DIMACS Center
Rutgers University

Special Focus on Communication Security and Information Privacy

Annual Report

April 2005

Participants who spent 160 hours or more

PI: Fred Roberts, DIMACS

Other Participants

Bill Aiello, University of British Columbia, Vice Chair of the Special Focus on Communication Security and Information Privacy organizing committee.

Ronitt Rubinfeld, MIT, chair of the Special Focus on Communication Security and Information Privacy organizing committee.

Workshop: Electronic Voting -- Theory and Practice
May 26 - 27, 2004

Organizers:
Markus Jakobsson, RSA Laboratories
Ari Juels, RSA Laboratories

Workshop: Security Analysis of Protocols
June 7 - 9, 2004

Organizers:
John Mitchell, Stanford
Ran Canetti, IBM Hawthorne

Working Group: Challenges for Cryptographers in Health Data Privacy
Date: June 30, 2004

Organizer:
Benny Pinkas, HP Labs

Workshop: Usable Privacy and Security Software
July 7 - 8, 2004

Organizers:
Lorrie Cranor, Carnegie Mellon University
Mark Ackerman, University of Michigan
Fabian Monrose, Johns Hopkins University
Andrew Patrick, NRC Canada
Norman Sadeh, Carnegie Mellon University

Working Group: Usable Privacy and Security Software
July 9, 2004

Organizers:

Lorrie Cranor, Carnegie Mellon University
Mark Ackerman, University of Michigan
Fabian Monrose, Johns Hopkins University
Andrew Patrick, NRC Canada
Norman Sadeh, Carnegie Mellon University

Workshop: Cryptography: Theory Meets Practice
Dates: October 14 - 15, 2004

Organizer:
Dan Boneh, Stanford

Workshop: Mobile and Wireless Security
Dates: November 3 - 4, 2004

Organizer:
Bill Arbaugh, University of Maryland

Working Group: Data De-Identification, Combinatorial Optimization, Graph Theory, and the Stat/OR Interface
Dates: November 9 - 10, 2004

Organizers:
Larry Cox, CDC
Brenda Latka, DIMACS
Fred Roberts, DIMACS

Workshop: Theft in E-Commerce: Content, Identity, and Service
Dates: April 14 - 15, 2005

Organizers:
Drew Dean, SRI International
Markus Jakobsson, Indiana University

Workshops to be held during this reporting period:

Workshop: Security of Web Services and E-Commerce
Dates: May 5 - 6, 2005

Organizer:
Brian LaMacchia, Microsoft

Graduate students who have undertaken small research projects under support of the project.

Arati Baliga, RU CS, winter 04/05:
Building robust systems that have fault tolerant and recovery oriented capabilities

Shu Chen, RU CS, winter 04/05:
Hierarchical Sensor Networks

Pandurang Kamat, RU CS, winter 04/05:
Privacy related challenges in sensor networks from several angles

Jaewon Kang, RU CS, summer '04:
Congestion controlling in highly dense sensor networks

Tuan Phan, RU CS, summer '04:
An approach to analyze faults in dependent distributed systems

Constantin Serban, RU CS, summer '04:
Security policies over synchronous communication

Student Visitors as part of the Special Focus:

Danny Harnik, Weizmann Institute, 6/6/04-7/15/04.
Yaron Sella, Hebrew University of Jerusalem, 4/4/04-5/1/04.

Student Writers of Workshop Reports:

Krishnaram Kenthapadi, Stanford University
Margaret McGaley, Computer Science Department, NUI Maynooth
Zhiqiang Yang, Department of Computer Science, Stevens Institute of Technology
Serge Egelman, School of Computer Science, Carnegie Mellon Univerisity
Ponnurangam Kumaraguru, School of Computer Science, Carnegie Mellon Univerisity
Constantin Serban, Department of Computer Science, Rutgers University
Yuan Yuan, Computer Science Department, University of Maryland
Martin Milanic, Rutgers Center for Operations Research, Rutgers University
Gautam Bhanage, Department of Electrical and Computer Engineering, Rutgers University

Other Collaborators

Mark Ackerman, University of Michigan, organizer of the Workshop and Working Group on Usable Privacy and Security Software.

Bill Aiello, University of British Columbia, Vice Chair of the Special Focus on Communication Security and Information Privacy organizing committee.

Bill Arbaugh, University of Maryland, organizer of the Workshop on Mobile and Wireless Security

Dan Boneh, Stanford University, organizer of the Workshop on Cryptography: Theory Meets Practice

Ran Canetti, IBM Hawthorne, organizer of the Workshop on Security Analysis of Protocols.

Larry Cox, CDC, organizer of the Working Group on Privacy / Confidentiality of Health Data and the Working Group on Data De-Identification, Combinatorial Optimization, Graph Theory, and the Stat/OR Interface

Lorrie Cranor, Carnegie Mellon University, organizer of the Workshop and Working Group on Usable Privacy and Security Software

Drew Dean, SRI International, organizer of the Workshop on Theft in E-Commerce: Content, Identity, and Service

Markus Jakobsson, RSA Laboratories, organizer of the Workshop on Electronic Voting -- Theory and Practice and the Workshop on Theft in E-Commerce: Content, Identity, and Service

Ari Juels, RSA Laboratories, organizer of the Workshop on Electronic Voting -- Theory and Practice

Hugo Krawczyk, Technion, member of the Special Focus on Communication Security and Information Privacy organizing committee

Brian LaMacchia, Microsoft, organizer of the Workshop on Security of Web Services and E-Commerce

John Mitchell, Stanford, organizer of the Workshop on Security Analysis of Protocols

Fabian Monrose, Johns Hopkins University, organizer of the Workshop and Working Group on Usable Privacy and Security Software

Andrew Patrick, NRC Canada, organizer of the Workshop and Working Group on Usable Privacy and Security Software

Benny Pinkas, HP Labs, organizer of the Workshop and Working Group on Privacy-Preserving Data Mining

Avi Rubin, AT&T, member of the Special Focus on Communication Security and Information Privacy organizing committee

Ronitt Rubinfeld, MIT, chair of the Special Focus on Communication Security and Information Privacy organizing committee

Norman Sadeh, Carnegie Mellon University, organizer of the Workshop and Working Group on Usable Privacy and Security Software

David Wagner, University of California Berkeley, member of the Special Focus on Communication Security and Information Privacy organizing committee.

Partner Organizations

Telcordia Technologies: Collaborative Research
Partner organization of DIMACS. Individuals from the organization participated in the program planning.

AT&T Labs - Research: Collaborative Research; Personnel Exchanges
Partner organization of DIMACS. Individuals from the organization participated in the program planning and research and workshop/working group organization.

NEC Laboratories America: Collaborative Research; Personnel Exchanges
Partner organization of DIMACS. Individuals from the organization participated in the program planning and research.

Lucent Technologies, Bell Labs: Collaborative Research
Partner organization of DIMACS. Individuals from the organization participated in the program planning.

Princeton University: Collaborative Research
Partner organization of DIMACS. Individuals from the organization participated in the program planning.

Avaya Labs: Collaborative Research
Partner organization of DIMACS. Individuals from the organization participated in the program planning.

HP Labs: Collaborative Research; Personnel Exchanges
Partner organization of DIMACS. Individuals from the organization participated in the program planning and research and workshop/working group organization.

IBM Research: Collaborative Research; Personnel Exchanges
Partner organization of DIMACS. Individuals from the organization participated in the program planning and research and workshop/working group organization.

Microsoft Research: Collaborative Research; Personnel Exchanges
Partner organization of DIMACS. Individuals from the organization participated in the program planning and research and workshop/working group organization.

