are Technical, Structural, Conceptual, and Symbolic. A definition of each, and its applicability to information systems security policy implementations are given.

C. The Technical Exercise of Power

The technical exercise of power occurs when policy agents identify specific ‘rules’ within a policy implementation plan which users explicitly object (at least initially). Even if users do not explicitly object to the policy implementation plan contents, the exercise of power has occurred if it is shown that users would have objected had they been aware of the agents’ identification of the plan content [19]. An example would be a policy that forces the use, and entry, of different passwords at multiple levels of applications, and the user’s desire is a password system that does not impeded their work (e.g., one password that is entered once).

D. The Structural Exercise of Power

The structural exercise of power is not as easily connected to the behaviors of individuals -- as the technical exercise of power can be. It occurs exogenous to any specific information systems policy implementation. This is where the agents exercise power over user behavior by imposing organizational structures or instituting routine procedures that cause the garnered formal authority over users, or cause the user to be dependent on them for resources.

This may be something as simple as the stipulation that certain systems security software must be used, and additionally, must be purchased from an organization’s software store (where prices are set by the owned security organization). Alternatively, it could be more structurally relevant -- such as the information systems security agent may have other authoritative positions (e.g., overall approver for all information systems acquisitions like hardware and software). This power exercise deals with the development of implementation plans, not the application to a specific information systems security policy. When these structural constraints on users exist, they can unnecessarily render a need for more direct forms of power use (e.g., technical exercise of power).

E. The Conceptual Exercise of Power

This exercise of power is relevant to an individual’s values about, and/or attitude toward, the issues of specific way the security policy is implemented, the charges for security software, or even the exercise of power itself. As stated by Lukes [19]:

A might exercise power over B by getting him to do what he does not want to do, but he also exercises power over him by influencing, shaping or determining his very wants. Indeed, is it not the supreme exercise of power to get others to have the desires you want them to have—that is to secure their compliance by controlling their thoughts and desires?

An information systems policy agent may conceptually exert power over employees by developing the objectives of a specific information systems security implementation plan. Conceptual refers to the design concept of the information systems security implementation plan. This is the overall objective and purpose of the plan that ultimately (supposedly) contains the specific details of the implementation plan.

The conceptual use of power is closely connected with the method used to assess the organization prior to policy implementation (inclusive of the actual specifics of the plan). While the implementation plan may be quite rigid and structured, it also could be very loose and conducted haphazardly. The questions asked, or even more importantly not asked, may prevent the employees from expressing certain views (e.g., preferences, likes, dislikes) about the implementation plan specifics and objectives.

F. The Symbolic Exercise of Power

This is where the information systems security policy agents shape employees' values and desires, exogenous to the context of the policy implementation. This type of power exercise occurs while the employee actually comply with information systems security policies. So often on television, and in magazines, there are articles that talk about the importance of information systems security and the woes that could occur due to not being secured. There are reports of malicious catastrophes that occur which are based on information systems security [22]. From all of these reports, individuals realize that the results of not being secure could be devastating, and thereby these occurrences act as symbols. Therefore, when employees allude to the fact that information systems security policy is necessary to protect the company's assets, or their own, they are portraying the remnants of a subtle force of symbolic power exercise.

V. MODEL OF INFORMATION SYSTEMS SECURITY POLICY AWARENESS OF POWER

While there are four different types of power exercise, the proposed model does not assume that an awareness of the power exercise is necessary at any point in the process (before, during, or after) for the model to be applicable. Actually, neither party needs to be aware that power is being exercised. This really means that even if a policy agent is unaware that they are altering an employee's behavior, they may be, just by whom they are. It should be understood that power is exercised if there is a change in either the organizational outcomes (because, for instance, the presence of the information systems security agent), or the employee's behavior.

However, both the attributions of legitimacy and the awareness of power exercise can be relevant. They will affect how an employee responds to the information systems policy agent and their implementation specifics. Additionally, Markus and Bjørn-Andersen [20] purport that unawareness can move to awareness. "... we believe that interventions that increase this awareness will pave the way to compromises by opening up previously covert issues." This increase in awareness should lead to results that are more positive for the organization.

Table II shows the taxonomy of different conditions of awareness. Any one of these four situations may be present given an exercise of power. The upper left quadrant is 'Deal Making.' This occurs when both the information systems security policy agent and the employee are aware that power is being exercised, there is room for negotiation -- resulting in a 'win-win' situation. This is because each party is aware of the agent's power and they know what is conceivable and what is not. The bottom right quadrant is 'Blind Influence.' It is called this because when neither party is aware of the use of power then making a deal is slim; they just go with the program and whatever happens, happens.

The remaining two quadrants of the taxonomy bring the most difficulty as is explained by changes agents. The result is a win-lose situation, where the result benefits only one party. This is where the aware party can take advantage of the other

party. When the information systems security policy agent is unaware, and the employee is aware, they are 'Policy

TABLE II
AWARENESS ABOUT POWER EXERCISE

| | | Employee | |
|---|---------|-----------------|-----------------|
| | | Aware | Unaware |
| Information Systems Security Policy Agent | Aware | Deal Making | Policy Forcing |
| | Unaware | Policy Dissents | Blind Influence |

Adapted from Markus & Bjørn-Andersen [20]

Dissenters' – at least this is how the agents view the employee. Conversely, when employees are unaware and agents are aware, the agent openly intends to influence unknowing employees – this is called 'Policy Forcing.'

VI. REVIEWING THE IMPLEMENTATION OF HIPAA AT HEALTHCO

This section analyzes the move within HealthCo to introduce the United States federally mandated HIPAA. The analysis is conducted using the power exercise model as described in the previous section of this paper.

A. Health Insurance Portability and Accountability Act of 1996

HIPAA was passed by the United States Congress on August 21, 1996. Congress included as part of this policy, regulations that promote the simplification of administrative health care transactions and those that ensure the security and privacy of patient information. There are four specific standards that are part of HIPAA: transaction and code sets, privacy, national identifiers and security [13]. All four standards are enforceable, with significant fines possible if the policies are not followed.

Of main concern are the privacy and the security policy of HIPAA in that both of these have security implications. The privacy policy set standards for the electronic financial and administrative transactions. The policy states that a party electronically maintaining or transmitting "protected health information," may not disclose or use the information except as permitted by federal regulation. Patients are also given the right to control how and when their information is used.

The confidentiality of health information is threatened not only by the risk of improper access to stored information, or the maintenance of that information, but also by the risk of interception during electronic transmission of the information. The security policy of HIPAA mandates the adoption of national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information. Prior to these rules, there were not any standard measures that existed in the health care industry that addressed all aspects of the security of electronic health information while stored, or transmitted, between entities (via either a local area or wide area network). Full compliance became mandatory on April 21, 2005. HealthCo, like all other health

care organizations, were mandated by the federal government to follow the HIPAA policy guidelines.

HealthCo

For anonymity purposes, the actual names of the organization, and the employee names, have been changed. The descriptions of the roles and responsibilities have not been altered. HealthCo provides medical care to low-income and uninsured patients, as well as offers education to their patients. Services specifically provided are comprehensive reproductive health services, teen pregnancy prevention programs, family planning, breast and cervical cancer screening, mammograms, sexually transmitted disease testing and treatment, HIV/AIDS testing and counseling, colonoscopy, and peri- and post-menopause services; among other women's, men's, and teenagers' health programs. HealthCo's mission is to provide high quality, affordable reproductive health care; promote education programs that empower all individuals to make informed and responsible reproductive choices; and to protect the right to make those choices. HealthCo is an affiliate of a much larger parental organization that has branches throughout the United States. The affiliate HealthCo operates six offices in a major metropolitan United States city and employees 135 employees. These employees are either a member of the administration department or the clinic services department.

B. Case Study Description

This section describes activities and information that were gathered at HealthCo over a six month period. Data was gathered from records and notes made during meetings with employees of HealthCo over the six month period, as well as from artifacts that were provided by HealthCo employees (e.g., organization charts, mission statements, policy statements). A program log was kept containing a record of all discussions, both formal and informal. Three department meetings were attended and nine in-depth semi-structured interviews with employees from different areas of HealthCo were held. Of importance to this study, six individuals' contributions are presented to show the exercise of power and policy implementation at HealthCo. Three of these interviews were with individuals in the administration department and three who are in the clinic services department. During the in-depth interviews, open-ended questions were asked. Although a short list of questions was used to start an interview, other areas of inquiry were investigated based on the interviewee's points of discussion. The questions that were asked varied, but were mainly those that caused discussions about HealthCo, HIPAA, the rollout of HIPAA, the management, the information technology department, and those responsible for enforcing HIPAA in the organization.

Direct quotes from the interviewees are shown in italics. Figure 1 shows a partial organization chart that details the role of each employee highlighted in this paper.

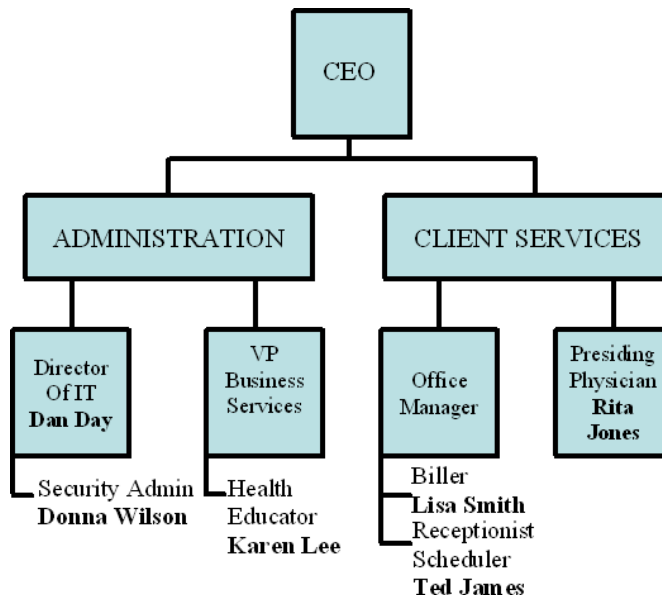


Fig. 1. HealthCo

C. Stakeholder Roles

The Director of IT, Dan Day, was given the responsibility of rolling out and enforcing HIPAA compliance at HealthCo. He was also responsible for HealthCo's overall information technology (IT) budget and ongoing IT expenditures. He reports to the CEO and she gave Day the authority to *make it happen*, no matter what it took. Making it happen meant that he, and his team, had to introduce HIPAA to the organization. Day and his team are management's agents. He was also responsible for enforcing employee compliance. During a staff meeting, where Day, Rita Jones, the office manager, and the VP of Business Services were present, the CEO made it clear that HIPAA violations would not be tolerated. She informed them that she gave Day the authority to *make it happen*. The CEO made it clear to her staff that an employee's employment at HealthCo would be in serious jeopardy if their non-compliance was discovered. The CEO informed her staff that violating HIPAA could possibly mean that HealthCo faced massive fines and penalties.

The authority that Day was given by the CEO gave him a lot of power in the organization; and he was aware of the power. Day was trained by Health and Human Services on HIPAA. Day stated:

A health care organization's non-compliance could have severe civil and criminal penalties... The CEO told me to make it happen. She didn't really care how I did it but she did say that she would even fire someone if they didn't follow the policy to the "t." I just need to let her know who isn't doing what they should be doing... I can also see what they do online and I had one of the technicians program the system so it made them have to change their passwords every 30 days. We never had anything like that before.

Day continued:

I think it is important but I don't like to manage with fear. You could tell a person to make sure that they locked their systems, or don't say a person's name on the phone out loud, or they may get fired. But what is that going to do? They would do it out of fear, rather than doing it because it's the right thing to do. I didn't tell Donna Wilson that the CEO said that she would fire somebody if they didn't follow the policy.

Wilson, who reports to Day, is the HIPAA security administrator. Since Wilson did not know that HIPAA compliance was one of the CEO's top priorities, to such an extent that a person could possibly be fired if reported, she was unaware of the power that she had. When asked to describe her role she said she was an educator and just sat down with people when they were hired and just described what HIPAA was. She also gave them a HIPAA pamphlet that she downloaded from the internet. Wilson had the responsibility for training new employees and the office staff, who reported to the office manager. The unfortunate part is that Wilson did not attend an external HIPAA training session, like her boss, Day. She was given a *train-the-trainer* session for about two hours on HIPAA by Day, and he did not inform her of the possible government penalties. One of the new people that Wilson trained was Ted James, the receptionist and scheduler, who reported to the office manager, who in turn reported to the CEO.

James was trained as a new employee and was oblivious to the healthcare environment. He had never worked in a hospital, a doctor or dentist's office, or a clinic prior to joining HealthCo. His role was to run the main HealthCo switchboard, route calls appropriately, and schedule client appointments. James did not know, understand, or seem to care about the power and politics that were present at HealthCo.

James iterates:

I just do my job. It's pretty straight forward. All the calls come into me and I forward them to the person. If they aren't there then they just go into voicemail. They don't go straight into voicemail, I was told, because of security reasons. They get a lot of treats here since this clinic performs abortions and they don't want people just getting through to anyone. I also schedule appointments here. [He opens up the office calendar and points to it. Revealed are clients' names and reasons for their appointments].

Jones is a doctor in the clinic and has been with HealthCo for six years. As the presiding physician, she reports directly to the CEO. Jones was quite aware of the importance of following HIPAA, and additionally, she knew of the possibility of large fines for non-compliance. She kept up with

her field and showed her level of understanding of HIPAA by stating:

HIPAA is the Act. It's a pain but it's important and you have to follow it. Patients don't want everyone knowing their personal information.

It is clear that the symbolic exercise of power in addition to legitimate authority was at play with Jones.

Karen Lee is a health educator. She reports to HealthCo's VP of Business Services, who reports to the CEO. The VP of Business Services knew the importance that the CEO placed on HIPAA; however, she did not stress its importance to her staff. Therefore, Lee was unaware of its priority at HealthCo and she did not know that repercussions were possible for non-compliance. Lee also did not deal directly with the IT organization, and therefore was unaware that Day signed off on all IT expenditures.

Lisa Smith is the billing administrator and reports to the office manager. As stated, the office manager reports directly to the CEO. At the initial rollout of HIPAA, the office manager informed her staff, including Smith about HIPAA. The office manager made it clear to Smith, and her colleagues, that HIPAA needed to be followed and that the CEO said it was important. Smith knew that if she was found to be in non-compliance, she could be terminated. She also knew that Day and Wilson were the HIPAA police, as her boss called them, and that Wilson was responsible for ensuring compliance of the office staff. Smith is clearly aware of the power and politics that the information systems implementation team has at HealthCo.

D. Discussion

Day, Jones, and Smith are very aware of the agent's power in implementing and ensuring the compliance of HIPAA at HealthCo. Wilson, James, and Lee are unaware of the power and politics that are occurring. Power and politics run rampant throughout HealthCo and affect the agent-employee dyads. Day knows that he has authority, given to him directly by the CEO. He also has power due to his information technology signoff authority. Wilson may not know that she has power, but she does. Her department is important to the organization and powerful as defined by the strategic contingency theory. Many other individuals in the organization know that compliance to HIPAA is mandatory at HealthCo.

As mentioned previously, Wilson is responsible for training and enforcing HIPAA compliance of all new hires, regardless of their position, and the office staff. Wilson is unaware of the power she has as the security administrator. Smith is quite aware of the power and politics in the organization and knows that she is supposed to comply. Unfortunately, even with knowing that she is supposed to comply, and additionally knowing that Wilson is responsible for enforcement, Smith states:

We have a lot of rules to follow... Since we have to change our password every 30 days and I can't for the life of me remember it. I just put it on a sticky and stick it here.

She points behind her monitor (out of sight of plain view) and then she smiles. As shown in Table III, Smith is a Policy Dissenter

Wilson is also responsible for new hire HIPAA training and compliance. James, the receptionist was HIPAA trained by

TABLE III
AWARENESS ABOUT POWER EXERCISE AT HEALTHCO

| Information Systems Security Policy Agent | Employee | |
|---|--------------------------------|--------------------------------|
| | Aware | Unaware |
| | Aware Day | Deal Making Day & Jones |
| Unaware Wilson | Policy Dissents Wilson & Smith | Blind Influence Wilson & James |

Wilson when he started. James is unaware of the power wield by Wilson or by IT. He does not fully comply with the rules of compliance either and in that he and Wilson are unaware of the power situation are in the Blind Influence stage (see Table III).

James said:

You know I've been a receptionist for a long time and I always learned that you acknowledge people by their name so I usually do – if no one is around my area listening. People want to be called by their name and acknowledged.

Day is responsible for training the Business Services department, of which Lee is a member. Lee is unaware of the power and politics at HealthCo. Since Lee is unaware of the power, and Day is aware, Day is 'Policy Forcing' and Lee does not comply (See Table III). She states in regards to passwords:

You're not suppose to use family members names because they say for security reasons somebody can figure them out. I just use my kids' and my husband's middle names and just add my address. Every once in a while you get locked out and you have to enter a new password. It won't let you enter a new one.

Day was also responsible for the training and ensuring compliance by the nurses and doctors. Since Jones was a member of the CEO's staff, she knew the power Day had. Not only did she know that a recommendation of termination to the CEO for non-compliance was possible, she also knew that Day approved the budget for IT and any interim IT expenditures. Her study outside of HealthCo, informed her of the importance of HIPAA and the ramifications possible. Table III shows that Day and Jones are 'Deal Making,' Jones says:

I know HIPAA is important, and I try to fully comply. There are a lot of rules but I try to stay up with them. A patients privacy is important and we need to keep their

information secure. People are really concerned about what people are finding out. Last week I read this article ...

VII. CONCLUSION

In this paper, the notions of power exercise and policy are used to present a new model of information systems security policy implementation. As was shown in the case study, an individual's awareness or unawareness of power exercise affects the outcome of an information systems security policy implementation. By raising the level of awareness of both the agents of information systems security policy, as well as the employees, there will be a mutual, consistent, effective, negotiated, and more efficient use of security policy.

From a practitioner's viewpoint, this research can assist in more effectively implementing information systems security policies. This can be done by ensuring that employees and policy agents in their organizations are aware of the exercise of power. They can also improve information systems security policy implementations and compliance by getting employees involved in the development, enforcement, and changing of the plans that are developed. This will in turn increase the employees' awareness levels of power use in the organization.

Policy implementation and power is a new research stream. With the many ways that researchers have purported that power and politics affects organizations, so too could these other power lenses be used to view information systems security policy implementations.

The limitations of this research present the future research possibilities. This research focused on the implementation of information systems security in organizations, purposely absent is looking at the development of these policies. Information systems security policy development can also be viewed from a power lens where the projected output is a security policy that is fair, manageable, and easily complied with by the entire organization. In addition, since as stated earlier, the awareness of power exercise does not exactly map to the types of power exercise, an exploration of the imperfect mapping of the two models is warranted.

While power is viewed in a variety of ways, it is important to see how it can be used to improve organizations, and specifically to increase the success rate of policy implementations. Clearly, the exercise of power, and more importantly the knowledge of such, is a vehicle in realizing this end. The optimal situation for an organization is where both the information systems security policy agent and the employee are aware of the exercise of power. If this is the case, they can mutually work together to make information systems security policy palatable for all.

REFERENCES

- [1] M.D. Abrams and D. Bailey, "Abstraction and refinement of layered security policy," in: *Information Security ± An integrated Collection of Essays*, M.D. Abrams, S. Jajodia and H.J. Podell (eds.), IEEE Computer Society Press, New York, 1995.
- [2] W.G. Astley and P.S. Sachdeva, P.S., "Structural Sources of Intraorganizational Power: A Theoretical Synthesis," *Academy of Management Review*, vol. 9, no. 1, pp. 104-113, 1987.

- [3] R. Baskerville and M. Siponen, "An Information Security Meta-policy for Emergent Organizations," *Logistic Information Management*, vol 15, no. 5/6, pp. 337-346, 2002.
- [4] N. Bjørn-Andersen and D. Kjaergaard, "Choices en route to the office of tomorrow," in *Technology and the Transformation of White Collar Work*, R. Kraut (ed.), Erlbaum, Hillsdale, NJ, 1987.
- [5] P.M. Blau, *Exchange and Power in Social Life* John Wiley & Sons, New York, 1964.
- [6] P. Bradshaw-Camball and V. Murray, "Illusions and other Games: A Trifocal View of Organizational Politics," *Organizations Science* vol. 2, no. 4, pp. 379-398, Nov. 1991.
- [7] D. Buchanan and R. Badham, *Power, politics, and organizational change: winning the turf*, Sage Publications, Thousand Oaks, CA, 1999.
- [8] G. Burrell, and G. Morgan, *Sociological paradigms and organisational analysis: elements of the sociology of corporate life*, Heinemann, London, 1979, pp. xiv, 432 p.
- [9] S. Clegg, *Frameworks of Power* Sage Publications, Newbury Park, CA, 1989.
- [10] R.A. Dahl, "Power," in: *International Encyclopedia of Social Sciences*, D.L. Sills (ed.), The Free Press, New York, 1968.
- [11] G. Dhillon, *Managing Information Systems Security* MacMillan Press, London, 1997.
- [12] M. Foucault, *Power/Knowledge: Selected Interviews and Other Writings, 1972-1977* Pantheon Books, New York, 1980.
- [13] S. Fuller, "Implementing HIPAA security standards - are you ready?," *Journal of the American Health Information Management Association* vol. 40, no. 9, pp. 36-40, Oct. 1999.
- [14] R.H. Hall, *Organizations: Structures, Processes, and Outcomes*, (7th ed.) Prentice Hall, Upper Saddle River, NJ, 1999.
- [15] D. Hardy, "The nature of unobtrusive power," *Journal of Management Studies*, vol. 22, no. 4, pp. 384-399, 1985.
- [16] D. Hickson, C. Hinings, C. Lee, R. Schneck, and J. Pennings, "A strategic contingencies theory of intraorganizational power," *Administrative Science Quarterly*, vol. 16, pp. 216-229, 1979.
- [17] J. Jaspersen, T. Carte, C.S. Saunders, B. Butler, H. Croes and W. Zheng, "Review: Power and Information Technology Research: A Metatriangulation Review," *MIS Quarterly*, vol. 26, no. 4, pp. 397-459, Dec. 2002.
- [18] J.H.C. Lucas, "Organizational Power and the Information Services Department," *Communications of the ACM*, vol. 27, no. 1, pp. 58-65, 1984.
- [19] S. Lukes, *Power: A Radical View* Macmillan, New York, 1974.
- [20] M.L. Markus and N. Bjørn-Andersen, "Power over users: Its exercise by system professionals," *Communications of the ACM*, vol. 30, no. 6, pp. 498-504, 1987.
- [21] M.W. Meyer, "Review of Power in Organizations," *Administrative Science Quarterly*, vol. 28, no. 2, pp. 301-303, 1983.
- [22] P.G. Neumann, "Risks to the public in computers and related systems," *ACM SIGSOFT Software Engineering Notes*, pp. 1-17, 1987.
- [23] Office for Civil Rights, "Summary of the HIPAA Privacy Rule," United States Department of Health & Human Services, Washington, DC, 2003.
- [24] A.M. Pettigrew, "Information Control as a Power Resource," *Sociology*, vol. 6, no. 2, pp. 187-204, 1972.
- [25] J. Pfeffer, *Power in Organizations* Pitman, Marshfield, MA, 1981.
- [26] R.S. Sandhu and P. Samarati, "Access control: principles and practice," *IEEE Communications*, pp 40-48, 1994.
- [27] C.S. Saunders and R.W. Scamell, "Intraorganizational distributions of power: Replication research," *Academy of Management Journal*, vol. 25, no. 2, pp. 192-200, 1982.
- [28] C.S. Saunders, C.S. and R.W. Scamell, "Organizational Power and the Information Services Department," *Communications of the ACM*, vol. 29, no. 2, pp. 142-147, 1986.
- [29] K.D. Schwartz, "Regulation Compliance Tops Companies' Security Concerns," in: *The Channel Insider*, 2004.
- [30] D.F. Sterne, "On the buzzword 'security policy'," Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy, pp. 219-230, 1991.
- [31] J. Viega and J. Voas, "The pros and cons of Unix and Windows security policies," *IEEE IT Professional*, vol. 2, no. 5, pp. 40-45, 2000.
- [32] G. Walsham, *Making a World of Difference: IT in a Global Context* John Wiley & Sons, Chichester, England, 2001.
- [33] C.C. Wood, *Information Security Policies Made Easy*, San Rafael, CA, 1999.

Federated Role-Based Access Control in Exertion-Oriented Programming

Satish Vellanki and Michael Sobolewski

Computer Science, Texas Tech University SORCER Research Group

Abstract— Federated computing environments expose lots of resources in order to serve their clients, which include system services, domain-specific services, and distributed file systems. A flexible and coordinated mechanism to control access to these resources is proposed which allows participants to form themselves into collaborative groups and secure access is granted to group members. Then, the participants can make resources available to a named group and manage locally the members in the group with required permissions across multiple domains. We explain how the proposed approach focused on user's local namespace is used in exertion-oriented programming and in particular in a SORCER federated file system where members of a group or delegated services can securely fetch any file replica that is available to a named group from any byte store service.

Index Terms—Federated computing, distributed systems, control access, group services.

I. INTRODUCTION

THE SORCER environment provides a way of creating service-oriented programs and executes them in a metacomputing environment. The service-oriented paradigm is a distributed computing concept wherein objects across the network play their predefined roles as service providers. Service requestors can access these providers by passing messages called service exertions. An exertion defines how the service providers federate among themselves to provide the requestor with required service collaboration. These services form an instruction-set of virtual metacomputer. Service provider can form a federation of services to provide the requested resources like computing, file systems. The federated environment requires an access

Manuscript received October 9, 2001. (Write the date on which you submitted your paper for review.) This work was supported in part by the U.S. Department of Commerce under Grant BS123456 (sponsor and financial support acknowledgment goes here). Paper titles should be written in uppercase and lowercase letters, not all uppercase. Avoid writing long formulas with subscripts in the title; short formulas that identify the elements are fine (e.g., "Nd-Fe-B"). Do not write "(Invited)" in the title. Full names of authors are preferred in the author field, but are not required. Put a space between authors' initials.

F. A. Author is with the National Institute of Standards and Technology, Boulder, CO 80305 USA (corresponding author to provide phone: 303-555-5555; fax: 303-555-5555; e-mail: author@boulder.nist.gov).

S. B. Author, Jr., was with Rice University, Houston, TX 77005 USA. He is now with the Department of Physics, Colorado State University, Fort Collins, CO 80523 USA (e-mail: author@lamar.colostate.edu).

