Software Security Workshop

Final Report

April 2004
Participants who spent 160 hours or more

PI: Fred Roberts, DIMACS

DIMACS Workshop on Software Security
January 6-7, 2003

Organizers:
   Gary McGraw (Chair), Cigital
   Ed Felten, Princeton University
   Virgil Gligor, University of Maryland
   Dave Wagner, University of California at Berkeley

Tutorial: Applied Cryptography and Network Security
August 4 - 7, 2003

Organizer:
   Rebecca Wright, Stevens Institute of Technology

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
Partner organization of DIMACS. Individuals from the organization participated in the program planning.

NEC Laboratories America: Collaborative Research
Partner organization of DIMACS. Individuals from the organization participated in the program planning.

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

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

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

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

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

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

Other Collaborators

Ed Felten, Princeton University, organizer of the Workshop on Software Security.

Virgil Gligor, University of Maryland, organizer of the Workshop on Software Security.


Dave Wagner, University of California at Berkeley, organizer of the Workshop on Software Security.

Rebecca Wright, Stevens Institute of Technology, organizer of the Tutorial on Applied Cryptography and Network Security.

Activities

The grant was for a workshop on Software Security. Since funds remained, we were given permission to spend the remaining funds on the DIMACS Special Focus on Communication Security and Information Privacy (See: http://dimacs.rutgers.edu/SpecialYears/2003_CSIP/). We used the remaining funds to partially support the Tutorial on Applied Cryptography and Network Security.

Tutorials and Workshops

DIMACS Workshop on Software Security
Date: January 6 - 7, 2003
Location: DIMACS Center, CoRE Building, Rutgers University
Organizers:
   Gary McGraw (Chair), Cigital
   Ed Felten, Princeton University
   Virgil Gligor, University of Maryland
The security of computer systems and networks has become increasingly limited by the quality and security of the software running on these machines. Researchers have estimated that more than half of all vulnerabilities are due to buffer overruns, an embarrassingly elementary class of bugs. All too often systems are hacked by exploiting software bugs. In short, a central and critical aspect of the security problem is a software problem. How can we deal with this?

The Software Security Workshop explored these issues. The scope of the workshop included security engineering, architecture and implementation risks, security analysis, mobile and malicious code, education and training, and open research issues. In recent years many promising techniques have arisen from connections among computer security, programming languages, and software engineering, and one goal was to bring these communities closer together and crystallize the subfield of software security.

As a result of the workshop, the following areas of interest were defined:

- Reconciling security goals and software goals, software quality management in commercial practice
- Security requirements engineering
- Design for security, software architecture, and architectural analysis
- Security analysis, security testing, and the use of the Common Criteria
- Guiding principles for software security, case studies in design and analysis, and pedagogical approaches to teaching security architecture
- Software security education; educating students and commercial developers
- Auditing software; implementation risks, architectural risks, automated tools, and technology developments (such as code scanning, information flow, and so on)
- Common implementation risks: buffer overflows, race conditions, randomness, authentication systems, access control, applied cryptography, and trust management
- Application security; protecting code post production
- Survivability and penetration resistance, type safety, and dynamic policy enforcement
- Denial-of-service protection for concurrent software
- Penetrate and patch as an approach to securing software
- Code obfuscation and digital content protection
- Malicious code detection and analysis

Some concrete open research problems that were posed include explaining why the software security problem is growing; quantifying, analyzing, and explaining bug/flaw categories; performing cost/benefit analyses to prove that early is good; untangling security software from software security at the requirements stage; exploring how to teach software security most effectively to students and professionals; and inventing and applying measures and metrics.
Talks and discussion in the workshop included:


Discussion - Outrageous Opinions (submitted by attendees);
  - Ed Felten: Nothing we do can improve security
  - Jon Pincus: Stop telling me I should be speaking Esperanto
  - Bill Pugh: It is time to abandon C and C++
  - Ben Laurie: TCPA and Palladium solve capabilities confinement
  - Dave Evans: Protecting bits with atoms (and vices with verses)
  - Steve Bellovin: We can't write secure programs
  - Crispin Cowan: Security and open source: the 2-edged sword