Stevens Institute of Technology: Collaborative Research; Personnel Exchanges
Partner organization of DIMACS. Individuals from the organization participated in the program planning and research and workshop/working group organization.

Centers for Disease Control and Prevention: Collaborative Research; Personnel Exchanges. Individuals from the organization participated in the program planning and research and workshop/working group organization.

Activities and Findings

Overview

Vitally important aspects of our modern society have become dependent on rapid and secure communication, which is increasingly electronic. The new electronic age offers vast potential for new services and applications, but gives rise to serious new vulnerabilities and security threats. Moreover, many of the most important new applications come at the price of threats to privacy. The “special focus” on Communication Security and Information Privacy, which began in summer 2003, is exploring the new vulnerabilities and threats and new methods for dealing with them.

Within the last decade a tremendous transition has taken place in communications networks. Previously, nearly all communication, whether data, voice or other media, was carried over private networks. Anyone who was not a customer of the network provider was not given physical access to the network. Securing such networks was relatively straightforward. While a great deal of data and media traffic still run over circuit switched or packet switched ATM or Frame Relay private networks, a huge amount and variety of data and media traffic now run over the public Internet, so much so that the Internet is now an important national infrastructure whose integrity is vital to the functioning of our economy, culture, and government. The migration of communication services to the Internet is still very much in progress. This migration brings with it new and complex challenges for maintaining communication security.

There are many factors driving the migration to the Internet. One is universal connectivity. The Internet protocol allows users with many different types of local area network technologies (e.g., Ethernet, and 802.11) to be integrated into a single large network. This allows for a type of positive feedback often referred to as the "network effect." The network grows quickly because the number of users, servers, and devices that are already reachable on the Internet make it very valuable to any new IP device. A second factor is unification. Unlike the circuit switched world for which signaling and data/media were carried by two separate networks, signaling and data/media can both be carried over the Internet. For network providers, migrating their services onto an Internet backbone means that they need only deploy, manage, and control a single network, thereby reducing their cost of providing services. Finally, the ultimate promise of the Internet is as a platform for integrating a variety of services such as voice, instant messaging, mobile presence, multimedia, Web and data services. While these are powerful factors driving the migration to IP communications, they have serious security repercussions. Indeed, securing an extremely large, shared services, packet-based IP network with a large number of administrative domains is a much more complex task than securing segregated/circuit switched networks.

Furthermore, through the collection and dissemination of vast amounts of data, the Internet allows users to take advantage of new functionalities that inherently require new notions of security. For example, new issues of privacy for Internet users and applications are arising due to the multitude of data available online. This new electronic reality and the vast potential for interaction between users and computers give rise to new digital applications and services once thought possibly only in the physical tangible world. This, in turn, creates the need for the invention and implementation of new security and cryptographic techniques. Enabling secure electronic commerce and securing digital rights management are some central examples of the new challenges faced in the security area.

Some of the most exciting progress in the fields of communication security and information privacy has come because of the interconnections of practitioners in these fields with researchers developing relevant methods of theoretical computer science and mathematics. We are exploring these interconnections in order to address some of the fundamental challenges to communication security and information privacy posed by the rapid transition and remarkable growth of new applications in today's communication networks. The project is centered around workshops and research “working groups,” with a tutorial, visitor program, and graduate student program.

The Themes of the Special Focus Include:

- Studying protocol and host vulnerabilities related to Internet communication. Among them are: the weakness or total lack of source authentication for the base protocols in the IP suite, lack of admission control mechanisms, vulnerability of hosts to implementation and configuration errors. What is more, protocol and host vulnerabilities can be exploited in tandem to create serious attacks such as distributed denial of service attacks.

- Securing the protocol layer. The special focus is analyzing a wide range of security issues related to newer technologies such as wireless access at the lower layers of the protocol stack, or Web services at the higher layer of the protocol stack, including issues dealing with ad-hoc trust establishment, secure roaming between overlay networks, the controlled execution of untrusted code, and peer-to-peer connection in pervasive networking scenarios.

- Seamless data movement vs. privacy and property rights. The power of service providers to automatically log and analyze information on site visitors or customers for collection and dissemination is so great that it must be properly managed or else there is a significant potential for abuse. The special focus is examining both violation of property rights and violation of

privacy both in the general context and in more specialized applications such as health care data and electronic voting.

- Cryptography and secure protocols. As technology evolves, cryptography faces the task of developing new security models and techniques such as developing a complete suite of solutions that can handle the concurrency and asynchrony of the Internet and obtaining information from multiple data sets while protecting privacy and confidentiality.

Tutorials, Workshops, and Working Groups During This Reporting Period

Workshop: Electronic Voting -- Theory and Practice
Dates: May 26 - 27, 2004
Location: DIMACS Center, CoRE Building, Rutgers University
Organizers: Markus Jakobsson and Ari Juels, RSA Laboratories
Attendance: 74

To many technologists, electronic voting represents a seemingly simple exercise in system design. In reality, the many requirements it imposes with regard to correctness, anonymity, and availability pose an unusually thorny collection of problems, and the security risks associated with electronic voting, especially remotely over the Internet, are numerous and complex, posing major technological challenges for computer scientists. The problems range from the threat of denial-of-service-attacks to the need for careful selection of techniques to enforce private and correct tallying of ballots. Other possible requirements for electronic voting schemes are resistance to vote buying, defenses against malfunctioning software, viruses, and related problems, audit ability, and the development of user-friendly and universally accessible interfaces.

The goal of the workshop was to bring together and foster an interplay of ideas among researchers and practitioners in different areas of relevance to voting. For example, the workshop investigated prevention of penetration attacks that involve the use of a delivery mechanism to transport a malicious payload to the target host. This could be in the form of a “Trojan horse” or remote control program. It also investigated vulnerabilities of the communication path between the voting client (the devices where a voter votes) and the server (where votes are tallied). Especially in the case of remote voting, the path must be “trusted” and a challenge is to maintain an authenticated communications linkage. Although not specifically a security issue, reliability issues are closely related and were also considered. The workshop considered issues dealing with random hardware and software failures (as opposed to deliberate, intelligent attack). A key difference between voting and electronic commerce is that in the former, one wants to irreversibly sever the link between the ballot and the voter. The workshop discussed audit trails as a way of ensuring this. The workshop also investigated methods for minimizing coercion and fraud, e.g., schemes to allow a voter to vote more than once and only having the last vote count.

This workshop was coordinated with the Special Focus on Computation and the Socio-Economic Sciences.

This workshop followed a successful first WOTE event, organized by David Chaum and Ron Rivest in 2001 at Marconi Conference Center in Tomales Bay, California (http://www.vote.caltech.edu/wote01/). Since that time, a flurry of voting bills has been enacted at the federal and state levels, including most notably the Help America Vote Act (HAVA). Standards development has represented another avenue of reform (e.g., the IEEE Voting Equipment Standards Project 1583), while a grassroots movement (http://www.verifiedvoting.org) has arisen to promote the importance of audit trails as enhancements to trustworthiness.

An extensive report on this activity is given in the **Report on DIMACS Workshop on Electronic Voting – Theory and Practice**, which can be found at http://dimacs.rutgers.edu/Workshops/Voting/e-voting-final.pdf.

Workshop: Security Analysis of Protocols

Dates: June 7 - 9, 2004
Location: DIMACS Center, CoRE Building, Rutgers University
Organizers: John Mitchell, Stanford and Ran Canetti, IBM Hawthorne
Attendance: 88

The analysis of cryptographic protocols is a fundamental and challenging area of network security research. Traditionally, there have been two main approaches. One is the logic approach aimed at developing automated tools for the formal verification of protocols. The other is the computational or complexity-theoretic approach that characterizes protocol security as a set of computational tasks and proves protocol security via reduction to the strength of the underlying cryptographic functions. Although these two lines of work share a common goal, there has been little commonality between them until the last year or two.

