Knobs, Levers, Dials and Switches: Now and Then

(please sir, may I have some more ?)

Draft-jones-opsec-02.txt
Draft-jones-opsec-info-00.txt

http://www.port111.com/george/talks/opsec-saag/

Will my router crash or be 0wN3d ?

(I need a fix, 'cause I'm going down)

- 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

The Long and Winding Road
(that leads...???)

- UUNET internal security requirements doc
- -00 draft
- BOF @ IETF57
- -01 draft
- NANOG, RIPE/EOF, nsp-sec input
- *-02 draft, *-info-00 draft (BCP/info split)

Overview: Major Sections

draft-jones-opsec-*.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 Counters
  - 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 selectively 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 designated management network.

Examples: Now

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 depredation may make it impossible to respond to attacks directed to or through the device.
- **Examples:** ASICs

Examples: Now

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.

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 implementations

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.

Details/BCP: Device Management

- Functional Reqs
  - 2.1 Device Management Requirements
  - 2.1.1 Support Secure Management Channels
  - 2.2 In-Band Management Requirements
  - 2.2.1 Use Encryption Algorithms Subject To Open Review
  - 2.2.2 Use Strong Encryption
  - 2.3 Out-of-Band (OoB) Management Requirements
  - 2.3.1 Support a Non-IP 'Console' interface
  - 2.3.2 Support A Simple Default Communication Profile...
  - 2.3.3 Support Separate Management Plane IP Interfaces
  - 2.3.4 No Forwarding Between Management Plane And Other Ifs..
  - 2.3.5 Provide Separate Resources For The Management Plane

Details/BCP: Config and Management

- Functional Reqs

2.4 Configuration and Management Interface Requirements
2.4.1 CLI Provides Access to All Configuration and Management Functions
2.4.2 CLI Uses Existing Authentication Mechanisms
2.4.3 CLI Supports Scripting of Configuration
2.4.4 CLI Supports Management Over 'Slow' Links
2.4.5 Support Software Installation
2.4.6 Support Remote Configuration Backup
2.4.7 Support Remote Configuration Restore
2.4.8 Support Human-Readable Configuration File

Details/BCP: IP Stack

- Functional Reqs

  2.5 IP Stack Requirements
  2.5.1 Ability to Identify All Listening Services
  2.5.2 Ability to Disable Any and All Services
  2.5.3 Listening Services Should Be Off By Default
  2.5.4 Ability to Control Service Bindings for Listening Services
  2.5.5 Ability to Control Service Source Address
  2.5.6 Support Automatic Anti-spoofing for Single-Homed Networks
  2.5.7 Directed Broadcasts Disabled by Default

Details/BCP: 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/BCP: 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 Without Performance Degradation
  2.7.5 Ability to Filter Updates
  2.7.6 Ability to Specify Filter Actions
  2.7.7 Ability to Log Filter Actions

Details/BCP: 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

Details/BCP: Filter Counters, Filter Misc

- 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
  - 2.10 Other Packet Filtering Requirements
  - 2.10.1 Filters...Must Have Minimal Performance Impact
  - 2.10.2 Ability to Specify Filter Log Granularity

Details/BCP: Event Logging

- Functional Reqs

  2.11 Event Logging Requirements
  2.11.1 Logging Facility Conforms to Open Standards
  2.11.2 Ability to Log to Remote Server
  2.11.3 Ability to Log Locally
  2.11.4 Ability to Maintain Accurate System Time
  2.11.5 Logs Must Be Timestamped
  2.11.6 Logs Contain Untranslated Addresses

Details/BCP: 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 Methods
  2.12.6 Support Local User Authentication Method
  2.12.7 Support Configuration of Order of Authentication Methods
  2.12.8 No Unencrypted Transmission of Reusable Plain-text Passwords

Details/BCP: AAA (2)

- Functional Reqs
  - 2.12.9 No Default Passwords
  - 2.12.10 Passwords Must Be Explicitly Configured Prior To Use
  - 2.12.11 Ability to Define Privilege Levels
  - 2.12.12 Ability to Assign Privilege Levels to Users
  - 2.12.13 Default Privilege Level Must Be Read Only
  - 2.12.14 Change in Privilege Levels Requires Re-Authentication
  - 2.12.15 Support Recovery Of Privileged Access
  - 2.12.16 Accounting Records

Details/BCP: Layer 2

- Functional Reqs
  - 2.13 Layer 2 Devices Must Meet Higher Layer Requirements

Details/BCP: Doc and Assurance

- Functional Reqs

3. Documentation Requirements
3.1 Document Listening Services
4. Assurance Requirements
4.1 Comply With Relevant IETF RFCs on All Protocols Implemented
4.2 Identify Origin of IP Stack
4.3 Identify Origin of Operating System

Details/BCP: 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-*.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 Counters
  - Other Packet Filtering
  - Event Logging
  - AAA
  - Layer 2
- Documentation
- Assurance
- Profiles

And in the end...

- Already having effects
  - Security engineer @ tier 1 NSP “[security requirements for our] next gen core routers is coming directly from the opsec draft”
  - Large ISP using opsec in testing/purchasing
  - CTO's office of large equipment mfg looking at opsec for product design/security ideas
  - Influenced internal “security roadmap” of router vendor.
  - Some cross-pollination with other IETF drafts

The Road Ahead

- Do we have the right areas ?
- Do we have the right/too many/too few reqs ?
- Do we have the BCP/info split right ?
- *-02 ==> BCP ?
- *-info-00 ==> ???

All we are saying is "give opsec a chance !"

- Time is short
- Mailing List: opsec[-request]@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-02.txt
- http://www.ietf.org/internet-drafts/draft-jones-opsec-info-00.txt
- Questions ? Comments ? War Stories ?