OPSEC Working Group
Internet-Draft
Intended status: Informational
Expires: September 21, 2007

G. Jones

R. Callon
Juniper Networks

M. Kaeo
Double Shot Security

March 20, 2007

Framework for Operational Security Capabilities for IP Network Infrastructure
draft-ietf-opsec-framework-05

Status of this Memo

Copyright Notice

Abstract

This document outlines work done and documents produced by the Operational Security Capabilities (OPSEC) Working Group. The goal of the working group is to codify knowledge gained through operational experience about feature sets that are needed to securely deploy and operate managed network elements providing transit services at the data link and IP layers.

The intent is to provide clear, concise documentation of capabilities necessary for operating networks securely, to assist network operators in communicating their requirements to vendors, and to provide vendors with input that is useful for building more secure devices. The working group produced a list of capabilities appropriate for large Internet Service Provider (ISP) and Enterprise Networks. This work is intended to refine [RFC3871].

This document also provides guidance for the creation of profile documents which are lists of security features needed in specific operating environments.

Table of Contents

1. Introduction

1.1. Goals

The goal of the Operational Security Working Group is to codify knowledge gained through operational experience about feature sets that are needed to securely deploy and operate managed network elements providing transit services at the data link and IP layers.

It is anticipated that the codification of this knowledge will be an aid to vendors in producing more securable network elements, and an aid to operators in increasing security by deploying and configuring more secure network elements.

This framework document provides an overview of the work done by the working group, and describes the documents produced in this effort.

1.2. Motivation

Network operators need the appropriate feature sets and tools on their infrastructure devices to ensure that they can effectively deploy and manage their networks securely while maintaining the ability to provide reliable service to their customers. Vendors need guidelines on which security features and functionality are critical for operators to be able to reach that goal.

1.3. Threat Model

1.3.1. Threats Addressed, Threats Not Addressed

This section describes the general classes of threats that this work intends to address. Specific threats and attacks are discussed in the documents which are referred to in this framework. Each of those documents enumerate the capabilities which are required to mitigate the risk of these specific threats.

The intent is to address real-world threats to and attacks on network infrastructure devices which have severely impacted network operations or have immediate potential to do so. The intent is NOT to build a complete theoretical threat model or list every possible attack.

The threats are limited to those that affect the management of network infrastructure and its ability to transit traffic. Threats to the confidentiality and integrity of transit traffic are not addressed.

1.3.2. Active, Passive and Combined Attacks

[RFC3552] describes a general Internet threat model which readers of this document should be familiar with. It defines a threat model to describes the capabilities that an attacker is assumed to be able to deploy against a resource. [RFC3552] classifies attacks into two main categories: passive attacks and active attacks. Passive attacks are ones where an attacker simply reads information off the network and obtains confidential and/or private information which can be used to compromise network systems. Active attacks are ones where the attacker writes data to the network and can include replay attacks, message insertion, message deletion, message modification and man-in-the-middle attacks. Often, these passive and active attacks are combined. For example, routing information is diverted via a man-in-the-middle attack to force confidential information to transit a network path on which the attacker is able to perform eavesdropping.

1.3.3. Categories of Threats

The following sections provide a model that can be used to further categorize attacks on infrastructure devices and/or the operating behavior of these devices, and also gives some examples of attacks which fall into each classification.

It is common to categorize threats based on the effects or damage caused by associated attacks. For example, threats generally fall under one of the three categories as defined in [RFC2196]:

- Unauthorized access to resources and/or information
- Unintended and/or unauthorized disclosure of information
- Denial of service

There are a number of attacks, any one of which, if exploited, can lead to any of the above mentioned threats. As one example, if an intruder has taken control of a router (for example by guessing the password) then he could potentially obtain unauthorized access to resources, could gain unauthorized disclosure of information, and could also deny service to legitimate users. This method of categorizing threats based on the result of the threat therefore results in categories which are orthogonal to the cause of the effect, and thus orthogonal to the device capabilities which are needed.

Categorization of attacks based on the capabilities required to mount the attack will allow the analysis and description of the attacks to be more closely aligned with the product capabilities required to

defeat or mitigate the attack.