The goal of this workshop was to promote work on security analysis of protocols and provide a forum for cooperative research combining the logical and complexity-based approaches.

The workshop included tutorials on the basics of each approach and allowed researchers from both communities to talk about their current work.

The topics of the talks included:

- Analysis methods involving computational complexity
- Game-theoretic approaches
- Methods based on logic and symbolic computation
- Probabilistic methods
- Model checking and symbolic search
- Formal proof systems
- Decision procedures and lower bounds
- Anything else that sounds like a great idea

An extensive report on this activity is given in the **Report on DIMACS Workshop on Security Analysis of Protocols**, which is in preparation.

Working Group: Challenges for Cryptographers in Health Data Privacy

Dates: June 30, 2004
Location: DIMACS Center, CoRE Building, Rutgers University
Organizers: Benny Pinkas, HP Labs
Attendance: 16

This meeting focused on the problem of computing with sensitive data while hiding sensitive information embedded in it, specifically, in the context of health care. One possibly relevant technique is secure computation, where different parties compute some function of their private inputs while hiding any additional information about their inputs. Another technique is publishing “sanitized” versions of

sensitive data, in which some elements are perturbed or suppressed in order to hide sensitive properties. Both "offline" and "online" versions of such techniques may be of interest. The meeting did not discuss the security of transferring data between locations/parties, since this problem has rather straightforward solutions.

Topics for discussion included:

A. Topics related to secure computation:
- A.1. A short introduction to secure computation
- A.2 Identifying functions of interest for healthcare applications
- A.3 Modeling the adversary

B. Topics related to data sanitization
- B.1 A short introduction to data sanitization
- B.2 Definitions of a privacy breach
- B.3 Modeling the adversary

C. Other topics
- C.1. Relation to DRM (Digital Rights Management)
- C.2 Online Query Auditing
- C.3 Post Query Auditing
- C.4 Other Privacy related problems

An extensive report on this activity is given in the **Report on DIMACS Working Group on Challenges for Cryptographers in Health Data Privacy**, which can be found at http://dimacs.rutgers.edu/Workshops/Cryptographers/crypto-health-data-6-04.pdf

Workshop: Usable Privacy and Security Software

Dates: July 7 - 8, 2004
Location: DIMACS Center, CoRE Building, Rutgers University
Organizers: Lorrie Cranor, Carnegie Mellon University; Mark Ackerman, University of Michigan; Fabian Monrose, Johns Hopkins University; Andrew Patrick, NRC Canada; Norman Sadeh, Carnegie Mellon University
Attendance: 79

This workshop and working group meeting were intended to bring together security and privacy experts with human-computer interaction experts to discuss approaches to developing more usable privacy and security software. The workshop sessions on July 7 and July 8 included invited talks and discussion.

The meeting began with a discussion of the challenges, approaches, and mental models, moderated by Lorrie Cranor. Andrew Patrick led a discussion on authentication. On the second day, Lorrie Cranor and Norman Sadeh moderated discussions on privacy, anonymity, and encryption tools, Mark Ackerman moderated the discussion on ubiquitous computing and Fabian Monrose moderated the discussion on administration and access control.

Keynote talks were given by Elizabeth Mynatt, Georgia Institute of Technology on Privacy and Security: Putting People First and Matt Blaze, University of Pennsylvania on Human-Scale Security.

In addition there were talks on the following topics:

Usable Security: Beyond the Interface
HCI Issues in Privacy
Security as Experience and Practice: Supporting Everyday Security
Best Practices for Usable Security In Desktop Software
Some Practical Guidance for Improved Password Usability
Fingerprint Authentication: The User Experience
Authentication for Humans
On User Choice in Graphical Password Schemes
Secure Web Authentication with Mobile Phones
Toward Usable Security
Cryptography and Information Sharing in Civil Society
Anonymity loves company: Usability as a security parameter
Making Security Visible
Techniques for Visual Feedback of Security State
Privacy Analysis for the Casual User Through Bugnosis
Protecting privacy in software agents: Lessons from the PISA project
Architectural issues in distributed, privacy-protecting social networking
Privacy in Instant Messaging
Knowing What You're Doing: A Design Goal for Usable Ubicomp Privacy
Privacy Challenges in Ubiquitous Computing
Semantic Web Technologies to Reconcile Privacy and Context Awareness
Better Tools for Security Administration: Enhancing the Human-Computer Interface with Visualization
Approaches for Designing Flexible Mandatory System Security Policies
Useless Metaphors: Why Specifying Policy is So Hard?
Chameleon: Towards Usable RBAC

The workshop concluded with a discussion of how to best organize another such meeting. Full details of this, along with future research directions and challenges are given in the **Report on Workshop/ Working Group on Usable Privacy and Security Software**, which can be found at http://dimacs.rutgers.edu/Workshops/Tools/dimacsrpt.pdf **.**

Working Group Meeting: Usable Privacy and Security Software

Date: July 9, 2004
Location: DIMACS Center, CoRE Building, Rutgers University
Organizers: Lorrie Cranor, Carnegie Mellon University; Mark Ackerman, University of Michigan; Fabian Monrose, Johns Hopkins University; Andrew Patrick, NRC Canada; Norman Sadeh, Carnegie Mellon University
Attendance: 53

This working group was a follow up to the July 7 and July 8 workshop. The invited participants spent the day identifying important problems, discussing some of the research issues raised during the workshop in more depth, and brainstorming about approaches to future research, collaboration, and more user-centered design of security and privacy software. There was discussion of important research questions, strategies, approaches, related work, research methodologies, and evaluation methodologies.

While many topics were touched on, it is clear that many future research challenges remain. Authentication schemes need to be studied so that a good median between usability and security can be reached. New tools need to be created for system administrators that increase security by allowing them to easily visualize problems. Finally, studies need to be conducted to educate users on more of the

privacy and security issues. This can be accomplished by making consequences more apparent and by creating tools to aid in policy development.

An extensive report on both the workshop and working group is given in the **Report on DIMACS Workshop/Working Group on Usable Privacy and Security Software**, which can be found at http://dimacs.rutgers.edu/Workshops/Tools/dimacsrpt.pdf.

Workshop: Cryptography: Theory Meets Practice

Dates: October 14 - 15, 2004
Location: DIMACS Center, CoRE Building, Rutgers University
Organizer: Dan Boneh, Stanford
Email: dabo@cs.stanford.edu
Attendance: 57

The role of cryptography as a central component in the design, analysis and implementation of secure systems and communications is clear today. The wide applicability of cryptography raises issues ranging from the creation of pure mathematical objects to the detailed engineering specification of complex cryptographic systems. Theoretical analysis and mathematical proof play an essential role in backing the security of cryptographic systems. In contrast to many other engineering areas, applied cryptography cannot use simulations or other empirical methods to "prove" that a given cryptographic construct meets its alleged security properties. It requires a mathematical proof based on a careful modeling of the security objectives of the construct and of the attacker capabilities. This situation gives rise to a challenging role for crypto theory: to provide models and constructions that represent in a satisfactory way the needs of actual cryptographic practice, in particular, the need to come up with relatively simple and efficient constructions while not giving up in the essential role of sound mathematical analysis. As a result of this close relationship between theory and practice in the cryptography and security areas, we have seen in recent years an increased influence of the crypto community in the development of standards and other widely used security systems. This workshop was intended to highlight, expose and encourage work that has a significant theoretical analysis component and, at the same time, has meaningful implications and relevance to practical cryptographic and security schemes. Work that highlights the cryptographic requirements of security systems was solicited as well. The interaction among cryptographic and security experts increased the awareness of the need of sound cryptography as the basis of actual security systems and contributed to a better understanding by the crypto community of the actual needs of practical security systems.

