Distributed Network Management Security

Paul Meyer

Secure Computing Corporation
2675 Long Lake Road
Roseville, MN 55113

Phone: (612) 628-2700
Fax: (612) 628-2701
email: paul_meyer@securecomputing.com
Problems with SNMPv2 Security

- Scalability with RFC 1441 - 1452
- Migration from existing SNMPv1 base
- Key Management
- The SNMPv2 ‘meltdown’
DNMS Solution

- Place SNMP Security Services on Firewall
- Add use of certificates for keys
- Allow SNMPv1 messages
- Autodetection of Management Entities
- Architecture on following slide
Crypto Service Functions
- ensure authentication seal for inbound traffic is authentic (if present)
- ensure outbound traffic contains authentication seal (if required)
- ensure data integrity for both inbound and outbound (if required)
- ensure confidentiality for outbound traffic (if required)
- decrypt inbound traffic and encrypt outbound traffic when required

Network Proxy
- Routing
- Talk NetMgmt Protocol

Crypto Services

Admin Proxy
- Access Control Checks
- Bandwidth Limits
- Content Filtering
- Talk NetMgmt Protocol

Outside

Inside

UDP
IP
Phys

UDP
IP
Phys
Type Enforcement

- Type Enforcement is a form of mandatory protection.
- Similar to ‘multilevel security’ but more flexible.
- Access rules based upon ‘domain’ and ‘type’
  - ‘domain’ is a program’s security attribute.
  - ‘type’ is a data item’s security attribute.
- Access is forbidden unless a rule specifically allows it.
  - Accesses can be read, write, execute, create, destroy, chtype, etc.
- Network separation can be guaranteed via Type Enforcement.
Pipelines in Type Enforcement

Domain 1

Object Type A

Domain 2

Object Type B

Domain 3

Object Type C

Object Type D
DNMS Use of Type Enforcement

- Each DNMS component runs in a distinct domain
- Network and Admin proxies defined only to external or internal network
- Message flow constrained through crypto proxy
- DNMS has no access to local management data
- Aids in future assurance of operation
Future DNMS Work

- Further use of centralized Key Management
- Add notifications (Traps and v2 Informs)
- Utilize SNMPv3
  - May move much of crypto services to network and admin proxies
- Really do autodetection
- Investigate use of network-level encryption in conjunction with DNMS/SNMP authentication.
DNMS as an SNMP Guard

- Add Access Control to flow
- Filter by SNMP views and objects
- Add filtering of content