T. C. Author is with the Electrical Engineering Department, University of Colorado, Boulder, CO 80309 USA, on leave from the National Research Institute for Metals, Tsukuba, Japan (e-mail: author@nrim.go.jp).

control mechanism to protect these resources of the metacomputer from unauthorized activities. This calls for a scalable authorization mechanism that scales along with the grid of resources while allowing the users to collaborate with each other. In group-based security in a federated file system, possible ways of constructing a group manager service are discussed with federated environments in view. In this paper we investigate ways to improve upon the concept by avoiding a global Certificate Authority (CA) while at the same time enabling users to share resources with people from any administration domain without a global authority. The rest of the paper is divided into the following sections: Section 2 describes background and literature review, Section 3 gives introduction to SORCER, Section 4 describes service messaging with exertions, Section 5 talks about authentication and authorization with exertions, Section 6 looks into a role-based access control framework for SORCER and Section 7 presents a deployment of the framework in a federated file system.

II. BACKGROUND AND LITERATURE REVIEW

Access control comprises of authentication, authorization, and auditing. Authentication is the process of verifying the identity of a user, service or a device. Authorization is the process of determining the access level of the authenticated identity on any requested resource. For example, allowing an authenticated user to read a file. Auditing allows us to review all authentication and authorization requests to determine system accountability and any gaps in security. For example, analysis of users logged sessions on a computer and updated resources. In this paper we concentrate on how to develop reliable authentication and authorization in federated environments across multiple administration domains.

A. Access Control Techniques

Access controls systems follow one of the following three approaches:

1. A mandatory access control system where any user who created an entity may not have all the rights on the entity. He/she may share it with other users but they cannot assume full control on this entity. The security policy on the entity is determined by the properties attached to it. Access to resource is allowed based on the security level of the user and the sensitivity labels attached to the resource. This kind of access control is usually required in military environments where any resource is dealt with utmost security.

2. In a discretionary access control system, the owner of a resource specifies who will be allowed the access to it and what kind of access is allowed. This is the most popular technique. Many existing file systems follow this access control technique. In a federated environment many users can collaborate to get a particular work done. Setting permissions for each user and following them through time is practically not possible. Rather users can be grouped according to some criteria and the access can be managed per group. Most existing systems do not allow a new group to be created by normal users. The administrator has to be involved in creating a new group, adding/removing users to/from it and in managing it. File systems in UNIX and Windows operating systems employ this approach.

3. In a role-based access control system permissions are defined for each group by a security authority on each resource. These roles usually do not change through the life of the system. The collection of roles is predefined. Each role is associated with a set of permissions. Any access to resource is granted if the requesting user belongs to any of the roles that allow access to this resource. Role-based access control is easier to manage and permissions can be granted and revoked any time.

Federated environments require the ability of a discretionary access control system while keeping the ease of use of a role-based access control system. Rather than predefining the roles, a user should be allowed to create roles according to his/her wish. The user can then set the permissions for the role on entities he/she owns. In this case these roles become local to the current user. A role or the permission of a role on any entity created by one user cannot be modified by another user.

Such a complex access control system that works with multiple domains and users usually makes the use of cryptographic keys. Public key cryptography or asymmetric cryptography makes use of a pair of cryptographic keys – a public key and a private key, in such a way that given the public key, the private key cannot be usually determined. Any content encrypted using one of these keys can only be decrypted using the other key. This adds lot of security to previously insecure communications and allows for unique authentication of the owner of the private key. The public key can be published in a common directory while the private key must be stored in a secure place. Any content sent to the owner of the key pair is encrypted with the owner's public key so that only the owner can decrypt it with the private key and read it. The owner can use the private key to sign messages that can be verified by any other person or system using the matching public key. This gives the possibility of having digital certificates that can be verified. While public key cryptography provides so many uses the greatest problem with it is determining the public key of an entity with who you wish to have a secure communication. The Public Key Infrastructure (PKI) has solved this problem, which is an arrangement to bind a public key to a user identity by a Certificate Issuing Authority (CA). The user identity or the

distinguished name should be globally unique in PKI. The CA verifies that the identity really belongs to the user in question before issuing a certificate. PKI enables the secure communication between two parties that have no prior knowledge of each other. As per definition, PKI can provide authentication of the owner of the key pair, but it cannot represent any form of authorization. Also CAs are possible cases for single points of failure in distributed systems and are not capable of scaling themselves with increasing loads of usage. Another public-key certificate standard – Simple Public Key Infrastructure/Simple Distributed Security Infrastructure (SPKI/SDSI) makes it possible to represent authorization grants using digital certificates without a need for global CA.

B. Simple Public Key Infrastructure

SPKI is a merger of two separate designs – SPKI and SDSI. SDSI allows defining groups and group membership certificates. SPKI concentrates on providing authorization certificates. Thus SPKI standard defines two certificate formats – name certificates and authorization certificates. The name certificates bind a public key to a name in the local namespace of the issuing authority. Any user who possesses a cryptographic key-pair can issue name certificates, which makes the user a certificate authority as in PKI. This is not possible in PKI where only few defined authorities can issue these certificates. The authorization certificate defines an authorization grant by the issuer of the certificate. It is possible to allow delegation of an authorization grant in these certificates.

SPKI by reducing the dependence on a central certificate authority allows the system to scale to any number of users from multiple domains. In fact SPKI designers believed that a central certificate authority serves no real purpose. A user can share his resources with any other user in the system provided he knows the public key of that user. He can add any user to his list of local users by importing their public keys. He can also give a friendly local name that he intends to use for this user. Authorization grants can be made using the local names or the recommended way of directly using public key in the certificates. SPKI/SDSI is defined in RFC specifications 2692 and 2693.

SPKI allows the authorization grant to be delegated by the grantee to others. The granter can decide whether to delegate or not when issuing the certificate. SPKI also defines *threshold subjects* where the authorization is granted when a minimum of k out of n granters concur to allow access to a resource.

III. SORCER

SORCER (Service Oriented Computing EnviRonment) is a federated service-to-service (S2S) metacomputing environment that treats service providers as network objects with well-defined semantics of a federated service object-oriented architecture. It is based on Jini semantics of services in the network and Jini programming model with explicit leases, distributed events, transactions, and discovery/join

protocols. While Jini focuses on service management in a networked environment, SORCER focuses on exertion-oriented programming and the execution environment for exertions. SORCER uses Jini discovery/join protocols to implement its exertion-oriented architecture (EOA) using federated method invocation, but hides all the low-level programming details of the Jini programming model.

In EOA, a service provider is an object that accepts remote messages from service requestors and execute on them. These messages are called service exertions and describe *service (collaboration) data, operations* and collaboration's *control strategy*. An *exertion task* (or simply a *task*) is an elementary service request, a kind of elementary federated instruction executed by a single service provider or a small-scale federation for the same service data. A composite exertion called an *exertion job* (or simply a *job*) is defined hierarchically in terms of tasks and other jobs, a kind of federated procedure executed by a large-scale federation. The executing exertion is dynamically bound to all required and currently available service providers on the network. This collection of providers identified in runtime is called an *exertion federation*. The federation provides the implementation for the collaboration as specified by its exertion. When the federation is formed, each exertion's operation has its corresponding method (code) available on the network. Thus, the network exerts the collaboration with the help of the dynamically formed service federation. In other words, we send the request onto the network implicitly, not to a particular service provider explicitly.

The overlay network of service providers is called the service grid and an exertion federation is in fact a *virtual metacomputer*. The metainstruction set of the metacomputer consists of all operations offered by all service providers in the grid. Thus, an exertion-oriented (EO) program is composed of *metainstructions* with its own *control strategy* and a *service context* representing the metaprogram data. The service context describes the collaboration data that tasks and jobs work on. Each provider guards the resources specified in service context with the help of two providers `Authenticator` and `Authorizer` described in Section 6. Each service provider offers services to other service peers on the object-oriented overlay network. These services are exposed *indirectly* by operations in well-known public remote interfaces and are considered to be elementary (tasks) or compound (jobs) activities in EOA. This indirectly means that you cannot invoke any operation defined in provider's interface directly. These operations can be specified in the requestor's exertion only, and the exertion is passed by itself on to the relevant service provider via the top-level `Servicer` interface implemented by all service providers called *servicers*—service peers. Thus all service providers in EOA implement the `service (Exertion, Transaction):Exertion` operation of the `Servicer` interface. When the servicer accepts its received exertion, the exertion's operations can be invoked by the servicer itself, if the requestor is authorized to do so, `Servicers` do not have

mutual associations prior to the execution of an exertion; they come together dynamically (federate) for a collaboration as defined by its exertion. In EOA requestors do not have to lookup for any network provider at all, they can submit an exertion, onto the network by calling `Exertion.exert(Transaction):Exertion` on the exertion. The `exert` operation will create a required federation that will run the collaboration as specified in the EO program and return the resulting exertion back to the exerting requestor. Since an exertion encapsulates everything needed (data, operations, and control strategy) for the collaboration, all results of the execution can be found in the returned exertion's service contexts. Domain specific servicers within the federation, or task peers (taskers), execute task exertions. *Rendezvous* peers (jobbers and spacers) coordinate execution of job exertions. Providers of the `Taker`, `Jobber`, and `Spacer` type are three of SORCER main infrastructure servicers—see Figure 1. In view of the P2P architecture defined by the `Servicer` interface, a job can be sent to any servicer. A peer that is not a `Jobber` type is responsible for forwarding the job to one of available rendezvous peers in the SORCER environment and returning results to the requestor.

Thus implicitly, any peer can handle any job or task. Once the exertion execution is complete, the federation dissolves and the providers disperse to seek other collaborations to join. Also, SORCER supports a traditional approach to grid

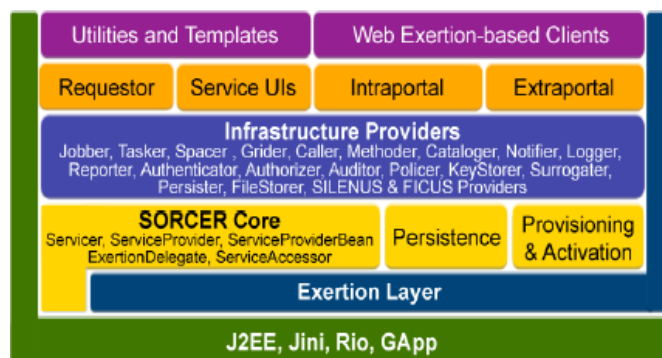


Fig. 1. The SORCER layered functional architecture

computing similar to those found, for example in Condor . Here, instead of exertions being executed by services providing business logic for invoked exertions, the business logic comes from the service requestor's executable codes that seek compute resources on the network.

Grid-based services in the SORCER environment include `Grider` services collaborating with `Jobber` and `Spacer` services for traditional grid job submission. `Caller` and `Methodor` services are used for task execution. `Callers` execute conventional programs via a system call, as described in the service context of submitted task. `Methoders` can download required Java code (task method) from requestors to process any submitted context accordingly with the code downloaded. In either case, the business logic comes from requestors; it is a conventional executable code invoked by `Callers` with the standard `Caller's` service context, or mobile Java code executed by `Methoders` with a matching

service context provided by the requestor.

IV. SERVICE MESSAGING AND EXERTIONS

In object-oriented terminology, a message is the single means of passing control to an object. If the object responds to the message, it has an operation and its implementation (method) for that message. Because object data is encapsulated and not directly accessible, a message is the only way to send data from one object to another. Each message specifies the name (identifier) of the receiving object, the name of operation to be invoked, and its parameters. In the unreliable network of objects; the receiving object might not be present or can go away at any time. Thus, we should postpone receiving object identification as late as possible. Grouping related messages per one request for the same data set makes a lot of sense due to network invocation latency and common errors in handling. These observations lead us to service-oriented messages called exertions. An exertion encapsulates multiple *service signatures* that define operations, a *service context* that defines data, and a *control strategy* that defines how signature operations flow in collaboration. Different types of control exertions (*IfExertion*, *ForExertion*, and *WhileExertion*) can be used to define flow of control that can also be configured additionally with adequate signature attributes.

An exertion can be invoked by calling exertion's `exert` operation: `Exertion.exert(Transaction) :Exertion`, where a parameter of the `Transaction` type is required when the transactional semantics is needed for all participating nested exertions within the parent one, otherwise can be `null`. Thus, EO programming allows us to submit an exertion onto the network and to perform executions of exertion's signatures on various service providers indirectly, but where does the serviceto-service communication come into play? How do these services communicate with one another if they are all different? Top-level communication between services, or the sending of service requests (exertions), is done through the use of the generic `Servicer` interface and the operation `service` that all `SORCER` services are required to provide—`Servicer.service(Exertion, Transaction)`. This top-level service operation takes an exertion as an argument and gives back an exertion as the return value. How this operation is used in the federated method invocation framework is described in detail in. So why are exertions used rather than directly calling on a provider's method and passing service contexts? There are two basic answers to this. First, passing exertions helps to aid with the network-centric messaging. A service requestor can send an exertion out onto the network—`Exertion.exert()`—and any `servicer` can pick it up. The `servicer` can then look at the interface and `PROCESS` operation requested within the exertion, and if it doesn't implement the desired interface or provide the desired operation, it can continue forwarding it to another provider who can service it. Second, passing exertions helps with fault detection and recovery, and security. Each exertion has its own completion state associated with it to specify who is invoking it, if it is yet to run, is already completed, or has

failed. Since full exertions are both passed and returned, the requestor can view the failed exertion composition to see what method was being called as well as what was used in the service context input nodes that may have caused the problem. Since exertions provide all the information needed to execute a task including its control strategy, a requestor would be able to pause a job between tasks, analyze it and make needed updates. To figure out where to resume a job, a rendezvous service would simply have to look at the task's completion states and resume the first one that wasn't/hasn't completed yet.

V. AUTHENTICATION AND AUTHORIZATION WITH EXERTIONS

Polymorphism enabled us to encapsulate a request then establish the signature of operation to call and vary the effect of calling the underlying operation by varying its implementation. The Command design pattern establishes an operation signature in a generic interface and defines various implementations of the interface. In Federated Method Invocation (FMI), the following three interfaces are defined with the following three commands: `Exertion.exert(Transaction):Exertion`—join the federation;

`Servicer.service(Exertion,Transaction):Exertion`—request a service in the federation from the top-level `Servicer` obtained for the activated exertion;

`Exerter.exert(Exertion, Transaction):Exertion`—execute the argument exertion by the target provider in the federation. These three commands define the Triple Command pattern that makes EO programming possible via various implementations of the three interfaces: `Exertion`, `Servicer`, and `Exerter`. The FMI approach allows for:

- the P2P environment via the `Servicer` interface,
- extensive modularization of programming P2P collaborations by the `Exertion` type,
- the execution of exertions by providers of the `Exerter` type, and
- vast common synergistic extensibility from the triple design pattern.

Thus, requestors can exert simple (tasks) and structured metaprograms (jobs with control exertions) with or without transactional semantics as defined in) above. The Triple Command pattern in `SORCER` works as follows:

An exertion is invoked by calling `Exertion.exert(Transaction)`. The `Exertion.exert` operation implemented in `ServiceExertion` uses `ServicerAccessor` to locate, at runtime, the provider matching the exertion's `PROCESS` signature. If a `Subject` in the exertion is not set, the requestor has to authenticate with the `Authenticator` service. After the successful authentication the `Subject` instance is created and the exertion can be passed onto the network. If the matching provider is found, then on its access proxy the `Servicer.service(Exertion, Transaction)` method is invoked. The matching provider first verifies if the requestor is authenticated; otherwise authenticates it with `Authenticator`. Then the provider consults the `Authorizer` service if the exertion's `Subject` is authorized

to execute the operation defined by the exertion's `PROCESS` signature. When the requestor is authenticated and authorized by the provider to invoke the method defined by the exertion's `PROCESS` signature, the provider calls its own `exert` operation: `Exerter.exert(Exertion, Transaction)`. `Exerter.exert` method calls `exert` either of `ServiceTasker`, `ServiceJobber`, or `ServiceSpacer` depending on the type of the exertion (`Task` or `Job`) and its control strategy. Permissions to execute the remaining signatures of `APPEND`, `PREPROCESS`, and `POSTPROCESS` type are checked with the Authorizer service for the executing Subject. If all of them are authorized, then the provider calls all the `APPEND`, next `PREPROCESS` methods, next the `PROCESS` method, and finally all the `POSTPROCESS` methods.

Individual service providers, either `Taskers` or rendezvous peers, implement their own service (`Exertion, Transaction`) method according to their service semantics and control strategy. However, all of them federate with available `Authenticator` and `Authorizer` providers in a uniform way using Java Authentication and Authorization Service (JAAS) as described later in Section 6.

VI. A ROLE-BASED FRAMEWORK

In order to make the process of authentication and authorization easier in the federated environment, the framework is divided into two major modules to handle cohesive functionality separately – one for authentication and another for authorization. These two modules are implemented as individual service providers in the `SORCER` environment. Multiple instances of both the services can be run for scalability. Both these services utilize the common infrastructure of `SORCER` and the key store module. Ideally, the key store has to be built as a separate service provider in the near future and all instances of the key store would communicate with each other in order to synchronize the access control lists, name and authorization SPKI certificates. Please note that digital certificates do not require a secure storage space but have to be verified before using them.

A. Architecture

The described Role-based Access Control Framework (RACF) uses JAAS but in the federated environment with distributed services. The authentication service acts as a login module while the requestor handles the JAAS login callbacks. The authenticator utilizes any configured legacy authentication system to authenticate the users and assigns the JAAS subject with some principals and credentials. The authorizer gets this subject through the resource providing services. The authorizer maintains the access control lists in form of SPKI authorization certificates.

B. Authentication Service

The requestors should be authenticated with the authentication service before they access any resource providing service. Requestors can be authenticated against any existing user databases. In our approach any legacy authentication module

supported by JAAS can be used.

How the authentication service works is described below. The service requestor gets the user name and hashed password from the user and sends it across to the authenticator. The authenticator service authenticates the user using the backend legacy authentication service. Upon successful authentication it generates a name certificate using the public key of the user. If the user is authenticating with the RACF system for the first time then a public/private key pair is generated for this user upon successful authentication with the legacy authentication service. This key-pair resides in any available, secure keystore. The authentication service then utilizes this key pair to generate a name certificate for the user. This name certificate is used as an authentication token since it is signed by the authentication service.

If the user is a returning user, his public key is simply fetched from the keystore and the name certificate is signed with the private key of the authentication service after he is authenticated with the legacy authentication service. All instances of authentication service use the same private key. The authentication service has to keep this private key secure, either by storing it in the key store provider or managing it by itself. The name certificate is then sent to the requestor. The requestor can use this name certificate along with the requests it makes for any resource to prove its identity. Any authorization service verifies the signature of the authentication service before providing any resource. A validity specification on the name certificate can be used to specify a time frame only within which the token is valid. After this timeout the requestor has to renew this token for further usage.

If the requestor has multiple accounts with the legacy authentication services then it is possible to have a single identity for this requestor in `SORCER`. For example, if a user has a UNIX account at the Computer Science Department and also a Windows account at the university then he/she can choose to have a single identity in `SORCER`. This is possible since we use a public-private key pair for the user, using which we identify the user after authentication. This allows him/her to access his/her resources using any legacy authentication service. It will not hinder the user from accessing his/her resources when one of the legacy authentication services cannot be used due to network problems or what so ever issues. Also users from any domain can be authenticated and issued a key pair, thereby breaking the administration domain barrier.

All requestors, to be able to identify by its name, can use the same name certificate created by the authentication service. When they wish to include the requestor in any role they can look for the requestor's name certificate and include it. Requestors can issue authorization grants without using name certificates as well, if they wish to, by using the public key as subject in their authorization certificates instead of their local names.

C. Authorization Service

The authorization service holds the access control lists and authorizes any request to access resources. The Authorizer itself does not guard the resources, but only provides a way to

verify if the subject in question has the permission to access the resource. The resource provider itself by any means should keep the actual resource secure. The authorization service also requires the keystore module. The keystore can be run as an independent service in the federated environment and multiple instances of it can be run for scalability. All keystore modules will have to synchronize the keys available in order for the authorization system to work.

When a request for a resource arrives at an actual service provider, such as SILENUS, it calls for the authorization service to verify the user identity and determine if the user is allowed to access the requested object. The authorization service verifies the user identity by simply verifying the signature of the name certificate sent across by the resource provider. This name certificate is supposed to be signed by the authentication service, whose public key the authorizer is aware of. The request is denied if the verification fails. Once this signature is verified, the authorization service proceeds to determine the access control on the requested object.

Access control objects are stored as authorization certificates in the keystore. These authorization certificates indicate the issuer, the subject, a tag, a bit field indicating if the subject can delegate this authorization grant and a validity specification. The tag specifies the object on which the authorization is granted and what type of access is allowed. The tag can be specified by the resource provider in any format suited for the application. As a case in point, the SILENUS file system puts the file name and access type (primarily read and/or write) in a way that authorization service can understand. In order to speed up the process of access checking, the authorization certificates are stored as 5-tuples, provided the storage area is secure. When that is not possible they can be stored as certificates and the individual fields can be determined when they are read.

The authorization service requests for the related authorization certificates from the keystore and runs a resolution algorithm to determine if the access is allowed. The algorithm checks if it can find a chain of delegated authorizations from the resource owner to the requestor under question on the requested object. If it can resolve the chain, access is allowed if the chain resolution fails the access will be denied. The Java implementation of SPKI/SDSI is utilized for this purpose. This library defines ways to create name certificates, authorization certificates, tags, and a keystore to store SPKI certificates along with many necessary mechanisms.

D. Group formation

Any user who wishes to share his/her resources with other users, has to create a group and then allow this group to access the resources accessible by him/her. The group name is local to the current user and does not reflect on the entire system; it is only visible in the user's local namespace. This group may include only one user in which case it will be like a local name for the subject. For example the user Alice can create a group named "friends" and add Bob and Carol to it. This is done by issuing two name certificates with Bob's public key and Carol's public key as subjects respectively. Alice can then issue an authorization certificate that specifies the

authorization grant in its tag field and the local name "friends" in the subject. The tag contains the resource objects id and the access control specification.

Assume that a name certificate is represented using the notation,

```
Issuer localname -> Subject
```

And authorization certificates are represented as

```
Issuer tag -> Subject
```

Then our example will be:

```
Alice friends -> Bob
```

```
Alice friends -> Carol
```

```
Alice (+read document.txt) -> friends
```

The tag indicates permission to read document.txt and the ability to delegate this permission to others by "friends".

The subject need not be a public key always; it could be a list of names too. Let's say Dave wants to let Alice's friends read his files too. He may issue a certificate

```
Dave (read mydoc.txt) -> Alice friends
```

This allows Alice's friends to be able to read Dave's mydoc.txt. The local name of Alice, "friends" has been used by Dave here.

VII. DEPLOYMENT IN SILENUS

The role-based access control framework has been deployed in the SORCER federated environment and validated successfully in the SILENUS file system with a file browser UI. The framework is built in Java using the JSDSI library. SILENUS provides a federated file system for SORCER. The system itself is made up of multiple service providers that collaborate with each other to provide a service-oriented file system. The most important ones are the metadata store and byte store providers. As the names indicate, the metadata store persists the meta information of the files such as file name, size, and mime type. It also saves a unique identifier to each file. When a byte store is contacted with this unique id, the file contents can be obtained. In order to provide access control to the SILENUS file system both metadata store and byte store have to be secure and have to utilize the access control framework. The SILENUS file system, instead of exposing each individual service provider, follows a façade design pattern where a façade service acts as the SILENUS entry service provider. The façade provides service UI, accepts requests from requestors, and forwards them to the appropriate service provider. The interaction of SILENUS with RACF has been depicted in Figure 2. For brevity some SORCER components are omitted.

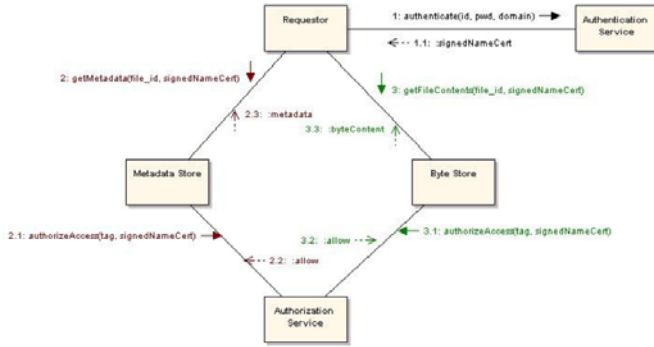


Fig. 2. SILENUS utilizing the role-based access control framework

The SILENUS façade manages all proxies for the underlying services. It acts as an entry point service for SILENUS service providers with multiple façade in the system at any time. All login requests are sent to the authentication service. The metadata store and the byte store request the authorization service to control access to their resources. When a requestor makes a request to access a file's content it sends the file information and signed public key that is obtained from authentication service to metadata store. The metadata store then requests the authorization service to determine if this access is allowed. Only when the authorization service signals go ahead the metadata store entertains the request. The byte store also works in a similar way with the authorization service.

The SILENUS façade provides an interactive user interface to access files without exposing the user to any complex access control behavior. In fact user-friendliness has been one of the major requirements for SILENUS.

The role-based federated access control framework has been utilized in a similar way for exertion-oriented programming by other SORCER services to provide a scalable and reliable authentication and authorization services so that resource providers do not have to handle it themselves in an ad-hock manner.

VIII. CONCLUSIONS

An access control mechanism is needed in federated environments where conventional solutions do not scale well. Most existing access control solutions are tightly coupled with the service provider or a part of a service provider and as such are not meant for federated environments. We propose a federated solution for access control that builds on top of JAAS framework. The proposed solution scales well with increasing resources and service providers simply by running more instances of authorizers. Along with providing a federated access control framework we also have concentrated on user collaboration where users can share resources with other users irrespective of the administration domain they come from. SPKI certificates are used to create local namespace thereby avoiding global naming conventions and central certificate authorities. SPKI also provides the facility to delegate authorization grants across exertion-based federations. Users and requestors can create roles in that user's namespace and can assign permissions to these roles

thereby avoiding the involvement of an administrator for day-to-day operations of users, which is highly required in a self-sustaining environment like SORCER. A successful validation of the presented framework was deployed in the SILENUS federated file system along with the same federated JAAS-based approach for all SORCER requestors and providers.