An extensive report on this activity is given in the **Report on DIMACS Workshop on Cryptography: Theory Meets Practice**, which is in preparation.

Workshop: Mobile and Wireless Security

Dates: November 3 - 4, 2004
Location: DIMACS Center, CoRE Building, Rutgers University
Organizer: Bill Arbaugh, University of Maryland
Email: waa@cs.umd.edu
Attendance: 44

The rapid growth of both voice and data wireless communications has resulted in several serious security problems in both the voice and data spaces. Unfortunately, many of the early security mistakes made with wireless voice communications were repeated with data communications, i.e. the use of flawed authentication and confidentiality algorithms. For example, the standards committee for 802.11 left many

of the difficult security issues such as key management and a robust authentication mechanism as open problems. This has led many organizations to use either a permanent fixed cryptographic variable or no encryption with their wireless networks. Since wireless networks provide an adversary a network access point that is beyond the physical security controls of the organization, security can be a problem. Similarly, attacks against WEP, the link-layer security protocol for 802.11 networks can exploit design failures to successfully attack such networks. This workshop focused on addressing the many outstanding issues that remain in wireless cellular and WLAN networking such as (but not limited to): Management and monitoring; ad-hoc trust establishment; secure roaming between overlay networks; availability and denial of service mitigation; and network and link layer security protocols. We sought to extend work on ad hoc networking from a non-adversarial setting, assuming a trusted environment, to a more realistic setting in which an adversary may attempt to disrupt communication. We investigated a variety of approaches to securing ad hoc networks, in particular ways to take advantage of their inherent redundancy (multiple routes between nodes), replication, and new cryptographic schemes such as threshold cryptography.

An extensive report on this activity is given in the **Report on DIMACS Workshop on Mobile and Wireless Security**, which can be found at
http://dimacs.rutgers.edu/Workshops/MobileWireless/dimacs-rpt-wireless-wrkshp5-nov5.pdf.

Working Group: Data De-Identification, Combinatorial Optimization, Graph Theory, and the Stat/OR Interface

Dates: November 9 - 10, 2004
Location: DIMACS Center, CoRE Building, Rutgers University
Organizers: Larry Cox, CDC; Brenda Latka, DIMACS; Fred Roberts, DIMACS
Email: lcox@cdc.gov, latka@dimacs.rutgers.edu, froberts@dimacs.rutgers.edu
Attendance: 20

In this meeting we explored problems in combinatorial optimization, graph theory, and the interface between statistics and operations research that arise from issues of data privacy and, more specifically, data de-identification.

This was an informal meeting, aimed at involving those with interests in combinatorial optimization, graph theory and the stat/OR interface in working on those problems that have become very important in applications such as health data privacy, government statistical data, and counter-terrorism. The emphasis was on identifying and working on problems of discrete optimization and on identifying and exploring relevant algorithms. No prior knowledge of the application areas was necessary.

Specific problems of interest discussed/examined from the OR perspective included combinatorial structure of the feasible region defined by a partially specified multi-dimensional table or by linked tables; generating extremal points and statistical samples from a feasible region defined by a system of multi-dimensional tabular constraints; and (near)-optimization of (nonlinear) statistical functions over a system of tabular constraints. These problems recently have been approached from the standpoint of the theory of Grobner bases but the intended focus here was on combinatorial and mathematical programming approaches and their computability.

An extensive report on this activity is given in the **Report on DIMACS Working Group: Data De-Identification, Combinatorial Optimization, Graph Theory, and the Stat/OR Interface**, which is in preparation.

Workshop: Theft in E-Commerce: Content, Identity, and Service

Dates: April 14 - 15, 2005
Location: DIMACS Center, CoRE Building, Rutgers University
Organizers: Drew Dean, SRI International, and Markus Jakobsson, Indiana University
Email: ddean@csl.sri.com, markus@indiana.edu
Attendance: 50

This workshop was focused on Theft in E-Commerce (of content, identity and service). While theft is an old problem, the automated nature of e-commerce introduces new opportunities for traditional forms of theft, as well as entirely new forms of theft. The centrality of computation makes these threats a part of computer security. This is an area of research where we are seeing a lot of activity, and where we believe there is a great potential for valuable research contributions. While the primary interest of the workshop was in defenses against theft, it was also interested in novel attacks and real data about attacks, as the defenders need to know what to defend against. This workshop stimulated such research by bringing together the leaders in this area.

In his evaluation of the workshop, Adam Young provided a summary of some of the highlights.

“Richard Parry, SVP JPMorganChase, lectured on the subject of identity theft. He illuminated problems that I did not even know existed such as the damage caused by the lack of a solid definition of identity theft in the industry. This problem causes funding to be thrown at solutions that do not always address the real problem, and he indicated that the industry is currently operating in a mode akin to "a chicken running with its head cut off." His work experience as a police officer in Hong Kong led to his understanding of how IDs are handled abroad. In China for instance, a citizen will land in jail for 5 years if they carry around a forged national ID card. Richard Parry suggested that the US government may need to assume more control of ID issuance (rather than outsourcing it), and assign stiffer penalties for violations. I agreed wholeheartedly with most of his talk.

One thing I learned at the DIMACS workshop on theft in e-commerce was how many researchers are trying to solve the Phishing problem: 8 out of the 22 talks discussed both proactive and reactive defenses against phishing. The research groups included Univ. of Indiana at Bloomington, Univ. of Arizona, Radix Labs, LECG LLC, and MIT. I was previously unaware of the solution that involved visual changes to the browser to alert users that the current site might be a phishing site. Min Wu from MIT provided a concrete analysis of the effectiveness of such tools.” Adam L. Young, PhD, LECG LLC

An extensive report on this activity is given in the **Report on DIMACS Workshop: Theft in E-Commerce: Content, Identity, and Service**, which is in preparation.

Workshops to be held during this reporting period:

Workshop: Security of Web Services and E-Commerce

Dates: May 5 - 6, 2005
Location: DIMACS Center, CoRE Building, Rutgers University
Organizer: Brian LaMacchia, Microsoft
Email: bal@microsoft.com
Attendance: 37 (Registration is still open for this workshop)

The growth of Web Services, and in particular electronic commerce activities based on them, is quickly being followed by work on Web Services security protocols. While core XML security standards like XMLDSIG, XMLENC and WS-Security have been completed, they only provide the basic building blocks of authentication, integrity protection and confidentiality for Web Services. Additional Web

Services standards and protocols are required to provide higher-order operations such as trust management, delegation, and federation. At the same time, the sharp rise in "phishing" attacks and other forms of on-line fraud simply confirms that all our work on security protocols is for naught if we cannot make it both possible and easy for the average user to discover when a security property has failed during a transaction. This workshop aims to explore these areas as well as other current and future security and privacy challenges for Web Services applications and e-commerce.

An extensive report on this activity will be given in the **Report on DIMACS Workshop on Security of Web Services and E-Commerce**, which will be prepared after the workshop.

