

Securing Email

Robert J. Hansen
The University of Iowa

The Scope of the Problem

- Competing standards (PEM, S/MIME, OpenPGP, various proprietary offerings)
- Interoperability problems even with standards (RC2 support in S/MIME, whether X.509 parameters should be NULL)
- And most damning, social obstacles

Current Usage Profile

- Vanishingly small fraction of all email traffic is encrypted (Gutmann, et. al.)
- End to end encryption is almost unknown
- SSL-to-server the most common form
 - Largely beyond this paper

Needs versus Wants

- Security is a *want*.
 - 79% worried about email security
 - 20% view privacy as the most important issue facing us electronically
- Convenience is a *need*.
 - Nobody wants to be bothered. Ever.

The Kelley Principle

- “The most powerful force in the world is necessity.” — D. Kelley
- Necessity and convenience form a sort of supply and demand curve
 - Where they overlap defines our adoption of technologies
- Nowhere is this clearer than email crypto!

The Kelley Principle II

- By making crypto more convenient, we can overcome reluctance to adopt
 - Lotus Notes, Groove, centralized X.509
- By making crypto more necessary, we can force adoption
 - HIPPA, Sarbanes–Oxley, etc.

The Potential Market

- Almost 60% of users don't know if their email client support crypto
- Almost 50% would be willing to change clients to get better crypto support
- Selection bias: this survey was given at *Financial Cryptography*.
- If only 40% of *FC* attendees know if their email client supports crypto, we've got problems.

Who Controls the Repo?

- Control issues also come into play
- If your keyserver is under your control, you're going to trust it more than if it's not
- The wisdom of this folk belief has not been firmly established
- Example: how many keys named "George W. Bush" are there on public keyservers?

Puddings and Proof

- The proof is in the pudding, as it were.
- “Everyone’s your brother until the rent comes due.”
- What people say they would do and what they actually do are two separate things.

Evidence Suggesting

- 44% say they don't know how to use crypto
- There is no cure for ignorance—upgrading email clients is easy, education is hard
- Most people are reluctant to learn new skills
- We need to facilitate the learning curve

Strategies for Human Nature

- Incremental deployment
 - Addresses the “only paranoids” issue
 - Today it’s just paranoids; tomorrow everyone
 - Allows an avoidance of the chicken and egg problem
- Deploy within centralized systems (AOL)

Strategies, II

- Webmail
 - Allows easy deployment to large numbers of users
 - Webmail increasingly defines email normalcy
 - Treats the paranoia issue

Strategies, III

- *Continuity* of identity versus *proof* of identity
- Frankly, I think they're nuts.
- Identity is a tricky concept—just ask the Philosophy Department
- Expecting users to see these subtleties is expecting too much

Future Research

- Most obvious: set up a Webmail site using S/MIME pervasively and see what adoption is like
- Sit back and watch S/MIME adoption in the enterprise
- Expect to be sitting a long, long time.

Questions for Authors

- S/MIME hasn't taken off; what does that say about the thesis of the paper?
- Aren't you handwaving the issue of user education?
- Aren't you handwaving the difference between what users say and what they'll do?
- Isn't there a huge selection bias by sending questionnaires to *Financial Cryptography* attendees?