Using SNMP to Communicate Security Info

Rick Crawford
Dan Zerkle

November 11, 1994

SNMP – Simple Network Mgmt Protocol

- SNMP protocol is <u>connectionless</u> – runs directly on UDP.

  Fairly robust in a glitchy network environment.

- SNMPv1 entity model envisions 2 levels – <u>Managers</u> and <u>Agents</u>.

  SNMPv2 supports multiple levels, Proxy relationships, and communication between Managers.

- Mgmt Info Base – MIB – database offers views of state variables.

  All devices of a certain class – e.g., routers – have the same state variables predefined on them.

- SNMP Manager issues commands to Agent – *GetRequest* and *SetRequest*.

  Agent responds with *GetResponse* or *Trap* data.

Why Use SNMP for Security?

- SNMPv1 is already in wide usage.

- Successful technology transfer requires easy integration of new security modules into existing network management tools.

- Need to make security an integral part of network management.

- SNMPv1 security is almost nonexistent. SNMPv2 adds authentication and encryption to the SNMP protocol.

Invoking Tripwire via SNMP

- Tripwire enhances security by detecting file modifications.
- UCD Security Lab has integrated Tripwire into SNMP.
- SNMP Manager requests an Agent to compute various crypto checksums for particular files.

Current Directions Using SNMP

- “MIB-ify” other security services – e.g., COPS, NSM.

- Performance checking in various network environments and intrusion scenarios.

- Analysis of SNMP protocols for crypto security and authentication integrity.