REFERENCES

- [1] M. Sobolewski, "Federated Method Invocation with Exertions," Proceedings of the 2007 IMCSIT Conference, PTI Press, ISSN 1896-7094, pp. 765-778, 2007. Available: <http://sorcer.cs.ttu.edu/publications/papers/96.pdf>
- [2] M. Sobolewski, "SORCER: Computing and Metacomputing Intergrid," 10th International Conference on Enterprise Information Systems, Barcelona, Spain, 2008. Available: <http://sorcer.cs.ttu.edu/publications/papers/2008/iceisintergrid-08.pdf>
- [3] D. Thain, T. Tannenbaum, and M. Livny, "Condor and the Grid," in Fran Berman, Anthony J.G. Hey, and Geoffrey Fox, editors, *Grid Computing: Making The Global Infrastructure a Reality*, John Wiley, 2003.
- [4] M. Berger and M. Sobolewski, "Group-based Security in a Federated File System," 2nd Annual Symposium on Information Assurance, Albany NY, June 6-7, 2007, pp. 56-63, 2007.
- [5] M. Berger and M. Sobolewski, "Lessons Learned from the SILENUS Federated File System," in Complex Systems Concurrent Engineering, Loureiro, G. and Curran, R. (Eds.), Springer Verlag, ISBN: 978-1-84628-975-0, pp. 431-440, 2007.
- [6] "Java Cryptography Architecture, Key Management," Available: <http://java.sun.com/javase/6/docs/technotes/guides/security/crypto/CryptoSpec.html#KeyManagement>
- [7] "Jini architecture specification, Version 2.1.," Available: <http://www.sun.com/software/software/jini/specs/jini1.2.html/jinititle.html>.
- [8] M. Gasser, "Building A Secure Computer System," pp. 45-58
- [9] R.S. Sandhu, E.J. Coynek, H. L. Feinsteink and C.E. Youmank, "Role-Based Access Control Models," *IEEE Computer*, vol. 29, no. 2, pp. 38-47, IEEE Press, 1996.
- [10] J. Weise, "Public Key Infrastructure Overview", Sun BluePrints, *SUN Microsystems*, Available: <http://www.sun.com/blueprints/0801/publickey.pdf>
- [11] C.M. Ellison, B. Franz, B. Lampson, R. Rivest, B. M. Thomas, and T. Ylonen. "SPKI Requirements, SPKI Certificate Theory, Simple public key certificate, SPKI Example," [Internet draft], Oct. 1998. Available: <http://world.std.com/~cme/spki.txt>
- [12] C. Ellison, "Establishing Identity Without Certification Authorities"
- [13] "JSDSI: A Java Implementation of Tools for SDSI Certificate Management," Available: <http://jsdsi.sf.net/>
- [14] Rivest and Lampson, "SDSI A Simple Distributed Security Infrastructure."
- [15] J. Garms and D. Somerfield, *Professional Java*.

IDKEYMAN: An Identity-Based Key Management Scheme for Wireless Ad Hoc Body Area Networks

Sriram Sankaran, Mohammad Iftexhar Husain, and Ramalingam Sridhar

Department of Computer Science and Engineering

University at Buffalo, The State University of New York, Buffalo, NY 14260

Abstract— Wireless Ad hoc Body Area Networks are primarily used in health-care applications for patient monitoring purposes. Publisher-Subscriber driven Body Area Networks enable publishers (medical sensors attached to patients) to disseminate medical data to numerous mobile heterogeneous subscribers (doctors or caregivers) through a subscription mechanism. Such an environment raises serious security concerns due to the privacy critical medical data coupled with the resource constraints of individual body sensors. To address this problem, we present an identity based key management scheme using Identity-Based Encryption (IBE). IBE facilitates faster key set-up in addition to being lightweight and energy-efficient. The proposed scheme uses IBE to set up pair-wise symmetric keys to preserve data confidentiality and integrity. Our prototype and evaluation of the proposed model validate the approach.

I. INTRODUCTION

Wireless Sensor Networks have been applied in health-care environments termed Wireless Ad hoc Body Area Networks, also referred as Body Sensor Networks (BSN). BSN comprises of a group of sensors either attached to or implanted inside the human body. These sensors are often resource-constrained and facilitate remote monitoring of patients in hospital or emergency conditions thereby reducing health-care costs.

BSN differs from traditional sensor networks in several ways. The main difference lies in the privacy-critical medical data of patients. A BSN is a real-time system i.e. the collected data has to be readily available in real-time in the event of an emergency while failing to provide could result in severe life threatening problems. Also, lifetime of BSNs is critical with the pressing resource constraints of individual body sensors.

Security in BSN is of paramount importance due to the criticality of the medical data coupled with the resource constraints of individual body sensors requiring lightweight solutions. Security must be provided between patients and their authorized doctors/caregivers through key management solutions.

Ideally, security solutions proposed for BSN must satisfy the following security traits. For instance, medical data must be accessible only by corresponding patients and his/her authorized physicians thus ensuring confidentiality, as per

HIPAA regulations [28]. To prevent medical data from getting into the hands of intruders/unauthorized people, medical data must be authenticated. With authentication in place, medical data must be integrity protected in order to prevent/detect data tampering. Finally, this data needs to be received and processed in real-time without incurring much delay.

In this paper, we consider publisher-subscriber driven body sensor networks, a key enabler for the design and development of CodeBlue system [2][3]. We propose a key management scheme, IDKEYMAN, for this communication model using Identity-Based Encryption (IBE). IBE facilitates faster key set up in addition to incurring low overhead. We use IBE to set up pair-wise symmetric keys between publishers and subscribers. Our scheme preserves the confidentiality, authenticity and integrity of safety critical medical data while also being energy-efficient. We tested our scheme on Prowler [12], a wireless sensor network simulator with Berkeley MICA mote [27] as the targeted platform.

II. RELATED WORK

Early research on key management for sensor networks focused on symmetric key based approaches since public key based approaches seemed to incur more overhead on the motes. Probabilistic key management was proposed by [4], where a pair of nodes wanting to communicate randomly picks keys from a key pool and communicates using the common shared key. Some variations were proposed to the above scheme termed as q-composite schemes and random pair-wise schemes in [7]. Q-composite scheme computes the pair-wise keys based on the hash of q-pre-distributed keys that the communicating entities share, thus decreasing the probability of node compromise. Random key improves on the q-composite scheme and further increases its resilience to node compromise by randomly picking its communicating entities, computing a random pair-wise key and attaching it to the key ring of the sensor's ID. Liu et al. [5] further study the probabilistic key approach proposed by [4] and construct a pool of several polynomials to generate pair-wise keys in contrast to key distribution based on a single polynomial to increase robustness towards node capture. Zhu et al. [8] combine the idea of probabilistic key approach and threshold key sharing to compute a pair-wise key between

communicating entities. Du et al. [6] improve Blom's scheme [20] and increase its network resilience by devising a pair-wise key pre-distribution scheme based on multiple key spaces in contrast to the single key space based approach proposed by [20]. While these schemes proposed for traditional sensor networks provide security support at the right time by resisting attacks, they may not readily satisfy the stringent resource constraints and real-time requirements of individual body sensors.

Recent research demonstrates public key methods such as Elliptic Curve Cryptography (ECC) to be feasible on the resource constrained nodes [3]. Public key based approaches offer several advantages over symmetric key based approaches due to the ability to bootstrap security using a trusted authority. Our scheme offers even more advantages that it avoids the need for distributing public keys using trusted authority since identity is used as the public key. Furthermore, our scheme pre-deploys the nodes with private keys making the private key generator unnecessary.

Elliptic curve based approaches have been proposed in the literature for security in sensor networks. Malasri et al. [1] devised an authentication scheme and an ECC based secure key exchange protocol for providing authentication of patients thereby ensuring message integrity and confidentiality. However, in contrast to their approach involving ECC, we have used identity based cryptographic primitives since it offers several advantages compared with ECC as mentioned above. In their scheme, Message Authenticated Code (MAC) was computed at every step of the key management process which makes it resource intensive and introduces delay in processing packets at the receiver. To minimize the processing delay, our approach involves computing the MAC only during data packet transmission phase.

Oliveira et al [9] proposed a security solution TinyTate for sensor networks based on IBE and claimed it to be feasible on the resource constrained nodes. In contrast to their approach involving a traditional sensor network with a standard communication model, we consider body sensor networks that comply with Publisher-Subscriber model practically implemented in CodeBlue, one of the most complete frameworks in the healthcare context. Their scheme involves senders to broadcast their identities without any security support which allows adversaries to launch DoS attacks by broadcasting several fake identities draining the precious power of the resource constrained nodes. To prevent DoS attacks, IDKEYMAN encrypts the identities of publishers using the public keys of subscribers. Tan et al. [11] proposed an Identity-Based cryptographic approach for security in body sensor networks which involves sensors to compute public keys by applying hash function on an arbitrary number of application dependent keys generated by them and stored on their flash memory and perform regular elliptic curve encryption/decryption using Elliptic Curve Digital Signature Algorithm (ECDSA). Their approach not only increases the storage on the flash memory but also incurs higher execution

time and energy consumption due to the overhead involved in computing public keys. In contrast, our approach employs similar but simple version of IBE by pre-deploying publishers with the public key of the subscribers and using it to establish session keys for data exchange periodically refreshed at regular intervals.

While the above proposed approaches show significant promise in providing security and privacy support, none have taken into account minimizing the trade-off between energy and security while addressing the key requirements of body sensors such as energy conservation and faster execution, since we believe that energy conservation is crucial for longer life time of the sensors and faster execution is necessary for meeting real-time deadlines. Thus, we attempt to propose such a security solution that strikes a suitable balance between providing robust security and minimizing the execution time and energy consumption of individual body sensors.

Security for publisher-subscriber driven networks was analyzed in [19] and key management based approaches have been proposed in [16], [17] and [18] to ensure confidentiality, integrity and availability. However, the applicability of these networks to a health-care scenario was first investigated by developers of CodeBlue, who utilized this model in their system. We attempt to develop a key management mechanism for CodeBlue system.

III. BACKGROUND

A. Publisher-Subscriber Architecture

In this architecture (Figure 1), publishers are the nodes attached to the patients and subscribers are their corresponding authorized doctors/care-givers typically holding a PDA/Laptop. Publishers monitor vital body signs of the patients and transmit the data to the subscribers who in turn accordingly initiate responses. On the other hand, a subscriber can also query the publisher real-time for patient's health status. This kind of architecture is mainly suited to a multi cast scenario where data from sender gets sent to multiple receivers to co-ordinate their actions. This scenario is analogous to the health-care environment where there can be more than one authorized doctor/caregiver to diagnose a patient.

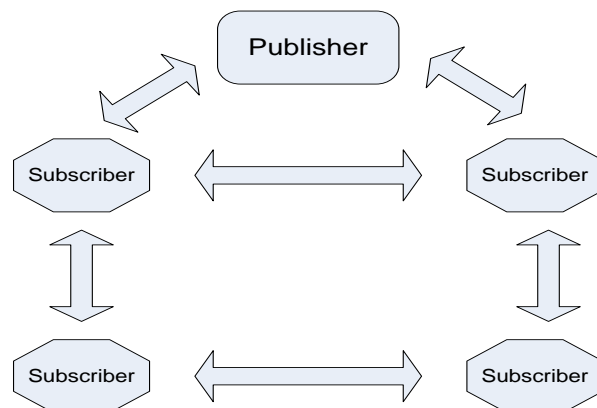


Fig. 1. Publisher-Subscriber Architecture

B. Identity- Based Encryption (IBE)

IBE, a public key based technology (Figure 2) is recently gaining attention among researchers due to rapid key generation and therefore making expensive operations of PKI unnecessary since node's identification information is used as the public key.

Typically nodes obtain their private key using a private key generator on providing its identification information as input. This is feasible compared to trusted certification authority based approach employed in a traditional PKI.

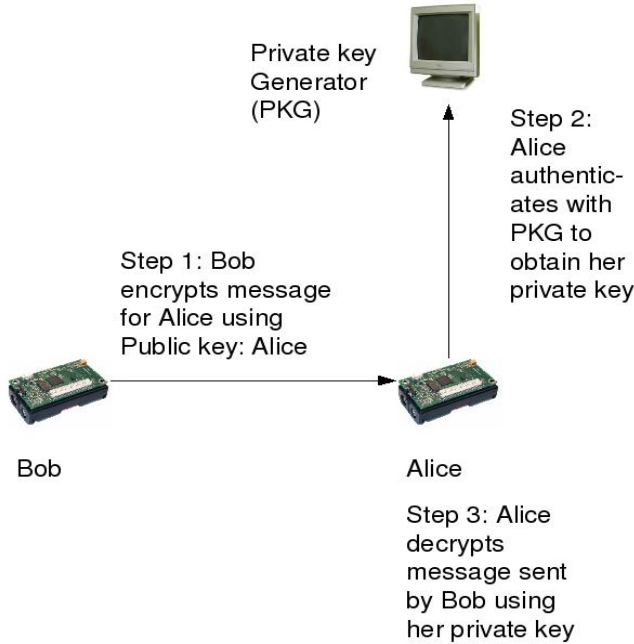


Fig. 2. Identity Based Encryption

IBE is based on Identity based cryptography, initially introduced by Adi Shamir in 1984. We found that traditional IBE incurs greater overhead than symmetric key based approaches [9]. Since, public key based approaches offer the greatest advantage of bootstrapping security, we use IBE only to exchange pair-wise symmetric keys between publishers and subscribers. The symmetric keys are used in subsequent communications thus reducing the computational overhead on the publishers. We elaborate on our approach in the next section.

IV. PROPOSED SCHEME: IDKEYMAN

We assume that authorized subscribers have access to the medical records of their corresponding patients. Our proposed scheme, IDKEYMAN, consists of two parts. We believe that it is necessary to identify and authenticate publishers (patients) during the key management phase. Let us look at the publisher authentication model and the identity based key management scheme below.

A. Publisher Authentication Model

In the publisher authentication model, RFID tags are integrated with wearable medical sensors allowing them to capture a unique identification (PID) of the patients. The publisher gathers the PID information and includes it in the key management scheme (See 4.2) where validation by subscribers takes place before data transfer/communication between publisher and subscriber takes place. Periodic authentication of patients through RFID tags would be essential to increase robustness of the system towards adversaries launching malicious attacks.

RFID technologies have recently been extensively deployed in hospitals [10] and we believe that this mechanism is sufficient to identify patients in hospitals.

B. Identity- Based Key Management Scheme

In accordance with the NIST recommendation on key management [26], our key management scheme (Figure 3) operates in pre-operational, operational, post-operational and destroyed phases.

Pre-operational phase:

We assume that each subscriber is pre-distributed with the private key K_s and public key K_{sub} in addition to a function that takes the ID of the publisher and outputs its corresponding public key. The public key of the subscriber, K_{sub} is programmed in the memory of the publishers. Let us look at the steps outlined below.

Operational Phase:

Step 1: Initially, when the medical sensor attached to the patient is powered on, the mote obtains the patient identification information PID from the RFID tag attached to the patient queried by RFID reader. Once the patient's information PID is obtained, the mote collects PID, its id MoteID, generates a nonce $n1$, encrypts message using public key of the subscriber K_{sub} and sends it securely to the subscriber. The main objective of using K_{sub} in the first place is to encrypt the patient identification information making it impossible for adversaries to spoof PID. Nonce $n1$ is included in the message to prevent replay attacks.

Step 2: The subscriber decrypts the received message using its private key K_s and verifies the authenticity of this patient using PID and MoteID. Then it uses received MoteID to derive public key (K_{pub}) for the corresponding publisher, generates pair-wise secret keys, encrypts message using K_{pub} and sends it securely to the publisher. This message contains the ids of both subscriber and publisher, id_s and id_p , pair-wise secret key $K_{p,s}$ along with the nonce that the publisher sent.

Step 3: The crucial part of our scheme is the confirmation from subscriber that publisher has received the correct pair-wise keys before initiation of medical data takes place. After decrypting the message using K_p and obtaining the pair-wise secret keys, publisher sends a message containing its ID and

subscriber's ID encrypted using the pair-wise secret key $K_{p,s}$, which is decrypted by subscriber and confirmed.

Step 4: Now, initiation of medical data takes place by encrypting data using pair-wise secret key $K_{p,s}$ along with the identities of publisher and subscriber and a new value for nonce computed using existing nonce.

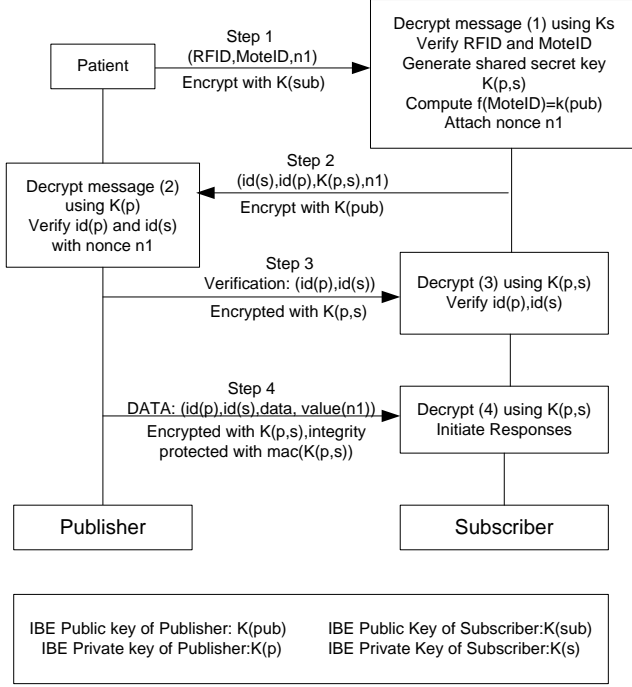


Fig. 3. Identity-based Key Management Scheme

A MAC ($\text{mac}_{K(p,s)}$) derived from pair-wise secret key $K_{p,s}$ is used to protect the message from unauthorized message tampering by adversaries. The subscriber decrypts it using the pair-wise secret key $K_{p,s}$ and accordingly initiates responses.

Post-operational Phase:

The pair-wise secret keys are used as session keys for future communications. To update the pair-wise secret keys, the publisher and subscriber exchanges new values of nonces and subscriber computes a new pair-wise key for communicating with the publisher.

Destroyed Phase:

In the destroyed phase, there can be two kinds of cases that need to be addressed with regard to key compromise. If the public key of the subscriber is compromised, we need to re-initialize the expensive pre-operational phase but there exists no other way to fix this issue. On the other hand, if the pair-wise or session key is compromised, initiating the key agreement process will help solve the problem.

V. SECURITY ANALYSIS

We analyze our proposed scheme for resistance against different kinds of attacks relevant to this application. Due to the privacy critical nature of the medical data, identity and data

tampering attacks dominate this area of discussion. Impersonation attacks are not possible since only legitimate nodes have access to the public key of the subscriber. Even without impersonation attacks, it is possible that attackers replay old data that may be appropriate for the patients. In that case, we require the subscribers to attach the nonces sent by publishers to prevent replay attacks. Publishers typically buffer their nonces to compare with those received from subscribers to check for consistency. If any kind of inconsistency is observed, the received packet is discarded.

Our scheme preserves the data integrity required for health-care environments apart from confidentiality by computing a MAC on the pair-wise symmetric key to provide increased level of security. Thus any kind of data tampering or false data injection attacks can be detected. Lastly, our scheme requires the generation of different session keys for ensuing communications by exchanging new values of nonces and old keys are erased from memory to prevent key compromise.

VI. IMPLEMENTATION AND PERFORMANCE EVALUATION

We have implemented IDKEYMAN in Prowler [12], a MATLAB based wireless sensor network simulator which simulates the Mica2 platform in conjunction with a Pairing Based Cryptography library (PBC) [13] in Perl to implement identity based encryption. We chose AES block cipher for symmetric encryption and SHA-1 for computing the hash function used for MAC. The following are the time and energy evaluations for the proposed scheme.

A. Energy Constraints

We evaluated the energy consumed in IDKEYMAN. Typically, energy consumed by a key management mechanism is determined by the energy required for execution of cryptographic operations along with energy required for transmission/reception. We begin our energy evaluation by computing the energy consumed during execution of cryptographic operations and also during transmission/reception and finally end with stepwise energy computations.

According to [15], we obtained the energy consumption for identity based key negotiation to be 0.44J. The size of each message is set to 512-bits depending on the key length and application headers in our key management scheme. According to [22], the transmission and reception of a single byte of data requires 59.2 μ J and 28.6 μ J respectively. Thus the transmission and reception of 512-bit message would consume 3.78mJ and 1.83mJ respectively. According to [22], energy consumed by a SHA-1 hash function was 5.9 μ J/byte. In our scheme, a 160-bit hash function for computing the identity based public key of the subscriber would consume 0.11mJ of energy.

We used the 128-bit AES cipher for establishing the symmetric key between publishers and subscribers. According to [25], generating a shared secret key using AES cipher consumes 7.87 μ J of energy. According to [22], encryption and decryption using AES cipher consumes 1.62 μ J and 2.49 μ J.

Thus the encryption and decryption of a 128-bit AES cipher would consume 0.025mJ and 0.039mJ of energy. According to [23], computing a MAC using AES consumes 2.31 μ J/byte of energy. Thus, computing a MAC using 128-bit AES would consume 0.036mJ of energy.

With the above computed data, we have evaluated the energy consumed at every step of our key management mechanism. Table 1 shows the stepwise energy computations for IDKEYMAN.

TABLE I
ENERGY CONSUMPTION OF IDKEYMAN

| IDKEYMAN | Energy Consumed |
|--------------|-----------------|
| Step 1 | 0.44J |
| Step 2 | 0.44J |
| Step 3 | 5.6mJ |
| Step 4 | 5.7mJ |
| Total Energy | 0.89J |

B. Time Constraints

The following is the time analysis of IDKEYMAN. Similar to energy computation, time taken by a key management mechanism is determined by the time required for execution of cryptographic operations along with time required for transmission/reception.

According to [21], encryption and decryption using IBE takes 35ms and 27ms respectively. We obtained both the transmission and reception times of MICA motes from [29] to be 0.41ms per byte. Thus the transmission and reception of 512-bit message would take 26ms. According to [24], generating a shared secret key for a 32-byte packet using AES takes 2070 μ s. Thus generating a key using 128-bit AES would take 1.033ms. SHA-1 hash function takes 1.62 ms for computing the hash for 29 bytes of data according to [23]. Thus, a 160-bit hash function for computing the IBE public key of the publisher would take 1.11 ms.

According to [23], encrypting 29 bytes of data using AES takes 2.14ms. Thus, encryption using 128-bit AES would take 1.17 ms. Finally, computing a MAC using AES for 29 bytes of data takes 5.34ms. Thus, computing a MAC using 128-bit AES takes 2.94ms.

With the above computed data, we have evaluated the time it takes to execute at every step of our key management mechanism. Table 2 shows the stepwise time computations for IDKEYMAN.

TABLE II
EXECUTION TIME OF IDKEYMAN

| IDKEYMAN | Execution Time |
|------------|----------------|
| Step 1 | 0.11s |
| Step 2 | 0.12s |
| Step 3 | 0.05s |
| Step 4 | 0.06s |
| Total time | 0.34s |

In our simulations, we considered the subscribers as motes

which resulted in similar message generation and verification times with that of the publishers. In reality, since subscribers typically hold PDAs/laptops having computation and communication power significantly higher than that of the motes, we expect this number to go down drastically.

C. Comparison

We compare the time and energy consumed in our approach with that of other approaches as shown in Table 3.

TABLE III
COMPARISON OF TIME AND ENERGY CONSUMPTION OF DIFFERENT SCHEMES WITH IDKEYMAN

| Scheme | Execution Time | Energy Consumed |
|---------------------|----------------|-----------------|
| Malasri et al. [1] | 18.41s | 0.11J |
| Oliveira et al. [9] | 0.06s | 0.44J |
| Tan et al. [11] | 2.70s | 45.66J |
| IDKEYMAN | 0.34s | 0.89J |

In Table 3, second column is the total time and third column is the total energy needed to generate and verify packets using keys. Table 3 and its corresponding graph (see figure 4) shows that IDKEYMAN facilitates faster key set-up time and at the same time consumes less energy compared with existing approaches. The faster key set-up time and lesser energy consumption is due to using the expensive IBE one-time to set up pair-wise symmetric keys reducing the computational overhead on the motes. Even though [9] executes the fastest consuming less energy, its vulnerability to DoS attacks as mentioned earlier prevents usage in safety-critical BSN. Similarly the higher execution time of [1] and [11] may not be suitable for deployment in real-time systems such as BSN. Further, IDKEYMAN is a complete key management scheme addressing pre-operational, operational, post-operational and destroyed phases. Thus, IDKEYMAN balances robust security with lesser energy consumption and faster execution making it satisfy the prime requirements of BSNs.

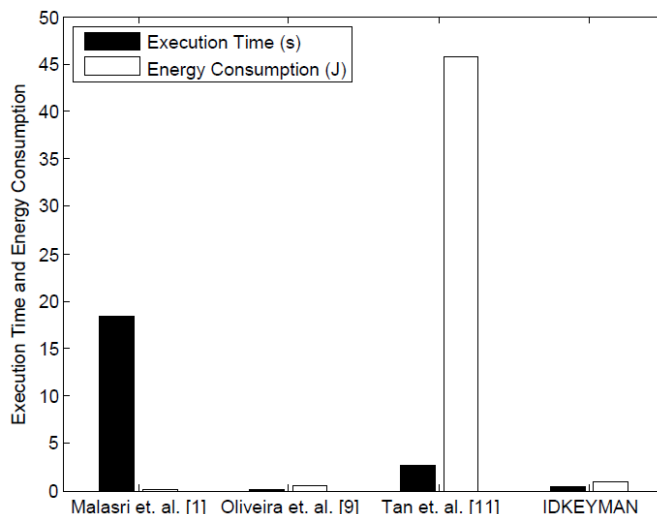


Fig. 4. Time and Energy Comparison with Existing Approaches

VII. CONCLUSION

In this paper, we have provided security and privacy support for publisher-subscriber driven wireless ad hoc body area networks, by presenting IDKEYMAN, a key management scheme using IBE. IDKEYMAN addresses the real-time and stringent resource requirements of individual body sensors while also being robust to attacks. We are currently working to extend this scheme to an emergency response scenario.

