SNMPv3 with Security and Administration

Dr. Jeffrey D. Case
SNMP Research Inc.

The Internet-standard management framework, based on the Simple Network Management Protocol, or SNMP, has become a global standard for managing internets and intranets. SNMP is being used to monitor and control not only the networks, but also the systems that connect to the network, the applications that run on those systems, and the services they provide.

As a result of these application environments, there are requirements for strong security for the management function in many environments.

SNMP version 1, or SNMPv1, has enjoyed unparalleled success as an interoperable management solution. However, it had multiple shortcomings, the most notable of which was its lack of strong security.

The standards community and vendors have addressed these shortcomings. A new version of the Internet-standard management framework, based on SNMP version 3, or SNMPv3, was introduced in early 1998. In 1999, the Internet Engineering Task Force (IETF), the relevant standards-setting body for the Internet, promoted the standards documents from proposed standards to draft standard, the penultimate level. The vendor support for SNMPv3 is also increasing. Multiple vendors began shipping off-the-shelf products, which had implemented the SNMPv3 in 1998. The numbers of available products, which support the SNMPv3, have increased continuously since that time.

The primary enhancements to the SNMPv3, which are likely to be of interest to the attendees of the 23rd National Information Systems Security Conference, are in the area of security and the administration thereof. SNMPv3 supports commercial-grade security, including authentication, authorization, access control, and privacy.

This panel session, led by one of the co-authors of SNMP, will describe SNMPv3, a worthy successor to SNMPv1 and SNMPv2c, from multiple viewpoints:

> o The standards view
> o The vendor view
> o The user view

The session will also address the security architecture, layering, and operations, including key management and coexistence and transition issues.