Findings

Preventing Spoofing and Establishing Credentials of Web Sites

In spite of the use of standard web security measures, sensitive web sites are being cloned for fraudulent purposes or graphics from such websites are used to present false credentials. This is causing substantial damage to individuals and corporations. Existing approaches to this problem are often inappropriate to non-expert web users and web-spoofing focuses on these naïve users. Amir Herzberg and Ahmad Gbara developed a simple and practical browser UI enhancement that allows secure identification of sites and validation of their credentials, preventing web-spoofing even for naïve users. The trusted credentials area is a fixed part of the browser window that displays only authenticated credentials. This will help users notice the lack of secure logos in spoofed sites.

Many of the participants in the special focus are actively working on problems that they bring with them to the workshops and working groups. They are often able to make major progress toward completion of their work based on the insights that result from their interactions with other workshop participants. Here are examples of such work.

Proving a Flaw Can't Be Corrected

The A-GDH.2 and SA-GDH.2 authenticated group key agreement protocols have been known to be flawed since 2001, a very long time in this field. As Special Focus participant Olivier Pereira and his collaborator Jean-Jacques Quisquater tried to design a fixed version of these protocols; they found that attacks could always be constructed against their candidates. They proved that it is in fact impossible to design a scalable authenticated group key agreement protocol using the technique adopted for the A-GDH protocols. Their proof proceeds by providing a systematic procedure to derive an attack against any A-GDH-type protocol with at least four participants. They also exhibited protocols with two and three participants that they cannot break. This appears to be the first generic insecurity result reported in the literature.

Data Quality and Data Confidentiality

National statistical agencies must fulfill two nearly contradictory missions. On the one hand, they must extract and disseminate useful information derived from sample surveys and censuses. But they must also protect the confidentiality of the data and the privacy of data subjects. Special focus participant Alan Karr and his collaborator Ashish Sanil have developed two formulations that balance data quality and disclosure risk. These formulations can inform the strategies used by agencies to construct microdata releases. The first involves data swapping, a technique for statistical disclosure limitation that protects confidentiality by modifying a fraction of the records in a database by exchanging a subset of attributes

between selected pairs of records. Karr and Sanil provide an explicit quantitative measure of data quality and disclosure risk that allows an optimal release to be identified. The second involves the integration of distributed databases. Many scientific and policy investigations require statistical analyses of data stored in multiple, distributed databases. Absent the ability to integrate the data, techniques can be used from computer science known as secure multi-party computation. Karr and Sanil illustrate this technique by doing a linear regression on horizontally partitioned data.

Among the variety of directions of work initiated as a result of the Special Focus, we also mention just a few examples of "works in progress" that are in their early stages.

Anti-phishing

Much of the spam today is sent by compromised end-user machines, making it untraceable. Most Internet worms exploit publicly known security vulnerabilities and are released after the release of a security patch. This is evident from many of the recent worm attacks on the Internet. For example, Slammer worm exploited Microsoft SQL server vulnerability, Code Red I and II exploited Microsoft IIS server vulnerability, and Nimba went a step further and exploited not just the IIS vulnerability but also the backdoors left open by Code Red. They all targeted a known vulnerability and the release of the patches before the release of the worm failed to provide sufficient defense in securing end-user machines. The damage incurred is usually immense because many users do not know that the patch concerns them. They are not aware that they are running the servers whose vulnerability is exploited by the worm.

Minaxi Gupta and Markus Jakobsson are developing a new anti-phishing direction they plan to pursue as a group with other colleagues. The research in informative and easy-to-use user interfaces would go a long way in preventing end-user machines from becoming phishing bots. In particular, we need user interfaces research to enable end-users to make decisions about what to install and run on their systems at what time. End users need to know in simple understandable terms what's running on their machine, how to uninstall or get rid of it, and how to run it if and when it is needed. This research can be best done by a team of security/networking/systems working with HCI folks because it requires understanding how various applications work on systems and networks, and what kind of security vulnerabilities they face before appropriate user interfaces can be designed.

Access Control Policies

Thu Nguyen, Rutgers University, and his student, Tuan Phan, whose project was supported under this special focus, have been evaluating a framework for enforcing sophisticated access control policies over accesses to an enterprise's server infrastructure. This framework combines a reference monitor running on each server with two trust management systems to enforce policies. Each reference monitor filters client requests in a similar fashion to a firewall, passing requests allowed by the policies in effect through to the server and blocking requests denied by the policies. They demonstrated the power of their framework and its decoupling from application implementations by using it to regulate accesses to a cluster of NFS and SMB servers without changing any client or server implementations. The example policy that they enforced encapsulates several important security principles including delegation, auditing, separation-of-duty, and automatic revocation of rights based on communal state. Measurements show that their framework imposes acceptable overheads when enforcing this policy. One problem with this authentication mechanism is that it relies on the integrity of the client's IP address. If IP spoofing is possible, it could lead to a compromise of the access control mechanism. Thu Nguyen and Tuan Phan plan to solve this problem by integrating their current implementation with IPSec. Beside NFS and SMB file system, they also want to implement their framework in wireless access authentication. That will

allow one to grant wireless access rights to short term visitors without the help of a network administrator.

Books

Amir Herzberg, *Introduction to Secure Communication and Commerce, with Applied Cryptography*, in preparation.

Jelena Mirkovic, Sven Dietrich, David Dittrich, and Peter Reiher, *Internet Denial of Service: Attack and Defense Mechanisms*, Prentice Hall, 2004.

Papers

M. Freedman, K. Nissim, and B. Pinkas, "Efficient Private Matching and Set Intersection," in *Proceedings of Eurocrypt '2004*, Springer-Verlag, LNCS **3027** (2004), 1-19.

L. Cox, J.F. Gonzalez, Jr., and M. Katzoff, "Effects of Rounding Continuous Data Using Specific Rules," to appear in *Proceedings of the ASA Joint Statistical Meetings Survey Research Methods Section*.

L. Cox, J.F. Gonzalez, Jr., and M. Katzoff, "Effects of Grouping Continuous Data on First and Second Distribution Moments," to appear in *Proceedings of the ASA Joint Statistical Meetings Survey Research Methods Section*.

A. Herzberg, "Preventing Spoofing, Spamming and Phishing," in preparation.

A. Herzberg and Ahmad Gbara, "Protecting (even) Naïve Web Users, or: Preventing Spoofing and Establishing Credentials of Web Sites," submitted to ACM CCS 2004..

M. Jakobsson and A. Young, "Distributed Phishing Attacks," submitted to IEEE Conference on Security and Privacy for Emerging Areas in Communication Networks.

Alan F. Karr and Ashish P. Sanil, "Data Quality and Data Confidentiality for Microdata: Implications and Strategies," to appear in *Bulletin of the International Statistical Institute*, 55rd Session.

Ralf Kuesters, Anupam Datta, John Mitchell, and Ajith Ramanathan, "On the Relationships Between Notions of Simulation-Based Security," *Proceedings of Theory of Cryptography: Second Theory of Cryptography Conference*, TCC 2005, Cambridge, MA, February 10-12, 2005.

Andis Kwan, et. al., "Privacy-preserving RFID-based protocol for electronic voting," in preparation.

Rafail Ostrovsky and Shailesh Vaya, "Almost-everywhere Secure Computation", in preparation.

Olivier Pereira and Jean-Jacques Quisquater, "Generic Insecurity of Cliques-Type Authenticated Group Key Agreement Protocols," submitted to *Journal of Computer Security*.

Thu Nguyen and Tuan Phan, "Enforcing Enterprise-wide Access Control Policies over Standard Client-Server Interactions," submitted to the 24th Symposium on Reliable Distributed Systems (SRDS 2005)

Talks

M. Freedman, K. Nissim, and B. Pinkas, “Efficient Private Matching and Set Intersection,” Eurocrypt 2004 conference at Interlaken, Switzerland, 2-6 May 2004.

