Enabling Email Confidentiality through the use of Opportunistic Encryption

Simson L. Garfinkel
MIT Laboratory for Computer Science
http://www.simson.net/

DEMO

I will conduct a demonstration of Stream, a C++ POP and SMTP proxy that provides opportunistic encryption to mail user agents (MUAs). The demo hardware shall consist of two copies of Stream running on a Macintosh laptop computer: one copy shall be proxy for an email account accessed through Apple Mail, the second shall proxy for an email account accessed through a copy of Eudora.

Using Stream, I will demonstrate how encrypted email messages can be exchanged between the Apple Mail and Eudora users without explicit key management. This is done with a “zero-click interface.”

After an exchange of messages, I will use the “Show Headers” feature to show how key information was exchanged in the RFC822 message headers. This will lead into a demonstration of the specific message formats used by the Stream system.