REFERENCES

- [1] K. Malasri and L. Wang, "Addressing Security in Medical Sensor Networks", In *Proceedings of ACM SIGMOBILE International Workshop on Systems and Networking Support for Healthcare and Assisted Living Environments (HealthNet'07)*, San Juan, Puerto Rico, USA, pp 7-12.
- [2] V. Shnayder, B. Chen, K. Lorincz, R. F. Thaddeus, J. Fulford and M. Welsh, "Sensor Networks for Medical Care", Technical Report TR-08-05, Division of Engineering and Applied Sciences, Harvard University, 2005.
- [3] D. Malan, T. Fulford-Jones, M. Welsh and S. Moulton, "Codeblue: An Ad hoc Sensor Network Infrastructure for Emergency Medical Care". In *Proceedings of MobiSys 2004 Workshop on Applications of Mobile Embedded Systems (WAMES 2004)* June 2004.
- [4] L. Eschenauer and V. D. Gligor "A Key Management Scheme for Distributed Sensor Networks", In *Proceedings of ACM Conference on Computer and Communications Security*, pp 41-47, November 2002.
- [5] D. Liu and P. Ning, "Establishing Pair-wise Keys in Distributed Sensor Networks", In *ACM Conference on Computer and Communications Security*, October 2003 pp 52-61.
- [6] W. Du, J. Deng, Y. S. Han and P. K. Varshney, "A Pair-wise Key Pre-Distribution Scheme for Wireless Sensor Networks", In *ACM Conference on Computer and Communications Security*, October 2003, pp 42-51.
- [7] H. Chan, A. Perrig, and D. Song. "Random Key Pre-distribution Schemes for Sensor Networks". In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2003, pp 197-213.
- [8] S. Zhu, S. Xu, S. Setia, and S. Jajodia. "Establishing Pair-wise Keys for Secure Communication in Ad hoc Networks: A Probabilistic Approach". In *Proceedings of the IEEE International Conference on Network Protocols (ICNP)*, November 2003, pp 326-335.
- [9] L. B. Oliveira, D. Aranha, E. Morais, F. Daguano, J. Lopez and R. Dahab, "TinyTate: Identity-Based Encryption for Sensor Networks", *Cryptology ePrint Archive*, vol. 2007/020, 2007.
- [10] H. A. Nahas and J. S. Deogun, "Radio Frequency Identification Applications in Smart Hospitals", In *Proceedings of IEEE International Symposium on Computer-Based Medical Hospitals 2007*. pp 337-342.
- [11] C. C. Tan, H. Wang, S. Zhong and Q. Li, "Body Sensor Network Security: An Identity-Based Cryptography Approach", In *Proceedings of ACM Conference on Wireless Security 2008*. pp 148-153.
- [12] G. Simon, P. Volgyesi, M. Maroti, and A. Ledeczi. "Simulation-based Optimization of Communication Protocols for Large-scale Wireless Sensor Networks", In *Proceedings of IEEE Aerospace Conference*, Big Sky, MT, March 2003. pp 1339-1346.
- [13] P. Miller, "Crypt: PBC Perl module", [Online] Available: <http://search.cpan.org/~jettero/Crypt-PBC/>
- [14] D. Boneh and M. Franklin, "Identity based Encryption from the Weil Pairing". In *Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology*, 2001, pp 213-229.
- [15] B. Doyle, S. Bell, A. F. Smeaton, K. McCusker and N. O' Connor, "Security Considerations and Key Negotiation Techniques in Power Constrained Sensor Networks", *The Computer Journal* (Oxford University Press), 49(4): 443-453, 2006.
- [16] L. I. W. Pesonen, D. M. Eysers and J. Bacon, "Access Control in Decentralized Publish/Subscribe Systems", *Journal of Networks*, Vol. 2, No.2, April 2007.
- [17] J. Bacon, D. Eysers, K. Moodys and L. Pesonen, "Securing Publish/Subscribe for Multi-domain Systems", *Lecture Notes in Computer Science*, Volume 3790, Springer Berlin/Heidelberg, 2005, pp 1-20.
- [18] M. Srivatsa and L. Liu. "Secure Event Dissemination in Publish-Subscribe Networks", In *Proceedings of International Conference on Distributed Computing Systems (ICDCS'07)*, Washington, DC, USA, June 2007, pp 22
- [19] L. Fiege, A. Zeidler, A. Buchmann, R. Kilian-Kehr and G. Muhl, "Security Aspects in Publish-Subscribe Systems" In *Third International Workshop on Distributed Event-based Systems (DEBS'04)*, Edinburgh, Scotland, UK, May 2004.
- [20] C. Blundo, A. De Santis, A. Herzberg, S. Kuttan, U. Vaccaro and M. Yung, "Perfectly- Secure Key Distribution for Dynamic Conferences". In *Proceedings of Annual International Cryptology Conference on Advances in Cryptology*, 1993, pp 471-486.
- [21] Multiprecision Integer and Rational Arithmetic C/C++ Library (MIRACL). [Online] Available: <http://www.shamus.ie/>
- [22] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Networks", In *Proceedings of IEEE International Conference on Pervasive Computing and Communications*, 2005, pp 324-328.
- [23] J. P. Kaps, "Cryptography for Ultra-Power Devices", Ph.D Dissertation, Department of Electrical Engineering, Worcester Polytechnic Institute, Worcester, MA, 2006.
- [24] H. Cam, S. Ozdemir, P. Nair, D. Muthuaviniashiappan and H. Ozgur Sanli, "Energy Efficient Secure Pattern based Data Aggregation". In *IEEE Computer Communications*, 29:446-455, 2006.
- [25] N. R. Potlapally, S. Ravi, A. Raghunathan and N. K. Jha, "Analyzing the Energy Consumption of Security Protocols", In *Proceedings of International Symposium on Low Power Electronics and Design (ISLPED '03)*, 2003, pp 30-35.
- [26] E. Barker, W. Barker, W. Burr, W. Polk and M. Smid. Recommendation for Key Management Part 1: General. NIST Special Publication 800-57, March 2007, National Institute of Standards and Technology.
- [27] J. Hill and D. Culler, "Mica: A Wireless Platform for Deeply Embedded Networks". *IEEE Micro*, 22(6): 12-24, November/December 2002.
- [28] J. K. O'Herrin, N. Foster and K. A. Kudsk, Health Insurance Portability Accountability Act (HIPAA) regulations: Effect on Medical Record Research, *Annals of Surgery* 239, pp 772-776, 2004.
- [29] J. Polastre, J. Hill and D. Culler, "Versatile Low Power Media Access for Wireless Sensor Networks", In *Proceedings of ACM Embedded Networked Sensor Systems (SenSys'04)*, Baltimore, Maryland, USA, November 2004. pp 95-107.

Keynote: Reflections on Emerging Cyber Threats and International Cooperative Responses

Raphael Perl, Head

Action Against Terrorism Unit, Organization for Security and Co-operation in Europe (OSCE)

GROWING dependence on information and communication technology has made a secure cyberspace absolutely essential for the functioning of modern countries and the world economy. The Internet has also become a key instrument for terrorists and other criminals and is used for a variety of purposes such as fraud; child sexual exploitation; identity and data theft; identifying, recruiting and training new members of a terrorist group; collecting and transferring funds; organizing terrorist acts; and inciting terrorist violence. Experts are alarmed by the continuous growth and annual cost of dealing with cybercrime and by the potential threat of the use of computer systems and the Internet as weapons for cyber-attacks by terrorists. International and regional organizations such as the Organization for Security and Co-operation in Europe (OSCE) have a key role in combating this threat. Building on previous OSCE efforts, notably in the area of combating the use of the Internet for terrorist purposes, the Organization has started to explore a possible role in promoting a comprehensive approach to enhancing cyber security. Such a comprehensive approach to enhancing cyber security, involving and utilizing the strengths of all stakeholders from the public as well as the private sector, may be the best viable option for national authorities and the international community in order to ensure long-term and sustainable cyber security. Drawing on the aforementioned issues, this address will explore the potential role for regional organizations and specifically the OSCE in promoting such a comprehensive approach and will provide concrete policy options for decision makers.

On Optimal AV System Strategies against Obfuscated Malware

Anshuman Singh*, Bin Mai†, Arun Lakhotia* and Andrew Walenstein*

*University of Louisiana at Lafayette, LA, USA

†Northwestern State University, Natchitoches, LA, USA

Abstract—Many Anti-Virus(AV) Systems are heterogeneous compositions of components, with each component specially tuned to work on a certain class of threat. Each component may have individually tunable parameters and different performance characteristics. No general theory is known for composing such components and assigning their individual parameters in order to ensure optimal resistance to attack. A particularly important question is posed by the possibility of obfuscated malware, which may fool the system into using different components. This paper introduces a framework for modeling composite AV Systems as classifiers wired together using selectors. It then uses game theory to analyze possible attacks. According to the game analysis, using a selector is beneficial only when the cost of developing obfuscated malware to game it is above a certain threshold. In this paper, we then *derive* the optimal configuration of detection components of an AV System such that the attacker’s use of obfuscation is rendered ineffective.

I. INTRODUCTION

MANY computer defense systems rely on multiple components that are composed into a single system that, in combination, is used to defend against attacks. For example, a mail server may pass incoming mail to multiple Anti-Virus(AV) products from different vendors before letting the mail through. And, at a finer level of granularity, a single AV product may also be composed of several discernible detector components. For example, a single product may include a component for matching cryptographic checksums, for ordinary signatures, for so-called "x-ray" scanning, for static behavior-based patterns, an emulation-based behavior matcher, and a run-time behavior matcher based on monitoring hooked system calls [1].

There are several important rationales for constructing heterogeneous AV Systems. First, it often is simply good software engineering practice to decompose large systems into smaller, well-defined components. Second, it may be the case that certain detector components are applicable to only certain inputs. For example, an AV system’s static behavior pattern matcher may be known to work well on only specific types of malicious files. Third, there may be important performance reasons for dividing the work up between components; in particular, certain components may incur much higher computational cost than others, so it is important to ensure that they are used in those situations in which they are most likely needed, and not on all files in general. Whatever the reasons for using multiple components, they must be wired together in a way that they work in coordination to perform the detection.

An essential piece is the logic used to select the inputs that the various components will work on, so that the computational costs are kept low and the components are used only on the appropriate inputs. Another issue to consider is the settings of tunable parameters for the components.

A critical concern is whether the system, as a whole, is made more resilient to attack by virtue of its combination of components and connection logic. A specific problem is caused by the possibility of using various anti-AV techniques, such as obfuscation, to game the selection of different classifiers. In particular, obfuscation may be used to fool a single detection component into making the wrong decision but, with selection logic added to the system, new obfuscation attacks are made possible directly on the selection logic. Thus new questions arise as to whether the compositions are more resistant than the individual components, and how to assign any detector parameters that are tunable. No generic framework or analysis method is known for answering such questions.

This paper proposes a modeling framework and analysis technique that can help begin answering such critical questions. The framework for modeling heterogeneous AV Systems treats them as a combination of classifiers connected together using probabilistic selectors. From such models, defense construction (AV Software setup) and attacks on them are treated as a game. For example, the virus-antivirus coevolution described by [2] can be modeled as a game in this framework. A game theoretic analysis can then be performed that can expose potential attack weaknesses. By setting up a game using variables in the models instead of actual constants, an abstract game model can be constructed. Though game theory has been applied in computer science in semantics of programming languages and logic systems(game semantics) [3], adversarial classification in KDD systems [4], and artificial intelligence [5], we apply it in a malware-anti-virus scenario and derive formally some interesting relationships among the parameters of the game.

Using a sample play of a game with a two-component AV System, the paper shows that interesting general characteristics of composite AV Systems can be extracted. Specifically, it characterizes the conditions in which the AV System as a whole is made weaker by the addition of a selector and specific classifier. More specifically, we found that, first, within our model setting, augmenting detection with a selector would not always benefit the AV System. The selector’s value can be fully realized only when the cost of obfuscating malware is above

a certain threshold; secondly, the AV System is always better off by configuring its classifiers so as to render the use of obfuscation in malware ineffective, and this can be achieved by decreasing the detection rate of the classifier designed for malware and increasing the detection rate of the classifier designed for the normal files. This implies that when cost of developing obfuscated malware is low and selection accuracy is high, the difference in detection rates of the classifiers should be low for optimal performance of the AV System.

The rest of the paper is organized as following: we give an overview of the basic concepts from game theory in Section 2. We then describe, in section 3, the design decisions used in modeling AV Systems. In section 4 we set up the Malware Author-AV System game and describe each play of the game as a configuration followed by payoff decision trees for each player. In section 5 we compute expected payoffs for the players and derive relationships between tunable parameters of the AV System and malware development cost. In Section 6, we discuss the implication of our results and conclude the paper.

II. BACKGROUND

Game theory, a branch of applied mathematics, is useful for making decisions in situations where two or more rational decision makers have conflicting interests. Applications of game theory attempt to find equilibria in these games-the combination of the strategies for each agent in which none of the agents have incentive to change their strategy. This is an analytical tool that is especially valuable in analyzing situations where there are strategic interactions among multiple agents and each agent's behavior and consequences are intricately related to each other's.

A game is a situation of strategic interdependence that consists of a set of players, a set of strategies available to those players, and a specification of payoffs for each combination of strategies. The extensive and the normal forms are used to define noncooperative games-games in which the goal of each player is to achieve largest possible individual gain. A normal-form representation of a game is a specification of players' strategy spaces and payoff functions that is graphically represented as a 2-d matrix for a two player game. A *strategy space* for a player is the set of all strategies available to that player, where a strategy is a complete plan of action for every stage of the game, regardless of whether that stage actually arises in play. A *payoff function* for a player is a mapping from the cross-product of players' strategy spaces to that player's set of payoffs. These payoffs are the sum of benefits and costs to the player obtained by choosing a strategy. The reader can refer [6] for a thorough introduction to game theory.

III. MODELING HETEROGENEOUS AV SYSTEMS

A simple AV System with a single detection component can be thought of, abstractly, as a classifier that classifies its inputs into one of possibly several categories. In this case, the inputs are potentially malicious programs, and the output classes might be, for example, clean, suspicious, and dirty. Classifiers such as these may be connected together in parallel so that

for any given input all classifiers are run, and the outputs are combined in some manner. An example is shown in Figure 1(a). In such configurations, well-understood analysis methods such as boosting can be found in the classifier literature [7].

For composite AV Systems such configurations are not desirable since not only is it too costly to run all classifiers on all inputs, it is frequently the case that certain classifiers are specialized to work only on certain subsets of the input space. The composite AV Systems can be modeled as a combination of classifiers connected together using probabilistic selectors (Figure 1(b)). The selector performs some form of lightweight scanning based on which it subjects the input to a specialized classifier. For example, most second generation AV scanners use as a selector a nearly exact identification method using cryptographic checksums ([1], p.437-8) and then based on selector's decision subject the suspected file to a particular algorithmic scanning method ([1], p.441) that can be considered as a specialized classifier.

As another example, consider the case of a normalizing detector for metamorphic malware similar to the one defined in [8]. Although the algorithm used is more efficient than semantics-based static normalization approaches, the normalization is likely most helpful only for a small number of files, so for performance reasons the normalizer is likely to be combined with a selector component that can quickly filter out the files that are highly unlikely to need the normalization. A fast statistical selector [9] might be used in combination with the normalizer. It selects whether the incoming file is likely to be metamorphic and in need of going through the normalization process described in [8]. In this way, the majority of files need not be scrutinized by the more heavyweight normalizer. This is a classic instance of a specialized classifier approach.

IV. THE MALWARE AUTHOR-SECURITY ANALYST GAME

Malware authors always try to develop malware that evades detection by an AV System and the Security analyst will always try to come up with a design and configuration of an AV System that improves the detection rate. This situation can be modeled as a game. The players involved in this game are malware author (MA) and security analyst (SA). The strategies for MA are either to develop a low cost unobfuscated malware (UM) or the more expensive obfuscated or metamorphic malware (OM). The strategies for SA are either to use a single classifier (C architecture) or two classifiers with a selector (S2C architecture) for the AV System as discussed in Section III. We assume the strategies are pure for each player, though a game with mixed strategies can also be modeled similarly. The game can be described in normal form as in Figure 2. MA's strategies are given in rows and SA's in columns. Each play of the game is called a configuration and there are four such configurations: UM-C (UMC), OM-C (OMC), UM-S2C (UMS2C) and OM-S2C (OMS2C). The payoffs for each player are given in the pair for the corresponding play of the game where each player has chosen one of the strategies. The first element of the pair is the expected payoff for the Malware Author and the second element is the expected payoff for the Security Analyst. The components of the AV System

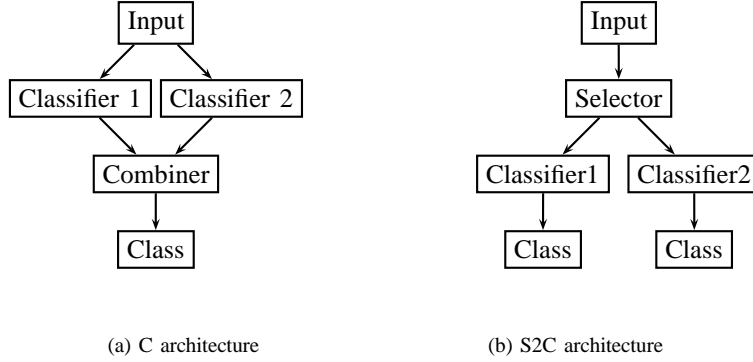


Fig. 1: Methods of composing multiple classifiers in an AV System

| | C | S2C |
|----|------------------------------------|--|
| UM | $(\pi_{UMC}^{MA}, \pi_{UMC}^{SA})$ | $(\pi_{UMS2C}^{MA}, \pi_{UMS2C}^{SA})$ |
| OM | $(\pi_{OMC}^{MA}, \pi_{OMC}^{SA})$ | $(\pi_{OMS2C}^{MA}, \pi_{OMS2C}^{SA})$ |

Fig. 2: The MA-SA game in normal form

make classification and selection decisions based on which the payoffs can be computed for each player for each decision path. The costs and benefits to players for various outcomes and the parameters of the AV system components are described below.

When normal files are sent to the AV System, SA derives a positive utility of ν . We assume that if AV System successfully detects the malware, she completely avoids any loss and MA gets μ_l payoff ($\mu_l > 0$ such that SA always has incentive to try to block an attack). If AV System fails to detect the malware, SA incurs a damage of d and MA obtains a payoff of μ_h ($\mu_h > \mu_l$). Once the AV System detects malware, regardless whether it is true positive or false positive, we assume SA would incur a cost of c for taking appropriate steps to protect itself. When MA notices that SA decides to configure the AV System such that it uses a Selector for pre-screening to choose between a lenient and stringent classifier, MA may attempt to develop obfuscated malware to make the Selector send its file to the lenient classifier. MA incurs an additional cost of Δ , to develop obfuscated malware. The benefits and costs are summarized in Table I.

| Input | Outcome | Benefits | | Costs | |
|------------------------|----------|----------|---------|-------|----------|
| | | SA | MA | SA | MA |
| Normal | Detected | ν | | c | |
| | Missed | ν | | | |
| Malware (unobfuscated) | Detected | | μ_l | c | |
| | Missed | | μ_h | d | |
| Malware (obfuscated) | Detected | | μ_l | c | Δ |
| | Missed | | μ_h | d | Δ |

TABLE I: Costs and benefits obtained by each agent for all possible outcomes

In the single classifier architecture (C) of the AV System,

let p_D denote the detection rate (true positive rate) of the classifier, i.e. the probability that classifier correctly detects MA's malware. Since the classifier can also give false positives when scanning through clean files, we denote the false positive rate by p_F . A classifier can be configured to operate at a specific combination of (p_D, p_F) values on its Receiver Operating Characteristics (ROC) curve, which specifies the permissible combinations for the device [10]. An ROC curve represents p_D as an increasing concave function of p_F . We assume that the ROC curve is given by the power function $p_D = p_F^r$, with $0 < r < 1$.

In S2C architecture of the AV System, for the selector (S) the probability of selecting a normal input file as normal is t_N and the probability of selecting input that is malware as malware is t_M . The file selected as normal is directed to the lenient classifier (LC) and the file selected as malware is directed to the stringent classifier (SC). The true positive rate and the false positive rate of the stringent classifier (SC) is p_D^S and p_F^S respectively. Similarly, the true positive rate and the false positive rate of the lenient classifier (LC) is p_D^L and p_F^L respectively.

Figures 3, 4, 5, 7, 6, 8 give the decision trees for each player for all the configurations of the game. Figure 4 gives the decision trees for SA for both UMC and OMC configuration since the payoffs remain the same. The outcomes 'Detected' and 'Missed' are represented by '+' and '-', respectively, in these figures.

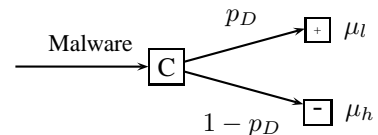


Fig. 3: MA's payoff in configuration UMC

V. AV SYSTEM OPTIMAL PARAMETERS

We now analyze the different game configurations by computing expected payoffs for the players. Maximizing the expected payoffs under certain conditions can help tuning the AV System parameters for optimal detection rates. This kind

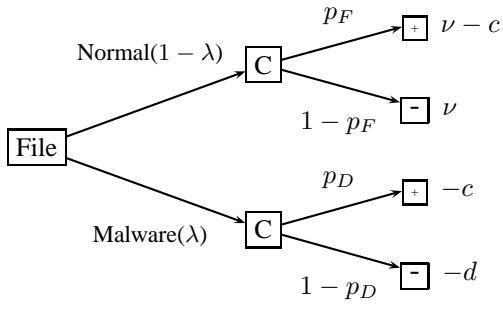


Fig. 4: SA's payoff in configuration UMC (OMC)

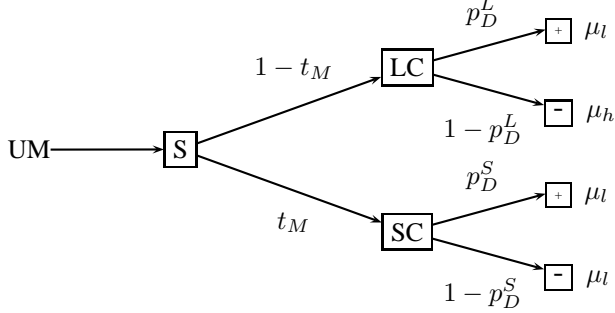


Fig. 5: MA's payoff in configuration UMS2C

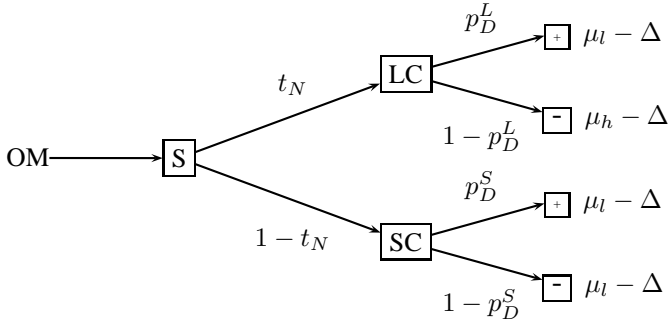


Fig. 6: MA's payoff in configuration OMS2C

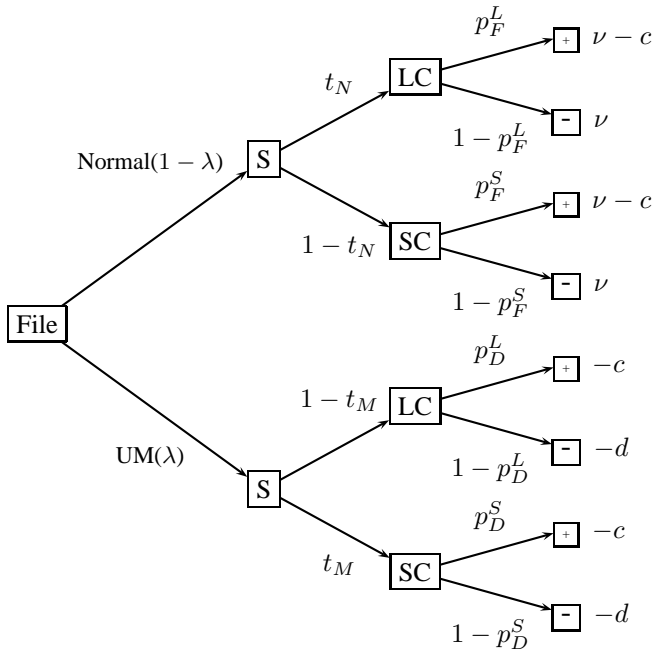


Fig. 7: SA's payoff in configuration UMS2C

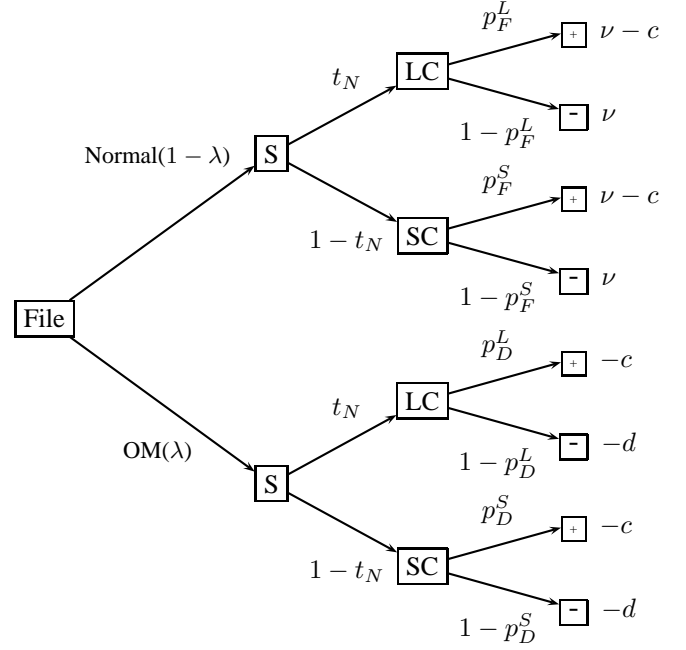


Fig. 8: SA's payoff in configuration OMS2C

of analysis helps in deriving interesting relationships between various parameters in the game. These relationships are based on formal and rigorous analysis instead of ad hoc heuristics. The variables used in decision trees and the expressions below are defined and explained in section IV and summarized in Table I.