J.F. Gonzalez, L. Cox, Kim, and M. Katzoff, “Effects of Rounding Continuous Data Using Specific Rules,” The American Statistical Association Joint Statistical Meetings (JSM 2004), *Statistics as a Unified Discipline*, Toronto, Canada, August 8-12, 2004.

J.F. Gonzalez, L. Cox, Kim, and M. Katzoff, “Effects of Grouping Continuous Data on First and Second Distribution Moments,” The American Statistical Association Joint Statistical Meetings (JSM 2004), *Statistics as a Unified Discipline*, Toronto, Canada, August 8-12, 2004.

S. Wiedenbeck, J. Waters, J-C. Birget, A. Broditskiy, and N. Memon, **“**Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice,” Symposium On Usable Privacy and Security Carnegie Mellon University, Pittsburgh, PA, July 7, 2005.

S.L. Garfinkel and R.C. Miller, “The Johnny 2 Standardized Secure Messaging Scenario,” Symposium On Usable Privacy and Security Carnegie Mellon University, Pittsburgh, PA, July 7, 2005.

R. DePaula, X. Ding, P. Dourish, K. Nies, B. Pillet, D. Redmiles, J. Ren, J. Rode, and R.S. Filho, “Two Experiences Designing for Effective Security,” Symposium On Usable Privacy and Security Carnegie Mellon University, Pittsburgh, PA, July 7, 2005.

C. Brodie, C-M. Karat, J. Karat, and J. Feng, **“**Usable Security and Privacy: A Case Study of Developing Privacy Management Tools,” Symposium On Usable Privacy and Security Carnegie Mellon University, Pittsburgh, PA, July 7, 2005.

N.S. Good, R. Dhamija, J. Grossklags, D. Thaw, S. Aronowitz, D. Mulligan, and J. Konstan, “User Study of Privacy, Notice and Spyware,” Symposium On Usable Privacy and Security Carnegie Mellon University, Pittsburgh, PA, July 7, 2005.

G. Iachello, I. Smith, S. Consolvo, M. Chen, and G.D. Abowd, “Developing Privacy Guidelines for Social Location Disclosure Applications and Services,” Symposium On Usable Privacy and Security Carnegie Mellon University, Pittsburgh, PA, July 7, 2005.

R. Dhamija and J.D. Tygar, “Dynamic Security Skins: Design of a Mozilla Browser Extension to Prevent Phishing Attacks,” Symposium On Usable Privacy and Security Carnegie Mellon University, Pittsburgh, PA, July 8, 2005.

P. DiGioia and P. Dourish, “Social Navigation as a Model for Usable Security,” Symposium On Usable Privacy and Security, Carnegie Mellon University, Pittsburgh, PA, July 8, 2005.

J.I. Hong, “User Interface Design, Prototyping, and Evaluation,” Carnegie Mellon University Symposium On Usable Privacy and Security, Carnegie Mellon University, Pittsburgh, PA, July 6, 2005.

S. Garfinkel, “Introduction to Computer Security and Privacy,” MIT Symposium On Usable Privacy and Security, Carnegie Mellon University, Pittsburgh, PA, July 6, 2005.

A. Karr, "Regression on Distributed Databases via Secure Multi-Party Computation,"ENAR Spring Meeting, Austin, TX, March 2005

R. Kuesters, Anupam Datta, John Mitchell, and Ajith Ramanathan, “On the Relationships Between Notions of Simulation-Based Security,” *Theory of Cryptography: Second Theory of Cryptography Conference*, TCC 2005, Cambridge, MA, February 10-12, 2005.

R. Peralta Plenary speaker: "Electronic voting in the US: where we are and how we got here", Collaborative Electronic Commerce Technology and Research Conference (LatAm 2004). Chile.

R. Peralta, "Multiplicative complexity, fractals, and applications to electronic commerce", invited talk, Tokyo Institute of Technology, 2004.

R. Peralta, "Dark Encounter Computations", invited talk, NTT Yokosuka Research Park, Japan, 2004.

R. Peralta, “Under-specification of crypto-protocols: a recipe for disaster,” invited talk, NATO's Advanced Research Workshop on Verification of Infinite-State Systems with Applications to Security, (VISSAS 2005), March 21, 2005, Romania.

Main website

http://dimacs.rutgers.edu/SpecialYears/2003_CSIP/

Other Specific Products

Web pages

DIMACS Workshop on Electronic Voting -- Theory and Practice
http://dimacs.rutgers.edu/Workshops/Voting/

DIMACS Workshop on Security Analysis of Protocols
http://dimacs.rutgers.edu/Workshops/Protocols/

DIMACS Workshop on Mobile and Wireless Security
http://dimacs.rutgers.edu/Workshops/MobileWireless/

DIMACS Workshop on Usable Privacy and Security Software
http://dimacs.rutgers.edu/Workshops/Tools/

DIMACS Working Group on Usable Privacy and Security Software
http://dimacs.rutgers.edu/Workshops/WGTools/

DIMACS Workshop on Cryptography: Theory Meets Practice
http://dimacs.rutgers.edu/Workshops/Practice/

DIMACS Workshop on Mobile and Wireless Security
http://dimacs.rutgers.edu/Workshops/MobileWireless/

DIMACS Working Group on Data De-Identification, Combinatorial Optimization, Graph Theory, and the Stat/OR Interface
http://dimacs.rutgers.edu/Workshops/Stat/

DIMACS Workshop on Theft in E-Commerce: Content, Identity, and Service
http://dimacs.rutgers.edu/Workshops/Intellectual/

DIMACS Workshop on Security of Web Services and E-Commerce
http://dimacs.rutgers.edu/Workshops/Commerce/

Reports

Report on DIMACS/PORTIA Workshop and Working Group on Privacy-Preserving Data Mining
Report Authors: Geetha Jagannathan, Department of Computer Science, SUNY at Stony Brook and Hong Jiang, Department of Computer Science, Yale University
http://dimacs.rutgers.edu/Workshops/Privacy/dimacs-report-crypto-workshop5-Jan18.pdf

Report on DIMACS Workshop on Electronic Voting – Theory and Practice
Report Author: Margaret McGaley, Computer Science Department, NUI Maynooth
http://dimacs.rutgers.edu/Workshops/Voting/e-voting-final.pdf

Report on Workshop on Security Analysis of Protocols
Report Author: Zhiqiang Yang, Department of Computer Science, Stevens Institute of Technology
In preparation.

Report on DIMACS Working Group on Challenges for Cryptographers in Health Data Privacy
Report Author: Krishnaram Kenthapadi, Department of Computer Science, Stanford University
http://dimacs.rutgers.edu/Workshops/Cryptographers/crypto-health-data-6-04.pdf

Report on Workshop/Working Group on Usable Privacy and Security Software
Report Authors: Serge Egelman and Ponnurangam Kumaraguru, School of Computer Science, Carnegie Mellon University
http://dimacs.rutgers.edu/Workshops/Tools/dimacsrpt.pdf

Report on Workshop on Cryptography: Theory Meets Practice
Report Author: Constantin Serban, Department of Computer Science, Rutgers University
In preparation.

Report on Workshop on Mobile and Wireless Security
Report Author: Yuan Yuan, Computer Science Department, University of Maryland.
http://dimacs.rutgers.edu/Workshops/MobileWireless/dimacs-rpt-wireless-wrkshp5-nov5.pdf

Report on Working Group on Data De-Identification, Combinatorial Optimization, Graph Theory, and the Stat/OR Interface
Report Author: Martin Milanic, Rutgers Center for Operations Research, Rutgers University
In preparation.

