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

Project: Jikzi: A Resilient Security Mechanism
Employer: University of Cambridge, Computer Laboratory, UK
Term: March 1998-January 2000

1) Application of theory
   a) Analysis of requirements
   On the Internet, we can see many web publications, and they give us a wealth of information, some useful and some not. Even useful information may disappear any time depending on the decision of the person who has published it, connection link problems, server faults, and so on. This is far different from the media that we have been used to.

   This project was begun to enhance the reliability of information published on the Internet. I tried to answer the question of how to manage web documents reliably and how to recover them when they are damaged.

   b) Design and construction
   First, I needed to have a standardised form of document definition so that a document could be accessible over time. I chose the Extensible Markup Language (XML) for the base language set to define the document structure, which became very popular now.

   To make the system resilient and secure, I designed a network of server clusters that store documents, chunk by chunk, so that each server does not have a whole document but it can show the document by communication between servers. When a server is damaged, the documents in the server can be recovered from other servers in the network. It works like a RAID disk arrays on distributed servers. Since a document is not stored in a server as a whole, no attackers of a server can fetch the full document. To enhance the reliability of document access, I built multiple sets of the server groups so that when a server group fails to deliver a document, another server group can provide it.

   I added some security features to this system that help us make it more reliable. They include a timestamping server based on the Network Time Protocol (NTP: IETF RFC 1305) and an image conversion server for document conversion to PDF or JPG.

2) Practical experience
The concept of this project largely affected the implementation of FiloSAFE, which is the main product of FILOSAFE Corporation, the company for which I have been working in last four years.

3) Communication skills
This project was supported by a grant from the UK's Engineering and Physical Science Research Council (EPSRC). We presented the results of this project in the book *Advances in Computers*, Volume 55, Chapter 6, published by Academic Press in 2001.