A. The UMC Configuration

In this configuration SA chooses to use only one classifier and does not pre-screen incoming files, thus every file is sent through the same classifier device. When the input file is normal and the classifier C incorrectly classifies it as a malware, the SA will get benefit ν for using the classifier and incur a cost c for incorrect classification of the input (see Table I). Thus, the payoff to SA will be $\nu - c$ (see Figure 4). As the probability of an input file being clean or normal is $1 - \lambda$ and the false positive rate of the classifier C is p_F , the weighted payoff to SA is $(1 - \lambda)p_F(\nu - c)$. The expected payoff for SA can be obtained by adding the weighted payoffs for all other paths in the decision tree. The expected payoff for SA in UMC configuration is:

$$\begin{aligned} \pi_{UMC}^{SA} &= (1 - \lambda)p_F(\nu - c) + (1 - \lambda)(1 - p_F)\nu + \\ &\quad \lambda p_D(-c) + \lambda(1 - p_D)\nu \\ &= \nu - (d + \nu)\lambda - c(1 - \lambda)p_F + (d - c)\lambda p_D \end{aligned}$$

SA can configure p_D to its optimal value by maximizing expected payoff for SA:

$$\frac{d(\pi_{UMC}^{SA})}{dp_D} = 0 \quad (1)$$

Solving (1) using $p_D = p_F^r$ yields \bar{p}_D , the optimal value of p_D :

$$\bar{p}_D = \left[\frac{c}{d - c} \cdot \frac{1 - \lambda}{\lambda} \cdot \frac{1}{r} \right]^{\frac{r}{r-1}} \quad (2)$$

If $\alpha = (1 - \lambda)/\lambda$ is the ratio of normal files to malware, $\delta = d/c$ is the damage to cost ratio and $\xi = \alpha/(\delta - 1)$, then (2) can also be written as:

$$\bar{p}_D = \left[\frac{\xi}{r} \right]^{\frac{r}{r-1}}$$

B. The UMS2C and OMS2C configuration

In OMS2C configuration, the expected payoff for MA can be computed from Figure 6 as:

$$\begin{aligned} \pi_{OMS2C}^{MA} &= (1 - t_N)\{p_D^S(\mu_l - \Delta) + (1 - p_D^S)(\mu_h - \Delta)\} + \\ &\quad t_N\{p_D^L(\mu_l - \Delta) + (1 - p_D^L)(\mu_h - \Delta)\} \\ &= t_N(\mu_h - \mu_l)(p_D^S - p_D^L) + p_D^S(\mu_l - \mu_h) + \mu_h - \Delta \end{aligned}$$

If $\pi_{OMS2C}^{MA} \leq 0$, MA will choose strategy UM. This occurs when

$$t_N(\mu_h - \mu_l)(p_D^S - p_D^L) + p_D^S(\mu_l - \mu_h) + \mu_h - \Delta \leq 0$$

and since $\mu_l - \mu_h < 0$

$$\Delta \geq t_N(\mu_h - \mu_l)(p_D^S - p_D^L) + \mu_h \quad (3)$$

If condition (3) holds, then optimal values of p_D^S and p_D^L can be obtained by maximizing the expected payoff for SA in UMS2C configuration. The expected payoff for SA in UMS2C configuration can be computed from Figure 7 as:

$$\begin{aligned} \pi_{UMS2C}^{SA} &= (1 - \lambda)t_N\{p_F^L(\nu - c) + (1 - p_F^L)\nu\} + \\ &\quad (1 - \lambda)(1 - t_N)\{p_F^S(\nu - c) + (1 - p_F^S)\nu\} + \\ &\quad \lambda(1 - t_M)\{(p_D^L(-c) + (1 - p_D^L)(-d))\} + \\ &\quad \lambda t_M\{p_D^S(-c) + (1 - p_D^S)(-d)\} \end{aligned}$$

Maximizing the above expression w.r.t. p_F^S , we obtain:

$$\bar{p}_F^S = \left[\frac{c(1 - \lambda)(1 - t_N)}{(d - c)\lambda r t_M} \right]^{\frac{1}{r-1}}$$

It follows that:

$$\bar{p}_D^S = \left[\frac{c}{d - c} \cdot \frac{1 - \lambda}{\lambda} \cdot \frac{1 - t_N}{t_M} \cdot \frac{1}{r} \right]^{\frac{r}{r-1}} \quad (4)$$

Similarly

$$\bar{p}_D^L = \left[\frac{c}{d - c} \cdot \frac{1 - \lambda}{\lambda} \cdot \frac{t_N}{1 - t_M} \cdot \frac{1}{r} \right]^{\frac{r}{r-1}} \quad (5)$$

Using notation from section V-A, (4) and (5) can be written as

$$\bar{p}_D^S = \left[\frac{\xi}{r} \cdot \frac{1 - t_N}{t_M} \right]^{\frac{r}{r-1}}$$

and

$$\bar{p}_D^L = \left[\frac{\xi}{r} \cdot \frac{t_N}{1 - t_M} \right]^{\frac{r}{r-1}}$$

If

$$\Delta < t_N(\mu_h - \mu_l)[\bar{p}_D^S - \bar{p}_D^L] + \mu_h$$

MA will choose the OM strategy but SA can render MA's use of obfuscation ineffective if the optimal values of p_D^S and p_D^L satisfy

$$p_D^S - p_D^L = \frac{\Delta}{t_N(\mu_h - \mu_l)} \quad (6)$$

and

$$(1 - t_N)(p_D^S)^{\frac{1-r}{r}} + t_N(p_D^L)^{\frac{1-r}{r}} = \frac{r\lambda(d - c)}{(1 - \lambda)c} \quad (7)$$

Condition (6) is condition (3) in equilibrium. (7) can be obtained by replacing p_D^S and p_D^L from (4) and (5), respectively, in the left hand side and simplifying.

From (3) (4), (5), (6) and (7) we obtain the following propositions.

Proposition 1: For a given cost of obfuscation (fixed Δ), $p_D^S - p_D^L$ is increasing in t_M and t_N if

$$\Delta \geq t_N(\mu_h - \mu_l)[\bar{p}_D^S - \bar{p}_D^L] + \mu_h$$

and is decreasing in t_M and t_N otherwise.

If developing obfuscated malware is relatively costly (high Δ), MA would not choose to develop obfuscated malware, and hence, as the selector's accuracy improves, SA designs more lenient classifier for those files selected as normal and a more stringent classifier for those files selected as malware. Thus, as conventional wisdom would suggest, the differentiation between the detection rates for the two types of files increases when selector becomes better at discriminating the two types. However, if the cost of obfuscation is sufficiently low, MA would use obfuscation to beat the selector. But SA can render MA's use of obfuscation ineffective by making the classifier for files selected as malware less stringent and the classifier for files selected as normal more stringent with an increase in selector's accuracy.

Proposition 2: For a given selection accuracy (i.e., fixed t_M and t_N), $p_D^S - p_D^L$ is increasing in the cost of obfuscation as long as

$$\Delta < t_N(\mu_h - \mu_l)[\bar{p}_D^S - \bar{p}_D^L] + \mu_h$$

and is constant otherwise.

When, for example, the detection rate of both classifiers is same, i.e., their difference is 0, MA will not invest on obfuscation as gaming the selector is of no use. On the other hand, when the detection rate of one classifier is 1 and the other is 0, i.e., the difference is maximum, MA will try her best to game the selector by putting more effort for obfuscation such that malware is directed to the classifier with the detection rate 0. Of course, this configuration may not give optimal expected payoff for SA due to increased false positives.

Proposition 3: For a given detection rate of the classifiers (fixed $p_D^S - p_D^L$), the cost of obfuscation required to render MA's use of obfuscation ineffective, increases with the selector's accuracy.

This proposition implies that with the increase of selector's accuracy, MA has more incentive to develop obfuscated malware. Therefore, to fully realize the benefits of having a selector to pre-screen incoming files, it should be costly enough for MA to develop obfuscated malware.

VI. CONCLUSION

In this paper, we construct a stylized game theoretic model to analyze the optimal configuration of a heterogeneous AV System with a selector component that pre-screens incoming files. Our model incorporates one crucial aspect of the game:

the strategic behaviour of malware authors who would invest to develop obfuscation techniques trying to beat the selector component of the AV System. Based on the analysis of our model, we obtain the following implications for the design and configuration of the classifiers.

When the cost of obfuscation for a malware author is sufficiently low, the difference between the optimal detection rates configured for the two classifiers will be decreasing in the selector's accuracy. This implies that when the selector's accuracy increases, it is optimal for a security analyst to maintain a less stringent classifier for malware and a more stringent classifier for normal files. Thus, SA can render MA's use of obfuscation ineffective by decreasing the difference of the detection rates of the two classifiers. Also, it was shown that the minimal cost for developing obfuscated malware sufficient to game the selector increases with the accuracy of the selector. Therefore, the cost of obfuscation should be considered an important factor, in addition to the discriminatory power of detection, when designing an AV System.

REFERENCES

- [1] P. Szor, *The Art of Computer Virus Research and Defense*. Addison-Wesley, 2005.
- [2] C. Nachenberg, "Computer virus-antivirus coevolution," *Communications of the ACM*, vol. 40, no. 1, pp. 46–51, January 1997.
- [3] S. Abramsky and R. Jagadeesan, "Games and full completeness for multiplicative linear logic," *Journal of Symbolic Logic*, vol. 59, pp. 543–574, 1994.
- [4] N. Dalvi, P. Domingos, Mausam, S. Sangha, and D. Verma, "Adversarial classification," in *KDD '04: Proceedings of the tenth ACM SIGKDD international conference on Knowledge discovery and data mining*, 2004, pp. 99–108.
- [5] A. Jafari, A. R. Greenwald, D. Gondek, and G. Ercal, "On no-regret learning, fictitious play, and nash equilibrium," in *ICML '01: Proceedings of the Eighteenth International Conference on Machine Learning*, 2001, pp. 226–233.
- [6] M. J. Osborne and A. Rubinstein, *A Course in Game Theory*. MIT Press, 1994.
- [7] J. Han and M. Kamber, *Data Mining: Concepts and Techniques*. Morgan Kaufmann, 2006.
- [8] A. Walenstein, R. Mathur, M. R. Chouchane, and A. Lakhota, "Normalizing metamorphic malware using term rewriting," in *Proceedings of the Sixth IEEE International Workshop on Source Code Analysis and Manipulation (SCAM 2006)*, 2006, pp. 75–84.
- [9] M. R. Chouchane, A. Walenstein, and A. Lakhota, "Statistical signatures for fast filtering of instruction-substituting metamorphic malware," in *Proceedings of the 2007 ACM Workshop on Recurring Malcode (WORM 2007)*, 2007, pp. 31–37.
- [10] J. P. Egan, *Signal Detection Theory and ROC Analysis*. Academic Press, 1975.

A Brief Letter on Reasoning about Information Assurance using the Semantic Web

Stephen F Bush

GE Global Research

URL: <http://www.research.ge.com/~bushsf>

Abstract—This is a brief letter outlining speculative ideas for semantic web reasoning about information assurance. Much work has been done on the development of semantic web applications for reasoning about information assurance. A significant portion of this work is focused upon semantic web ontologies and reasoning about security policies and the underlying implementation of those policies. While numerous semantic web-based security policy ontologies and reasoners exist, both academically and commercially, I will briefly focus on ideas related to solutions to the problem of managing semantic web rules using algorithmic information theory.

I. INTRODUCTION

Complexity and Algorithmic Information Theory (AIT) have been explored as a means of fundamentally characterizing information assurance [1], [2], [3], [4]. AIT can also be applied to semantic web reasoning engines as we will describe in this paper.

The goal of the semantic web is to make the information that one typically finds in web pages today understandable by machines. Once enough organizations and people adopt a common “semantic” framework, such as that specified by the W3C, one can expect a phase transition (or sudden jump due to the degree of connectivity of ontologies and rules) in the amount of reasoning capability on the web.

Semantic web reasoning capability has been harnessed by researchers in academia and industry who are attempting to understand and reason about information assurance. The number researchers who have built semantic web reasoning for security and policy using ontologies and reasoning systems is too numerous to list exhaustively, however we note a few here [5], [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27], [28].

II. THE SEMANTIC WEB

The Semantic Web Rule Language (SWRL) would appear to be the standard framework for rules on the semantic web. This will be the framework within which we must reason about security and policies. There is much that we can learn from expert systems that were studied decades ago. I suggest that there is a strong relationship between information theory, namely source coding, and the design of the expert system rule-base.

Before going into this relationship, it should be mentioned that information assurance is a hard problem because a precise definition of information is still lacking [29]. However, for

the purposes of this short letter, I follow the line of reasoning originating from Kolmogorov and Chaitin [30] through Minimum Description Length (MDL) [31] regarding the nature of information and complexity.

The purpose of an expert system rule-base is to “reason” about something, in our particular case, to reason about information assurance and the policies that, along with the underlying device configuration and security technologies, provide assurance. I assume a law of conservation for information, namely, that information cannot be created or destroyed. Thus, the “amount” of information that is ingested by an expert system must equal the “amount” that either comes out in the form of a result, or is simply ignored. Typically, a human wants the most simple and concise result possible; thus, relevant information has been compressed and irrelevant information has been ignored. Lossy coding theory attempts to compress information to its smallest size while allowing the loss of irrelevant information; rate distortion theory attempts to understand the amount of compression versus the amount of lost information.

III. INFORMATION THEORY AND SEMANTIC WEB RULES FOR INFORMATION ASSURANCE

Indeed, information theory has been applied to automatically infer new rules in an expert system [32], [33]. However, with the re-emergence of rule-based systems for the semantic web and the opportunities to merge ontologies and rule-bases, one can foresee the need to manage and align large rule-bases. As source coding removes redundancy in information compression, [34] provides a procedure for discovering and removing redundant logic in SWRL. [35] examines metrics for the complexity of an expert system. Thus, as one constructs a rule-base, for each new rule that is added, does the increase in complexity of the rule-base due to the newly added rule yield a corresponding gain in performance? What new rules are best to add? How should they best be positioned relative to existing rules?

If one has *a priori* knowledge of the “typical” input to the expert system and the desired result for each input, one can determine the probabilities that rules will fire and utilize this knowledge to optimize the rule-base, using an analogy with rate-distortion.

In addition, one would expect the complexity of the rule-base to “mirror” the complexity of the system being modeled. If the rule-base is less complex than the system being modeled,

then one might expect that the rule-base has not captured enough information to adequately describe it. If the expert system is too complex, then it may over-fit the actual system. Thus, complexity measures such as MDL plays a role in determining when the expert system has “enough” rules in the right combination.

Finally, alignment of ontologies and rules are necessary to cause the phase transition on the semantic web mentioned earlier in this letter. Finding the point of minimum complexity may be an aid to finding the optimal alignment of both the ontology and the rules.

IV. CONCLUSION

In this short letter, we have looked at the well established role of information assurance and policy reasoning via the semantic web. In particular, we focused on semantic web rule maintenance from the point of view of algorithmic information theory and the relationship between compression and rule-base construction.

REFERENCES

- [1] S. F. Bush and T. Hughes, “On the effectiveness of kolmogorov complexity estimation to discriminate semantic types,” in *Proceedings of the SFI Workshop on Resilient and Adaptive Defense of Computing Networks 2003*, Nov 2003, Santa Fe Institute, Santa Fe, NM. [Online]. Available: <http://www.research.ge.com/~bushsf>
- [2] S. F. Bush, “Extended abstract: Complexity and vulnerability analysis,” in *Complexity and Inference*, Jun 2003, DIMACS Center, Rutgers University, Piscataway, NJ. [Online]. Available: <http://www.research.ge.com/~bushsf>
- [3] S. Goel and S. F. Bush, “Kolmogorov complexity estimates for detection of viruses in biologically inspired security systems: A comparison with traditional approaches,” in *Invited Paper: SFI Workshop: Resilient and Adaptive Defense of Computing Networks 2003*. Santa Fe Institute, Santa Fe, NM, Nov 2003. [Online]. Available: <http://www.research.ge.com/~bushsf/pdfpapers/ImmunoComplexity.pdf>
- [4] S. F. Bush, “Extended abstract: Complexity and vulnerability analysis,” in *Invited Paper: SFI Workshop: Resilient and Adaptive Defense of Computing Networks 2003*, Complexity and Inference. DIMACS Center, Rutgers University, Piscataway, NJ, Jun 2003. [Online]. Available: <http://dimacs.rutgers.edu/Workshops/Inference/abstracts.html>
- [5] B. Shepard, C. Matuszek, C. B. Fraser, W. Wechtenhiser, D. Crabbe, Z. Güngördü, J. Jantos, T. Hughes, L. Lefkowitz, M. J. Witbrock, D. B. Lenat, and E. Larson, “A knowledge-based approach to network security: Applying cyc in the domain of network risk assessment,” in *AAAI, M. M. Veloso and S. Kambhampati, Eds. AAAI Press / The MIT Press*, 2005, pp. 1563–1568.
- [6] C. D. Almut Herzog, Nahid Shahmehri, “An ontology of information security,” *International Journal of Information Security and Privacy*, vol. 1, no. 4, pp. 1–23, 2007, <http://www.ida.liu.se/iislab/projects/secont/>. [Online]. Available: www.infosci-journals.com/downloadPDF/pdf/ITJ3908_HWARQa2D9b.pdf
- [7] C. Blanco, J. Lasheras, R. Valencia-Garcia, E. Fernandez-Medina, A. Toval, and M. Piattini, “A systematic review and comparison of security ontologies,” in *Proc. Third International Conference on Availability, Reliability and Security ARES 08*, 2008, pp. 813–820.
- [8] M. Chamoun, R. Kilany, and A. Serhrouchni, “Proposition of a network policy management ontology,” in *Proc. Fourth IEEE International Symposium on Signal Processing and Information Technology*, 2004, pp. 262–266.
- [9] S. Davy, B. Jennings, and J. Strassner, “Using an information model and associated ontology for selection of policies for conflict analysis,” in *2008 IEEE Workshop on Policies for Distributed Systems and Networks*, 2008. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04556583>
- [10] M. Donner, “Toward a security ontology,” *IEEE Security and Privacy*, vol. 1, no. 3, pp. 6–7, 2003. [Online]. Available: <http://csdl.computer.org/comp/mags/sp/2003/03/j3006.pdf>
- [11] A. Ekelhart, S. Fenz, M. Klemen, and E. Weippl, “Security ontologies: Improving quantitative risk analysis,” in *Proc. 40th Annual Hawaii International Conference on System Sciences HICSS 2007*, 2007, pp. 156a–156a.
- [12] S. Fenz, G. Goluch, A. Ekelhart, B. Riedl, and E. Weippl, “Information security fortification by ontological mapping of the iso/iec 27001 standard,” in *Proc. 13th Pacific Rim International Symposium on Dependable Computing PRDC 2007*, 2007, pp. 381–388.
- [13] S. Fenz and E. Weippl, “Ontology based it-security planning,” in *Proc. 12th Pacific Rim International Symposium on Dependable Computing PRDC '06*, 2006, pp. 389–390.
- [14] Z. Gao, L. Meng, X. Qiu, and X. Fu, “The interoperability and shared management information model,” in *Proc. First Asia International Conference on Modelling & Simulation AMS '07*, 2007, pp. 116–122.
- [15] D. Z. G. Garcia and M. Toledo, “A web service privacy framework based on a policy approach enhanced with ontologies,” in *Proc. 11th IEEE International Conference on Computational Science and Engineering Workshops CSEWORKSHOPS '08*, 2008, pp. 209–214.
- [16] G. Goluch, A. Ekelhart, S. Fenz, S. Jakoubi, S. Tjoa, and T. Muck, “Integration of an ontological information security concept in risk aware ; business process management,” in *Proc. 41st Annual Hawaii International Conference on System Sciences*, 2008, pp. 377–377.
- [17] M. Karyda, T. Balopoulos, S. Dritsas, L. Gymnopoulos, S. Kokolakis, C. Lambrinouidakis, and S. Gritzalis, “An ontology for secure e-government applications,” in *Proc. First International Conference on Availability, Reliability and Security ARES 2006*, 2006, pp. 5 pp.–.
- [18] F.-H. Liu, “Constructing enterprise information network security risk management mechanism by using ontology,” in *Proc. 21st International Conference on Advanced Information Networking and Applications Workshops AINAW '07*, vol. 1, 2007, pp. 929–934. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=4221177&isnumber=4221006>
- [19] M. Mao, Y. Peng, and M. Spring, “A profile propagation and information retrieval based ontology mapping approach,” in *Proc. Third International Conference on Semantics, Knowledge and Grid*, 2007, pp. 164–169.
- [20] S. Muthaiyah and L. Kerschberg, “Dynamic integration and semantic security policy ontology mapping for semantic web services (sws),” in *Proc. 1st International Conference on Digital Information Management*, 2007, pp. 116–120.
- [21] F. Naufel do Amaral, C. Bazilio, G. M. Hamazaki da Silva, A. Rademaker, and E. H. Haeusler, “An ontology-based approach to the formalization of information security policies,” in *EDOCW '06: Proceedings of the 10th IEEE on International Enterprise Distributed Object Computing Conference Workshops*. Washington, DC, USA: IEEE Computer Society, 2006, p. 1. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04031261>
- [22] G. M. H. da Silva, A. Rademaker, D. R. de Vasconcelos, F. N. Amaral, C. Bazilio, V. Costa, and E. H. Haeusler, “Dealing with the formal analysis of information security policies through ontologies : A case study,” in *Third Australasian Ontology Workshop (AOW 2007)*, ser. CRPIT, T. Meyer and A. C. Nayak, Eds., vol. 85. Gold Coast, Australia: ACS, 2007, pp. 55–60. [Online]. Available: <http://crpit.com/confpapers/CRPITV85daSilva.pdf>
- [23] B. Tsoumas and D. Gritzalis, “Towards an ontology-based security management,” in *Proc. 20th International Conference on Advanced Information Networking and Applications AINA 2006*, vol. 1, 2006, pp. 985–992.
- [24] A. Uszok, J. M. Bradshaw, J. Lott, M. Breedy, L. Bunch, P. Feltoovich, M. Johnson, and H. Jung, “New developments in ontology-based policy management: Increasing the practicality and comprehensiveness of kaos,” in *Proc. IEEE Workshop on Policies for Distributed Systems and Networks POLICY 2008*, 2008, pp. 145–152.
- [25] A. Vorobiev and J. Han, “Specifying dynamic security properties of web service based systems,” in *Proc. Second International Conference on Semantics, Knowledge and Grid SKG '06*, 2006, pp. 34–34.
- [26] P. Yan, Y. Zhao, and C. Sanxing, “Ontology-based information content security analysis,” in *Proc. Fifth International Conference on Fuzzy Systems and Knowledge Discovery FSKD '08*, vol. 5, 2008, pp. 479–483.
- [27] S. F. Yusufvna, “Advanced security policy implementation for information systems,” in *Proc. International Symposium on Ubiquitous Multimedia Computing UMC '08*, 2008, pp. 244–247.
- [28] Z. Zhou, Z. Lu, and J. Gu, “Towards an ontology-based content security scheme,” in *Proc. Fifth International Conference on Fuzzy Systems and Knowledge Discovery FSKD '08*, vol. 4, 2008, pp. 385–390.

- [29] S. F. Bush, "A philosophy of information assurance," in *1st Annual Symposium on Information Assurance (ASIA 06)*, 2006. [Online]. Available: http://www.research.ge.com/~bushsf/pdfpapers/Bush_KeyNote_Speech.pdf
- [30] G. J. Chaitin, "On the length of programs for computing finite binary sequences," *Journal of the ACM*, vol. 13, pp. 547–569, 1966.
- [31] A. Barron, J. Rissanen, and B. Yu, "The minimum description length principle in coding and modeling," *Information Theory, IEEE Transactions on*, vol. 44, no. 6, pp. 2743–2760, 1998. [Online]. Available: <http://dx.doi.org/10.1109/18.720554>
- [32] P. Smyth and R. M. Goodman, "An information theoretic approach to rule induction from databases," *IEEE Trans. Knowl. Data Eng.*, vol. 4, no. 4, pp. 301–316, 1992.
- [33] M. Muselli and D. Liberati, "Binary rule generation via hamming clustering," *IEEE Trans. Knowl. Data Eng.*, vol. 14, no. 6, pp. 1258–1268, 2002.
- [34] Y. Sun, J. Zhang, W. Zhao, and Y. Tian, "Managing and refining rule set for swrl," in *Proc. 4th International Conference on Wireless Communications, Networking and Mobile Computing WiCOM '08*, 2008, pp. 1–5.
- [35] Z. Chen and C. Y. Suen, "Complexity metrics for rule-based expert systems," in *Proc. International Conference on Software Maintenance*, 1994, pp. 382–391. [Online]. Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=336756&isnumber=7911>

Invited Talk: Social and Behavioral Approaches to Information Assurance

H.R. Rao

University at Buffalo, State University of New York

INFORMATION Assurance (IA) concerns operations that protect information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of systems by incorporating protection, detection, and reaction capabilities. Much of the information assurance literature is technical in nature. However, it is important that use of technology must be shaped by social policies and legal and ethical issues. This talk will focus on social and behavioral issues in Information Assurance and touch on topics such as risk, quality of information, prospect theory, social engineering, psychology of response and reaction. Real life caselets will be used to illustrate concepts.

Re-evaluating Single Sign-On System Design Risks: An Activity Theoretic Approach

Manish Gupta, Kranti Banala, and Raj Sharman
School of Management, State University of New York at Buffalo
Amherst, New York, USA, 14260

Abstract—Single Sign-On (SSO) systems provide users the convenience of accessing multiple applications and systems while having to provide credentials only once. Organizations across industries have started to evaluate and deploy Single Sign-On systems in their environment. SSO systems provide a range of benefits including improved productivity, reduced complexity, improved user convenience, facilitated business and improved compliance to security policies. While SSO systems have shown to provide many economic benefits, there are inherent risks that arise from the fact that in SSO environment, only one password or one set of authentication factor is needed. This creates a situation typically understood as ‘single-point of failure’. In an event the SSO password is breached, all of the applications covered under SSO will be exposed to huge risks. We use activity theory principles to understand how applications should be categorized to design SSO systems. The research develops a process guided by activity theory to unravel some of the hidden design tenets that should guide SSO deployments.

I. INTRODUCTION

AS IT systems elevate their role from “supporting” to “enabling” business processes, end users, system designers, managers and technicians are coping with an increasing complexity of maintaining an ever growing portfolio of applications and ensuring their system security. Users typically have to sign-on to multiple systems, necessitating an equivalent number of sign-on dialogues, each of which may involve different usernames and authentication information [12]. As a result users resort to committing serious security flaws like writing down passwords on paper or using passwords that can be easily guessed. Single sign-on (SSO) system enables the user to use a single user-id and password pair to access all authorized computer resources in a distributed, multiplatform computing environment, without authenticating multiple times [1]. Increased security and compliance, improved user productivity and convenience and real cost savings are few motivations that drive SSO implementation [16]. According to a Gartner report Single Sign-On system can save up to \$300 per user per year which can account to huge amounts [5]. By the use of single sign-on, user identity is consolidated to a single digital identity and this helps reduce administrative burden and meet regulatory and compliance needs of the organization like

HIPAA, Sarbanes-Oxley act, UK data protection act, European Union Privacy Act etc. Using SSO, users need to manage only one set of authentication credentials in order to log into the services they subsequently use [32]. A single sign-on system should provide secure storage of user passwords, support for more than one user password, as well as support for multiple target logon methods [4]. After authenticating to the SSO system, when users access target systems, the SSO agent passes the appropriate target system's credentials to those systems and logs in the user with no additional action required on their part. SSO has been proposed as a solution to improve employee productivity, reduce information systems administrative costs and increase system security [11]. Organizations that have five or more heterogeneous Windows, Web and terminal-based applications that users must sign on to every day are “feeling the pain” of user complaints via high numbers of help desk calls, stand to gain the most from SSO tools [20]. Over the years, enterprise-class Single Sign-On products have matured and today, they provide value for enterprises with users who must sign on to multiple applications. Users can be prompted for passwords and password changes. Passwords can be created as random character strings by the SSO tool and can be made as strong as allowed by the target systems, and changed without placing burden on the users. Through 2009, a Global 2000 enterprise that purchases an enterprise Single Sign-On tool will continue to use it for five or more years (0.8 probability) [20].