_The Microsoft Trustworthy Computing Initiative from the Inside_, Michael Howard, Microsoft (Author of _Writing Secure Code_)

Discussion - Security Engineering
  - Requirements
  - Architecture and design
  - Coding and testing
  - Manageability

Discussion - On Architecture and Implementation
  - Design risks
  - Implementation risks
  - Technology tradeoffs
  - Experience and expertise

_Coding Excellence: Security as a Side Effect of Good Software_, Brian Kernighan, Princeton University

Discussion - Security Analysis
  - Role of expertise
  - Auditing design
  - Auditing code
  - Security testing

Discussion - Mobile Code and Malicious Code
  - .NET and Java
  - Web services
  - Modern malicious code

_Software Security in the Big Picture: Repeating Ourselves all Over Again_, Dan Geer, @stake

Discussion - Open Research Issues
  - Hard problems

Discussion - Education and Training
  - Academia
  - Industry developers

The intention of this tutorial was two-fold. One, it was a stand-alone condensed course on cryptography and its applications to secure networking and electronic commerce, giving an introduction to some of the fundamental issues in this field. Two, it was designed to provide background knowledge to researchers and graduate students who wished to participate in the DIMACS Special Focus on Communication Security and Information Privacy. The tutorial appears to have been successful in both regards. For example, several graduate student participants have returned or plan to return for later workshops in the special focus and have said that they feel the tutorial helped them to get more out of the workshops than they otherwise would have. Another participant, a professor at an undergraduate college, was attending the tutorials in order to help him with curriculum development in cryptography and security at his college. On a more personal level, due to interactions initiated at the tutorial, the graduate student author of the report on the tutorial is now a Ph.D. student at Stevens Institute of Technology under the guidance of tutorial organizer Rebecca Wright. Each tutorial day included both lectures and problem sessions. The following were the topics of the lectures:

- cryptographic primitives and protocols: symmetric key cryptography, public key cryptography, authentication, and key exchange protocols
- key management and access control: public key infrastructures and trust management
- network security: snooping, spoofing, distributed denial of service attacks, SSL, SSH, IPsec.
- electronic commerce: electronic payments protocols, auctions

There were 41 participants in the tutorial in addition to the 5 lecturers. The academic participants included slightly more students than faculty. About a quarter of the participants were from industry. In addition to the United States participants, there were students and faculty from South Korea and Canada.

The lectures were:

- *Principles of Security and Modern Cryptography, Symmetric Encryption*, Amir Herzberg, Bar-Ilan University
- *Rijndael*, Arta Doci, University of Colorado
- *Hashing*, Amir Herzberg, Bar-Ilan University
- *Message Authentication Codes (MAC)*, Hugo Krawczyk, Technion
- *Public Key Cryptography*, Rebecca Wright, Stevens Institute of Technology
- *Public Key Infrastructures (PKI), Access Control, Trust Management*, Amir Herzberg, Bar-Ilan University
Resilience to Key Exposure: Revocation, Forward Security, Secret Sharing, Threshold and Proactive Security, Amir Herzberg, Bar-Ilan University
Distributed Denial of Service Attacks, Software Security, Angelos Keromytis, Columbia University
Internet Crypto Tools, Amir Herzberg, Bar-Ilan University
Electronic Commerce: Payment Protocols and Fair Exchange, Markus Jakobsson, RSA Laboratories

In addition to the lectures, each day included a one-hour problem session. During these sessions, Nelly Fazio interactively led the tutorial participants in working through a number of exercises, some of which had been handed out the day before. These sessions were designed to make the learning experience more complete by giving participants a chance to try to solve some problems on their own and then see how well they had done.

An extensive report on this activity is given in Report on DIMACS Tutorial on Applied Cryptography and Network Security, which can be found at http://dimacs.rutgers.edu/Workshops/ComputerSecurity/appl-crypt-8-03.pdf

Books


Papers


Amir Herzberg, “Preventing spoofing, spamming and phishing,” in preparation.


