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

Project: X.509-compliant Certification server
Employer: SoftForum, Inc., Korea
January 1998-February 1999

1) Application of theory

a) Analysis of requirements

Public key algorithms use a pair of keys: one for the key owner and another one for the communication peer. The key for the owner never travels on the network and remains under the owner's control; this property can give stronger security than conventional ciphers and reduce the burden of key management when there are a number of communication peers. However, there is a big threat to the public key mechanism: the communication peer can be easily impersonated. So people introduced the idea of having a trusted third party for the communication based on public keys, which is the so-called certification authority. The role of the certification authority is to issue a certificate for each public key and to prove which key belongs to whom. We can filter out trials with impersonated keys, if we use the certification authority. The role of the certification authority includes technical parts and administrative parts, and we designed and developed a certificate server that performs the technical parts of a certification authority.

The main functions of a certificate server include issuing a certificate for a public key and verifying to whom a certificate belongs. Since there is no face-to-face contact in online communication, it is not certain to whom we are talking. The certificate server tells us who the owner of the certificate is. Technically, the certificate server is the most important part of a public key infrastructure.

b) Design and construction

This project was to implement an ITU-T X.509-compliant certificate server forming a public key infrastructure. Since most certificate service providers and web browsers have supported ITU-T X.509 certificates, the X.509 certificate became a major certificate standard on the Internet, and we decided to implement an X.509-compliant certificate server so that an organisation can issue a certificate to its members for internal services and communications rather than using a certificate from a commercial certificate service provider. It is more sensible for an organisation to issue its own certificates to its members for the internal use, since it can verify its members better than a third party can.

Based on the ITU-T X.500-series recommendations and RSA Security's PKCS specifications, we designed the architecture of our certificate server. At the time, both standards were incomplete, and this might have created problems of interoperability. We omitted the functions for interoperable certificates. This part was standardised in 2002.

c) Quality control

We applied fundamental black box and white box tests and then collected a group of beta testers so that they could use the certificate server and report bugs. Those bug reports turned out to be very useful to enhance the quality of the product.

2) Management of engineering

Since the concept of the X.509 certificate server was quite new at the time, we needed to train developers on how public key algorithm works and why we need certificates. We organised a series of seminars on the foundations of modern cryptography. For this seminar, I wrote a book about modern cryptography and then published it. The developers were eager to learn new concepts and the seminars stimulated them to concentrate on the project and made them more productive.

3) Communication skills

To make developers understand the concept of public key cryptography, I gave presentations about the foundation of the public key infrastructure. During the project, I published a book about modern cryptography explaining various types of cryptosystems, algorithms, protocols, standards, and their applications.

4) Social implication of engineering

Since a public key infrastructure was not a commonly recognised idea at the time of implementation, it was quite new to the market, and I am sure that our implementation gave a positive impact to the security industry in Korea. A government agency related to intelligence services was interested in our implementation, and we provided it for their trial. One year later, I found that there were many variants of our product in the market. I believe that we had shaped and led the market.