Session Title: Unfinished Business: What's Next for IPsec?

Chair: Dr. Stephen Kent, BBN Technologies
Panelists: Roy Pereria, TimeStep Corporation
Dr. Steven Bellovin, AT&T Research
Luis Sanchez, BBN Technologies

Abstract:

Late last year, the IPsec working group of the Internet Engineering Task Force (IETF) published the long awaited Ipsec standards, as RFCs 2401-2410. Many vendors are implementing IPsec in end user systems and in security gateways, and an ongoing testing program has uncovered and resolved many details necessary to ensure cross-vendor interoperability. However, as deployment of IPsec has progressed, concerns have been raised about interactions with various aspects of deployed networks, e.g.,, firewalls, intrusion detection systems, network address translation (NAT), and wireless retransmission schemes. Others have raised questions about the ability to IPsec to address security problems in more complex network topologies. This panel brings together individuals who play a major role in the development of IPsec and related standards. They will discuss activities underway in the IETF to address the questions raised above.

Presentations:

Stephen Kent, author of the IPsec architecture document and of the AH and ESP protocol standards, will provide an overview of IPsec, setting the context for the panel.

Roy Pereria, chairs a newly formed IETF working group standardizing the use of IPsec for remote access, e.g., road warriors and telecommuters. He will discuss some of the problems that being addressed by this IETF working group.

Steven Bellovin is the author of a proposal for a "transport friendly" version of ESP, designed to permit disclosure of selected transport protocol control data. He will discuss the sorts of problems that arise when such data is concealed by ESP, and possible solutions.

Luis Sanchez chairs a newly formed IETF working group that is developing standards for policy management in the IPsec context. He will describe how the output of this IETF working group will facilitate use of IPsec in more complex Internet and intranet topologies.

Audience Profile:

This panel session is appropriate for attendees interested in the issues surrounding use and deployment of IPsec, e.g., individuals responsible for network management and security administration.

Biographies:

Stephen Kent is Chief Scientist- Information technology for BBN Technologies, and Chief Technical Officer for CyberTrust, both parts of GTE. Over the last 20 years his R&D activities have included the design and development of user authentication and access control systems, network layer encryption and access control systems, secure transport layer protocols, secure e-mail technology, multi-level secure (X.500) directory systems, public-key certification authority systems, and key recovery (key escrow) systems. His most recent work focuses on public-key certification infrastructures for government and commercial applications and security for Internet routing. Dr. Kent has published numerous papers, served as general chair, program committee chair and review for several security conferences, and has lectured on network security throughout the world. He is a Fellow of the ACM and received the PhD in Computer Science from MIT.

Roy Pereira is the senior product manager for TimeStep Corporation, a Newbridge affiliate dedicated to developing secure virtual private network (VPN) solutions. At TimeStep, he is heavily involved with product management, product direction, product integration and security. Roy is an active member and an author in IETF's IPsec and IP Compression working groups. His previous position was that of security architect where he was involved in Internet standards and new technology. After having completed undergraduate computer science studies at Carleton University, Roy has over 11 years experience in the software development industry with a focus on Internet protocols, telecommunications protocols, software APIs, and email systems.

Luis A. Sanchez is a Senior Scientist in the Department of Internetwork Research of BBN Technologies. He is co-principal investigator of the External Routing Intrusion Detection System (ERIDS) and Lead Designer/Developer of the Policy Based Security Management System (PBSM) both DARPA funded projects. He co-designed Rapid Authentication for Mobile IP. Mr. Sanchez also designed and implemented BBNPlanet's first ISM wireless network that used IPsec protocols to protect all IP traffic. He also designed the 3rd generation of BBNPlanet's Firewall service which provides VPN capabilities using swIPe. Mr. Sanchez is the author of several Internet Drafts and co-chairs the IPsec Policy WG of the Internet Engineering Task Force. He received his B.Sc. degree in electrical engineering from the University of Puerto Rico, Mayaguez Campus, in 1989 and a MS degree in electrical engineering from Boston University in 1994. He is currently a full-time employee at BBN Technologies and a part-time PhD candidate at Boston University

Steven M. Bellovin received a B.A. degree from Columbia University, and an M.S. and Ph.D. in Computer Science from the University of North Carolina at Chapel Hill. While a graduate student, he helped create netnews; for this, he and the other perpetrators were award the 1995 Usenix Lifetime Achievement Award. He joined AT&T Bell Laboratories in 1982. Despite the fact that he has not changed jobs, he is now at AT&T Labs Research, working on networks, security, and why the two don't get along. He was named an AT&T Fellow in 1998. Bellovin is the co-author of the book ``Firewalls and Internet Security: Repelling the Wily Hacker'', and holds several patents on cryptographic

and network protocols. He served on a National Research Council study committee on information systems trustworthiness is a member of the Internet Architecture Board, and is currently focusing on how to design systems that are inherently more secure.

Contact Information:

Stephen Kent
BBN Technologies /GTE Corporation
10 Fawcett Street
MS 11/2A
Cambdidge MA, 02139
Voice: (617) 873-3988
Fax: (617) 873-4086
Email: kent@bbn.com

Roy Pereira
TimeStep Corporation
voice: (613) 599-3610
fax: (613) 599-3610
email: rpereira@timestep.com

Luis A. Sanchez
BBN Technologies/GTE Corporation
10 Moulton St.
Cambridge, MA 02138
Tel: (617)873-3351
Fax: (617)873-6091
lsanchez@bbn.com