1.3.4. Threat Sources

The sources of threats in an operational network take many forms. Some sources can be intentional, such as a malicious intruder actively gaining access to an unauthorized resource or causing a denial of service attack. Other sources can be unintentional but still render the network unusable, such as software bugs or configuration mistakes. Many of the unintentional threat sources can be difficult to recognize or prevent. However wherever possible, capabilities and functionality is defined which minimizes the extent of the damage done under these circumstances.

Threats can originate from outside or inside and can be due to vulnerabilities in a device or weaknesses in operational processes. Inside threats pertain to an authorized participant in the operation of the network performing unauthorized actions. Outside threats pertain to any unauthorized network devices or person causing havoc with normal network operations.

On Path network devices are able to read, modify, or remove any datagram transmitted along a given path. Off-path hosts can transmit arbitrary datagrams that appear to come from any hosts but cannot necessarily receive datagrams intended for other hosts.

1.4. Attacks

This section specifies attack categories based on the capabilities required to mount the attack and provides more granular detail of many of the identifiable and recognized threats to which network infrastructure devices are susceptible.

1.4.1. Passive attacks

Passive attacks are ones where an attacker simply reads information off the network and obtains confidential and/or private information which can be used to compromise network systems.

1.4.2. Eavesdropping/Sniffing

The most common form of passive attack is eavesdropping, where the attacker is able to read the data which is being transmitted from the sender to the receiver. In any operational network, the entire data path and every device involved in the data path must be considered for this type of attack. Any information which could be used to potentially gain unauthorized access to a device or is private must be protected. This includes passwords, configuration files and log

files. It is common to think only of protecting the data path and to make sure that data is not diverted along a different path which may be easier to eavesdrop on, such as a wireless network. In many instances it would be wise to consider cryptographically protecting data confidentiality wherever sensitive information is involved.

1.4.3. Off-line Cryptographic Attacks

These attacks typically capture some data which has been cryptographically protected and then use varying means to try and recover the original data. Poor password protection protocols can easily be reverse engineered and poorly chosen passwords can also be easily deciphered. As described in [RFC3552], a number of popular password-based challenge response protocols are vulnerable to a dictionary attack. The attacker captures a challenge-response pair and then proceeds to try entries from a list of common words (such as a dictionary file) until he finds a password that produces the right response.

1.4.4. Active Attacks

Active attacks are ones where the attacker writes data to the network. Generally, any part of a data packet can be forged. When the source IP address is forged, the attack is generally referred to as a spoofing attack. These attacks can be mitigated by filtering traffic based on IP addresses to only allow legitimate traffic to/ from a network.

Not all active attacks require forged addresses and most systems are susceptible to a number of common attack patterns which are described in the next sections. Note that any type of active attack can be used for Denial of Service if the traffic is sent at such a rate that it exceeds a networks link capacity or exhausts device resources.

1.4.5. Replay Attacks

A replay attack is a combination of a passive and an active attack. In this type of attack, the attacker records some number of messages off of the wire and then plays them back to the original recipient. Note that the attacker does not need to be able to understand the messages. He merely needs to capture and re-transmit them.

1.4.6. Message Insertion

In a message insertion attack, the attacker forges one or more messages and injects them into the network. Often these messages will have a forged source address in order to disguise the identity of the attacker.

Message insertion attacks can be used to exploit known vulnerabilities in protocol software. Routers and switches implement protocols which in some cases make use of software which is well known and widely deployed. Malicious attackers therefore may be familiar with the protocol software and be able to exploit known vulnerabilities.

1.4.7. Message Modification

In a message modification attack, the attacker removes a message from the wire, modifies it, and then resends it. The contents of the message may be modified and/or the intended recipient. For example, a hacker might try to modify a DNS response, in order to redirect a client to the wrong server.

1.4.8. Message Deletion

In a message deletion attack, the attacker simply removes a message from the wire.

