Matt Blaze - Research Summary and Bio

Secure Systems and Cryptology

My research focuses on the architecture and design of secure systems based on cryptographic techniques, analysis of secure systems against practical attack models, and on finding new cryptographic primitives and techniques. This work has led directly to several new cryptographic concepts, including: "Remotely-Keyed Encryption," which allows the use of inexpensive, low-bandwidth secure hardware to protect high-bandwidth communication and stored data, "Atomic Proxy Cryptography," which allows re-encryption by untrusted third parties, and "Master-Key Encryption," which provides a systematic way to design (and study) ciphers with built-in "back doors."

I am especially interested in the use of encryption to protect insecure systems such as the Internet. I was a designer of *swIPe*, a predecessor of the now standard IPSEC protocol for protecting Internet traffic. Another project, *CFS*, investigated and demonstrated the feasibility of including encryption as file system service.

Recently, I've applied cryptologic techniques to other areas, including the analysis of physical security systems; this work yielded a powerful and practical attack against virtually all commonly used master-keyed mechanical locks.

Trust Management

I coined the term, and am one of the inventors of, *Trust Management,* which provides the abstract layer in which a system decides whether to allow some potentially dangerous action. This work has led to two trust management languages, *KeyNote* and *PolicyMaker,* that provide tools for specifying policy, delegating authority, and controlling access. In addition to providing a useful framework for studying and proving security properties of distributed systems, our tools have been used to build powerful policy control mechanisms into several important applications, including the OpenBSD IPSEC implementation.

Technology and Public Policy

Cryptology and computer security have important relationships to vital areas of public policy, and my work has touched on these in several ways. In 1994, I discovered a serious flaw in the US Government's "Clipper" encryption system, which had been proposed as a mechanism for the public to encrypt their data in a way that would still allow access by law enforcement. I have edited several influential reports on encryption policy, including the 1998 study of "key escrow" systems that demonstrated that such systems are inherently less secure and more expensive than systems without such a feature. This work contributed to the recent shift in U.S. encryption policy. More recently, I have been active in the analysis of the FBI's ``Carnivore" Internet wiretap system. I have testified before various comittees of the US Congress and European Parliament several times, providing technical perspective on the problems surrounding law enforcement and intelligence access to communications traffic and computer data.

Biographical Information

Education:

- Princeton University, Ph.D., Computer Science, January 1993. (Thesis: Caching in Large-Scale Distributed File Systems.)
- Princeton University, M.A., Computer Science, June 1989.
- Columbia University, M.S., Computer Science, May 1988.
- City University of New York (Hunter College) B.S., January 1986.

Current Appointments

- University of Pennsylvania, Philadelphia, PA. Associate Professor of Computer and Information Science.

Home page: http://www.crypto.com/

Blog: http://www.crypto.com/blog