11. Digital Signatures

Digital signatures, and the digital keys that create these signatures, are an important tool in creating an infrastructure that could prevent identity theft. A digital signature is based on two digital keys: a secret key and a public key. The individual holds the secret key, and only the individual can know that secret key. Each key is a special kind of number that is very large, consisting of hundred of digits.[14] The keys must be created in pairs, so that for every secret key there is one corresponding public key.

The public key can decrypt or unlock anything encrypted with the secret key. The secret key can decrypt anything encrypted with the public key. Encrypting twice with either key only makes it necessary to decrypt twice with the other key.

Imagine a drop box. A drop box that is open to the public, where anyone can use the public key to open it and place material in. By its nature as a drop box, putting something in is simple. Everyone has the capacity to drop; everyone has access with the key to the drop box. The drop box, the key and the information dropped in it, are of course, all bits. In the digital dimension, dropping in the box is encrypting with the public key. Only the person with the matching secret key can unlock the encrypted material.

Imagine that each drop box has a number associated with it. You have a check to deliver to a particular person. How do you know in which place to drop it? The association between individual and key created by the public key infrastructure -- a way for everyone to know which drop box uniquely belongs to which individual. Thus the infrastructure that associates the key pair to the individual is critical for digital signatures to work.

Retrieving the material requires the individual's single-person secret key that is the other half of the unique pair. In digital terms, this means decrypting that material that was dropped in through encrypting with the associated public key.

The ability to retrieve is created by the knowledge of the secret key. The association of the secret key, the public key and the person who knows the secret key is created by the public key infrastructure – the PKI.

PKI can be implemented in practice to mean a single identity for all uses in the digital realm: to send and receive email, to authorize payments, to log in at work, or at a government website. In the original vision, PKI would have been ubiquitous in that there would be a single great identity hierarchy,

---

[14] The secret key can be held on any type of computing device: a smart card, a computer, or a mobile phone. The key can be unlocked by any type of authentication; for example, biometrics on a smart card or a pass phrase on a computer.

like one giant phone book for everyone and every institution on the Internet. Anyone who has tried to look up an old friend using Internet white pages realizes how difficult it is to associate exactly one name with one unique number and have no confusion or overlap.

In the original PKI vision, each person would have one pair of keys (a secret and the corresponding public key) that corresponds to his or her "true name." Obviously that has not and cannot happen; however there are a many smaller implementations of smaller PKIs in companies and commerce. For example, the lock on the browser window is a result of a set of competing PKI creating by companies that sell the authentication of the websites with these locks. [15] The proposals for a single national ID all depend on this fundamental idea.

A PKI has two core things: a cryptographic record of the public key of the key pair, and a way to link that record to a larger database of attributes, credentials or identifiers. Recall that the possession of the secret key authenticates the link between the public and the secret key.

However, computers are not as seamless as human beings. So linking a person to a computer record to a larger database is not so easy if you are linking in human terms.

So developing a system that identifies humans in computer terms is not trivial. We identify each other by context, by integrating information. Humans build on context. Computers determine by categorization and parsing. People integrate, computers parse.

The Public Key Infrastructure

A PKI can prevent identity theft by having secure key storage and specified uses. Or a PKI can make identity theft worse though weak security for key storage and strong liability for digital signatures. PKI can enable weak, centralized identity systems or decentralized strong dedicated identity systems. Taking public keys and stapling them onto off-line identities should not be the goal of a Public Key Infrastructure. Obviously, no one suggested an Infrastructure in this manner. Instead, PKI was described as a "digital signature". "Digital signatures" is a powerful metaphor; in fact, too powerful. The signature metaphor implies that everyone has exactly one for every occasion, like a hand written signature. Cryptographic keys can be thought of as physical keys, for all the possible different locks and doors in life. Cryptographic keys can also be thought of credentials, for movie tickets to lifetime memberships.

---

[15] The browser lock indicates that the transmissions are being encrypted and thus cannot be simply read off the wire. The most common use of this encryption technology (Called Secure Sockets Layer) is to protect credit card numbers as they are transmitted over the Internet.