Dave Kettyle

Technical Staff, Center for Election Integrity/ Public Monitor

Work Experience

August, 2006 – Present

Center for Election Integrity
Cleveland State University, Cleveland, OH
Technical Staff, Public Monitor of Cuyahoga Election Reform

- Evaluated election technology from Diebold Election Systems, Inc., as configured, deployed and operated in Cuyahoga County, OH.
- Identified potential technical risks and appropriate safeguards to help the County's effort to hold a successful election in November 2006.
- Monitored a significant portion of the election systems preparation and testing preceding the November 2006 election, as well as the conduct of the election and tabulation.
- Performed an in-depth, post-election analysis of computer-generated election system event logs to identify areas of success and failure in the technical operations of the Cuyahoga County Board of Elections and in the election systems produced by Diebold Election Systems.

May – July, 2006

Cuyahoga Election Review Panel (CERP)
Cleveland, OH
Technical Issues Lead

- Investigated the electronic voting technology used in Cuyahoga County and its role in the troubled election held in May 2006.
- Concentrated on the GEMS election management system from Diebold Election Systems, its design and operation, and its suitability for the County's election needs.
- Drafted findings and recommendations regarding election technology for the Panel's final report.

2001 – 2005

Advanced Visual Systems, Inc.
Waltham, MA
Lead Software Engineer

- Managed a team of engineers designing a new line of data visualization software tools based on OpenViz® business intelligence technology.
- Supervised supporting engineers in maintaining legacy software products.
- Assisted software developers at client sites in integrating data visualization capabilities into existing applications.
- Served as the technical consultant for marketing and pre-sales efforts.

1998 – 2001

Advanced Visual Systems, Inc.
Waltham, MA
Software Engineer

- Participant in development of OpenViz, a component-based software toolkit for creating large scale data visualization programs for use in scientific, industrial and business applications.
- Author of whitepapers on the potential uses of data visualization techniques for various science and engineering disciplines and associated best practices.
- Developer of numerous example software applications demonstrating best practices for implementation of interactive data visualization software.

Summer 1995

Sun Microsystems, Inc.
Palo Alto, CA
Technical Intern

- Wrote technical specifications and test plans for a suite of software tools for inclusion in Solaris operating system.
- Participated in extensive usability evaluations for user interface prototypes.

Education

2005 - Present

Case Western Reserve University School of Law
Cleveland, OH
J.D. expected in 2008

Merit Scholarship

1993 - 1997

Stanford University
Stanford, CA
B.S., Computer Science

1989 - 1993

Milton Academy
Milton, MA
High School Diploma

Eric Rescorla

Employment History

March 1999-present, Network Resonance, Inc., Palo Alto, CA — Chief Scientist

August 1998-present, RTFM, Inc., Palo Alto, CA —Principal Engineer

October 1995-August 1998, Terisa Systems, Inc., Los Altos, CA — Principal Engineer

July 1992-October 1995, Enterprise Integration Technologies, Inc., Menlo Park, CA — Senior Software Engineer

Education

May 1992, B.S. Chemistry, Yale University.

Boards, etc.

Member, Voltage Security Technical Advisory Board

March 2001-present, Member, Internet Architecture Board (IAB)

January 2001-present, IETF Security Directorate

July 2001-present, IETF Transport Area Directorate

October 2001-present, IETF Operations Area Directorate

Academic Papers

Bellovin, S., and Rescorla, E., *Deploying a New Hash Algorithm*, to appear NIST Hash Function Workshop, October 2005.

Shacham, H., Boneh, D., and Rescorla, E. *Client-Side Caching for TLS* ACM Trans. Info. & Sys. Security, 7(4):553-75, November 2004.

Rescorla, E., *Is finding security holes a good idea?*, 2004, IEEE Security and Privacy, August 2004.

Modadugu, N. and Rescorla, E., *The Design and Implementation of Datagram TLS*, Proceedings of ISOC NDSS 2004, February 2004.

Rescorla, E., *Security Holes... Who cares?*, to appear in Proceedings of the 12th USENIX Security Symposium, 2003.

Rescorla, E., Cain, A., Korver, B., *SSLACC: A Clustered SSL Accelerator*, in Proceedings of the 11th USENIX Security Symposium, pp. 229-246, August 2002.

