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

Project: Authentication system in Digital Cellular Network
Employer: Electronics and Telecommunications Research Institute, Korea
Term: January 1996-August 1996

1) Application of theory
   a) Analysis of requirements
   This project was to design an authentication system for a digital cellular network. Since there is no confidence on the identity of a cellular phone, the cellular communication service provider would like to make sure to whom they are providing services. Without this knowledge, they do not have any protection against cellular call frauds and lawbreakers masquerading as legal subscribers.

   We proposed an authentication system based on a cryptographic digital identity embedded in a mobile phone so that the service provider could verify the identity of the subscriber.

   b) Design and construction
   Since mobile communication networks use a narrower bandwidth than wired network and the efficiency of cellular bandwidth usage directly affects the revenue of the service provider, we should minimise bandwidth usage for authentication.

   Our system included a symmetric cipher and a public key infrastructure. To issue a digital identity, we use a certificate server that becomes a main part of the public key infrastructure. To minimise the calculation, we developed a symmetric cipher to encrypt the subscriber's public key, which could run on a less powerful processor on the mobile terminal.

   Since this project is about the design of an authentication system, we delivered the design document of the system and the implementation of the cipher. The overall authentication system was not implemented by us.

   c) Asset management
   Because of the nature of cipher and authentication for a public service, the documents and cipher were registered in a government agency and classified as a secret for some period.

2) Practical experience
Since this project was issued by SK Telecom, a leading mobile communication service provider in Korea, we had periodic meetings with their technical teams. During discussions of the requirements of the system, we found many constraints derived from the practical application of cryptographic elements to the cellular system and tried to find more efficient ways to deliver the same functionality with minimum consumption of resources.

3) Communication skills
We had a series of meetings with the project issuer and produced meeting minutes. At the end of the project, we produced a report summarising all aspects of the project including the system design, an application model to the current system, the analysis of resource consumption, and the algorithm of the cipher.