Report on Workshop on Theft in E-Commerce: Content, Identity, and Service
Report Author: Gautam Bhanage, Department of Electrical and Computer Engineering, Rutgers University
In preparation.

Report on Workshop on Security of Web Services and E-Commerce

Report Author: Gautam Bhanage, Department of Electrical and Computer Engineering, Rutgers University
In preparation.

Contributions

Contributions within Discipline

The "discipline" of this project is computer science, broadly speaking, with related areas of mathematics, statistics and electrical engineering. The main contribution of this project at this stage is twofold.

1. Each of the activities has contributed to the explicit description of a myriad of open questions and research challenges. These are discussed in great detail in the individual workshop reports.
2. The interactions among the participants have already led to new research collaborations and potential collaborations as well as new research directions for existing research groups. See sections on Activities, Findings, and Contributions to Human Resource Development.

Additional results of the project are books, new conferences, presentations at professional meetings, new courses and units of courses by participants back on their own campuses, and the development of research directions for graduate students and new research directions for researchers.

The Workshop on Usable Privacy and Security Software has led to the establishment of a Symposium on Usable Privacy and Security (SOUPS) - see http://cups.cs.cmu.edu/soups/. The first Symposium on Usable Privacy and Security (SOUPS) will be held July 6-8, 2005 at Carnegie Mellon University in Pittsburgh, PA. This symposium will bring together an interdisciplinary group of researchers and practitioners in human computer interaction, security, and privacy. The program will feature refereed papers, tutorials, a poster session, panels and invited talks, and discussion sessions. SOUPS is being organized by the CMU Usable Privacy and Security Laboratory (CUPS), with funding provided by Carnegie Mellon CyLab.

The Working Group: Challenges for Cryptographers in Health Data Privacy which met on June 30, 2004 served as an impetus for the project "Data Confidentiality, Data Quality and Data Integration for Federal Databases: Foundations to Software Prototypes" (IIS-0131884). The lead institution for this project is the National Institute of Statistical Sciences (NISS). This working group and the subsequent project led to the development of new methods for (among other things)
- Releases of conditional distributions (tables in which rows sum to one, for example).
- Secure analysis of distributed databases without data integration, using secure multi-party computation.
- Regression servers, which disseminate statistical analyses of data rather than data themselves.
Five postdoctoral fellows and six graduate students are engaged in research that was begun at NISS.

We have received very positive responses to the Special Focus. Some examples are:

"I attended the DIMACS Symposium on Usable Privacy and Security in the summer of 2004 and found it one of the best conferences I had participated in the intersection of privacy, security, and HCI. Your support of this conference allowed many key people to come together and talk and to actually begin a professional community for this emerging domain. I cannot thank you enough for the ideas, social network connections and discussions that I experienced as part of the event." Clare-Marie Karat,IBM TJ Watson Research Center

“Prof. Jakobsson and I have changed our paper on distributed phishing attacks as a result of some of the feedback we received from the DIMACS participants. This paper is currently in submission to the IEEE Conference on Security and Privacy for Emerging Areas in Communication Networks.” Adam Young

Markus Jakobsson, Indiana University, the organizer of the workshop on E-Commerce, noted that the workshop had led to new collaborations, new research ideas, and identification of new problem areas in anti-phishing. The workshop “brought people together in phishing to talk to each other. That's the first such meeting that I know of (researchers focusing on phishing).” Markus Jakobsson

“I attended two DIMACS workshops until now, and was very happy for it both times. They have been excellent opportunities for discussing ongoing works with other researchers in my field, probably for two main reasons:

- The number of attendees was relatively small, but counted a lot of very interesting people
- The duration of the talk allowed presenting works in more details than during large and regular conferences, allowing me to better understand research areas related to mine.

The discussions I had during the last workshop (DIMACS Workshop on Security Analysis of Protocols) allowed me to improve previous results, notably those presented in the paper "Generic Insecurity of Cliques-Type Authenticated Group Key Agreement Protocols" I submitted to the Journal of Computer Security.” Olivier Pereira

“With Dr. Juan Garay from Lucent and a student of mine we started a research direction that is leading to a new and exciting results in the area of secure Multi-Party Computation. I expect our research will yield a paper in this area. It would be impossible without my initial visit to DIMACS.” Rafail Ostrovsky, UCLA

“At my workshop and working group on privacy-preserving data mining, attendees Hillol Kargupta (a data mining researcher) and Poorvi Vora (an information theorist) met for the first time, and put together for the working group a brief 5-minute presentation on some very preliminary ideas they had. Although they have not yet continued towards a research collaboration, they have continued their professional relations (for example, Vora reviewed a paper for Kargupta.” Rebecca N. Wright

Sven Dietrich, CERT Research - Software Engineering Institute, reported that new collaborations resulting from the Special Focus led to the book **Internet Denial of Service: Attack and Defense Mechanisms** with co-authors Jelena Mirkovic, David Dittrich, and Peter Reiher. It was published by Prentice Hall in December 2004. The impact of this book on the discipline is documented in its reviews, such as the following.

“There are obviously a multitude of ways an attacker can take your site down. One way is via a denial of service attack. There's a new book out that covers just that attack in great detail: Internet Denial Of Service - Attack and Defense Mechanisms by Jelena Mirkovic, Sven Dietrich, David Dittrich, and Peter Reiher (Prentice Hall).

The book covers (in deep detail) how bot or zombie networks are developed and utilized to launch these types of attacks. Walking away from this book, you don't get a warm, fuzzy feeling about the current situation. Regardless of what steps you take, there is no current sure-fire method for defending these attacks. But by reading Internet Denial of Service, you'll be far more prepared to understand what's going on and what realistic options do exist. Better yet, it also gives you the steps you need to take to prepare your site for this type of incursion beforehand. If you've mapped out your plan ahead of time, you can definitely minimize (to some extent) the damage that can occur.

This is a good read for any security professional tasked with security and availability of an organizational website. Reading this now could save your job later" Thomas Duff, Portland, OR, February 5, 2005

Contributions to Other Disciplines

Many of the problems analyzed in this Special Focus involve issues of law, ethics, or the social sciences. Of particular note is the workshop on electronic voting. It was jointly sponsored by the DIMACS Special Focus on Computation and the Socio-Economic Sciences.

Contributions Beyond Science and Engineering

In a very real sense, this project's most significant contributions are beyond science and engineering. The computer science, mathematics, and statistics of this project are motivated by vitally important problems in our modern society. Our society has become dependent on rapid and secure communication, which is increasingly electronic. The new electronic age offers vast potential for new services and applications, but gives rise to serious new vulnerabilities and security threats. Moreover, many of the most important new applications come at the price of threats to privacy. Within the last decade a tremendous transition has taken place in communications networks. A huge amount and variety of data and media traffic now run over the public Internet, so much so that the Internet is now an important national infrastructure whose integrity is vital to the functioning of our economy, culture, and government. The migration of communication services to the Internet brings with it new and complex challenges for maintaining communication security. Furthermore, through the collection and dissemination of vast amounts of data, the Internet allows users to take advantage of new functionalities that inherently require new notions of security. For example, new issues of privacy for Internet users and applications are arising due to the multitude of data available online. This new electronic reality and the vast potential for interaction between users and computers give rise to new digital applications and services once thought possible only in the physical tangible world. This, in turn, creates the need for the invention and implementation of new security and cryptographic techniques. Enabling secure electronic commerce and securing digital rights management are some central examples of the new challenges faced in the security area.