Talks


Main website

http://dimacs.rutgers.edu/Workshops/Software/

Other Specific Products

Main Web page with Schedule for Software Security Workshop:

http://www.cigital.com/ssw/presentations.php

Individual Talks in Software Security Workshop:

Gary McGraw, Cigital
The Art and Science of Software Security
http://www.cigital.com/ssw/presentations/gem/

Ed Felten, Princeton University
Nothing we do can improve security
http://www.cigital.com/ssw/presentations/felten/

Dave Evans, University of Virginia
Protecting Bits with Atoms (and Vices with Verses)
http://www.cigital.com/ssw/presentations/evans/
Crispin Cowan, WireX Communications, Inc.
Security and Open Source: the 2-Edged Sword
http://www.cigital.com/ssw/presentations/dimacs_opensource/

Michael Howard, Microsoft
The Microsoft Trustworthy Computing Initiative from the Inside
http://www.cigital.com/ssw/presentations/howard.ppt

Brian Kernighan, Princeton University
Coding Excellence: Security as a Side Effect of Good Software
http://www.cidental.com/ssw/presentations/kernighan/

Dan Geer, @stake
Software Security in the Big Picture
http://www.cidental.com/ssw/presentations/geer/

BREAKOUT: Open Research Issues
http://www.cidental.com/ssw/presentations/landwehr/

Workshop wrap-up
http://www.cidental.com/ssw/presentations/gem_end/

Web pages

**DIMACS Tutorial on Applied Cryptography and Network Security**
http://dimacs.rutgers.edu/Workshops/ComputerSecurity/

*Program for Tutorial:*
http://dimacs.rutgers.edu/Workshops/ComputerSecurity/program.html

Reports

*Workshop on Software Security, January 6 - 7, 2003: Report to the National Science Foundation under Grant 0302708*
Report Date: March 27, 2003
http://dimacs.rutgers.edu/Workshops/Software/SoftSecReport.pdf


*Report on DIMACS Tutorial on Applied Cryptography and Network Security*
Report Author: Geetha Jagannathan, Department of Computer Science, SUNY at Stony Brook
Date of report: December 3, 2003
http://dimacs.rutgers.edu/Workshops/ComputerSecurity/appl-crypt-8-03.pdf
Contributions

Contributions within Discipline

The workshop on Software Security established the language, defined the problems, and set the focus for a field that was in its infancy. It established a new software security paradigm. Since the workshop was held, this field has blossomed. Many books have been published with a substantial portion of them authored by participants in the workshop. See for instance: John Viega and Matt Messier, Secure Programming Cookbook for C and C++, O’Reilly&Associates (July 2003) and Mark Graff and Kenneth VanWyk, Secure Coding: Principles and Practices, O’Reilly & Associates (July, 2003). A best practices report, Processes to Produce Secure Software, has been co-authored by Gary McGraw, co-organizer of the Software Security Workshop and a member of the National Cyber Security Partnership Task Force software process subgroup. This 123 page report to the U.S. Department of Homeland Security, issued April 2, 2004, gives preliminary recommendations for improving software security by addressing security throughout all phases of the software development lifecycle.

Among the key recommendations:

- Awareness & Education: Improving the education of current and future software developers.
- Process Improvement: Adopting software development practices that can measurably reduce software specifications, design, and implementation defects.
- Redesign of Flawed Systems: Encouraging software producers to recognize systems with unacceptable architectures and designs and re-architect and redesign them with proper characteristics for security, using quality software development processes.

The Tutorial on Applied Cryptography and Network Security has provided its participants with an introduction to some of the fundamental issues in this field, giving them the background knowledge to enable them to participate in the Special Focus on Communication Security and Information Privacy.

