

encryption vendor RSA Data Security Inc. and digital certificate vendor VeriSign Inc. have jointly revealed their intent to interoperate through a set of APIs. If the network security framework, called SecureONE, emerges as planned, it could make it easier to implement security in important applications, such as remote access and electronic commerce, that expose sensitive data to the largely non-secure and unpredictable Internet environment. Initially, the vendors are cross-licensing their products to one another, with the intent of bundling or otherwise integrating their products. RSA's toolkits will incorporate McAfee's Virus Interface for Protective Early Response API announced with the framework. Security Dynamics Enterprise Security Services API for its SecurID user-authentication and information access products; RSA's APIs for its digital signature, cryptographic, messaging and transaction security engines; and VeriSign's Developer Kit APIs for access to its certificate services. Although the framework claims to address firewalls as well as screening of hostile Sun Microsystems Inc. Java applets and Microsoft Corp. ActiveX technology, they are not market-leading features. The vendors are seeking out other vendors in the areas of firewalls, Java/ActiveX security, auditing, and intrusion detection for framework incorporation. Some in the industry feel the development of SecureONE is a move by the vendors to solidify a stranglehold on the market and crush its competition. *LANTimes*, August 18, 1997, p. 11.

Computer doctor busy fighting 'viruses', *Cho Yoon-jung*. Dr Ahn Cheol-soo goes by the popular title of 'computer doctor'. He is Korea's undisputed authority on computer viruses. It was while he was working in a medical lab back in 1988 that he came up with a vaccine for Korea's first known computer virus, the Brain Virus. For a long time, Dr Ahn's doctoring was a hobby. His vaccine program V3+ was distributed for free as was his advice on how to fix new viruses. In March 1995, Ahn set up Dr Ahn's Anti-Virus Laboratory and now the company supplies 95% of all Korea's anti-virus software. The establishment of the company was a timely decision. Statistics show that there were few viruses discovered in Korea before 1994. But since then, the number has almost doubled every year, growing from 128 in 1995 to 225 last year.

The main product produced by Dr Ahn's lab is the V3 series of vaccine software. V3 Pro95 was the lab's first commercialized vaccine program designed for use with Windows 95. Another thing the company is looking into is security software. The lab continues to run a service which receives over 100 calls a day. *Korea Newsreview*, July 19, 1997, pp. 26-27.

The cherished keys to the kingdom, *Robert Moskowitz*. Public key cryptography and public key certificates are two of the most important enabling security technologies. Public key certificates have three principle mathematical systems: RSA, DSS and Elliptic Curves. RSA is the de facto standard in the business world, DSS is the US Government standard and Elliptic Curves is the Institute of Electronic and Electrical Engineers (IEEE) proposal. These identifiers allow for identifying the person opening the lock; but trusting the source of the key is another matter. Other information in the certificate, such as the certificate signer and the expiration date, can be used to establish firm trust of the certificate owner's identity. With these two pieces of information, systems can determine the validity of the certificate. With this information packed into a string of bits, public key certificates seem to be the answer to all of the clamoring for solid authentication and encryption. So why aren't public key certificates more widely used? Certificates need a deployed, trusted infrastructure in which to be stored. The automotive industry has announced plans to require public certificate-based secure communications based on the IPsec technology for trading partner communication. The banking industry has developed Secure Electronic Transactions (SET) technology for merchant class commerce and customer-to-bank communication. And the Federal Government, through Federal Public Key Infrastructure initiatives, will have a number of government-with-business and government-with-citizen public certificate-based systems. Many of these will use Secure Multipurpose Internet Mail Extension or Secure Sockets Layer. These efforts will raise some interesting issues about trusting different public key infrastructures. *Network Computing*, July 15, 1997, pp. 37-40.

Telecoms systems insecurity, exploitation, fraud, *Tony Crilly*. Today's business user has access to a