The activities in this project have created a dialogue among the principal players protecting against Internet attacks, conforming to new laws safeguarding health data privacy, and enabling collaborative research using privacy protected data. Lawyers, epidemiologists, cryptographers, and statisticians are sharing their areas of expertise to define the problems and the approach to their solutions. Private sector Internet service providers are sharing information and data with computer scientists and statisticians to understand the nature of past Internet attacks and forecast and protect against future attacks.

The special focus workshop on Electronic Voting -- Theory and Practice in May 2004 brought together researchers and practitioners in several different areas of relevance to voting, creating a lively interplay of ideas. One of the outcomes of the meeting (and its predecessor called WOTE) was a new organization of members of the technical community to establish specific performance rating guidelines for voting systems. Voting Systems Performance Rating (VSPR) is expected to be launched in December 2004. VSPR will greatly improve the quality of our election systems by providing objective measures of voting system performance, thus encouraging competition in the marketplace to produce systems with the highest rankings. Features of voting systems will be rated much as automobile safety and fuel efficiency are now. A set of well-defined properties would encourage the development and commercialization of better voting systems, especially when combined with objective ways to measure performance with respect to those properties. The overall result would then resemble the quantitative federal ratings for automobiles, where features such as vehicle safety and fuel efficiency form a basis for *Consumer Reports*-

style comparative tables. This also meets the request to the technical community of the U.S. Federal Election Assistance Commission (EAC) for help in defining standards.

Rene Peralta had this to say about the influence of the E-voting workshop. “The topic is of current relevance to an ongoing national debate. I continue to participate in this debate. There are many open problems and research ideas (and very little funding to pursue these matters). My participation in the DIMACS workshop did lead to new contacts and discussions which are ongoing.”

Contributions to Human Resources Development

Graduate students have authored reports for each of the program activities. To produce the reports, the students engaged in significant interaction with the organizers and the speakers, making contacts that would almost surely not have developed otherwise. Both graduate students and undergraduates have been given the opportunity to make presentations. The following are typical reactions of Ph.D. students participating in the special focus.

“Thank you for arranging the DIMACS workshop. My first attendance at DIMACS was last year. Since then, I visited 4 DIMACS workshop under the auspice of Communication Security and Information Privacy program, 3 in summer 2004 and 1 in April 2005. My advisor, Prof Michael Anshel, introduced me to the Electronic Voting workshop last summer. Since then, I signed up for the workshops: Security Analysis of Protocols, Usable Privacy and Security Software, and Theft in E-Commerce. Each of the workshops has a good mix of the social and technical aspects of information security. In addition to learning about the frontier and direction of the research field, the best part for me is that I talk in person to the researchers and practitioners whose names I read on academic papers. I found my research dissertation topic and explored new ways to conduct electronic voting. My research interest is how to protect personal privacy and digital intellectual property in a ubiquitous and distributed computing environment. My dissertation is tentatively titled ‘Privacy protocol for electronic voting.’ Recently, I have been experimenting with a new class of cryptographic primitive. The workshops shed light on some concrete areas that can benefit from these seemingly experimental mathematical structures and respective algorithms. Right now, I am just putting my proposal together.” Andis Kwan, Graduate Center and Baruch College

“Before attending the workshop last year, I was generally interested in the area of database privacy. My area of research is cryptography, and I worked as a database consultant helping to build data warehouse applications for large corporations before I became a graduate student. The conference was very helpful in providing me with insight into the current work in the area and how to think about the problems not just from a security perspective, but also from a philosophical and practical perspective. Recently the security and database groups here have begun some joint work on these problems and are hoping to bring them to publication soon.” Scott Russell, Ph.D. student, Dept. of Computer Science, Boston University

The special focus activities also influence the teaching and course development work of the participants. Some examples are the following:

“I got a good introduction to electronic voting and its research problems. Since the workshop, I used some of the materials from the workshop in designing students' projects for an introduction CIS class at Baruch College. Many sophomore students got a kick out of the pro and con of electronic voting, the stakes involved. A recent workshop of Identity Theft on Ecommerce has also provided good reference points for sophomore students who write research summaries on the current social and technological issues. My side interest on computing science education is that spreading the latest research and raising students' awareness on what's hot and what's not can ultimately draw some undecided students to major in CIS or mathematical science. Having spent a few years in the IT industry and teaching in CUNY for 4 years, I

think of an educator's perspective, 'how does one get students involved in CIS earlier?' Our computing discipline has not presented the best argument to attract, involve and retain able and outstanding undergraduate students. Our enrollment in CIS suffers. DIMACS's interdisciplinary focus on Computation and the Socio-Economic Sciences and Communication Security and Information Privacy has been an excellent exception." Andis Kwan, Graduate Center and Baruch College

"I include e-voting as a problem area when I teach cryptology courses." Rene Peralta, Yale University

The influence of the Special Focus is often felt for years after the participant was at DIMACS. For example Michael Olan, Stockton College, is working to add an Information Assurance emphasis to their Computer Science curriculum. The tutorial he attended as part of the Special Focus was helpful to him "to get ideas about specific security topics that are important. Also, it was valuable for the contacts I made there, specifically with Rebecca Wright who provided valuable information about a proposed computer security undergraduate major at Stevens." Michael Olan, Stockton College

Here is a brief description of Stockton College's new emphasis:

The extensive dependence on computers and networks by individuals, industry and government organizations has produced a critical need to make these systems secure and to assure their availability. Consequently, Information Assurance and Security (IAS) has become a rapidly growing high-priority field with excellent career opportunities for researchers, instructors, and practitioners. The CSIS Program at Stockton offers a rich set of courses and experiences to provide students with the foundation for professional employment and graduate level study in IAS. Courses with an Information Assurance and Security focus include:

CSIS	3381	Information Assurance & Security
CSIS	4135	Web Service Engineering
CSIS	4222	Computer Networks
CSIS	4481	Cryptography & Data Security
CSIS	4485	Software & Security Engineering I
CSIS	4985	Software & Security Engineering Internship I
CSIS	4486	Software & Security Engineering II
CSIS	4986	Software & Security Engineering Internship II
CSIS	4491	Research Topics in Parallel & Distributed Computing

Effects on more established researchers and their students have also been demonstrated. Many new collaborations have begun. Some examples are the following:

"A connection made via DIMACS interactions (between researchers at HP Labs in Princeton and Rutgers grad students) resulted in a fruitful summer internship" Stuart Haber, HP Labs

"I have benefited a lot from attending the workshop on privacy-preserving data mining (March '04). In particular, I was exposed to problems and ideas from the areas of data-mining and statistical data privacy to which I had no previous exposure. While I cannot point at the moment a specific research idea or new collaboration that resulted from this workshop, I feel that it had a very positive general impact on my research." Yuval Ishai, Technion

In addition, the following graduate students have undertaken small research projects under support of the project.

Arati Baliga, RU CS, winter 04/05:
Building robust systems that have fault tolerant and recovery oriented capabilities

Shu Chen, RU CS, winter 04/05:
Hierarchical Sensor Networks

Pandurang Kamat, RU CS, winter 04/05:
Privacy related challenges in sensor networks from several angles

Jaewon Kang, RU CS, summer '04:
Congestion controlling in highly dense sensor networks

Tuan Phan, RU CS, summer '04:
An approach to analyze faults in dependent distributed systems

Constantin Serban, RU CS, summer '04:
Security policies over synchronous communication

The following students were visitors as part of the Special Focus:

Danny Harnik, Weizmann Institute, 6/6/04-7/15/04.
Yaron Sella, Hebrew University of Jerusalem, 4/4/04-5/1/04.