1.4.9. Man-In-The-Middle

A Man-In-The-Middle attack combines the above techniques in a special form: The attacker subverts the communication stream in order to pose as the sender to receiver and the receiver to the sender. This differs fundamentally from the above forms of attack because it attacks the identity of the communicating parties, rather than the data stream itself. Consequently, many techniques which provide integrity of the communications stream are insufficient to protect against man-in-the-middle attacks.

Man-in-the-middle attacks are possible whenever peer entity authentication is not used. For example, it is trivial to mount man-in-the-middle attacks on local networks via ARP spoofing where the attacker forges an ARP with the victim's IP address and his own MAC address to gain access to a network. The attacker can then do further damage by sending forged messages. Imagine if the victims IP address was that of a TFTP server. The attacker could potentially download invalid system images or configuration files to a network device and subsequently compromise that network device.

1.4.10. Invalid Message

An invalid message attack refers to situations which can be either deliberately invoked or are due to some non-malicious software or configuration error. This attack can be realized if vendors do not conform to standards and send inappropriate control packets which can cause routing loops or neighboring routers to go down. Also, a

malicious individual may launch DoS attacks which flood a device's control plane with enough messages that the device becomes inoperable due to resource starvation.

1.5. Scope

The working group produced a lists of capabilities appropriate for:

- Internet Service Provider (ISP) Networks
- Enterprise Networks

The following are explicitly out of scope:

- general purpose hosts that do not transit traffic including infrastructure hosts such as name/time/log/AAA servers, etc.,
- unmanaged devices,
- customer managed devices (e.g. firewalls, Intrusion Detection System, dedicated VPN devices, etc.),
- SOHO (Small Office, Home Office) devices (e.g. personal firewalls, Wireless Access Points, Cable Modems, etc.),
- confidentiality of customer data,
- integrity of customer data,
- physical security.

These limitations have been made to keep the amount of work and size of documents manageable. While the capabilities listed here may apply to systems outside the scope, no capabilities have been added to account for their unique needs.

While the examples given are written with IPv4 in mind, most of the capabilities are general enough to apply to IPv6.

1.6. Intended Audience

There are two intended audiences: the network operator who selects, purchases, and operates IP network equipment, and the vendors who create these devices.

1.7. Format and Definition of Capabilities

Separate documents were created for specific categories of capabilities. Each individual capability has the following elements:

Capability (what)

The capability describes a policy to be supported by the device. Capabilities are described in terms of "The device is able to...". Capability descriptions do not use [RFC2119] keywords, e.g. they are not phrased as "The device MUST...".

Capabilities should not refer to specific technologies. It is expected that desired capability will change little over time.

Supported Practices (why)

The Supported Practice section cites practices described in [RFC4778] that are supported by this capability. The need to support the cited practices provides the justification for the feature.

In a few cases, practices not listed in [RFC4778] may be listed at the end of the capability document and cited as justification for a capability. This may be necessary if a practice becomes common after [RFC4778] is finished or if there is widespread consensus that the practice would improve security but it is not, for whatever reason, in widespread deployment.

Current Implementations (how)

The Current Implementation section is intended to give examples of implementations of the capability, citing technology and standards current at the time of writing. Examples of configuration and usage may also be given.

Considerations

The Considerations section lists operational and resource constraints, limitations of current implementations, tradeoffs, etc.

1.8. Applicability

These capabilities are intended to give guidance on how best to protect communications infrastructure. Service Providers, Network Operators, and Equipment Suppliers are encouraged to study these capabilities, and prioritize the extent and manner in which they may

implement and/or deploy equipment supporting these capabilities.

Decisions of whether or not to support a specific capabilities are intended to be left with the responsible organization (e.g., Service Provider, Network Operator, or Equipment Supplier). Due to the continuously evolving nature of security threats to networks, and due to significant variations in the specific security threats and requirements in different network environments, it is not appropriate to mandate implementation of these capabilities through legislation or regulation, nor would any mandate be consistent with their intent.

1.9. Intended Use

It is anticipated that the capabilities in these documents will be used for the following purposes:

- as a checklist when evaluating networked products,
- to create profiles of different subsets of the capabilities which describe the needs of different devices, organizations, and operating environments,
- to assist operators in clearly communicating their security requirements,
- as high level guidance for the creation of detailed test plans.
- as guidance for vendors to make appropriate decisions for engineering feature roadmaps.

