Knobs, Levers, Dials and Switches: Now and Then

(please sir, may I have some more ?)

Draft-jones-opsec-01.txt

opsec@ops.ietf.org (mailing list)

October 20, 2003

George M. Jones <gmjones@mitre.org>

Will my router crash or be 0wN3d ?

- Have you ever been in the middle of tracking/stopping an attack and wondered if your router would crash when you hit return to apply an ACL ?
- Have you ever worried that some script kiddie might be able to knock down your core ?
- Have you every wondered why you still have to uses telnet with clear-text passwords or TFTP with no passwords ?

Do I have the tools I need ?

- Two approaches
  - Muddle through with what you have
  - Ask vendors for better features
- IETF draft(s)
  - BCP == “Now” (the good)
  - Info == “Then” (the bad, the ugly)
- Goal: Security of the network itself

Overview: Major Sections

draft-jones-opsec-01.txt

- Functional
  - Device Management
  - In-Band Management
  - Out-of-Band (OoB) Management
  - User Interface
  - IP Stack
  - Rate Limiting
  - Basic Filtering Capabilities
  - Packet Filtering Criteria
  - Packet Filtering Counter
  - Other Packet Filtering
  - Event Logging
  - AAA
  - Layer 2
- Documentation
- Assurance
- Profiles

Examples: Now

Secure Management Channels

- **Requirement:** Support secure end-to-end channels for all management traffic.
- **Justification:** Insure confidientiality and integrity of management traffic...or “who knows the address of my AAA servers and how do I know some 'miscreant' hasn't redirected them ?”
- **Examples:** IPsec, TLS, SSH, SNMPv3, ?serial console?

Examples: Now

Ability to Identify All Listening Services

- **Requirement:** Provide a means to display all listening services.
- **Justification:** Needed to facilitate risk assessment ("what ports/protocols can attackers see/hack")
- **Examples:** Show listening tcp ports (telnet,ssh,ftp,etc.), which addresses+interfaces are bound.

Examples: Now

Ability to Disable All Listening Services

- **Requirement:** Provide a means to selectevly disable all listening services.
- **Justification:** Reduce risk. Unused services provide potential attack vectors. Allow implementation of local policy.
- **Examples:** Turn off telnet, SNMPv1, echo, chargen...

Examples: Now

Ability to filter traffic TO the device

- **Requirement:** It must be possible to filter traffic directed TO any interface on the device, including loopbacks.
- **Justification:** This allows filters to be applied that protect the device itself from attacks and unauthorized access.
- **Examples:** A global access control list for all "inbound" traffic that only permits traffic from a desginated managemnt network.

Examples: Then

Ability to filter traffic at line rate

- **Requirement:** Filtering must work at line rate on all interfaces.
- **Justification:** Line-rate filtering enables implementation of policy. Performance degradation may make it impossible to respond to attacks directed to or through the device.
- **Examples:** ASICs

Examples: Then

Ability to Withstand Well-Known Attacks

- **Requirement:** The vendor should provide software updates or configuration advice “in a timely fashion” to mitigate the effects of “well known” vulnerabilities and “well known exploits”
- **Justification:** Script kiddies et cetera will try exploits.
- **Examples:** CERT Advisories, CVE entries, Nessus plugins

Examples: Then

Ability to Select Reliable Log Delivery

- **Requirement:** It must be possible to select reliable, sequenced delivery of log messages.
- **Justification:** Reliable logs are needed for investigation of incidents, evidence as well as operations.
- **Examples:** RFC3195, but no implemenations.

Examples: Then

Ability to Log All Security Related Events

- **Requirement:** The logging system must be capable of logging all info related to system security.
- **Justification:** Security related log information is needed to support accountability, incident handling, etc.
- **Examples:** Filter matches, authentication, authorization, configuration, device/interface status change. Problem: no standard list.

Examples: Then

Support Scripting of Management Functions

- **Requirement:** The device must support scripting of all management functions.
- **Justification:** Scripting is necessary when the number of managed devices is large and/or when changes must be implemented quickly.
- **Examples:** Attack tracking, updating filters, config fetching/auditing. Command Line Interface, IETF netconf WG.