Password related threats including social engineering are an undeniable and pervasive threat to the security of information systems of an organization due to its reliance on the social nature of human beings [14]. Activity theory offers the options for understanding use and system design for computer applications as well as other parts of the work activity is constantly reconstructed to meet the dynamic demands of any organization. An explicit awareness of these hidden trends may change our way of doing design [11]. Researchers [19, 21] have proposed AT-based methodologies for software development. Several other disciplines have used Activity Theory to understand their processes and constructs. It is evident from the literature review that role engineering is an increasingly critical and vital process at any organization from both functionality and

TABLE I
EXAMPLE TECHNICAL AND FUNCTIONAL
REQUIREMENTS FOR A SSO SYSTEM

| REQUIREMENT | DESCRIPTION |
|---------------------------|--|
| Single sign-on | One password to access multiple applications |
| Authenticator choice | Choice of multiple back-end password stores |
| Mobility support | Support for roaming profiles |
| Workstation sharing | Multiple users can share the same workstation |
| Automated password change | Product changes the password based on application level security |
| Event Logging | Automatically log events such as logons, password changes |
| Auto Prompt | Prompts for a new password-protected application |
| Common passwords | Multiple applications can share the same password |
| Central administration | All configurations and settings are centrally manageable |
| Automatic Backup/Restore | Automatically back up user credentials to a remote location |
| Customization | Modifiable templates for corporate policy |
| Secure architecture | The agent is designed to be highly secure and tamper-resistant. |

security viewpoints. It is also revealed through literature review that activity theory has not been used, thus far, to analyze and understand role-engineering process to design effective and secure roles within an organization. With Activity theory's immense benefits, we analyze role-engineering process and principles to unravel some of the human and social facets that are not evident from traditional role engineering frameworks. The paper is organized as follows: In next section, we present background and preliminaries on different concepts used in the research. Section 3 presents activity theory guided evaluation of risks on SSO systems and applications. Section 4 presents an illustrative case study to show how activity has been used to uncover some risks hidden in user assignments to role in the context of two applications.

II. BACKGROUND AND PRELIMINARIES

A. Single Sign On

A single sign-on (SSO) system provides mechanisms and supporting technologies to support different authentication mechanisms including storing passwords and other credentials [4]. SSO system should have support for varying types of authentication mechanisms from simple passwords to complex biometrics. The SSO should be flexible enough to accommodate requirements of infrastructure and business based on agreed upon trust requirements, Authentication schemes (e.g., those based on passwords, certificates, biometric techniques, smart cards, etc.) are employed depending on the trust-level requirement(s) of an information resource (or information resources) to be accessed [31]. SSO has been shown to improve security, usability and infrastructure maintenance while improving the end user's convenience and trust [32]. Empowering the user with a Single Sign-On capability has multifold benefits. It greatly improves the user experience and relieves the user from the burden of remembering multiple user-id and

password pairs. Enterprises hope that Single Sign-On protocols will significantly decrease customer-care costs related to forgotten passwords and increase e-commerce transactions by enhancing the user experience [24]. "On the administrative side, help desk costs are noticeably reduced and security improved, as users are not tempted to 'store' multiple passwords in written form" [1]. With identity management systems, new user accounts can be setup and accounts of those leaving the organization can be deleted in a few minutes resulting in a huge productivity boost. SSO significantly improves convenience and ease of use of different kinds of systems [10]. According to Forrester Research, as much as 30% of helpdesk time is spent in dealing with password-reset issues [30]. With the cost of a single help desk call estimated at £13 to £20, these password problems can quickly add up to hundreds of thousands of pounds per year, for even mid-sized companies. When assessed against the cost of implementing and maintaining the Single Sign-On, the return on investment becomes apparent [28].

There are a plethora of SSO products available in the market. Oracles, IBM Tivoli access manager, Sun Microsystems Open SSO, Novell, Courion, CA are few of the leading SSO product vendors [4, 23]. Most of the identity management products fall into the four major areas- Identity intelligence, Identity administration, Identity verification and Access management. SSO systems perform authentication and authorization functions in the identity management systems. Most of the commercial identity management vendors contain an array of products for user provisioning, self administration and single sign-on. Oracle, IBM Tivoli, Sun, Novell and CA qualify under single provider portfolios as they have products required for a complete identity management system [23]. Table I presents some of most common requirements for a SSO System. Most of the identity management vendors charge either per user enrolled under the system or have a single product cost. Single Sign-On solutions find their application in wide variety of domains like healthcare, education, retail, finance, banking etc. Identity management as a service (also by *Symplified* [27]) is one of the latest developments in this arena. These activities involve huge costs and put IdM options out of the financial reach of small and midsized businesses [15].

B. SSO Standards and Architectures

Federated identity management is a version of single sign-on that spans across different organizational boundaries. It is enabled by sharing common authorization and authentication data between these organizations [9]. Remote systems control access to resources based on the roles assigned to the person trying to access them. Liberty Alliance project and *Incommon* Federation establish standards, specifications and policies for identity assurance and identity governance framework like SAML/2.0 – standardized XML documents for sharing identities, ITU-T X.509v3 – standardized digital certificate etc [17, 30]. Detailed information about

TABLE II
COMPARISON OF REQUIREMENTS ENGINEERING APPROACHES
(ADAPTED FROM [3])

| Dimension | Focus | Goal Oriented | Function Based | Adapted Activity Theory |
|-------------|---|---------------|----------------|-------------------------|
| Goal | Intention | X | | X |
| People | Individual (role) | X | X | X |
| | Community (group, role) | | | X |
| Process | Division of Labor (rule, task assignment) | | | X |
| | Activity and Activity Structure | X | X | X |
| | Object Hierarchy | X | X | X |
| Technology | Instrument (form) | | | X |
| Environment | Context Awareness | X | X | X |
| | Social Issues | | | X |
| | Environment Issues | | | X |
| Interaction | Contradictions | X | | X |

standards, policies and specifications can be found at Liberty Alliance specifications [17].

Single sign-on systems rely on other infrastructure like the authentication system, identity management/ registration, web servers etc [9]. Single Sign-On can be realized in many ways either by using browser cookies, HTTP redirects, user access tokens (Kerberos, SAML etc..) ticket granting systems, Digital certificates, by having a central authentication and authorization server, LDAP and active directories [22] Biometrics, smart cards or USB tokens with certificates/ login passwords, Radio badges using RFID technology can be integrated with SSO to provide multi-factor authentication [18].

C. Activity Theory

Activity Theory (AT) seeks to explain social and cultural work practices by relating them to the cultural and historic context in which the work activity, which is the basic unit for analysis, is taking place [2]. AT gives us guidelines and concepts to analyze “the actions and interactions with artifacts within a historical and cultural context” [25].

Activity theory offers the options for understanding use of system design for computer applications as well as other parts of the work activity that are constantly reconstructed to meet the dynamic demands of any organization. An explicit awareness of these hidden trends may change our way of doing design [11]. Researchers [19, 21] have proposed AT-based methodologies for software development. Several other disciplines have used Activity Theory to understand their processes and constructs. However, due to origins and wide applications of Activity theory in social and psychological areas, it is vastly underutilized in information security domain.

Activity theory has evolved through two generations of research [7] since introduced by several Russian scholars using Marx’s political theory [26]. The most common, by Engestrom [6, 7, 8] (Figure 1), is concerned with the process of social transformation and incorporates the structure of the

social world and aims to understand dialogues, multiple perspectives and networks of interacting activity systems.

In Engestrom’s original work [6], activity systems included subject, tool, object, rules, community, distribution of labor, and outcomes (as shown in Figure 2). *Subjects* are participants of activity and tools are resources that the subjects use to obtain the object or the goal. *Rules* are guidelines or restrictions that are considered during interactions and social dynamics amongst subjects and objects. The *community* is a group that subjects belong to and *division of labor* is the shared responsibilities determined by the community. Finally, the *outcome* is the consequence that the subject faces as a result of the activity. Activity systems analysis was developed to explore and document the sources of tensions in human individual or collective activities.

III. ACTIVITY THEORY GUIDED EVALUATION OF SSO RISKS

As we discussed above, there are several SSO benefits to individuals and organizations. However, there are various risks that arise from the fact that different applications share different characteristics and bringing them (a set of



Fig. 1. Engestrom’s extended Activity System

applications) without considering those characteristics will expose the environment to severe threats. Activity theory (AT) is widely used for different applications in IT ranging from software development to secure role development [13]. Because of the unique insights and perspectives that AT offers in understanding not only technical and systemic features but also dynamic interactions amongst individuals and communities, it is a very apt approach for understanding and revealing some of the risks arising from SSO. Some of these critical risks cannot be brought under consideration for SSO design without the use of AT. Table II (adapted from [3]) shows different dimensions that are covered from under various approaches to under system behavior. As is evident from the table, use of AT brings more dimensions under the lens for evaluation of systems. More specifically, the ones that pertain most towards AT’s contributions are People, technology, environment and interaction dimensions.

Figure 2 shows adapted AT with different risk factors from application standpoint and from SSO system standpoint. In Figure 2, (A) denotes the risk factor is application specific and (S) denotes SSO denotes system specific. The figure uses AT as base and then represents

various risk issues and factors for each of the system components of AT. The risk factors are presented next to each system component, in italics within parenthesis. Using Figure 2 as guide we can analyze each application and SSO

system to lead to a risk-managed selection process. The end result is selection of applications for each SSO system given application characteristics and SSO system specific details.

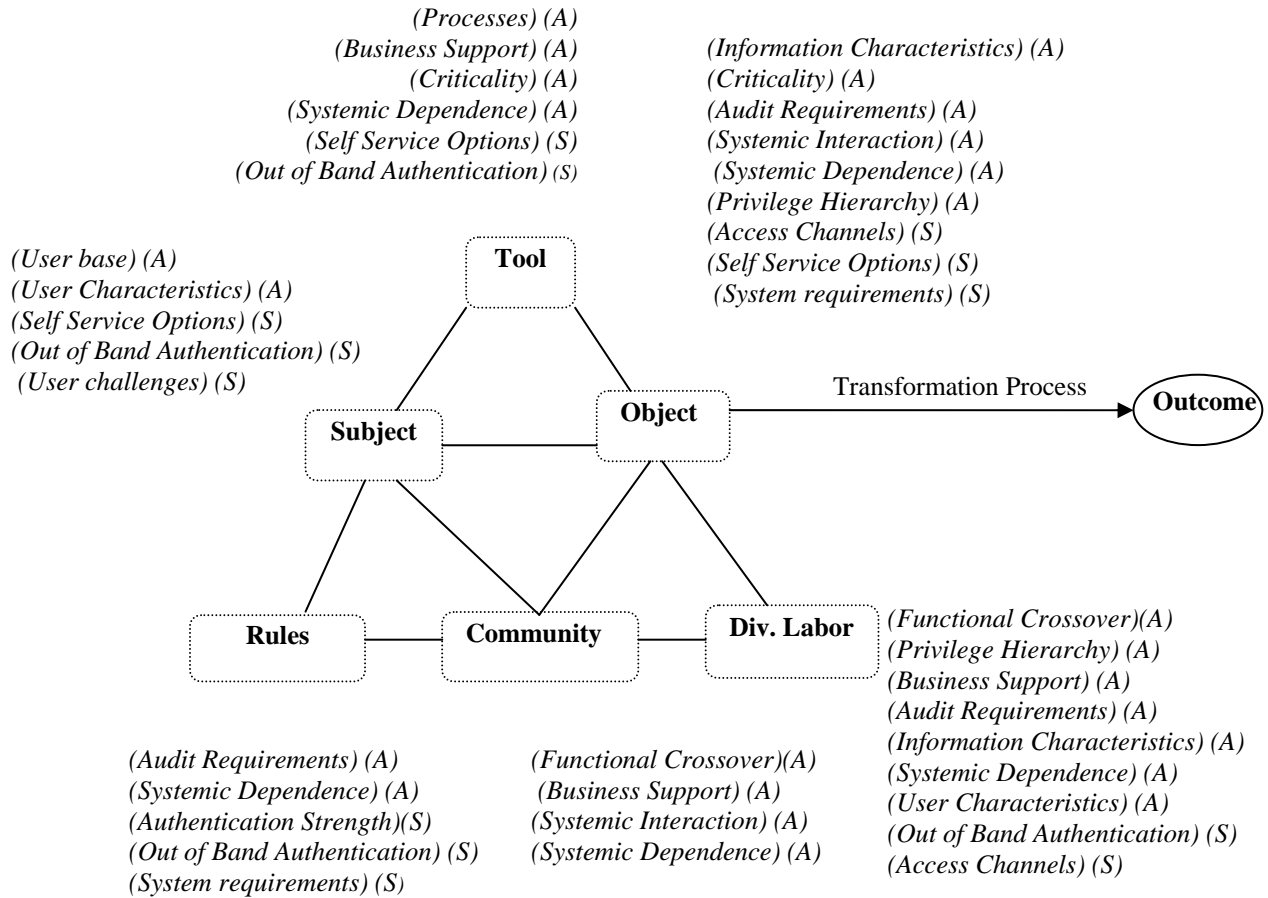


Fig. 2: Activity Theory Components with SSO and Application Risk Factors

A. SSO System Specific Risks

TABLE III
SSO SPECIFIC RISKS AND AT COMPONENTS

| SSO Specific Risk | AT Components | Description |
|----------------------------|-------------------------------------|---|
| Authentication Strength | Rules | Strength of authentication factor such as simple passwords or complex passwords, password policies, number of factors, hardware or token. |
| Access Channels | Object, Div. Of Labor | Number of channels to access the user interface for SSO system |
| Self Service Options | Tool, Object, Subject | Options where users can reset their own passwords, modify profile or request additional accesses. |
| Out of Band Authentication | Tool, Div. Of Labor, Rules, Subject | Bypassing SSO system to access an application and having credentials reset over phone. |
| System Requirements | Object, Rules | Technical and functional requirements of the SSO system. Some common ones are listed in Table 1. |
| User Challenges | Subject | Ease of use of the SSO system and HCI issues. |

There are several risks that emanate from various aspects of SSO systems including technology, environment, deployment architecture, people and processes (See Table III). Weak passwords in a single sign-on environment have been widely reported as one of the greater risks of SSO systems. Compromise of password can result in unauthorized access to information that can be potentially confidential and the incident can be detrimental to the organization. In the same light, applications processing sensitive information should implement stronger password policies or use multi-factor authentication such as token or biometrics so that the risk of SSO being a central point of attack is mitigated. There are several threats to privacy as well in an environment where a user's identity is shared amongst teams. Towards usability of SSO systems, user interface is considered to be one of most important and inadequately addressed component. Many of the phishing attacks are launched due to weakness in secure-proofing the user interface without putting undue burden on users. Many of the SSO systems that enable SSO amongst web-based applications heavily rely on cookies. There have been several reported vulnerabilities and threat specific to browsers and other technological components that bear severe consequences. Organizations should consider not only acquisition costs while selecting an SSO system, but also ongoing and maintenance costs. For example, while

selecting password based authentication which may appear simple and cost-effective choice, it should be considered that on an average, it costs about \$70 for each password reset. SSO helps lower these password-reset costs as there would be only one password for multiple applications which makes it easier for users to remember. The technical environment where SSO is going to be implemented should also be factored in selecting an SSO solution. Table III shows some of the most common SSO specific risks and how analyzing those using listed AT component(s) help understand the nature of risks and suggests ways to mitigate them. In absolute terms, authentication mechanism that uses more than one factor is considered stronger than a single factor (such as password), however careful risk assessment should be made to introduce additional factors which will presumably incur higher costs. Identified risks should justify higher costs and since the SSO can be used for multiple applications, this should drive motivation for multi-factor SSO. However, it should be considered that only applications that process high risk transactions such as financial systems or systems containing confidential information such as SSN should be included in multi-factor SSO.

B. Application Specific Risks

There are several characteristics of an application that give unique risks to authentication and authorization process for the application. Applications serve one or more business objectives for an organization, which can aid decision-makers in understanding the criticality of the application to the business. With that in light, both security and usability has to be balanced while selecting an authentication solution. Besides, while using SSO for authentication to that application, the authentication is delegated to the SSO system. Also, based on the user characteristics and nature of activities performed on the application, organizations must decide if additional layers of authentication are required and then an SSO system meeting their requirements should be deployed. More often than not, businesses will have applications sharing some of their prime features, which will further help organizations plan likewise considering the economies of scale that SSO systems provide. For example, enterprise applications that handle employees' sensitive information such as payroll, HR, medical and insurance records should have stronger authentication mechanisms. Besides information characteristics, user characteristics are also equally important. For example, a financial institution may choose to use multiple factor

TABLE IV
APPLICATION SPECIFIC RISKS AND AT COMPONENTS

| Application Specific Risk | AT Components | Description |
|-----------------------------|--|---|
| Business Support | Tool, Div of Labor, Community | Business functions and processes supported or enabled by the application. |
| Processes | Tool | Processes automated or facilitated by the application, usually electronic forms, work flows and transactions. |
| Privilege Hierarchy | Object, Div of Labor | Different roles within application that ascertains access to and responsibility for different classifications of information. |
| Criticality | Tool, Object | How critical is the application for the specific business function? Usually business continuity exercises determine recovery time objectives that assign criticality to applications. |
| Systemic Interaction | Object, Community | Extent of information exchange and communications with other systems, processes and people. |
| Functional Crossover | Community, Div. Of Labor | How many different functional units from the organizations perform their duties on the application? |
| Systemic Dependence | Tool, Object, Div of Labor, Community, Rules | Does this application relies on other application(s) for its functioning (processing, storing and transmitting information) or do other applications rely on this application for their successful operation? |
| Audit Requirements | Object, Div of Labor, Rules | Are there specific audit and compliance requirements or specific guidelines (or recommendations) for the application such as SOX, GLB, FFIEC etc. |
| Information Characteristics | Object, Div of Labor | What is classification of data that passes through the application? Which roles have access to data from which classification level? |
| User Base | Subject | How many users access the application and what is the frequency of usage? |
| User Characteristics | Subject, Div of Labor | What are the characteristics of users that access the application? Customers or employees? Important customers? Administrators? |

authentication-based SSO system for commercial customers who execute financial transactions in large monetary terms, while retaining password-based authentication for retail customers (though enforcing stronger password policies). SSO systems provide organizations the agility to add more similar applications to SSO, which is scalable by design. This also creates a portfolio of applications for users for which they will have to authenticate only once. For many applications, multi-factor authentication options can be selected depending on some of the application-specific characteristics such as businesses that the application supports, privilege hierarchy, functional crossover, and audit and compliance requirements. There are four levels of authentication strength as proposed by NIST standard: SP 800-63.

The factors that NIST standard suggests to account for when selecting an authentication solution include use of tokens for identity verification, identity proofing during on-boarding and de-provisioning, remote authentication mechanisms and security information assertion. Some of the application specific risks and the way in which AT components help provide insight into their working is provided in Table IV. Description of each risk is also provided in the table to illustrate the contribution of the risk consideration. Analyzing application characteristics using AT and its components help managers and architects on making judicious decisions in selecting the most appropriate SSO system based on risk assessment, including cost.

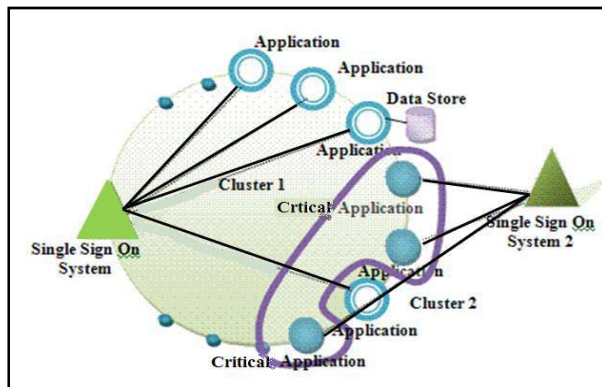


Fig. 3. Systemic View of interaction of SSO with applications

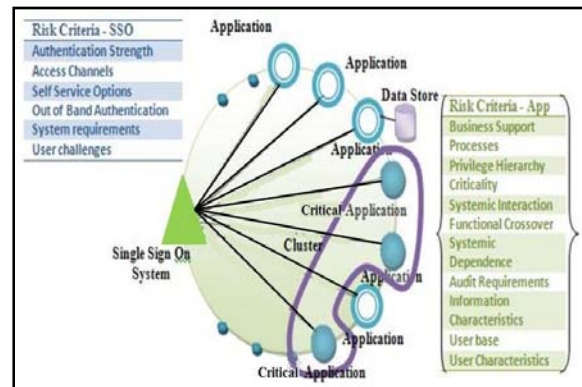


Fig. 4. Decoupling Applications to form separate SSOs

C. SSO Design: Application Selection

SSO systems provide a mechanism for users to authenticate only once and access a portfolio of applications. Figure 3 illustrates how SSO interacts with different applications for verifying the user's authentication and authorization statuses. The Figure shows criteria for risk assessment of each application to decide whether it should be brought under a specific SSO system. Also shown are some factors to consider when designing SSO system (the list on the top left corner). Most applications need a data store, temporal and persistent, for its operation. The data accessed and processed by application supports business goals and objectives. The more critical the data is for the business, the stronger the authentication that is required to access it. In the same vein, organizations should deploy more than one SSO system while putting applications that share risk characteristics under a specific SSO system. The user base and characteristics can also impose severe restrictions on selection of a specific SSO system. For example, applications used by customers who are available over public domain such as Internet should go through a rigorous risk assessment to select best risk-managed SSO solution. At the same time different SSO systems are built for varying loads of performance, so user base is also an important factor in its selection.

Similarly there are several other risk factors (Table IV) associated with the application that should be used to select the SSO system. AT concepts and component(s) shed light into each risk factor from a more comprehensive view while addressing some of the most ignored risk concerns such as the role of community in an organization and dynamics of interaction between people. For instance, by use of AT component, division of labor, we can delineate risks from social engineering, collusion and unauthorized escalated privileges. While most of the risk assessment methodologies only factor in technological, business and procedural aspects of business functions, AT, while covering those also incorporates community, division of labor, tools and rules. Use of these additional lenses in risk assessment in conjunction with traditional ones provides a holistic and more accurate posture of risks. Sometimes it makes better decision to decouple applications from under an existing SSO solution after performing an AT based risk assessment of applications. In Figure 4, we show how we can break an SSO system into 2, based on criteria presented above. For example, initially one SSO system was one-factor (password) based (SSO system specifics).

However, on review of applications under the system, it was unraveled that some of the applications (solid circles in Figure 4) process sensitive/private corporate information (based on internal organizational data classification). So it is imperative that a 2-factor authentication should be used for the SSO system (which is shown as SSO 2 in the figure).

IV. ILLUSTRATIVE EXAMPLE: A CASE STUDY ON APPLICATION RISKS

Next we present an example where Activity Theory is used to uncover some of the threats inherent in traditional role engineering process. These same issues surrounding users, communities, interactions and access channels as they relate to application specific risks apply to our discussions on SSO system design. Gupta [13] in an exploratory case study illustrates how role engineering is performed in organizations and how the activity theory principles and concepts can aid managers and designers engineer effective and secure roles at a mid-sized US financial institution. This paper leverages the work of Gupta [13] in the development of the constructs for this research. There were 6 people at the financial institution who aided us understand their role engineering process. Researchers met them to 1) educate them on activity theory and theory behind RBAC though they were

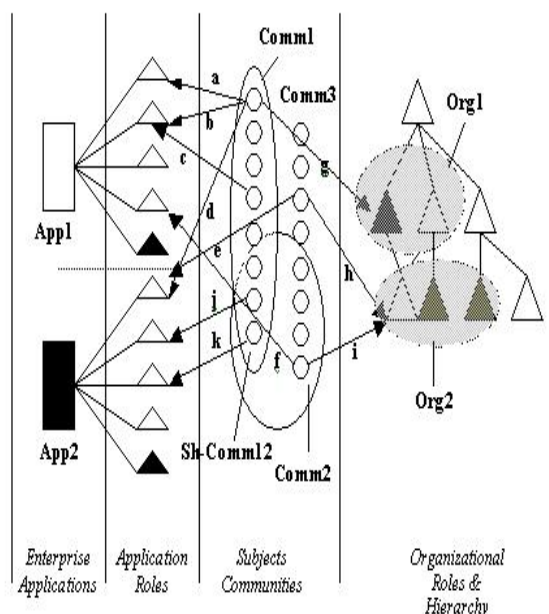


Fig. 5. Application Specific Risks as illustrated through example of two real world applications

not aware of terms used for formal RBAC representations. Based on discussions with the managers at the financial institution, we collectively came up with a situation where role engineering process can utilize activity theory principles to better understand the implications of role engineering process.

Also, this will aid managers understand and unravel social and community-based facets of environment that are ignored in traditional role engineering process. In the Figure 5, App1 and App2 are two applications for which the roles are to be engineered.

The triangles in the section right of applications are the application roles. In the subjects' section, circles are users and ovals represent user communities (Comm1-3). Shared communities are the communities that belong to the same users (Sh-Comm12). Only one such community is shown in the figure to keep the case simple. Right most section shows organizational roles within the enterprise (Org1 and Org2). These can denote same functional or positional roles in an organization. The small cased letters in Figure 5 denote assignments of application roles and organizational roles to users. Table V shows assignments with the exact mappings of users, communities, roles and applications. Third column (Emphasis) presents the linkage that is most vital in understanding applicability of activity theory

TABLE V
USER ASSIGNMENT TO ROLES IN APPLICATIONS

| Assignments | Mappings | Emphasis |
|-------------|---|----------------|
| a | User(Comm1) ₁ - Role(App1) ₁ | User-role |
| b | User(Comm1) ₁ - Role(App1) ₂ | User-role |
| c | User(Comm1) ₂ - Role(App1) ₂ | User-role |
| d | User(Comm1) ₁ - Role(App2) ₁ | User-role |
| e | User(Comm3) ₁ - Role(App2) ₁ | User-role |
| f | User(Comm2) ₁ - Role(App1) ₁ | User-role |
| g | User(Comm1) ₁ -Org ₁ | User-org |
| h | User(Comm2) ₁ -Org ₂ | User-org |
| i | User(Comm2) ₁ -Org ₂ | User-org |
| j | User(Sh-Comm12) ₁ - Role(App2) ₂ | User-Community |
| k | User(Sh-Comm12) ₁ - Role(App2) ₃ | User-Community |

to role engineering for this scenario (Figure 5). Table VI below represents different interactions amongst the user assignments (column 2) and how they result in various threats to specific component of RBAC (column 3). Column 4 in Table VI represents unit of focus or the component that is most likely hit due to that particular interaction of assignments. The last column provides description of the interaction.