1.10. Definitions

NOTE: The following definitions are take from RFC3871. Unless otherwise stated, the working group documents use these terms as defined below.

Bogon.

A "Bogon" (plural: "bogons") is a packet with an IP source address in an address block not yet allocated by IANA or the Regional Internet Registries (ARIN, RIPE, APNIC...) as well as all addresses reserved for private or special use by RFCs. See [RFC3330] and [RFC1918].

CLI.

Several capabilities refer to a Command Line Interface (CLI). While this refers at present to a classic text oriented command

interface, it is not intended to preclude other mechanisms which may provide all the capabilities that reference "CLI".

Conformance.

Adherence to proposed standards.

Console.

Several capabilities refer to a "Console". The model for this is the classic RS232 serial port which has, for the past 30 or more years, provided a simple, stable, reliable, well-understood and nearly ubiquitous management interface to network devices. Again, these capabilities are intended primarily to codify the benefits provided by that venerable interface, not to preclude other mechanisms that provide the same capabilities.

Filter.

In this document, a "filter" is defined as a group of one or more rules where each rule specifies one or more match criteria.

In-Band management.

"In-Band management" is defined as any management done over the same channels and interfaces used for user/customer data. Examples would include using SSH for management via customer or Internet facing network interfaces.

High Resolution Time.

"High resolution time" is defined in this document as "time having a resolution greater than one second" (e.g. milliseconds).

IP.

Unless otherwise indicated, "IP" refers to IPv4.

Management.

This document uses a broad definition of the term "management". In this document, "management" refers to any authorized interaction with the device intended to change its operational state or configuration. Data/Forwarding plane functions (e.g. the transit of customer traffic) are not considered management. Control plane functions such as routing, signaling and link management protocols and management plane functions such as remote access, configuration and authentication are considered to be

management.

Martian.

Per [RFC1208] "Martian: Humorous term applied to packets that turn up unexpectedly on the wrong network because of bogus routing entries. Also used as a name for a packet which has an altogether bogus (non-registered or ill-formed) Internet address." For the purposes of this document Martians are defined as "packets having a source address that, by application of the current forwarding tables, would not have its return traffic routed back to the sender." "Spoofed packets" are a common source of martians.

Note that in some cases, the traffic may be asymmetric, and a simple forwarding table check might produce false positives. See [RFC3704]

Out-of-Band (OoB) management.

"Out-of-Band management" is defined as any management done over channels and interfaces that are separate from those used for user/customer data. Examples would include a serial console interface or a network interface connected to a dedicated management network that is not used to carry customer traffic.

Open Review.

"Open review" refers to processes designed to generate public discussion and review of technical solutions such as data communications protocols and cryptographic algorithms with the goals of improving and building confidence in the final solutions.

For the purposes of this document "open review" is defined by [RFC2026]. All standards track documents are considered to have been through an open review process.

It should be noted that organizations may have local requirements that define what they view as acceptable "open review". For example, they may be required to adhere to certain national or international standards. Such modifications of the definition of the term "open review", while important, are considered local issues that should be discussed between the organization and the vendor.

It should also be noted that section 7 of [RFC2026] permits standards track documents to incorporate other "external standards and specifications".

PBR.

Policy Based Routing.

Resource Starvation.

A condition where resources necessary for communication and proper functioning of a network element are unavailable. Such resources might include Bandwidth of a link, memory of a routing device, or CPU time on a routing processor.

Secure Channel.

A "secure channel" is a mechanism that ensures end-to-end integrity and confidentiality of communications. Examples include TLS [RFC4346] and IPsec [RFC4301]. Connecting a terminal to a console port using physically secure, shielded cable would provide confidentiality but possibly not integrity.

Service.

A number of capabilities refer to "services". For the purposes of this document a "service" is defined as "any process or protocol running in the control or management planes to which non-transit packets may be delivered". Examples might include an SSH server, a BGP process or an NTP server. It would also include the transport, network and link layer protocols since, for example, a TCP packet addressed to a port on which no service is listening will be "delivered" to the IP stack, and possibly result in an ICMP message being sent back.

