PANEL: IPSEC: FRIEND OR FOE

Panel Chair: Dan Nessett (3Com Corporation, United States)
Rodney Thayer, EIS Corporation
Bob Braden, USC/ISI
Steve Bellovin, AT&T Labs Research

While IPSec solves a number of significant security problems, it introduces problems of a different kind. For example, when IP packets are encrypted using ESP, any TCP/UDP port information they contain cannot be used for packet classification in intermediate routers. This has a deleterious effect on certain QoS services provided in routers and managed by protocols such as RSVP. Other network services, such as those gathering RMON2 data, also rely on the ability of intermediate network devices to observe transport protocol port information. Thus, encrypting packets using IPSec can interfere with network management. Finally, network intrusion systems utilize information gleaned from network traffic to recognize potential network attacks. When this information is encrypted, intrusion detection is complicated.

This panel will examine the advantages of IPSec and compare them to its disadvantages. It is organized so that one panel member will present the case for IPSec, another the case against it, and a third will explore how the disadvantages of IPSec might be mitigated.