

ERIC C. CRONIN

ADDRESS

University of Pennsylvania
School of Engineering and Applied Science
Department of Computer and Information Science
3330 Walnut St.
Philadelphia, PA 19104
E-mail: ecronin@cis.upenn.edu
Homepage: <http://www.cis.upenn.edu/~ecronin/>

EDUCATION

University of Pennsylvania Ph.D. in Computer and Information Science, Pursuing
Advisor: Matt Blaze

University of Michigan M.S.E. in Computer Science and Engineering, August, 2003
Ph.D. candidate in Computer Science and Engineering, December, 2002
Advisor: Sugih Jamin

University of Michigan B.S.E. in Computer Engineering *Summa Cum Laude*, December, 2000

RESEARCH EXPERIENCE

Electronic Voting Machine Evaluation
Performed the first public security analysis of the Election Systems & Software suite of election management tools and optical scan/touch screen voting hardware.

Network Wiretapping
Studied the challenges and limitations to performing eavesdropping on Internet hosts. Identified flaws in existing tools allowing for evasion and the insertion of false records. Developing techniques to avoid or detect attacks.

Voice Wiretap Vulnerabilities
Evaluated a “loop extender” style wiretap commonly used by law enforcement agencies. Identified several large security vulnerabilities including allowing the wiretap to be remotely disabled without authorization.

Protocol Confusion
Studied the limitations of network eavesdropping due to protocol ambiguities. Developed tools to exploit ambiguities to increase confusion.

Security Vulnerabilities in the Movie Production and Distribution Process
Examined the properties of copyrighted movies found on peer-to-peer filesharing networks. Determined source of leaks and characterized quality of downloadable movies.
More information: http://www.user-agent.org/movies/insider_samples.html

Forward-Secure Signatures

Designed, implemented, and evaluated a library for Forward-Secure Signature schemes constructed from traditional digital signatures.

More information: <http://www.cis.upenn.edu/~ecronin/Projects/FSS/>

Multiplayer Games

Designed and implemented a novel synchronization technique for distributed multiplayer games. Designed improved cheatproofing protocol for multiplayer games utilizing dead reckoning.

More information: <http://warriors.eecs.umich.edu/games/>

IDMaps Project

Designed and performed experiment gathering Internet traceroute data from public Traceroute Gateway servers to thousands of hosts for study of web-server mirror placement.

Key Distribution Hierarchy

Redesigned and implemented a Certificate Authority daemon and client library for Public Key Hierarchy using Windowed Revocation. Added secure, authenticated submission to programming assignment used for submitting homework and future programming assignments in undergraduate course.

PROFESSIONAL EXPERIENCE

University of Pennsylvania, Research Assistant, 2003–Present, with Prof. Matt Blaze

Researched many areas in network, host and physical security. Developed the concept of “confusion” in third-party interpretation of communications. Explored the security of large-scale deployed systems such as electronic voting and voice telephony.

AT&T Labs - Research, Research Intern, November 2002–August 2003, with Dr. Patrick McDaniel

Designed, constructed, and evaluated reference implementation of forward-secure signatures. Studying scalable security vulnerabilities and their prevention through the use of diversity.

University of Michigan, Research Assistant, 1999–2002, with Prof. Sugih Jamin

Explored various topics including multiplayer games, secure online distribution and updating of software and source code, Internet Denial-of-Service attack detection, and public key infrastructures.

TEACHING EXPERIENCE

Grader, Distributed Systems (CIS 505). Spring 2008

Performed hands-on grading of group project demos; guest lectured on security and cryptography.

Co-Instructor, Operating Systems Lab (CSE 381). Fall 2005, Fall 2006, Fall 2007

Created and presented series of tutorial lectures on operating system and programming topics; organized staff of 7 TAs and Co-Instructors; evaluated individual and group projects, homeworks, exams; updated and modified project assignments and grading criteria; held office hours on programming assignments.

Teaching Assistant, Computer and Network Security (CSE 551). Spring 2005

Created projects for redesigned course; evaluated projects and exams; held office hours on lecture material and projects.

Teaching Assistant, Operating Systems Lab (CSE 381). Fall 2004

Evaluated group and individual projects, homeworks, exams; helped design project assignments and grading criteria; held office hours on programming assignments.

PUBLICATIONS

Journal Papers

- Eric Cronin, Micah Sherr, and Matt Blaze, On the (Un)reliability of eavesdropping. *International Journal of Security and Networks*, 3(2), 2008.
- Micah Sherr, Eric Cronin, Sandy Clark, and Matt Blaze, Signalling Vulnerabilities in Wiretapping Systems. *IEEE Security & Privacy*, 3(6), Nov/Dec 2005.
- Simon Byers, Lorrie Cranor, Eric Cronin, Dave Kormann, and Patrick McDaniel, Analysis of Security Vulnerabilities in the Movie Production and Distribution Process. *Telecommunications Policy*, 28(8), Aug 2004.
- Eric Cronin, Burton Filstrup, Anthony R. Kurc, and Sugih Jamin, An Efficient Synchronization Mechanism for Mirrored Game Architectures (Extended Version). *Kluwer Multimedia Tools and Applications*, 23(1), May 2004.
- Eric Cronin, Sugih Jamin, Cheng Jin, Anthony R. Kurc, Yuval Shavitt, and Danny Raz, Constrained Mirror Placement on the Internet (Extended Version). *IEEE Journal on Selected Areas in Communications*, 20(7), Sep 2002.