Session.

An instance of protocol establishment, e.g. telnet, BGP, OSPF, etc.

Single-Homed Network.

A "single-homed network" is defined as one for which

* There is only one upstream connection

* Routing is symmetric.

See [RFC3704] for a discussion of related issues and mechanisms for multi-homed networks.

Spoofed Packet.

A "spoofed packet" is defined as a packet that has a source address that does not correspond to any address assigned to the system which sent the packet. Spoofed packets are often "bogons" or "martians".

Secure Network

For the purposes of these documents, a secure network is one in which:

* The network keeps passing legitimate customer traffic (availability).

* Traffic goes where it is supposed to go, and only where it is supposed to go (availability, confidentiality).

* The network elements remain manageable (availability).

* Only authorized users can manage network elements (authorization).

* There is a record of all security related events (accountability).

* The network operator has the necessary tools to detect and respond to illegitimate traffic.

2. Documents

The following describes the documents produced by the OPSEC working group. Each document covers an area important to secure operation of large network infrastructure.

2.1. Framework Document

This document.

2.2. Operator Practices Survey

[RFC4778].

This document provides a survey of current operator practices in the area of securing networks. It lists current practices that are cited as justification for capabilities. It defines a general threat model and classes of attacks.

2.3. Standards Survey

[I-D.ietf-opsec-efforts].

This document provides an overview of other efforts in developing standards, guidelines, best practices, or other information intended to facilitate improvement in network security. Any effort which is known, such as the ANSI T1.276, the NRIC V "Best Practices", ITU-T M.3016 and X.805, the T1S1 effort on securing signaling will be included. The intent is to provide a clear understanding of which efforts are complementary and/or contradictory such that any efforts of future cross-certification of standards may be facilitated.

2.4. Capabilities Documents

[I-D.ietf-opsec-filter-caps],
[I-D.ietf-opsec-logging-caps],
[I-D.ietf-opsec-routing-capabilities].

Capability documents list capabilities needed to support security practices. Each capability document lists capabilities of one logical group of functions (e.g. logging, filtering, etc.). They define a threat model, list individual capabilities, cite practices supported in the Operator Practices Survey and in few cases may define additional practices.

2.5. Profile Documents

Profile documents are intended to list capabilities appropriate to different operating environments such as large Network Service Provider (NSP) core or edge devices or enterprise networks.

Appendix B provides guidance to organizations in creating their own profiles.

3. Security Considerations

Security is the entire focus of this document.

4. IANA Considerations

This document has no actions for IANA.

5. Acknowledgments

The authors gratefully acknowledge the contributions of:

- Pat Cain who agitated for inclusion of the profile guide.

6. Non-Normative References

[I-D.ietf-opsec-efforts]
Lonvick, C. and D. Spak, "Security Best Practices Efforts and Documents", draft-ietf-opsec-efforts-05 (work in progress), December 2006.

[I-D.ietf-opsec-filter-caps]
Morrow, C., "Filtering and Rate Limiting Capabilities for IP Network Infrastructure", draft-ietf-opsec-filter-caps-05 (work in progress), March 2007.

[I-D.ietf-opsec-logging-caps]
Cain, P. and G. Jones, "Logging Capabilities for IP Network Infrastructure", draft-ietf-opsec-logging-caps-02 (work in progress), March 2007.

[I-D.ietf-opsec-routing-capabilities]
Zhao, Y., "Routing Control Plane Security Capabilities", draft-ietf-opsec-routing-capabilities-01 (work in progress), February 2007.

[RFC1208] Jacobsen, O. and D. Lynch, "Glossary of networking terms", RFC 1208, March 1991.

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, October 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2196] Fraser, B., "Site Security Handbook", RFC 2196, September 1997.

[RFC3330] IANA, "Special-Use IPv4 Addresses", RFC 3330, September 2002.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, July 2003.

[RFC3704] Baker, F. and P. Savola, "Ingress Filtering for Multihomed Networks", BCP 84, RFC 3704, March 2004.

[RFC3871] Jones, G., "Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure", RFC 3871, September 2004.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4346] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006.

