Operational Security Requirements

or

“Give Us The Knobs We Need”

draft-jones-opsec-01.txt

opsec@ops.ietf.org (mailing list)

September 3, 2003

George M. Jones <gmjones@mitre.org>

Agenda

- Welcome and discussion of agenda
- Goals
- History and Current Status
- Related Work
- Overview
- Next Steps, Work Areas, Milestones

Goals

- Goals: The End Game
  - Managed IP network infrastructure devices that can be deployed in a secure fashion, or “Give us the knobs we need”
  - A guide for developers and testers
  - Ongoing discussion of operational security needs
- Methods:
  - Publish BCP RFC (current features)
  - Publish Info RFC (future requirements)

Goals

- Goals: Today
  - Give overview of the document and direction
  - Request feedback on the substance of the document
  - Identifying people interested in contributing

History and Current Status (1)

- Originally a UUNET testing document
- Used as the basis for security qualifications, mostly backbone and edge devices.
- Tired of vendors bringing in boxes that could not be operationally secured
- Tired of hearing “but you're the only one who wants...”
- Decided to get feedback and publish

History and Current Status (2)

- It was thought that many of the requirements where general or generalizable.
- Much musing about scope. Heritage and operating assumptions still show.
- Several restructurings (profiles, etc.) and reformatting (xml2rfc)
- Several rounds of internal and external review.
- Some informal review @ IETFs 55+56
- BOF @ IETF 57 (July 2003)

History and Current Status (3)

- -00 draft published , 6/03, trial balloon
- -01 draft published, 8/03, incorporated feedback
- Collecting comments, will go to -02, then decide where to go

Related Work (1)

- Related Efforts – IETF
  - Netconf
  - syslog
  - Forces
- Related Efforts – Non-IETF
  - Common Criteria
  - ANSI/T1M1 (management, etc.)
  - ANSI/T1S1 (control plane)
- Other ?

Comparison of Requirements Docs

	CC/R&S Profile	ANSI/T1	OPSEC
Produced By	NSA	T1	UUNET/gmj/many
Audience	Device vendors		IP netops, vendor
Goal	Security	Sec. Mgt, etc.	Secure ops.
Scope	IP & ATM	Telecom infra.	IP Infra.
Target(s)	Vendors	Telecom infra.	Routers, switches
Status	Certified	Published Std.	WIP
Published by	NIAP	ANSI/T1	IETF
Costs	0	??	0/participation
Who Certifies ?	Certified lab	??	Self

Overview: Goal

- Goal: “***The goal of this document is to define a list of operational security requirements for network infrastructure devices that implement Internet Protocol (IP). The intent of the list is to provide consumers of IP network infrastructure a clear, concise way of communicating their security requirements to equipment vendors***”

Overview: Scope (1)

- Scope: “***The primary scope of these requirements is intended to cover the*** infrastructure of large IP networks (e.g. routers and switches). Certain groups (or "profiles", see below) apply only in specific situations (e.g. edge or core routers). The requirements listed in the minimum profile are intended to apply to all managed infrastructure devices.
- General purpose hosts ... are explicitly out of scope.

Overview: Structure

- Functional Requirements
  - Device Management...
- Documentation Requirements
- Assurance Assurance
- Profiles
  - Minimum Requirements
  - Layer 3 Core
  - Layer 3 Edge...

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

Overview: 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 ?*

Overview: 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*

Overview: 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

Overview: 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

Overview: 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

Overview: Rate Limiting

- Functional Reqs

  2.6 Rate Limiting Requirements

  2.6.1 Support Rate Limiting

  2.6.2 Support Rate Limiting Based on State

Overview: 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?*

Overview: 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*

Overview: 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

Overview: 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

Overview: 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*

Overview: 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

Overview: 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

Overview: 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

Overview: 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 Catalog of Log Messages Available
  3.2-3.4 ==> info draft, no BCP

Overview: Assurance

- Documentation Reqs

4. Assurance Requirements
4.1 Ability to Withstand Well-Known Attacks and Exploits
4.2 Vendor Responsiveness
==> *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

Overview: 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

Work Areas

- Resolve tensions (for discussion now)
  - BCP vs. non-BCP/info
  - Relationship to other efforts (IETF and non-IETF)
- Simplify compound requirements
- Refine profiles

Next Steps and Milestones

- [done] Publish -01 (August, 2003)
- Solicit more feedback from RIPE, NANOG, other sources (operators).
- Split draft into BCP, non-BCP (Info)
- Publish -02 (October, 2003)
- Decide on future direction, consult IETF Ads
- Publish Informational RFC, merge with ANSI/T1, form Working Group(s).

Adjourn

- Mailing List: opsec@ops.ietf.org, to subscribe: “echo 'subscribe opsec' | mail \ majordomo@ops.ietf.org”
- Archives @ http://ops.ietf.org/lists/opsec/
- Continued feedback/comments welcome.