Details: Device Management

Requirement #s (1.2.3) listed from -01 draft. Possible disposition in -02 indicated by "==> *action/placement" (discussion, please)*

- Functional Reqs

2.1.1 Support Secure Management Channels
2.1.2 Support Remote Configuration Backup
2.1.3 Support Remote Configuration Restore
2.1.4 Support Management Over Slow Links
2.1.5 Support Scripting of Management Functions
==> *restore CLI and/or on-the-box management reqs to support management in crisis settings ?*
2.1.6 Restrict Management to Local Interfaces
==> *seperate "info" draft ?*

Details: In-Band Management

- Functional Reqs

  2.2 In-Band Management Requirements
  2.2.1 Use Non-Proprietary Encryption
  2.2.2 Use Strong Encryption
  2.2.3 Key Management Must Be Scalable
  ==> *info draft, no BCP*

Details: Out-Of-Band Management

- Functional Reqs

  2.3 Out-of-Band (OoB) Management Requirements
  2.3.1 Support Out-of-Band Management (OoB) Interfaces
  2.3.2 Enforce Separation of Data and Management Channels
  2.3.3 Separation Not Achieved by Filtering
  2.3.4 No Forwarding Between Management and Data Planes

  2.3.2-2.3.4 => info draft, no BCP

Details: User Interface

- Functional Reqs
  - 2.4 User Interface Requirements
  - 2.4.1 Support Human-Readable Configuration File
  - 2.4.2 Display of 'Sanitized' Configuration
  - 2.4.3 Display All Configuration Settings
  - *2.4.2-2.4.3 ==> info draft, no BCP*

Details: IP Stack

- Functional Reqs

  2.5.1 Ability to Identify All Listening Services
  2.5.2 Ability to Disable Any and All Services
  2.5.3 Ability to Control Service Bindings for Listening Services
  2.5.4 Ability to Control Service Source Address
  2.5.5 Support Automatic Anti-spoofing for Single-Homed Networks
  2.5.6 Ability to Disable Processing of Packets Utilizing IP Options
  ==> *info draft, no BCP*
  2.5.7 Directed Broadcasts Disabled by Default
  2.5.8 Support Denial-Of-Service (DoS) Tracking
  2.5.9 Traffic Monitoring
  2.5.10 Traffic Sampling
  2.5.8-2.5.10 ==> info draft, no BCP

Details: Rate Limiting

- Functional Reqs

  2.6 Rate Limiting Requirements
  2.6.1 Support Rate Limiting
  2.6.2 Support Rate Limiting Based on State

Details: Basic Filtering

- Functional Reqs

2.7 Basic Filtering Capabilities
2.7.1 Ability to Filter Traffic
2.7.2 Ability to Filter Traffic to the Device
2.7.3 Ability to Filter Traffic Through the Device
2.7.4 Ability to Filter Updates
2.7.5 Ability to Specify Filter Actions
2.7.6 Ability to Log Filter Actions
2.7.7 Ability to Filter Without Performance Degradation
==> *info draft, ?no BCP?*

Details: Filtering Criteria

- Functional Reqs

2.8 Packet Filtering Criteria
2.8.1 Ability to Filter on Protocols
2.8.2 Ability to Filter on Addresses
2.8.3 Ability to Filter on Any Protocol Header Fields
2.8.4 Ability to Filter Inbound and Outbound
2.8.5 Ability to Filter on Layer 2 MAC Addresses

==> *info draft, no BCP*

Details: Filtering Criteria

- Functional Reqs

  2.9 Packet Filtering Counter Requirements

  2.9.1 Ability to Accurately Count Filter Hits

  2.9.2 Ability to Display Filter Counters

  2.9.3 Ability to Display Filter Counters per Rule

  2.9.4 Ability to Display Filter Counters per Filter Application

  2.9.5 Ability to Reset Filter Counters

  2.9.6 Filter Counters Must Be Accurate

Details: Other Filtering Reqs

- Functional Reqs
  - 2.10 Other Packet Filtering Requirements
  - 2.10.1 Filter, Counters, and Filter Log Performance Must Be Usable
  - 2.10.2 Ability to Specify Filter Log Granularity