[RFC4778] Kaeo, M., "Operational Security Current Practices in Internet Service Provider Environments", RFC 4778, January 2007.

Appendix A. Sample Capability Description

This appendix provides a sample capability description. Note the lack of the use of "MUST", etc in the description of the capability. Also note that in the supported practices section it refers both to the current practices document [RFC4778] and to sections of the same document (xxx.1, xxx.2) that describe practices that were not covered in the current practices document.

A.1. Filtering TO the Device

A.1.1. Ability to Filter Traffic on All Interfaces TO the Device

Capability.

The device provides a means to filter IP packets on any interface implementing IP that are non-transit packets.

Supported Practices.

* Profile Current Traffic (Section xxx.1)
* Block Malicious Packets (Section xxx.2)
* Limit Sources of Management ([RFC4778], Section 2.8.2)

Current Implementations.

Many devices currently implement access control lists or filters that allow filtering based on protocol and/or source/destination address and or source/destination port and allow these filters to be applied to interfaces.

Considerations.

None.

Appendix B. Guide to writing profiles

B.1. Introduction

This section provides guidelines for creating security capability profiles. A profile is a list of features that are required to operate a device in a a secure manner in a specific environment.

The determination of which capabilities are requirements is a local decision driven by policy and operational need. In addition, the needed capabilities are likely to change over time as operational requirements and security threats change. Profile writes are encouraged to share their output with the broader Internet community to learn from others experiences.

It is likely that there are or will be other sources of capabilities that could be cited in developing a profile. For example, [I-D.ietf-opsec-efforts] could be used to identify industry-specific standards or regulations that a specific network would need to support.

B.2. Guidance

Profiles should:

- Be uniquely named
- Contain a brief description of the profile
- Describe the context/environment to which they apply
- Reference capabilities defined in appropriate documents. It is assumed that referenced capabilities contain the elements outlined in Section 1.7 and Appendix A, i.e. that there is no need for a detailed description of the capability, justification, etc. in the profile. If referencing documents that do not contain such information, it might have to be included in the profile.
- Be broken down into functional sections (logging, filtering...)
- Indicate level of need for each capability ("required", "recommended"...) in the defined context (NOT in the [RFC2119] sense).

B.3. Sample Profile

The following is an incomplete sample of a profile for edge routers:

B.3.1. Required Capabilities for Edge Routers

Name: Edge Router Profile

Description: This profile defines the capabilities necessary for a network edge device

Context: Large NSP/ISP network providing transit services.

The following are requirements for edge routers:

B.3.1.1. Packet Filtering Profile

- Select by Protocol, [I-D.ietf-opsec-filter-caps] Section 3.5
- Select by Addresses, [I-D.ietf-opsec-filter-caps] Section 3.6
- Select by Protocol Header Fields, [I-D.ietf-opsec-filter-caps] Section 3.7

.
.
.

B.3.1.2. Logging

- Logs Sent To Remote Servers, [I-D.ietf-opsec-logging-caps] Section 2.2
- Ability to Select Reliable Delivery, [I-D.ietf-opsec-logging-caps] Section 2.3
- Ability to Remotely Log Securely, [I-D.ietf-opsec-logging-caps] Section 2.4
- Ability to Log Locally, [I-D.ietf-opsec-logging-caps] Section 2.5

.
.
.

B.3.2. Recommended Capabilities for Edge Routers

The following are desired capabilities for edge routers:

B.3.2.1. Packet Filtering Profile

- Minimal Performance Degradation, [I-D.ietf-opsec-filter-caps] Section 6

.
.
.

Authors' Addresses

George M. Jones

Phone: +1 703 488 9740
Email: gmj3871@pobox.com

Ross Callon
Juniper Networks
10 Technology Park Drive
Westford, MA 01886
U.S.A.

Phone: +1 978 692 6724
Email: rcallon@juniper.net

Merike Kaeo
Double Shot Security
3518 Fremont Avenue North #363
Seattle, WA 98103
U.S.A.

Phone: +1 310 866 0165
Email: merike@doubleshotsecurity.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).