Jong-Hyeon Henry Lee <jhlee@acm.org>

Project: Global Internet Trust Register
Employer: University of Cambridge, Computer Laboratory, UK
Term: September 1997-August 1999

1) Application of theory

a) Analysis of requirements

On the Internet, the concept of "trust" was not defined properly, and it has been misused. Trust on the network could be very fragile, owing to the nature of the Internet: you do not have a physical contact of the communication peer when you write or talk to the peer on the network. To propose a way to build up trust among users of the Internet, we defined rules of accumulating trust by adopting a chain of trust and demonstrated a network of propagated trust.

b) Design and construction

At the time we performed this project, Phil Zimmerman's Pretty-Good-Privacy (PGP) was widely used in academic and technical societies. We defined the key identification information of PGP keys including email address, key length, name, and fingerprint.

The network of trust was defined in the following way: if we had a face-to-face contact with a person and the person proved his key matches with the published fingerprint on a certified PGP key server, we gave the highest mark "A" for his or her key. If a person was verified in the same way by an "A"-marked person, the person's key got the mark "B." The lowest mark was "D," and we gave "D" to keys that can be found in a PGP key server without the verification process.

After we sorted out keys, we made a key directory with our trust marks. This directory was published in the form of a book. Since some countries have import and export controls over security products, we published it in the form of a book, which can be delivered everywhere without restriction.

c) Quality control

Since the identity verification of each member in the trust network is a key to the success of this project, we set up identity verification protocols for each mark and stuck to the protocols without exception. We compiled tens of thousands of keys and cross checked the marks of classified keys.

2) Social implication of engineering

The result of this project was published by a British publisher and MIT Press in USA, since it was an important trial to build a type of trust on the Internet. We also received a number of recognitions from well-known security experts around the world. Whitfield Diffie, one of the inventors of the Diffie-Hellman algorithm and now Chief Security Officer of Sun Microsystems, wrote a foreword to the book published by MIT Press. The book title is "The Global Internet Trust Register."

3) Communication skills

During the project, we had been dealing with thousands of people via email or in person, and we had eventually built up a trust structure from a number of discussions and email communications with them. As a by-product, I had a comprehensive understanding of digital fingerprinting and published this knowledge and presented it in the book "Information Hiding Techniques for Steganography and Digital Watermarking" published by Artech House in 2000. This book and my chapter are well-recognised by some media including Slashdot.