Network Security Management

Brandon Hill

April 29, 2008
What is network security management?

Security Management is the process of controlling the security of a complex data network so as to maximize the security level that it provides to its’ users.
What forms of management are there?

- Management of network security
- Securing the network management
What kinds of security are there?

Simple security taxonomy:
- Traffic-based security vs. User-based security
- Prevention vs. Detection
Firewalls and Routers

- Both can serve as a preventative, traffic-based security
- Both regulate traffic between networks (sometimes networks of different trust levels)
- Firewalls often stand as the first line of defense for a network (sometimes the only defense)
- Can also encrypt data, act as a NAT server, or a proxy server to mask a network
Authentication, Authorization, and Accounting

Authentication validate a user as being who they claim to be
Authorization restrict user access to those part of the network they need to use
Accounting track user usage patterns
Different forms:

- Userid/passwd management (NIS, LDAP, ActiveDirectory, Kerberos)
- Access code management
- Remote access management (PPP, SLIP, ARAP, VPN)
Most of the listed systems can also be set to aid the detection of security breaches.

- Firewalls can detect peaks of certain packet types (DOS attacks)
- Routers can detect strange packet behavior
- User management systems can detect strange usage patterns
- Intrusion Detection Systems (IDS) can be set to watch for patterns of behavior on the network
Coordination

With all of these systems, how are they coordinated? How are all the abberant behaviors reported?

With networks being made from a collection of devices from different vendors, a common protocol is needed. Today that protocol is Simple Network Management Protocol (SNMP). Tomorrow it may be Web-Based Enterprise Management (WBEM). Either way, it is this protocol that allows different devices from different vendors to speak to different network management software systems.
Requirements of a Network Management Protocol

For a network management protocol to be useful on a large scale, it must be able to have some control over the network devices. But being able to control network devices directly is a huge security risk. These messages must be encrypted. This is the security of the network management.
SNMP didn’t get any significant security measures until version 3

- encryption
- authentication
- access control
- counters to fight playback attacks

WBEM was built with security in mind

- authentication
- authorization
- secure messaging
- auditing
- role assumption
SNMP and WBEM are just protocols. The security management is done with tools that use these protocols.

- Cisco Active Network Abstraction A network resource management platform for large networks
- Hewlett Packard OpenView framework
- Microsoft Operations Manager (MOM)
- NetDirector open source change and configuration management
- ProCurve Manager (PCM+) Comprehensive Management Software
- CiscoWorks CiscoWorks Lan Management Solution Manager enterprise switching networks
- and so many more... (the list is real long)
The thing that gets left out of most network security management systems is people.

Beyond user-based management, there is people management.

85% of all network breaches are inside jobs. A network must be as secure from the inside as it is from the outside.