Panel Title:
Security for High-Speed Internets

Chair
Jeff Ingle, Community Management Staff

Panelists
Chris Kubic, National Security Agency

The explosion in the growth of the Internet and private networks has been driving faster network speeds and increased services. New technologies and protocols are fueling this growth and are expected to meet the increasing bandwidth demands. Security could be an enabling factor in this growth, but there are some strong challenges in providing the security and survivability for future networking. Commercial security needs are driven in part by electronic commerce and the need for reliable communications as a critical part of everyday business. Likewise, the government has similar needs for protected communications and intends to use available technology in shared networks. Some of the security and survivability challenges in future networking include encryption, authentication, key management, data integrity, the role of firewalls and guards, and scaling network and security management.

Along with networking capacity is increased awareness that security plays an increasing role (ecommerce, business to business or B2B, on-line banking, gaming) in an increasing threat environment (hackers demonstrating more sophisticated attacks, more destructive and fast-propagating viruses). The increasing market and threat combine to bring more security into play.

With high-speed networks, business-to-business and internal corporate operations are relying more on Virtual Private Networking (VPN) to connect employees and customers securely. VPNs are often created with firewalls that also do encrypted tunneling between sites to be protected, through specialized encryption products, or even with embedded encryption in end systems or computers. There are a number of companies creating and selling VPN solutions, for example … This panel will discuss some of the government and commercial products emerging for the high-speed network market.

High-speed encryption is not the only security concern for the new networks. In the increasingly interconnected world, authentication and integrity are playing stronger roles. Authentication of users and even processes like agents or search engines, are being recognized as critically important. As users access complex databases, file systems, and the web, stronger yet user-friendly authentication plays a key role in accessing crucial resources. Technologies like PKI and kerberos are beginning to be deployed and used for wide-spread authentication. Integrity of data has also grown in importance as more business is done on the Internet. Although technical approaches for integrity are available with separate security mechanisms or through encryption and authentication, other issues remain for legal acceptance and easier understanding and use.

And with the hostile threat environment of sophisticated hackers and viruses, improving firewalls, intrusion detection, and on-line virus checking become more important. However, many of these products are making a difficult transition to the higher Internet speeds since they are inherently more software-based in order to be flexible and rapidly reconfigurable. New approaches, along with faster underlying processors, will be needed to match the higher network speeds. And finally, more attention will have to be given to robust configuration of the network. Since the Internet and private networks are being relied on more heavily, and in many cases exclusively, for everyday business, network outages have moved from the realm of inconvenience to real business loss. Failure prevention, detection and rapid reaction should be applied to the networks for higher availability, as it has for the power grid, air safety, and emergency response. Robust network architectures, monitoring and configuration control are key areas for creating the networks on which the economy can live.

Jeff Ingle is the Lead of the Special Projects Team of the Community Management Staff, Advanced Technology Group. He is on detail from the National Security Agency. One of his primary tasks is as the Program Manager for IC TestNet, an Intelligence Community experimental network to explore new networking technologies, security and collaborative applications. While at NSA, he was the Chief of the High-Speed Security Solutions branch in the Information Assurance Research Office. He led electronics and optics teams to research basic technologies and security techniques to protect high-speed and all-optical networks. He received a Bachelor of Science degree in Electrical Engineering from the University of Alabama in 1985 and a Master of Science degree in Optical Sciences from the University of Arizona in 1989. His interests include network security and survivability, information assurance architecture and system engineering, all-optical networks, high-speed microelectronics and photonics technologies, and technology forecasting.

Mr. Chris Kubic is Technical Director of the Global Grid Networking Technologies Division in the National Security Agency’s Information Assurance Solutions Group. Mr. Kubic is responsible for development of High Assurance In-line Network Encryption products, Network Security Standards, and Infrastructure Hardening initiatives.