Adam Stubblefield

http://www.cs.jhu.edu/~astubble/
astubble@cs.jhu.edu

Education

Ph.D. in Computer Science Johns Hopkins University, May 2005.
Dissertation: *New Techniques for Analyzing Applied Computer Security Systems*
Advisor: Avi Rubin

M.S.E. in Computer Science Johns Hopkins University, May 2005.

B.A. in Mathematics Rice University, May 2002.

Employment

Co-founder (2005 - Present) Independent Security Evaluators.
Founded company to provide advanced computer security analyses and research to industrial and governmental clients.

Assistant Research Professor (2005 - Present) Johns Hopkins University.
Teaches courses on computer security and cryptography, advises students, and runs the JHUISI RFID Security Research Lab.

Research Intern (Summer 2002) Microsoft Research. Mentor: Dan Simon
Investigated human factors issues in the design of security systems. Conducted security design reviews for product groups.

Research Intern (Summer 2001) AT&T Labs-Research. Mentor: Avi Rubin
Researched security in wired and wireless networks. Demonstrated that a theoretical attack on RC4 could be used to break 802.11 WEP.

Research Intern (Summer 2000) PARC. Mentors: Drew Dean & Matt Franklin
Developed methods for detecting and preventing Distributed Denial of Service (DDoS) attacks.

Intern (1998-1999) Wang Government Services. Mentor: Mike Focke
Developed new features for and performed analysis of the NSA B3 certified XTS-300 STOP Operating System.

Honors and Awards

2005: MIT TR35 Young Innovator Award
2002: JHUISI Fellowship
2002: CRA Outstanding Undergraduate Award
2001: USENIX Scholars Fellowship

Teaching

650.443 Researching Security Systems (Fall 2005) Instructor, Johns Hopkins.
Designed and taught graduate course on how to do research on topics in computer security.

600.304 Physical Security Systems (Winter 2005) Instructor, Johns Hopkins.
Designed and taught an intersession course on how to evaluate security systems designed to protect physical assets.

650.412 Designing Security Systems (Fall 2004) Instructor, Johns Hopkins.
Designed and taught a new graduate course on the methods and limitations of provable security models.

600.412 Attacking Security Systems (Spring 2004) Instructor, Johns Hopkins.
Highest rated undergraduate Computer Science course, Spring 2004.
Designed and taught a new advanced undergraduate course on how security systems are compromised and how what we've learned about such attacks can be applied to the design of new systems.

COMP527 Computer Systems Security (2001-2002) Teaching Assistant (Instructor: Dan Wallach), Rice.
Gave selected lectures and created homework assignments for Rice's graduate-level computer security course.

Presentations and Talks

Conference Talks:
Full length talks at NDSS 2001, USENIX Security 2001, NDSS 2002, IEEE Security and Privacy 2004. Numerous short works-in-progress talks.

Invited Talks and Panels:
2005: University of Massachusetts at Amherst
2005: University of California at Berkeley
2005: American Association for the Advancement of Science
2004: Yale Law School
2004: DIMACS Workshop on Cryptography: Theory Meets Practice
2004: Library of Congress
2004: Caltech/MIT Voting Project
2004: University of Chicago
2003: IBM Research
2002: Microsoft Research

Service

Program Committees:
2006: Financial Cryptography
2006: ISOC NDSS

2005: USENIX Security Symposium
2003: WWW2003
2002: USENIX Security Symposium

Also reviewed for numerous other conferences and journals.

Publications

Journal Articles
Adam Stubblefield, Dan S. Wallach, and Aviel D. Rubin, *Managing the Performance Impact of Web Security with WISPr and SCREAM*, Electronic Commerce Research Journal, *to appear*.

Adam Stubblefield, John Ioannidis, and Aviel D. Rubin, *A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP)*, ACM Transactions on Information and System Security (May, 2004).

Drew Dean, Matt Franklin, and Adam Stubblefield, *An Algebraic Approach to IP Traceback*, ACM Transactions on Information and System Security (May 2002).

Conference Papers

Zachary Peterson, Randal Burns, Joseph Herring, Adam Stubblefield, and Avi Rubin. *Secure Deletion for a Versioning Filesystem*, Proc. USENIX Conference on File and Storage Technologies, San Francisco, California (December 2005), *to appear.*

Steve Bono, Matt Green, Adam Stubblefield, Ari Juels, Avi Rubin and Michael Szydlo. *Security Analysis of a Cryptographically-Enabled RFID Device* Proc. USENIX Security Symposium, Baltimore, Maryland (August 2005). *Best Student Paper Award.*

Zachary N.J. Peterson, Randal Burns and Adam Stubblefield. *Limiting Liability in a Federally Complient Filesystem* Proc. PORTIA Workshop on Sensitive Data in Medical, Financial, and Content-Distribution Systems, Stanford, California (July 2004).

Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, *Analysis of an Electronic Voting System,* Proc. IEEE Symposium on Security and Privacy, Oakland, California (May, 2004).

Adam Stubblefield, John Ioannidis, and Aviel D. Rubin, *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*, Proc. ISOC Symposium on Network and Distributed System Security, San Diego, California (February, 2002).

Drew Dean and Adam Stubblefield, *Using Client Puzzles to Protect TLS*, Proc. 10th Annual USENIX Security Symposium, Washington, D.C. (August, 2001).

Scott A. Craver, Min Wu, Bede Liu, Adam Stubblefield, Ben Swartzlander, Dan S. Wallach, Drew Dean, and Edward W. Felten, *Reading Between the Lines: Lessons from the SDMI Challenge*, Proc. 10th USENIX Security Symposium, Washington, D.C. (August, 2001).

Drew Dean, Matt Franklin, and Adam Stubblefield, *An Algebraic Approach to IP Traceback*, Drew Dean, Matt Franklin, and Adam Stubblefield, Proc. 2001 Network and Distributed Systems Security Symposium, San Diego, California (February 2001). *Best Paper Award*

Technical Reports

Edward W. Felten, Aviel D. Rubin, and Adam Stubblefield, *Analysis of Voting Data from the Recent Venezuela Referendum***,** available online at http://www.venezuela-referendum.com.

Adam Stubblefield and Dan Simon, *Inkblot Authentication*, Tech report MSR-TR-2004-85, Microsoft Research.

Adam Stubblefield and Dan S. Wallach, *Dagster: Censorship-Resistant Publishing Without Replication*, Tech report TR-01-380, Department of Computer Science, Rice University.

Adam Stubblefield and Dan S. Wallach, *A Security Analysis of My.MP3.com and the Beam-it Protocol*, Tech report TR-00-353, Department of Computer Science, Rice University.