Rescorla, E., Dick, K., *Secure Auditing for SSL*, preprint.

Books

Rescorla, E., *SSL and TLS: Designing and Building Secure Systems*. Addison-Wesley, 2000.

General Audience Publications

Rescorla, E., *Damage Control*, Better Software Magazine, October 2004.

Rescorla, E., *An Introduction to OpenSSL Programming*, Linux Journal, September-October 2001.

RFCs and Internet Drafts

Dierks, T., Rescorla, E. (editors), *The TLS Protocol, Version 1.1* draft-ietf-tls-rfc2246bis-13.txt, June 2005.

Rescorla, E., *HTTP Over TLS (HTTPS)*, RFC 2818, May 2000.

Rescorla, E., Schiffman, A.M., *The Secure HyperText Transfer Protocol*, RFC 2659, August 1999.

Rescorla, E., *Diffie-Hellman Key Agreement Method*, RFC 2631, June 1999.

Rescorla, E., *Preventing the Million Message Attack on CMS*, RFC 3218, January 2002. 2001.

Rescorla, E., Tuexen, M., Jungmaier, A., *TLS over Stream Control Transmission Protocol*, RFC 3436, December 2002.

Rescorla, E., et al., *Guidelines for Writing RFC Text on Security Considerations*, RFC 3552, July 2003.

Rescorla, E., et al., *Writing Protocol Models*, RFC 4101, June 2005.

Rescorla, E., and Modadugu, N., *Datagram Transport Layer Security*, draft-rescorla-dtls-05.txt, June 2005 (approved for RFC publication).

Rescorla, E., *A Survey of Authentication Mechanisms*, draft-iab-auth-mech-04.txt, September, 2005.

Handley, M., Rescorla., E. *Internet Denial of Service Considerations*, draft-iab-dos-03.txt, September, 2005.

Talks and Seminars

Rescorla, E., *What can the evidence tell us about information security?*, Information Security Decision Conference, May 2005.

Rescorla, E., *What's the worst that could happen?*, DIMACS Workshop on Cryptography: Theory Meets Practice, October 2004.

Rescorla, E., *Is finding security holes a good idea?*, 2004, Workshop on Economics and Information Security, March 2004.

The Internet is too secure already, invited talk at the 12th USENIX Security Symposium, August 2003.

Security holes... Who cares?, ICSI Center for Internet Research, Berkeley, CA, September 2002; Information Sciences Institute East, November 2002; Stanford Security Seminar, January 2003.

A Crash Course in SSL and TLS, 11th USENIX Security, August 2002; ISOC NDSS February 2002.

Guidelines for Authors of Security Considerations, IETF Plenary, Yokohama, Japan, July 2002.

Secure Auditing for SSL, Stanford Security Seminar, July 2002; Information Sciences Institute East, November 2002.

Funding

Principal Investigator, *Authoritative SSL Auditing*, HSARPA Science and Technology, 2004.

Principal Investigator, *SSL Auditing*, DARPA Advanced Technology Office (ATO), 2002.

Patents and Patents Pending

Dick, K., Rescorla, E., *System, method and computer program product for guaranteeing electronic transactions*, August 2002. (granted)

Dick, K., Rescorla, E., *System, method and computer program product for providing an effi cient trading market*, May 2001.

Dick, K., Rescorla, E., *System, method and computer program product for providing an IP datalink multiplexer*, May 2001.

Dick, K., Rescorla, E., *System, method and computer program product for analyzing data from network-based structured message stream*, May 2001.

Dick, K., Rescorla, E., *System, method and computer program product for auditing XML messages in a network-based message stream*, May 2001.

Rescorla, E., Cain, A., Korver, B., *Method and apparatus for clustered SSL accelerator*, March 2002.

Professional Activities

Chair, IETF Transport Layer Security Working Group.
Program Committee Member, ISOC NDSS 2004, 2005.
Program Committee Member, IEEE Security and Privacy, 2005.
September 2002, External reviewer for IEEE Infocom.
July 2002, External reviewer ACM Transactions on Computer Science.
2000-present, External reviewer for Addison-Wesley.
2001-present, External reviewer for Prentice-Hall.
March 2002, External reviewer for O'Reilly.