Details: Event Logging

- Functional Reqs

2.11 Event Logging Requirements
2.11.1 Ability to Log All Events That Affect System Integrity
==> *info draft, no BCP, seperate draft ?*
2.11.2 Logging Facility Conforms to Open Standards
2.11.3 Ability to Log to Remote Server
2.11.4 Ability to Select Reliable Delivery
==> *info draft, RFC 3195, but implementations lagging*
2.11.5 Ability to Log Locally
2.11.6 Ability to Maintain Accurate System Time
2.11.7 Logs Must Be Timestamped
2.11.8 Logs Contain Untranslated Addresses
2.11.9 Logs Do Not Contain DNS Names by Default
==> *info draft, no BCP*

Details: AAA (1)

- Functional Reqs

  2.12 Authentication, Authorization, and Accounting (AAA)

  2.12.1 Authenticate All User Access

  2.12.2 Support Authentication of Individual Users

  2.12.3 Support Simultaneous Connections

  2.12.4 Ability to Disable All Local Accounts

  2.12.5 Support Centralized User Authentication

  2.12.6 Support Local User Authentication

  2.12.7 Support Configuration of Order of Authentication Methods

  2.12.8 Ability to Authenticate Without Reusable Plaintext Passwords

  2.12.9 No Default Static Authentication Tokens (Passwords

  2.12.10 Static Authentication Tokens (Passwords) Must Be Configured

Details: AAA (2)

- Functional Reqs

  2.12.11 Enforce Selection of Strong Local Static Authentication Tokens (Passwords)

  2.12.12 Support Device-to-Device Authentication

  2.12.11-2.12.12 => info draft, no BCP

  2.12.13 Ability to Define Privilege Levels

  2.12.14 Ability to Assign Privilege Levels to Users

  2.12.15 Default Privilege Level Must Be Read Only

  2.12.16 Change in Privilege Levels Requires Re-Authentication

  2.12.17 Accounting Records

Details: Layer 2 Reqs

- Functional Reqs

  2.13 Layer 2 Requirements

  2.13.1 Filtering MPLS LSRs

  2.13.2 VLAN Isolation

  2.13.3 Layer 2 Denial-of-Service

  2.13.1-2.13.3 ==> info draft, no BCP

  2.13.4 Layer 3 Dependencies

Details: Documentation

- Documentation Reqs

  3. Documentation Requirements
  3.1 Document Listening Services
  3.2 Provide a List of All Protocols Implemented
  3.3 Provide Documentation for All Protocols Implemented
  3.4 Catalogue of Log Messages Available

  3.2-3.4 ==> info draft, no BCP

Details: Assurance

- Documentation Reqs

4. Assurance Requirements
4.1 Ability to Withstand Well-Known Attacks and Exploits
4.2 Vendor Responsiveness
==> *4.1-4.2, info draft, no BCP*
4.3 Comply With ... RFCs on All Protocols Implemented
4.4 Identify Origin of IP Stack
4.5 Identify Origin of Operating System

Details: Profiles

A.1 Minimum Requirements Profile
A.2 Layer 3 Network Core Profile
A.3 Layer 3 Network Edge Profile
A.4 Layer 2 Network Core Profile
A.5 Layer 2 Edge Profile

Review: Major Sections

draft-jones-opsec-01.txt

- Functional
  - Device Management
  - In-Band Management
  - Out-of-Band (OoB) Management
  - User Interface
  - IP Stack
  - Rate Limiting
  - Basic Filtering Capabilities
  - Packet Filtering Criteria
  - Packet Filtering Counter
  - Other Packet Filtering
  - Event Logging
  - AAA
  - Layer 2
- Documentation
- Assurance
- Profiles

So What ?

- You choices
  - Continue to muddle through, hoping the vendors “do the right thing”
  - Work together to tell the vendors what you need

How you can help

- In between fighting fires
  - List the security features you use most
  - List the missing security features you curse vendors for omitting
  - Write a quick "wish list"
- When you have a little time (a dull moments during NANOG ?)
  - Review draft-jones-opsec-01.txt

Keep those cards and letters coming...

- Time is short (IETF draft cut-off October 27)
- Mailing List: opsec@ops.ietf.org, to subscribe: “echo 'subscribe opsec' | mail \ majordomo@ops.ietf.org”
- Archives @ http://ops.ietf.org/lists/opsec/
- Feedback to opsec-comment@ops.ietf.org
- **http://www.ietf.org/internet-drafts/draft-jones-opsec-01.txt**
- Questions ? Comments ? War Stories ?