TABLE VI
APPLICATION RISKS FROM INTERACTION ASSIGNMENTS TO ROLES

| SCENARIO | INTERACTION | RESULT | RISK FOCUS | DESCRIPTION |
|----------|------------------|---------------------------------|--------------|---|
| I | a + b | Multiple role | User | <i>One user having more than 1 role in the same application</i> |
| II | b+ c | Shared role | Role | <i>Same application role assigned to multiple users from the same non-shared community</i> |
| III | a+ d | Cross-application roles | User | <i>One user assigned roles from multiple applications</i> |
| IV | a+ c | Community Role | Community | <i>Multiple users from the same community having access to multiple roles in same application</i> |
| V | d + e | Across-community role | Role | <i>Users from multiple communities having access to the same role</i> |
| VI | j + k | Shared Community application | Application | <i>Users from shared communities access multiple roles from same application</i> |
| VII | e + h & d + g | Across Org. role | Role | <i>Same application role assigned to users from multiple organizational role</i> |
| VIII | a + b + g | Across application role | Application | <i>Users from same organizational role have access to different application roles</i> |
| IX | f + I & e + h | Across application and org role | Applications | <i>Users from same organizational role have access to different roles from different applications</i> |

TABLE VII
ACTIVITY THEORY PRINCIPLES LEGEND

| Abbrev. | AT System Elements (Engestrom's System Model, 1997) |
|------------------------|---|
| Tool | To |
| Subject | S |
| Object | Ob |
| Rules | R |
| Community | C |
| Division of Labor | D |
| Transformation Process | Tr |
| Outcome | Ot |

Based on discussions with the managers at the financial institution where this case study was carried out and analyses of the case study dynamics, managers consented on applicability of different principles and concepts of Activity Theory, as they would apply to role engineering process. Tables VII and VIII present abbreviations for RBAC and AT components used in Table IX. The threat scenario number from Table VI is presented in column 1 in Table IX. Table IX shows which component and consideration in the role engineering process (column 2) would be affected by Threat Scenario (Table VI). Next column in any row (read threat scenario) of the table present Activity theory principles (Engestrom's System Model, 1997) that should be used to further unravel any interactions that may arise inefficient and insecure roles.

For example, row 3 of the table represents Threat Scenario III (arising due to Cross-application roles). For this scenario user-assignment to roles, separation of duties and application role hierarchy are the most important components of RBAC that should be

TABLE VIII
RBAC COMPONENTS LEGEND

| Abbrev. | Role Engineering Components |
|---------|----------------------------------|
| UA | User Assignment |
| PA | Permission Assignment |
| SOD | Separation of Duties Constraints |
| ARH | Application Role Hierarchy |
| ORH | Organizational Role Hierarchy |
| S | Sessions |

closely scrutinized. At the same time, managers at the financial institutions, feel that Internalization/externalization and Object-orientedness are the principles from Kaptelinin and Nardi [33] Activity Theory Artifact that can aid in further understanding of the social dynamics within organization that can uncover some vital scenarios that should be

accounted for in role engineering. Similarly, last column shows Activity Theory System Elements, consideration of which will significantly mitigate the risks of insecure role creation by analyzing the context of the users and roles (both application and organizational).

V. DISCUSSION

In the paper we discussed concepts and

TABLE IX
APPLICATION OF ACTIVITY THEORY TO ROLE ENGINEERING DESIGN

| Scenario | Role Engineering Components | Activity Theory System Elements (Engestrom's System Model, 1997) |
|----------|-----------------------------|--|
| I | UA, PA, SOD | S, To, D, Tr |
| II | SOD, ARH | To, S, Ob, C, D |
| III | SOD, UA, ARH | Ob, S, D, Tr |
| IV | UA, ARH, ORH | S, D, Tr, C |
| V | UA, ORH | S, Ob, T, C, D |
| VI | ARH, ORH, PA | S, Ob, T, C, D |
| VII | ORH, PA | S, T, C, Tr, To |
| VIII | ARH, ORH, UA | S, T, C, Ot |
| IX | ARH, ORH, UA | S, Ob, T, C, D, Ot |

frameworks of single-sign-on systems and activity theory. Some common drawbacks of traditional SSO system design were presented. In light of unique insights that activity theory can provide in the SSO design process while considering specific risks from two perspectives (SSO system-specific and application-specific), we analyzed how different risk considerations and activity theory can be brought together for secure SSO system design. To illustrate relevance and utility of using AT in SSO design, we presented a case study where AT was used to help design secure role engineering process. The basic concepts and workings, we believe, will remain similar for SSO systems as well. The paper's main contributions are 1) application of activity theory to help identify risks and 2) identification of different types of risks that SSO system's deployment introduces in an environment (Table III and Table IV) and how they relate to different Activity theory principles. We are in process of gathering information on SSO design practices utilized by as many as fifteen different organizations representing various industries. Future work on this study is to show how the organizations can use activity theory to improve their SSO systems to mitigate risks arising from the deployment of SSO systems. Investigation will entail showing a system designed without considering AT principles and then analyzing how AT can be used to reveal risks.

REFERENCES

- [1]. D. Anchan, and M. Pegah, "Regaining single sign-on taming the beast", in *Proceedings of the 31st annual ACM SIGUCCS conference on User services SIGUCCS '03,2003*.
- [2]. O. W. Bertelsen and S. Bodker, "Activity Theory" in *HCI Models, Theories, & Frameworks: Toward a Multidisciplinary Science*. Carroll, J (ed), pp 294-324, 2003.
- [3]. R. Chen, R. Sharman, N. Chakravarti, H.R. Rao, and S. Upadhyaya, "Emergency Response Information System Interoperability: Development of Chemical Incident Response Data Model", *Journal of the Association of Information Systems*, Volume 9, Issue 3/4, pp. 200-230, Special Issue 2008.
- [4]. R. J. Cohen, R.A. Forsberg, P.A. Kallfelz, J. R. Meckstroth, C.J. Pascoe, and A.L. Snow-Weaver, "Coordinating user target logons in a single sign-on (SSO) environment", *Patent number: 6178511*, Filing date: Apr 30, 1998, Issue date: Jan 23, 2001, Assignee: International Business Machines Corporation
- [5]. P. Connolly, "Single Sign-on dangles prospect of lower help desk costs" Retrieved march 21, 2009, from infoworld: <http://www.infoworld.com/articles/es/xml/00/10/02/001002esnso.html>
- [6]. Y. Engestrom, *Learning by expanding: An activity-theoretical approach to developmental research*. Helsinki: Orienta-Konsultit Oy, 1987.
- [7]. Y. Engestrom, "Activity theory and individual and social transformation". In Y. Engestrom, R. Miettinen, & R.-L. Punamaki (Eds.), *Perspectives on activity theory* (pp. 19–38). New York: Cambridge University Press, 1999.
- [8]. Y. Engestrom and R. Miettinen, "Introduction", in: Y. Engestrom, R. Miettinen, R. Punamaki (Eds.), *Perspectives on Activity Theory*, Cambridge University Press, Cambridge, 1999, pp. 1–16.
- [9]. Federated Identity Management, Retrieved March 22, 2009, from Tech-faq: <http://www.tech-faq.com/federated-identity-management.shtml>, 2009.
- [10]. T. Fleury, J. Basney and V. Welch, "Single sign-on for java web start applications using myproxy", *Workshop On Secure Web Services archive, Proceedings of the 3rd ACM workshop on Secure web services*, Alexandria, Virginia, USA, SESSION: Security architecture, pp. 95 – 102, 2006
- [11]. T. Gordon, *Quantifiable Benefits of Implementing Identity management systems*. Retrieved 3/22/09, from University of Salford: www.ils.salford.ac.uk/about/projects/idm/docs/Stageand%20ISDSQuantBenefits.pdf
- [12]. O. Group, *Introduction to Single Sign-On*, 2001. Retrieved March 22, 2009, from The Open Group : http://www.opengroup.org/security/sso_intro.htm
- [13]. M. Gupta, "Activity Theory Guided Role Engineering", *Proceedings of 14th Americas Conference on Information Systems (AMCIS 2008)*, Toronto, Canada, August 14-17, 2008.
- [14]. M. Gupta and R. Sharman, "Social Network Theoretic Framework for Organizational Social Engineering Susceptibility Index", *Proc. of 12th Americas Conference on Information Systems*, Acapulco, Mexico, Aug 4-6, 2006.
- [15]. G. Hulme, *Identity management as a service*. Retrieved march 22, 2009, from Information week: http://www.informationweek.com/blog/main/archives/2008/07/identity_manage.html, 2008.
- [16]. Imprivata, *Benefits of Single Sign on*. Retrieved March 22, 2009, from Imprivata: <http://www.imprivata.com/contentmgr/showdetails.php?id=1170>
- [17]. Incommon *policies and practices*, Retrieved March 22, 2009, from Incommon federation: <http://www.incommonfederation.org/policies.cfm>
- [18]. L. Jerphanion, "Enterprise single sign on", *evidian white paper*. EvidianInc. *Liberty Alliance specifications*. (n.d.). Retrieved March 22, 2009, from project liberty: http://www.projectliberty.org/liberty/resource_center/specifications
- [19]. M. Korpela, H.A. Soriyan and K.C. Olufokunbi, "Activity Analysis as a Method for Information System Development." *Scandinavian Journal of Information Systems* (12): 191-210, 2000.
- [20]. G. Kreizman, "Enterprise Single Sign-On Provides Value for Complex Environments", *Gartner Research Publication*, ID Number: G00138179, 22 March 2006.
- [21]. D. Mwanza, "Where theory meets practice: A case for an Activity Theory based methodology to guide computer system design" *INTERACT'2001*, Oxford, UK, IOS Press.
- [22]. D. Orrell, Authentication systems and single sign on, *EuroCAMP*. Porto, Portugal, Nov 7-9, 2005.
- [23]. E. P. Perkins, *Magic Quadrant for User Provisioning*. Gartner Research Report, 2004.
- [24]. B. Pfizmann, and M. Waidner, M, "Analysis of liberty single-sign-on with enabled clients" IBM Zurich Res. Lab., Ruschlikon, Switzerland; *IEEE Internet Computing*, Nov.-Dec. 2003, Volume: 7, Issue: 6, pp. 38- 44
- [25]. Y. Rogers, "New theoretical approaches for HCI". In ARIST: Annual Review of Information Science and Tech - 38, B. Cronin (Eds), 2003.
- [26]. A. Stetsenko, "Activity as object-related: Resolving the dichotomy of individual and collective planes of activity", *Mind, Culture, and Activity*, 12(1), 70–88.
- [27]. Symplified. (n.d.). Retrieved March 22, 2009, from symplified: <http://www.symplified.com/>
- [28]. D. Ting, "Biometrics and single sign-on", *Biometric Technology Today*, Volume 13, Issue8, September-2005, Pages 8-9.
- [29]. Wiki.ihe, *Federated Identity Management Profile*. Retrieved March 22, 2009, from Wiki.ihe: http://wiki.ihe.net/index.php?title=FEDidMGT_-_Federated_Identity_Management_Profile, 2007.
- [30]. R. Woo, "Password Reset Software Can Reduce Help Desk Costs", *Forrester Research IdeaByte*, March 30, 2001. Retrieved from <http://www.forrester.com/Research/LegacyIT/Excerpt/0,7208,18845,00.html>
- [31]. D. Wood, P. Weschler, D. Norton, C. Ferris, Y. Wilson and W. Soley, "Log-on service providing credential level change without loss of session continuity", *Patent number: 6609198*, Filing date: Aug 5, 1999, Issue date: Aug 19, 2003, Assignee: Sun Microsystems, Inc.
- [32]. G. Zhao, D. Zheng, and K. Chen, "Design of single sign-on", *IEEE International Conference on E-Commerce Technology for Dynamic E-Business*, 2004. pp. 253 – 256
- [33]. V. Kaptelinin and B.A. Nardi, "Activity Theory: Basic Concepts and Applications", *Conference on Human Factors in Computing Systems*, 25-27 March 1997

Bridging Practice and Research: Secure Data Management in the Classroom

Work in Progress

Richard Savacool and Rajendra K. Raj

Rochester Institute of Technology, Computer Security and Information Assurance Program

Abstract—In recent years, information security and assurance has received considerable attention from the computing community, with universities revamping course offerings in areas such as cryptography, network security, enterprise systems security, secure coding, and digital forensics. Although secure data management is a major aspect of overall information systems security, it has received less attention than it deserves. This has not been the case at the Rochester Institute of Technology (RIT) where a course in secure database systems has been offered since 2003. The course has undergone revisions over the years and it was recently converted to be an online course.

The authors have worked in the area of information security from different perspectives. The first author, who has over a decade of practical experience in security in computer systems and holds several industry security certifications, recently took the secure database systems course at RIT as a student. The second author, who is the faculty member at RIT who developed and teaches the secure database systems course, previously worked as a software developer and manager in the financial services industry working with secure data in globally distributed systems. Based on their complementary experiences and using RIT's existing secure data management course, this work-in-progress paper describes how research and practice have been blended to create an effective course in secure data management.

Index Terms—Database security, computer security, secure data management, database systems.

I. INTRODUCTION

ALTHOUGH most organizations view their data assets as their *crown jewels* [3], keeping such data—typically stored in relational database systems—safe and secure, however, remains one of the weakest areas in information security. Security breaches in databases, including credit card and other personal financial information, have led to many states and countries enacting laws such as New York State's Information Security Breach and Notification Act to deal with such breaches. Other examples of the need for secure data management (SDM) include electronic voting systems (safety, security, and provenance of voting data), data privacy as exemplified by Health Insurance Portability and Accountability Act (HIPAA), and data outsourcing (preservation of confidentiality and integrity of personal, medical, and enterprise data). SDM is thus critical in the contemporary global marketplace, and computing students must be trained to meet its challenges.

With security having taken centerstage in an increasing number and variety of computing applications, it is

increasingly necessary to bridge the gulf between current research and industry practice in security and incorporate both into the modern computing curricula. It is also imperative that security curricula remain flexible to deal with changes in the computing world. Traditional approaches to teaching are therefore not sufficient to address the challenges of designing and developing secure computing systems. Appropriate pedagogical approaches are needed to integrate state-of-the-art security research and current practices from industry, government, and military.

Many universities have addressed the needs of information security by developing courses in cryptography, secure networking, and secure coding techniques. Few universities worldwide offer courses in SDM; the ones that do typically offer either graduate courses that focus on SDM research or undergraduate courses that present basic security features available in SQL and commercial database systems. Few attempts, if any, have been made to develop an SDM course that covers both commercial practice and current research in a holistic manner.

Rochester Institute of Technology (RIT) has offered a graduate course in SDM since 2003. This course, developed by the second author, covers basic concepts of secure data management and also includes a study of commercial practice and current research in this area. The first author who has extensive experience in the practice of secure systems recently took the course as a student. This report represents the collaboration between the two authors to identify the strengths and weaknesses of the current course and to identify opportunities to develop a more effective course that blends practice and research better.

In this work-in-progress report, we present our initial results of the effectiveness of blending practice with research in our course on secure data management. We begin by describing the course design and content, the pedagogical approach, and then discuss the most recent offering of the course. Initial evaluation of data collected over the last two offerings of the course is discussed next to determine the effectiveness of the course. We conclude by describing the current status and discuss future directions for the course.

II. COURSE DESIGN AND PEDAGOGY

A. Background

As stated in its course description, the Secure Database

Systems at RIT is a graduate course that “explores the policies, methods and mechanisms for protecting enterprise data. Topics include data reliability, integrity, and confidentiality; discretionary and mandatory access controls; secure database architectures; secure transaction processing; information flow, aggregations, and inference controls, and auditing; security models for relational, object-oriented, statistical, XML, and real time database systems.”

As prerequisite, students are expected to know fundamental database concepts including database design and modeling, architectures, database connectivity, and data organization and management. Students are also required to be competent programmers in Java, C, or C++. Students traditionally come from two majors: MS students in Computer Security and Information Assurance (CSIA) and MS students in Computer Science (CS). In recent years, graduate students in related disciplines such as Information Technology (IT) and undergraduate students in Computer Science have also opted to take this course.

Although the course includes an overview of overall system security, secure coding, network security, and basic privacy issues, it does not discuss those issues unless they arise in the context of secure data management. This approach permits focus on the many issues underlying secure database systems.

B. Course outcomes

With increased emphasis on student learning by accrediting commissions such as the Middle States Commission on Higher Education, courses at RIT emphasize course (learning) outcomes; thus, course content and student learning are guided primarily by the course outcomes. For the Secure Database Systems course, successful course completion means that a student must be able to do all of the following:

- 1) Explain basic concepts, policies, and mechanisms for building reliable and efficient secure relational database systems. [*Concepts*]
- 2) Explain how these concepts, policies, and mechanisms can be adapted for building reliable and efficient secure non-relational database systems. [*Non-relational*]
- 3) Demonstrate the design and implementation of secure policies and mechanisms to build a secure database system using a specific modern relational database system. [*Practice*]
- 4) Identify and investigate active areas of research in secure database systems. [*Research*]
- 5) Describe legal, privacy, and ethical issues in securing data and database systems. [*Ethics*]

Each outcome’s label, bracketed in italics above, serves as shorthand to remind faculty and students about the essence of the outcome. Course outcomes thus make it easier for both students and faculty to focus on the most important aspects of the course as they deal with various course activities.

C. Course topics

Course topics covered in the course essentially follow from the course outcomes. The course is structured to deal with the

two main categories of students: those with a strong security background (the CSIA students) and those with a strong database background (the CS and IT students). For the former, an overview of database topics is needed and for the latter, an overview of basic security concepts is needed. The topics covered in this course are broadly classified into three buckets.

- 1) General Topics. Included here are basic security concepts and terminology, access control mechanisms used in database systems, and integrity models and mechanisms. This is needed to introduce all students to standard terminology used in secure data management and ensure they are ready to read the current research papers in secure data management
- 2) Research. Included here is a historical research perspective covering basic multi-level secure (MLS) relational models and architectures for database systems, inference mechanisms in MLS and non-MLS systems, non-relational database systems, and a variety of topics selected from current research in secure data management. In the latest offering of the course, topics included the role of cryptography in database security, secure provenance, watermarking issues in relational databases, limiting disclosure through attribute security, forensic analysis of database logs, data inference in social networks, encrypting databases without altering structure, auditing the integrity of a database, and querying encrypted XML documents
- 3) Practice. Practitioner books by Ben Natan [3] and Litchfield [7] help to provide a list of suitable topics, which include the need to place database management system (DBMS) security within general security landscape; viewing the DBMS as a server; the role for secure communications between clients and servers; application security and proper database usage; database Trojans and database rootkits; regulations, compliance, and ethics; auditing; and DBMS case studies of Oracle, IBM DB2, or Microsoft SQL Server.

Table I shows the approximate time spent on the major topics in the course. Many of these topics have both a research and practice component. It should be noted that the time allocated is not necessarily proportional to the importance or relevance of the topic.

D. Pedagogic approach

From its inception in 2003, this course has used a pedagogic approach based on active learning (constructivist approach), and has minimized the use of passive learning (objectivist approach). Constructivism argues that students need to be active learners and construct knowledge individually based on what they already know [4]. This is arguably the only reasonable approach for learning in this course, given the constant updates to course materials as dictated by current research and industry practices. Section IV presents initial evaluation of the assessed data about this pedagogic approach.

TABLE I
APPROXIMATE TIME ALLOCATION TO EACH MAJOR COURSE TOPIC

| Major Topic | Approximate Time Allocation |
|--|-----------------------------|
| Reliability, integrity & confidentiality | 15% |
| Access control and MLS | 15% |
| Inferencing & information flow | 10% |
| Secure database architectures | 10% |
| Secure transaction processing | 10% |
| Auditing and reporting | 10% |
| Application data security | 10% |
| Encryption | 15% |
| Non-traditional DBMS | 05% |

For the past two years, this course has also been presented in a distance learning (or online) format, as well as a blended format. Distance learning courses are conducted exclusively online and leverage collaborative learning tools such as web-based discussion forums, video conferencing, and instant messaging. The SDM course continues to use a constructivist approach to pedagogy, with traditional in-class active learning components such as discussions now moving online to discussion forums. Although the online SDM course tends to be less formal than a traditional one, students continue to be engaged in *active learning* online.

The SDM course is also offered in a *blended learning* format. Although blended learning is hard to define precisely and universally, a blended course at RIT [8] incorporates all of the following: (1) some online learning activities to complement face-to-face work, (2) around half the classroom time is replaced instructor-guided learning activities in asynchronous or synchronous interaction online, and (3) the online and face-to-face components of the course are integrated pedagogically valuable manner to ensure the best use of in-classroom and online aspects.

Both the totally online and blended sections of the course are integrated online, with the major difference being that the blended course has a weekly physical classroom meeting. The physical classroom “lecture” has tended to be student-demanded mini-lectures by the instructor and sometimes by

TABLE II
MAPPING GRADED COMPONENTS TO COURSE OUTCOMES

| Graded Component | Course Outcomes Addressed |
|--|--|
| Team project | 1 (Concepts), 3 (Practice), 4 (Research) |
| Research paper reviews and discussions | 2 (Non-relational), 4 (Research), 5 (Ethics) |
| Cooperative discussions | 1 (Concepts), 3 (Practice), 5 (Ethics) |
| Final exam | 1 (Concepts), 3 (Practice), 4 (Research) |

other students or teams.

III. MOST RECENT COURSE OFFERING

The most recent offering of the course was in the Winter 2008-09 quarter. We present highlights of the course offering by describing the textbooks and other readings, online discussions, and the course project. Table II presents the various course components (in the left column) used for grading students in terms of the attainment of proficiency and in terms of the SDM course outcomes (in the right column).

Each component contributes to attainment of multiple course outcomes and each course outcome is dependent on multiple components. Section IV provides additional details about this mapping and how it is used to measure outcome achievement.

A. Textbooks and readings

The “textbooks” currently used in the course are practitioners’ books by Ben Natan [3] and Litchfield [7]. These books are supplemented by older textbooks to provide a historical perspective, for example the collection of essays on Information Security, edited by Abrams et al. [1]. Additional readings include a set of research papers, a set of industry reports, and reports of data breaches forming case studies. Previous course offerings used Afyouni [2] and Litchfield et al. [6] that are still used as supplementary sources.

Research papers are primarily accessed from the IEEE or ACM digital libraries, with the primary source of the papers being the premier database research conferences such as ICDE, SIGMOD, and VLDB, with additional content from security conferences that include data management.

B. Discussions

Because peer-based teaching [5] is a powerful learning tool, this course has been organized to foster learning through in-class discussions (for blended format students), online discussions, and research paper-driven discussions. Individual contributions are measured by both in-class and online discussions, while the paper-based discussions are more collaborative in nature.

In addition, the instructor provides the student teams each week with a set of questions on various research and practice concepts in SDM. It is left to the discretion of each collaborative team to develop a productive way of handling these discussions. Students are free to divide the work among teammates as they see fit, and often use one of two common approaches: (1) delegate specific questions to specific team members, and (2) collectively answer the questions as a group. Each group may adopt any approach for learning as long as each student has an opportunity to learn all of the material.

C. Group project

The group project requires the design and development of a two-tier or three-tier relational database application, typically built in using Oracle or Microsoft SQL Server. With the popularity of web interfaces and ease of web development, teams often choose to implement the front-end in a web-friendly format such as PHP or Java. Although much of the implementation is left to the student, the project has some minimum requirements:

- 1) Design and implement a multi-user database application.
- 2) Build an application front-end and database back-end.
- 3) Secure database applications using various best practices.
- 4) Document system architecture and security features.
- 5) Provide the project to two other teams in the class for detailed security analysis and penetration testing.
- 6) “Attack” the projects of two other teams to discover problems and report these problems to these teams.
- 7) Implement recommendations made by the two teams to mitigate discovered security issues.

Students are required to incorporate and experiment with SDM issues selected from research and practice. The project also includes developing an overall security policy for the team’s database system and application, supporting attribute- and tuple-level security and exploring auditing techniques such as custom audit triggers and fine-grained auditing.

Teams are also provided with detailed criteria for grading the team and each team member individually.

D. Use of the virtual machine lab

A notable aspect of this offering of the SDM course was the utilization of RIT’s virtual machine lab based on VMware Lab Manager. This agile development lab environment facilitates learning in security courses, for example, it is possible to have “real” network and database attacks. Systems can be run on different operating systems with different versions of database servers. The infrastructure provides increased flexibility to share workspaces among team members and to provide duplicate environments to attacking teams. The virtual machine lab provides several advantages over traditional physical machine infrastructure, for example, a quicker time-to-market, safety via snapshots in the event of failure, and a flexible software development environment.

IV. INITIAL ASSESSMENT AND EVALUATION

Our initial evaluation is based on the assessment data collected for 51 students from the last two offerings of the course as they were fairly similar in content. Results of the initial evaluation are presented here, but it should be noted that the evaluation phase is still in progress.

A. Course effectiveness

Only instructor-observed measurements of student performance were used for assessment because these direct measurements are more reliable than student self-assessments.

Table II showed how each course outcome maps to each graded course component. By mapping instructor-grades for various graded components, we can measure progress made by each student in attaining proficiency in each course outcome. It should be noted that the approach to assessment used here is the standard assessment approach used by the CS department for our accrediting agencies. That is, data being gathered and evaluated here follows our standard approach to assessment data handling used for Middle States accreditation.

Levels of proficiency reached by students on each course outcome are computed based on performance on appropriate

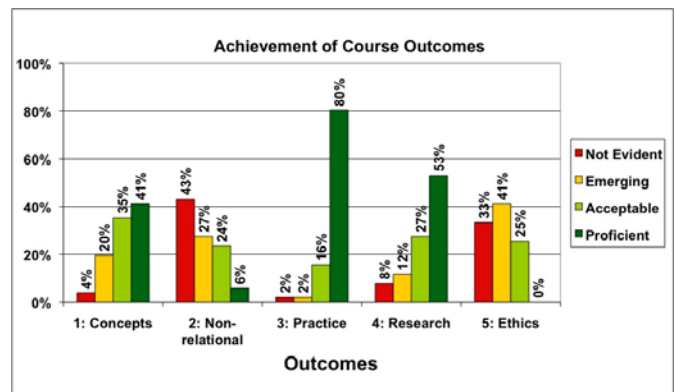


Fig. 1. Student achievement by course outcome (number of students = 51). Each bar shows percentage of students achieving that level of proficiency.

grading components used to assess that outcome. The levels of proficiency are *Not Evident*, *Emerging*, *Acceptable*, and *Proficient*. Fig. 1 displays student achievement of proficiency in each of the SDM course outcomes. For example, for the first course outcome that focused on students learning basic concepts, 41% of the students were considered to be proficient, 35% to be acceptable, 20% had emerging knowledge, and 4% had not shown any measureable evidence of learning. In other words, 76% of the students attained an acceptable or proficient level for this outcome.

High levels of achievement are also observed for the Practice outcome (96% of students attaining acceptable or better) and the Research outcome (80% of students attaining acceptable or better). On the other hand, substantially lower levels of achievement are observed for the Non-relational outcome (30% attaining acceptable or better) or for the Ethics outcome (25% attaining acceptable or none achieving proficiency). Initial analysis of these unsatisfactory numbers reveals that fewer than usual papers covering XML databases and other non-relational data were assigned. For the Ethics outcome, the problem was not that legal, privacy, and ethics were not covered in the course, but that no grading activity (in discussions, paper reviews or final exam) had been assigned to assess this outcome. This initial analysis makes it obvious that additional papers, instructor-guided discussion questions, or perhaps an exam question are needed for secure management of non-relational data. Also indicated is a final exam question to assess student knowledge and application of ethics.

