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

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.