Conference Papers

- Eric Cronin, Micah Sherr, and Matt Blaze, On the Reliability of Current Generation Network Eavesdropping Tools. In *Advances in Digital Forensics II: Proc. of 2nd Annual IFIP WG 11.9 International Conference*, Jan 2006.
- Simon Byers, Lorrie Faith Cranor, Eric Cronin, Dave Kormann, and Patrick McDaniel, Exposing digital content piracy: approaches, issues and experiences. In *Conf. Rec. of 38th Asilomar Conference on Signals, Systems and Computers*, Nov 2004.
- Eric Cronin, Sugih Jamin, Tal Malkin, and Patrick McDaniel, On the Performance, Feasibility, and Use of Forward-Secure Signatures. In *Proc. of 10th ACM Conference on Computer and Communications Security*, Oct 2003.

Workshop Papers

- Adam Aviv, Pavol Černý, Sandy Clark, Eric Cronin, Gaurav Shah, Micah Sherr, and Matt Blaze, Security Evaluation of the ES&S Voting Machines and Election Management System. In *Proc. of 3rd USENIX/ACCURATE Electronic Voting Workshop*, Aug 2008.
- Micah Sherr, Eric Cronin, and Matt Blaze, Measurable Security through Isotropic Channels. To appear in *Security Protocols 2007, 15th International Workshop. Revised Selected Papers*, Apr 2007.
- Madhukar Anand, Eric Cronin, Micah Sherr, Matt Blaze, Zachary Ives, and Insup Lee, Sensor Network Security: More Interesting Than You Think. In *Proc. of 2nd Workshop on Hot Topics in Security*, Aug 2006.
- Eric Cronin, Micah Sherr, and Matt Blaze, Listen too closely and you may be confused. To appear in *Security Protocols 2005, 13th International Workshop. Revised Selected Papers*, Apr 2005.
- Simon Byers, Lorrie Cranor, Eric Cronin, Dave Kormann, and Patrick McDaniel, Analysis of Security Vulnerabilities in the Movie Production and Distribution Process. In *Proc. of 2003 ACM Workshop on Digital Rights Management*, Oct 2003.
- Eric Cronin, Burton Filstrup, and Sugih Jamin, Cheat-Proofing Dead Reckoned Multiplayer Games. In *Proc. ADCOG 2003*, Jan 2003.

- Eric Cronin, Burton Filstrup, Anthony R. Kurc, and Sugih Jamin, An Efficient Synchronization Mechanism for Mirrored Game Architectures. In *Proc. NetGames2002*, Apr 2002.

Technical Reports and ePrints

- Madhukar Anand, Eric Cronin, Micah Sherr, Matt Blaze, and Sampath Kannan, Security Protocols with Isotropic Channels. Report 2006/396, IACR Cryptology ePrint Archive, Nov 2006.
- Madhukar Anand, Eric Cronin, Micah Sherr, Matt Blaze, and Sampath Kannan, Security Protocols with Isotropic Channels. Report TR-CIS-06-18, University of Pennsylvania, Nov 2006.
- Eric Cronin, Micah Sherr, and Matt Blaze, The Eavesdropper’s Dilemma. Report MS-CIS-05-24, University of Pennsylvania, Aug 2005.
- Eric Cronin, Sugih Jamin, Tal Malkin, and Patrick McDaniel, On the Performance, Feasibility, and Use of Forward Secure Signatures. Technical Report TD-5QHGBK, AT&T Labs – Research, Aug 2003.
- Simon Byers, Lorrie Cranor, Eric Cronin, Dave Kormann, and Patrick McDaniel, Analysis of Security Vulnerabilities in the Movie Production and Distribution Process. Technical Report TD-5N6SJ4, AT&T Labs – Research, Aug 2003.

Book Chapters

- Eric Cronin, “Availability” and “Denial-of-Service”. *Encyclopedia of Information Security*, Henk C.A. van Tilborg Ed., Springer US, 2005.

Under Preparation and Other

- Patrick McDaniel, Matt Blaze, and Giovanni Vigna et al., *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and testing – Academic Team Report*. Ohio Secretary of State, Dec 2007.

INVITED TALKS AND PRESENTATIONS

- *Signaling Vulnerabilities in Wiretapping Systems*, Second European Conference on Computer Network Defense, October 5, 2007
- *Signaling Vulnerabilities in Law Enforcement Wiretap Systems*, Pennsylvania State University Computer Science and Engineering Department Colloquium, September 18, 2006
- *Sensor Network Security: More Interesting Than You Think*, First Workshop on Hot Topics in Security, July 31, 2006
- *Law Enforcement Wiretaps: Background and Vulnerabilities*, HOPE Number 6, July 22, 2006
- *On the Reliability of Current Generation Network Eavesdropping Tools*, Second IFIP WG 11.9 International Conference on Digital Forensics, January 30, 2006
- *Signaling Vulnerabilities in Wiretapping Systems*, University of Pennsylvania Department of CIS Research Symposium, December 1, 2006
- *On the Performance, Feasibility, and Use of Forward-Secure Signatures*, 10th ACM CCS, October 28, 2003
- *Cheat-Proofing Dead Reckoned Multiplayer Games*, ADCOG ’03, January 6, 2003
- *An Efficient Synchronization Mechanism for Mirrored Game Architectures*, NetGames2002, April 17, 2002

PROFESSIONAL SERVICE

Program Committee Member Fourth Annual European Conference on Computer Network Defense, 2008.

Program Committee Member Third Annual European Conference on Computer Network Defense, 2007.

Program Committee Member Security and Privacy Track, The Thirteenth International World Wide Web Conference, 2004.

AFFILIATIONS

USENIX Advanced Computing Systems Association (Student Member)

Association for Computing Machinery (Student Member)

Institute of Electrical and Electronics Engineers (Student Member)

Eta Kappa Nu (Beta Epsilon Chapter, Alumni)

Last Updated: August 13, 2008