Fig. 2 displays mean proficiency achieved by students on each outcome and immediately confirms the improvements

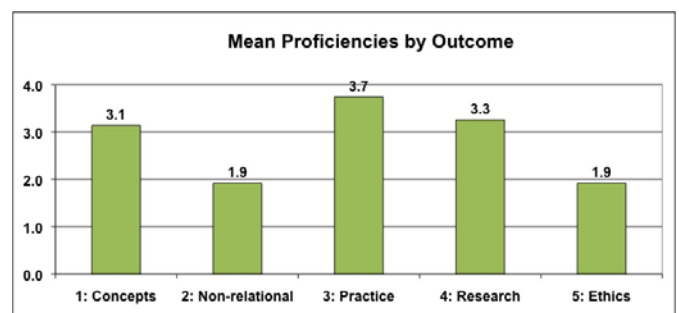


Fig. 2. Mean student proficiency by outcome (number of students = 51).

needed for Outcomes 2 and 5.

B. Students' assessment of the course

Assessment of student perceptions was also done using Likert scale measures in the earlier of the two offerings of the course. To improve objectivity, this student survey was online, anonymous, and optional, and did not contribute to the student grade. 14 out of a total of 26 students filled out this survey.

Although the sample size was small (14), an overwhelming majority—12 or higher out of 14 students—agreed or strongly agreed that the following were extremely useful in helping them understand the material: (a) individual discussions with the rest of the class, (b) paper reviews, (c) collaborative team discussions of the instructor-guided questions on research and practice, (d) collaborative teamwork on the course project, and (e) their team's attacks on other team projects. As the number of students who filled out the survey is fairly small, we do plan to assess students in future offerings of the course and report these results in a subsequent paper.

C. Challenges to learning

One of the challenges to learning often reported by students is RIT's quarter system. As each quarter is 10 weeks long, without disciplined attention to deliverables, it can be easy for students to fall behind. Careful pacing by the instructor is required to prevent course requirements from becoming overwhelming. To help mitigate this issue, an online calendaring system is used within the SDM course page to track deliverables and assist students with workload planning.

Class size also influences the level of effort associated with participatory activities such as online discussions. For example, in the most recent SDS course offering, 28 students generated nearly 400 postings for one week's online discussion; this is less of an issue with class sizes smaller than 20. Despite subsequent efforts to reduce online workload (for example, by encouraging quality over quantity in online discussions), this course achieved the dubious distinction of being rated the topmost heavy-hitter in RIT's computing college by RIT's Online Learning group that manages the university online courses environment.

Blending research with practice in the high-paced quarter schedule is indeed challenging, but student feedback indicates they prefer the current high-paced course instead of a two-quarter sequence of courses that allows both research and practice to be covered at a slower pace.

V. CONCLUSIONS

A. Current status

The course has been offered at RIT annually since 2003. It has been well received by the student community at RIT, with over 170 students having completed the course since its inception. A majority of these students have been MS students in Computer Science for whom it serves as an elective course for students specializing in Data Management. The course is

required for MS students in Computer Security and Information Assurance. Both types of students have brought diverse strengths to the course, from programming knowledge to overall secure systems knowledge, and have contributed to the overall dynamism in the course.

B. Contemplated changes

No structural changes are currently contemplated for the course. The set of research papers assigned for reading will continue to be revised each year, as will course discussions, which are based on the latest data breaches reported (which unfortunately continue to proliferate). The use of hardware (virtual or otherwise), software, and textbooks will continue to reflect the latest releases of database system and related system software.

Changes will be made to address shortcomings identified by our initial evaluation discussed in the Section IV. The next offering of the course will include a more thorough coverage of concepts and tools for secure management of non-relational data including XML data and unstructured data (e.g., blogs or web documents). While legal, privacy, and ethical issues are covered adequately at present, future course offerings will also conduct appropriate assessment for these components.

C. Final words

Over half of RIT's computer science, information technology, and computer security and information assurance graduates go on to develop, manage, or maintain systems containing sensitive data. It is therefore critical that computing students are grounded in the principles of secure data management.

RIT's SDM course bridges the divide between research and practice effectively by incorporating a variety of active learning or constructivist exercises such as the group project and cooperative discussions. The course also emphasizes how theory and pure research can be applied to solve a variety of real-world secure data management problems including data breaches and leakage. We are continuing to revise the course and working on improving our assessment of its effectiveness.

REFERENCES

- [1] M. D. Abrams, S. Jajodia, and H. J. Podell, *Information Security: An Integrated Collection of Essays*. IEEE Computer Society Press. Essays 0-3, 19-26. Available: <http://www.acsac.org/secshelf/book001/book001.html>
- [2] H. A. Afyouni, *Database Security and Auditing: Protecting Data Integrity and Accessibility*. Thomson Course Technology, Florence, KY, 2005.
- [3] R. Ben Natan, *Implementing Database Security and Auditing*. Elsevier Digital Press, Burlington, MA, 2005.
- [4] N. Crumpacker, "Faculty pedagogical approach, skill, and motivation in today's distance education milieu," *Online Journal of Distance Learning Administration*, State University of West Georgia, Distance Education Center, Winter 2001. Available: <http://www.westga.edu/~distance/ojdl/winter44/crumpacker44.html>.
- [5] M-J. Eisen, "Peer-based learning: a new-old alternative to professional development," *Adult Learning*, American Association for Adult and Continuing Education, Jan 2001. Available: http://www.accessmylibrary.com/coms2/summary_0286-7343233_ITM.

- [6] D. Litchfield, C. Anley, J. Heasman, and B. Grindlay, *The Database Hacker's Handbook: Defending Database Servers*. Wiley, Indianapolis, IN, 2005.
- [7] D. Litchfield, *The Oracle Hacker's Handbook: Hacking and Defending Oracle*. Indianapolis, IN: Wiley, 2007.
- [8] RIT Online Learning, Blended Courses. Available:
<http://online.rit.edu/faculty/blended/>.

Roundtable Discussion: Forensic Education

Fabio R. Auffant II
*Technical Lieutenant,
Computer Crime Unit, NYS Police*

Cristian Balan
*Program Director, Computer and Digital
Forensics Program, Champlain College*

Sean Smith
*Technical Resource Attorney
NY Prosecutors Training Institute*

THE field of computer and digital forensics is changing rapidly and our dependence on computers and network is increasing. Techniques from computer and digital forensics are being used not only for investigating crime, but also for auditing systems as well as for recovery of lost data. Computer and digital forensics involves data not only from computers, but also from servers, networks, and mobile devices. The needs of the public sector workforce are growing as the demand for such expertise increases within existing IT departments and new forensics divisions are created in agencies. However, they are competing with the private sector, which often lure prospective employees with better salaries. Knowledge of computer and digital forensics has become a necessary component of any IT specialist, but due to the changing environment, it is also important to adapt by continuing to learn new tools and techniques.

Back by popular demand from last year, this round-table features a panel of experts who will discuss the challenges faced by educators/trainers, law enforcement, and prosecution in terms of training, retraining, and retaining a computer and digital forensics capable workforce. It will also cover novel ways to ensure continuous training to security and forensics professionals. The panelists at the round-table come from law enforcement, prosecution and academia and each brings their unique perspectives to the discussion.

AUTHOR BIOGRAPHIES

Fabio R. Auffant II

Technical Lieutenant, New York State Police, Computer Crime Unit
FAuffant@troopers.state.ny.us

Fabio R. Auffant II has been employed by the New York State Police for the past 23 years. He is a Technical Lieutenant in the Computer Crime Unit and Manager of the Computer Forensic Laboratory located in the Forensic Investigation Center in Albany, NY. He has received extensive computer forensics training, holds several certifications in Computer and Digital Forensics; he has conducted forensic examinations and data analysis in hundreds of investigations, as well as testified extensively throughout the State. T/Lt. Auffant is a member of several professional organizations such as, High Technology Crime Investigation Association (HTCIA), International Association of Computer Investigative Specialists (IACIS), Institute of Computer Forensic Professionals (ICFP), and InfraGard. He has provided training and lectured to government and law enforcement personnel in the field of Digital and Computer Forensics, as well as academic institutions such as John Jay College Criminal Justice School, University of Albany Business School and NY Prosecutors Training Institute Summer College. T/Lt. Auffant is an adjunct professor at Columbia Greene Community College in the Computer Security/Forensics degree program and is the chairperson of the NY State Technical Working Group on Digital & Multimedia Evidence.

Cristian Balan

Program Director, Computer and Digital Forensics Program, Champlain College
balan@champlain.edu

Professor Cristian Balan is the Program Director of Computer and Digital Forensics Program at Champlain College in Burlington, VT. He has extensive consulting experience working with the law enforcement community on both the system administration and information security. He is an active member of the Burlington Chapter of Infragard, and FBI sponsored organization, and is the Chief of the Vermont Army National Guard Computer Network Defense Team. CPT Balan and his team respond to Cyber incidents on the VT Army National Guard computer networks and the larger US Army network. CPT Balan is a National Guardsman with 25 years of experience with the last 8 years spent in the Information Assurance field. CPT Balan holds DOD Certification in Information Assurance Level III both technical and management. Professor Balan holds the CISSP Certification from the International Information Systems Security Certification Consortium, Inc. [(ISC)²] and the Certified Hacking Forensic Investigator designation from the EC-Council. He is the owner and managing consultant of NY Computer Networks, a 5 year old consulting firm specializing in managing cyber risk for a wide range of clientele in both the public and private sector. Professor Balan invites his students to work with him on vulnerability assessments and consulting for government organizations and non-profits that cannot otherwise afford the services of a security expert. Professor Balan came to Champlain College in the summer of 2007 with a great deal of teaching experience at both the undergraduate and graduate level. He held the position on Distance Learning Coordinator at several colleges to include SUNY at Plattsburgh, SUNY at Potsdam and Clinton Community College. Professor Balan believes in teaching Digital Forensics using a great deal of hands –on and lab projects. He actively works with the Digital Forensics Association, a student lead organization which boasts the second largest membership on campus right after the ski club, to create opportunities for students to interact with experts from the field. In 2008 Professor Balan and ten Champlain students attended the NY Cyber Security Conference where they had a chance to meet with Forensic experts, prosecutors and leading scientist in the field.

Kranti Banala

Management Information Systems, University at Buffalo, The State University of New York

Kranti Banala is a graduate student in the Department of Management Science and systems at the State University of New York, Buffalo. Kranti has worked for several years in the area of infrastructure support at General Electric Co in India. His research interests include Information Assurance and Database Systems. He holds a bachelors degree in Mechanical Engineering. He is an Oracle Certified Associate and Six Sigma Green Belt Certified professional.

Jon Blue

Accounting & MIS, Alfred Lerner College of Business & Economics, University of Delaware
bluej@lerner.udel.edu

Jon Blue is currently an Assistant Professor of MIS in the Department of Accounting & MIS in the Alfred Lerner College of Business & Economics at the University of Delaware. He graduated with a Ph.D. in 2006 in Business from Virginia Commonwealth University, a Masters of Business Administration from Santa Clara University and a B.S. in Computer Science and Mathematics from the University of California, Davis. His publications discuss topics such as use of XML/XBRL databases, health management information system strategy and accountability, decision-support systems, and project management.

Stephen F. Bush

Algorithmic Communications Network Theory, GE Global Research Center
bushsf@research.ge.com

Stephen F. Bush (M'01- SM'02) was born in Long Beach, CA. He received a B.S. in electrical and computer engineering from Carnegie Mellon University, Pittsburgh, PA in 1985, a MS in computer science from Cleveland State University, Cleveland, OH, in 1987, and a PhD in electrical engineering from the University of Kansas, Lawrence, KS in 1997.

He is a researcher in algorithmic communications network theory at the GE Global Research Center where he explores novel concepts in complexity and algorithmic information theory for applications ranging from network management and wireless ad-hoc networking to RNA sequence analysis and novel concepts in nanotechnology-based networking.

Jeffrey Carr

Principal, GreyLogic
jeffreyc@greylogic.us

Jeffrey Carr is a cyber intelligence expert who writes the IntelFusion blog and specializes in the investigation of cyber attacks against governments and infrastructures by State and Non-State hackers. His work has been quoted in The New York Times, The Washington Post, The Guardian, BusinessWeek, WMD Insights, The Industry Standard, and InfoSecurity News. His book, Inside Cyber Warfare, will be published by O'Reilly Media in late 2009.

Mr. Carr is also the Principal Investigator for Project Grey Goose, an Open Source intelligence investigation into the Russian cyber attacks on Georgia, the Indian Eastern Railway Website defacement and the Israeli-Palestine war in 2008 and 2009.

Gurpreet Dhillon

Virginia Commonwealth University
gdhillon@vcu.edu

Dr. Gurpreet Dhillon is Professor of Information Systems in the School of Business, Virginia Commonwealth University, Richmond, USA. He holds a Ph.D. from the London School of Economics and Political Science, UK. His research interests include management of information security, ethical and legal implications of information technology. Gurpreet has published over 100 research manuscripts in some of the leading journals in the field. He has also authored six books including Principles of Information Systems Security: text and cases (John Wiley, 2007). He is also the Editor-in-Chief of the Journal of Information System Security.

Manish Gupta

M&T Bank Corporation, Buffalo, NY
mgupta3@buffalo.edu

Manish is currently an executive in M&T Bank Corporation, Buffalo, NY, USA and also adjunct instructor/professor (Fall 2007) at State University of New York at Buffalo. He received his bachelor's degree in mechanical engineering from Institute of Engineering and Technology, Lucknow, India in 1998 and an MBA in Information Systems from State University of New York, Buffalo in 2003. He is also a Ph.D. candidate at State University of New York, Buffalo. With more than a decade of experience in information systems, policies and technologies, he has published 3 books in the area of information security, ethics and assurance including Managing information Assurance in Financial Services (publisher: Idea Group Inc.). He serves in editorial boards of International Journal of Electronic banking and International Journal of Liability and Scientific Enquiry (IJLSE) and has served in program committees of several international conferences. He holds several professional designations including CISSP, CISA, CISM, ISSPCS and PMP. He has also received advanced certificates in information assurance (SUNY, Buffalo), IT Benchmarking (Stanford University) and cyber law (Asian School of Cyber Law).

Mohammad Iftekhar Husain

Computer Science and Engineering, University at Buffalo, The State University of New York
imhusain@cse.buffalo.edu

Mohammad Iftekhar Husain is a PhD candidate at the CSE department of University at Buffalo (SUNY-Buffalo). His research interests include but not limited to: Social Network Analysis-based Network Security, Steganography and Economics of Information Security. Mohammad has completed his Masters degree in 2008 from the same department. He has a BS in Computer Science from Yamagata University, Japan. Mohammad has received multiple international scholarships including Rotary Ambassadorial Scholarship and Monbusho Scholarship for academic achievements.

Arun Lakhotia

Center for Advanced Computer Studies
Computer Science, University of Louisiana at Lafayette
arun@louisiana.edu

Dr. Arun Lakhota is a Professor of Computer Science at the Center for Advanced Computer Studies in the University of Louisiana at Lafayette. He is also Director of Software Research Lab, which specializes in malware analysis. His research has led to new ways to counter metamorphic viruses, to deobfuscate code, and to detect new viruses by comparing their code with previously known viruses. Dr. Lakhota teaches a course on malware analysis and has given tutorial on the subject in IEEE Working Conference in Reverse Engineering. He is recipient of the 2004 Louisiana Governor's University Technology Leader of the Year award. He received his Ph.D. from Case Western Reserve University in 1990.

Bin Mai

CIS, College of Business, Northwestern State University
maib@nsula.edu

Dr. Bin Mai is currently an Assistant Professor of CIS in College of Business, Northwestern State University. He obtained his Ph.D. and MS degrees, both in MIS, from University of Texas at Dallas and Texas Tech University, respectively. His main research interest is IS security and information privacy. He currently lives in Natchitoches, LA.

Raphael Perl

Head, Action Against Terrorism Unit
Organization for Security and Cooperation in Europe (OSCE)

Raphael Perl is currently the head of the Action Against Terrorism Unit at the Organization for Security and Co-operation in Europe (OSCE). Prior to assuming his current position, Dr. Perl served as the senior analyst for terrorism policy with the Congressional Research Service of the Library of Congress in Washington, D.C. A graduate of Georgetown University's Foreign Service and Law Schools, he is the author of more than 100 congressional and academic publications on the topics of international terrorism, trends in terrorism, combating terrorism and related subjects. Mr. Perl speaks regularly at academic institutions and governmental policy fora. He also has testified before Congress on terrorism policy issues, including the 9/11 Commission Report recommendations and has addressed the U.N. General Assembly on the role of regional organizations in implementation of its global counter-terrorism strategy. Under his leadership the OSCE Action against Terrorism Unit has redoubled its efforts in combating terrorist use of the Internet and has begun to explore options for comprehensively enhancing cyber security. As an Adjunct Professor at George Washington University, he taught a graduate course on global terrorism. As a fellow at the National Academies, he was project director for an interdisciplinary team involved in assessing terrorist risk. He is actively involved with the U.S. National Research Council and the U.S. National Academy of Engineering, as well as the Russian Academy of Sciences in projects to combat terrorism in Russia. He also serves on a "brain trust" advisory group to the United States National Counter Terrorism Center charged with making recommendations on monitoring terrorist trends.

H. Raghav Rao

School of Management, State University of New York at Buffalo
mgmtrao@buffalo.edu

Dr. Rao has a Ph.D from Purdue University, an M.B.A from Delhi University, and a B.Tech. from the Indian Institute of Technology. His interests are in the areas of management information systems, decision support systems, and expert systems and information assurance. He has chaired sessions at

international conferences and presented numerous papers. He has authored or co-authored more than 100 technical papers, of which more than 60 are published in archival journals. His work has received best paper and best paper runner up awards at AMCIS and ICIS. Dr. Rao has received funding for his research from the National Science Foundation, the Department of Defense and the Canadian Embassy and he has received the University's prestigious Teaching Fellowship. He has also received the Fulbright fellowship in 2004. He is a co-editor of a special issue of The Annals of Operations Research, the Communications of ACM, associate editor of Decision Support Systems, Information Systems Research, and IEEE Transactions in Systems, Man and Cybernetics, and co-Editor-in-Chief of Information Systems Frontiers.

Daniel O. Rice

Technology Solutions Experts, Inc.
dan@danorice.com

Dr. Daniel Rice is the Senior Scientist at Technology Solutions Experts, Inc. (TSE), the developers of the Infantry Warrior Simulation (IWARS) for the US Army and located in Natick, Massachusetts. Dr. Rice conducts research in the areas of constructive simulation, operations, information systems, and computer security. He has presented his work at numerous international forums including the 11th Annual New York State Cyber Security Conference ('08), the 9th INFORMS Telecommunications Conference ('08), the International Conference on Security and Counter Terrorism Issues at Lomonosov Moscow State University ('07), the IEEE Conference on Information Science and Systems (CISS '07), HICSS '06. He has published in leading peer reviewed publications including Decision Support System (DSS), IEEE Transactions SMC, Online Information Review (OIR), and the International Journal of Information and Computer Security (IJICS). Dr. Rice has earned a Ph.D. in Information Systems and MBA in Finance from the University of Connecticut in 2004 and 1998 respectively and a BS in Naval Architecture and Marine Engineering from the United States Coast Guard Academy in 1990.

Sriram Sankaran

Computer Science and Engineering, University at Buffalo, The State University of New York
ss346@cse.buffalo.edu

Sriram Sankaran is currently a Ph.D candidate at the Department of Computer Science and Engineering, University at Buffalo where he completed his Masters degree in 2008. He obtained his B.Tech (Honors) in Computer Science and Engineering from Malaviya National Institute of Technology, Jaipur, INDIA (formerly Regional Engineering College). His research interests include wireless networks and embedded security.

Richard Savacool

Computer Security and Information Assurance, Rochester Institute of Technology
ras6937@rit.edu

Richard Savacool has a B.S. in Computer Engineering Technology from the Rochester Institute of Technology, and is currently working towards his MS degree in Computer Security and Information Assurance from Rochester Institute of Technology. During his seventeen years in the computer industry, Rich Savacool has leveraged his experience in LAN/WAN security, networking, and project management to provide incident response; deploy firewalls and intrusion detection; as well as integrate high availability network solutions for large commercial and government clients. In addition, he holds many industry certifications including the CISSP, CCE, CEH, and SANS GPEN.

Raj Sharman

School of Management, State University of New York at Buffalo
rsharman@buffalo.edu

Dr. Raj Sharman is an assistant professor in the School of Management at the State University of New York, Buffalo, New York. He received his Bachelors degree in Engineering and Masters Degree in Management from the Indian Institute of Technology, Bombay, India. He also received a Masters in Industrial Engineering, and a Doctoral degree in Computer Science from Louisiana State University. His research interests are in the areas of Information Assurance, Disaster Management, and Internet Technologies. He is a recipient of several grants, both internal and external grants in the area of Information Security. His publications appear in peer reviewed journals and international conferences in both the Information Systems and the Computer Science disciplines. Dr. Sharman serves as an associate editor for the Journal of Information Systems Security.

Rajendra K. Raj

Computer Science, Rochester Institute of Technology
rkrics@rit.edu

Rajendra K. Raj is Professor of computer science at the Rochester Institute of Technology. His current interests include data management; secure systems, and reliable distributed systems. Dr. Raj teaches a wide variety of courses from the undergraduate to doctoral levels in core areas of computing and in his areas of interest. Prior to joining RIT, Dr. Raj was a Vice President in information technology at Morgan Stanley & Co, New York, where he helped to manage and develop leading edge global distributed database infrastructures for a variety of financial applications. Dr. Raj previously taught at SUNY Oswego. He received his Ph.D. from the University of Washington, Seattle, where he investigated software composition and reuse in object-oriented programming languages.

Anshuman Singh

Center for Advanced Computer Studies, University of Louisiana at Lafayette
axs6222@cacs.louisiana.edu

Anshuman Singh is a PhD student at Center for Advanced Computer Studies, University of Louisiana at Lafayette. He is studying applications of game theory and abstract interpretation to program obfuscation. He received his MS in Computer Science from University of Louisiana at Lafayette. His research interests include theory of computer viruses, abstract interpretation, program analysis and theory of computation.

Sean Smith

Technical Resource Attorney, New York Prosecutors Training Institute
Sean.Smith@nypti.org

Since 1997 Mr. Smith has been an attorney with the New York Prosecutors Training Institute in Albany, New York. In this capacity, Mr. Smith assists prosecutors with issues arising in felony cases, and assists prosecutors across the country by providing them with valuable information on expert witnesses. In addition, as the Technical Resource Attorney Mr. Smith has provided technical trial assistance in numerous high profile cases by both developing and presenting in-court multi-media presentations. Mr.

Smith regularly consults with prosecutors from across New York on using technology to help present cases to juries.

Michael Sobolewski

Director, SORCER Laboratory
Computer Science, Texas Tech University
sobol@cs.ttu.edu

Dr. M. Sobolewski (<http://sobol.cs.ttu.edu>) joined, as a Professor, the Computer Science Department, Texas Tech University in September 2002. He is the Principal Investigator and Director of the SORCER Laboratory focused on research in network, security, service, exertion- oriented programming, and metacomputing. While at GE Global Research Center he was the chief architect of the Federated Intelligent Product EnviRonment (FIPER) project, and developed other seventeen successful distributed systems for various GE business components. Prior to coming to U.S., during 18-year career with the Polish Academy of Sciences, Warsaw, Poland, he was the head of the Picture Recognition and Processing Department, the head of the Expert Systems Laboratory, and was doing research in the area of knowledge representation, knowledge-based systems, pattern recognition, image processing, neural networks, and graphical interfaces. He has served as visiting professor, lecturer and consultant in Sweden, Finland, Italy, Switzerland, Germany, Hungary, Czechoslovakia, Poland, Russia, and USA. He has over thirty years of experience in the development of large scale computing systems.

Ramalingam Sridhar

Computer Science and Engineering, University at Buffalo, The State University of New York
rsridhar@cse.buffalo.edu

Ramalingam Sridhar received a B.E. (Honors) degree in Electrical and Electronics Engineering from Guindy Engineering College, University of Madras in 1980, MS and PhD in Electrical and Computer Engineering from Washington State University in 1983 and 1987 respectively. Since 1987 he has been with the University at Buffalo, The State University of New York where he is an Associate Professor in the Department of Computer Science and Engineering.

His research interests are in Wireless and sensor network security, pervasive and RFID systems, secure architectures, Embedded technologies, deep submicron VLSI systems, Clocking and Synchronization, and memory circuits & architecture. He was an IEEE CAS Distinguished Lecturer. He has served as Program Chair and General Chair of ASIC/SoC Conference and has served in the editorial board of many journals and technical committee of numerous conferences in wireless systems and VLSI.

Satish Vellanki

SORCER Research Group
Computer Science, Texas Tech University
satish.vellanki@ttu.edu

Satish Vellanki is a graduate student at Texas Tech University, Lubbock, TX working on his thesis "Role-based access control in federated environments". He is with the SORCER Research Group since Fall 2006 and is focused on security in federated metacomputing environments. He received his Bachelor of Technology from Jawaharlal Nehru Technological University, Hyderabad, India where he majored in Computer Science. He interned at Microsoft and Qualcomm previously and is adept at object-oriented programming with Java, C++, and is a Linux expert.

Andrew Walenstein

Center for Advanced Computer Studies

Computer Science, University of Louisiana at Lafayette

walenste@ieee.org

Dr. Andrew Walenstein is an Assistant Professor at the Computer Science Department at the University of Louisiana at Lafayette. He is currently studying methods for malware analysis, and brings in experience from the area of reverse engineering and human-computer interaction. He received his Ph.D. from Simon Fraser University in 2002.

INDEX OF AUTHORS

| | | | |
|----------------------|----------|---------------------|----------|
| Auffant II, Fabio R. | p. 56 | Rao, H. Raghav | p. 39 |
| Balan, Cristian | p. 56 | Rice, Daniel O. | p. 2 |
| Banala, Kranti | p. 40-49 | Sankaran, Sriram | p. 23-28 |
| Blue, Jon | p. 7-15 | Savacool, Richard | p. 50-55 |
| Bush, Stephen F. | p. 36-38 | Sharman, Raj | p. 40-49 |
| Carr, Jeffrey | p. 1 | Raj, Rajendra K. | p. 50-55 |
| Dhillon, Gurpreet | p. 7-15 | Smith, Sean | p. 56 |
| Gupta, Manish | p. 40-49 | Sobolewski, Michael | p. 16-22 |
| Husain, Mohammad I. | p. 23-28 | Singh, Anshuman | p. 30-35 |
| Lakhotia, Arun | p. 30-35 | Sridhar, Ramalingam | p. 23-28 |
| Mai, Bin | p. 30-35 | Vellanki, Satish | p. 16-22 |
| Perl, Raphael | p. 29 | Walenstein, Andrew | p. 30-35 |