Secure Electronic Mail: It's Ready for Prime Time

Panel Chair

Russell Housley, SPYRUS

Panelists

John Pawling, J.G. Van Dyke & Associates

Michael Elkins, Network Associates, Inc.

Session abstract from Panel Chair

The Internet community has developed two standards for secure electronic mail: S/MIME version 3 and OpenPGP. Now that proposed standards have been developed for both protocols, vendors are implementing. The marketplace will ultimately decide which of the two protocols provides the required features. This panel will provide information about the standardization and implementation of S/MIME version 3 and OpenPGP.

Russell Housley will discuss the status of the IETF S/MIME version 3 protocol standard.

John Pawling will discuss the status implementations of the S/MIME version 3 standard.

Michael Elkins will discuss the status of the IETF OpenPGP protocol standards as well as the status implementations of the OpenPGP standard.

Short bio of panel chair and speakers

Russell Housley is the Chief Scientist of SPYRUS; he has over 18 years of communications and computer security experience. His expertise is in security protocols, system engineering, system security architectures, and product definition. He is the chairman of the IETF S/MIME Working Group. He is the author of the Cryptographic Message Syntax (CMS), the security foundation for S/MIME version 3. He is one of the authors of the Internet X.509 Certificate Profile (RFC 2459), commonly called PKIX Part 1. He is one of the authors of the SDNS Message Security Protocol (MSP), the security cornerstone of the U.S. Defense Message System (DMS). He is one of the authors of the IEEE series of LAN/MAN security standards (IEEE 802.10). He is a member of the President's Export Council - Subcommittee on Encryption (PECSENC). He holds a M.S. in Computer Science from George Mason University and a B.S. in Computer Science from Virginia Tech.

John Pawling is the lead engineer of the J.G. Van Dyke and Associates, Inc, (VDA) team developing the S/MIME Freeware Library reference implementation of the IETF S/MIME Version 3 specifications. He is an active member of the IETF S/MIME working group and has made major contributions to the Enhanced Security Services for S/MIME document. He led the VDA team that developed the reference implementation of the Message Security Protocol (also known as ACP120) for the Department of Defense. He played a significant role in developing the security related specifications being implemented in the Defense Message System. He holds a M.S. in Computer Science from

Johns Hopkins University and a B.E. in Computer Science/Electrical Engineering from Vanderbilt University.

Michael Elkins is a software development engineer working for NAI Labs, the Security Research Division of Network Associates, Inc. (NAI). He is currently working on the incorporation of X.509 capabilities, including a PKIX-conformant certificate validation system, into the PGP software development kit. His expertise is in networking protocols and applied cryptography. He is the author of the PGP/MIME specification (RFC2015), and recently submitted a draft of the OpenPGP/TLS specification to the IETF. He has implemented most of the Public Key Cryptography Standards, including PKCS#7 (S/MIME v2). Prior to work on PGP, he implemented the IDUP-GSS-API and worked on the implementation of the MIME Object Security Services (MOSS, RFC1848). He holds a B.S. in Physics from Harvey Mudd College.

Background of intended audience

Technical audience. Most people are already electronic mail users, but the discussion will include protocol issues associated with digital signatures and encryption of message content. There will also be some discussion of cryptographic algorithms.