Contributions outside Discipline

Contributions beyond Science and Engineering

In a very real sense, this project’s most significant contributions are beyond science and engineering. The computer science of this project is motivated by vitally important problems in our modern society. Computer system and network security is increasingly limited by the quality and security of the software running on constituent machines. Researchers estimate that more than half of all vulnerabilities are from buffer overruns,
an embarrassingly elementary class of bugs. Worse, more complex problems such as race conditions and subtle design errors wait in the wings for the buffer overflow’s demise. Software security problems will be with us for years, and hackers will continue to exploit systems via software defects. Clearly, a central and critical aspect of the computer security problem resides in software. Software security—the idea of engineering software that continues to function correctly under malicious attack—is not new, but it is receiving renewed interest as reactive network-based security approaches such as firewalls prove to be ineffective. Unfortunately, today’s software is riddled with both design flaws and implementation bugs, which result in unacceptable security risks. As security researcher and DIMACS workshop participant Steve Bellovin puts it, “any program, no matter how innocuous it seems, can harbor security holes.” This notion is common knowledge, and yet developers, architects, and computer scientists only recently began systematically to study how to build secure software. In fact, the first books on software security and security engineering were published in 2001. With the software security workshop, this field now has focus and direction and the computer science results will have impact in private industry, academia, and government, specifically on homeland security.

Already, several new start up companies have been established to provide software security tools for developers. These include:

- Fortify Software
- Ounce Lab
- Secure Software
- Co-verify
- Reflective

The importance of this rapidly developing field has been recognized in the press, not only in media aimed at those in the field but also the business press. For example, the APRIL 13, 2004 Business Week Online SPECIAL REPORT: A CEO’S GUIDE TO TECHNOLOGY included the article “Info Security ‘from the Ground Up,” about Gary McGraw’s article of that name. Business Week states that “With more threats and stricter laws, being ‘reactive’ isn't enough. Now companies are building safety directly into their systems.”

Another article is “Start-up Takes a Crack at Blocking Hackers,” by Matt Hines, CNET News.com, April 6, 2004. Hines informs his readers about “A Silicon Valley start-up launched on Tuesday with the goal of helping software companies shut out hackers. The Menlo Park, Calif.-based company, Fortify Software, is offering a set of tools designed to test software for potential flaws, while products are still being built. The tools allow companies to examine the underlying code programmers write more closely, cutting down on the likelihood of security weaknesses, according to Fortify.”

Contributions to Human Resources Development

The following is a typical reaction of a teaching faculty member participating in the Software Security Workshop.

“I attended the DIMACS workshop on Secure Software in January 2003. I teach at a very small undergraduate only school, so serious research is hard to come by. I did find the course very useful. I took material from the course and incorporated into my lecture notes for both the Introduction to Computer Science course and the Data Structures course. Furthermore, we added an upper-level course in Secure Software that I hope I can teach Spring of 2005. It certainly paid off for me.” - John Slimick, University of Pittsburgh at Bradford, Bradford PA

As stated in the section on Research and Education Activities, as a result of the Tutorial: Applied Cryptography and Network Security several graduate student participants have returned or plan to return for later workshops in the Special Focus on Communication Security and Information Privacy and have said that they feel the tutorial helped them to get more out of the workshops than they otherwise would have. Another participant, a professor at an undergraduate college, was attending the tutorials to help him with curriculum development in cryptography and security at his college.

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. Due to interactions initiated at the Tutorial on Applied Cryptography and Network Security, the graduate student author of the report is now a Ph.D. student at Stevens Institute of Technology under the guidance of workshop organizer Rebecca Wright.

To give an example of the impact of the special focus on a more established research participant, we note the following from Amir Herzberg, Computer Science Department, Bar Ilan University,

"I was the principal lecturer in DIMACS Tutorial on Applied Cryptography and Network Security, August 4 - 7, 2003. I prepared a substantial amount of lectures for this course, and I am still using these lectures in my university classes and in other forums; I also make all of my lectures (including these) available in my website (with a lot of downloads). I am now working on a book on Introduction to Secure Communication and Commerce, with Applied Cryptography, and I believe the lectures I gave will help me in this project.

I also believe that preparing these lectures, and esp. the PKI and SSL/TLS lectures, helped me identify important problems and solutions in security of web and e-mail, which I am now describing in a paper tentatively titled “Preventing Spoofing, Spamming and Phishing.”
In summary: I hope this course gave the participants as much as it helped me... I'll definitely be happy to repeat the experience!