Web of Trust Analogy

We had a question last time looking for more detail on the web of trust idea. Why does a widely disseminated public key reduce the chance of forgery. There is an analogy with timekeeping: a man with two watches that disagree knows that he does not know the time, that is, error detection is provided. Someone who has two public keys for Steve Jobs knows that one of them must be a forgery. A man with three watches can use “majority decoding” to make a best guess for the time, and someone who has 99 copies of one key and only 1 of the other can put more trust in the more widely disseminated key.

Identity Based Encryption

On of my mailing lists had a question about identity based encryption (IBE) this morning, which reminded me to mention something about it. This is an “old” idea of Shamir’s (old means 1980s: to an American, 100 years is old, but to an Englishman 100 miles is far): develop a public key cryptosystem that allows an arbitrary string as the public key. Thus, Alice could send a secure email to Bob using bob@bobscompany.com as his public key. This has several advantages [reference: Boneh and Franklin, SIAM J. Computing 32(2003), pp. 586 – 615]

IBE has the obvious advantage of making the public key easy to remember, but there are many other advantages.

• A key of the form bob@bobscompany.com || expiration-date is automatically revoked on the indicated expiration date.

• User credentials are easy to grant and revoke, so if Bob’s security clearance is revoked, the private key can also be revoked, and Bob will be unable to read secure email. This is done using public keys like

bob@bobscompany.com || expiration-date || security-level.

• Use of daily private keys means that Bob can put them on a laptop, and only compromise one day’s worth of traffic if the laptop is stolen. A similar analysis would apply to use of public internet access points, as discussed below.

• Bob can delegate work if Alice uses the subject line in the key; the key would be tied to a private key held by Bob’s accounting manager. Thus, those from other departments would not have access. Such a key might look like

bob@bobscompany.com || accounting.
The best success with IBE has come from elliptic curve cryptography, as expored by Boneh and Franklin. This is also in the book *Advances in Elliptic Curve Cryptography*, which we discussed earlier.

---

**More on S/MIME**

There are a couple of points about S/MIME that slipped through the cracks the other day. First, S/MIME data must be decrypted outside any firewall or gateway; if not, the firewall cannot scan the data at all, and may allow malware in.

Second, S/MIME and PGP are unsuited to webmail clients, because of their need for the user’s private key. Thus, a travelling salesman who checks her email using a browser will be unable to read any S/MIME encrypted mail. Why? First, the internet cafe browser does not have her private key, so she must provide it, using, say, a memory stick. But then her private key is floating around in some unsecured machine on the street in Osaka. *Iku ja nai!*

---

**S/MIME implementation**

S/MIME is implemented as part of OpenSSL. The man pages are posted, or use PuTTY to log in to a Unix server.