OPSEC
Internet-Draft
Intended status: Best Current Practice
Expires: February 14, 2008

P. Cain
The Cooper-Cain Group, Inc.
G. Jones
Port111 Labs.
August 13, 2007

Logging Capabilities for IP Network Infrastructure
draft-ietf-opsec-logging-caps-04

Status of this Memo

Copyright Notice

Abstract

This document lists logging capabilities originally identified in Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure [RFC3871] and needed to support current operational practices, including those described in Operational Security Current Practices In Internet Service Provider Environments [RFC4778]. Logging is defined as the delivery of messages about the device, the data passing through the device, or the device's interaction with another device and has been traditionally provided via the syslog or SNMP protocols.

Table of Contents

1. Introduction

This document defines a set of capabilities for network equipment that generates event logs or performs event logging in the environments defined by Operational Security Current Practices In Internet Service Provider Environments [RFC4778]. Its goal is to identify capabilities required of the network equipment to generate and forward messages from the network equipment to an event logging system.

Although most people equate logging with using the syslog protocol [RFC3164], other protocols such as SNMP [RFC3411] are quite capable of generating a log entry for transmission to a remote log entry collector.

RFC4778 defines the goals, motivation, scope, definitions, intended audience, threat model, and potential attacks for each of the practices currently in use by network operators. Those current practices have been identified and refined to generate the capabilities listed in this document.

1.1. Security Overview

The logging capabilities defined in this document are derived from observations and experiences in real world networks where unexpected activities in a network infrastructure caused concern to the network operator. Examples of such activities are:

An adversary or unauthorized user login into an infrastructure

device. The risk is that the configuration or other operating parameter could be modified.

A device becomes overwhelmed, throttles, or crashes. Without logging or some other mechanism to notify the operator of the condition, the operator will not know that an action is required to return the device to optimal operating condition.

Network problems cannot be properly diagnosed without sufficient information, which if not captured, will not be available for diagnose activities.

The main threat in a logging infrastructure is that a bad event may happen and the operator of the infrastructure may not be made aware of that event and therefore cannot correct or respond to it. This document is concerned solely with the ability of the network device to generate appropriate messages. For guidance on transport and secure delivery see The BSD Syslog Protocol [RFC3164]. For a logging infrastructure introduction and guidance on building a secure

infrastructure see NIST Publication 800-62, Guide to Security Log Management. [SP800-92]

One threat to the logging infrastructure is a self-inflicted denial of service attack due to an overwhelming amount of log messages generated on the local machine. This could be caused by the local system using all its available effort to generate log messages or congestion through the network between the log generator and the log collector, such that the remote system is inaccessible to management operations. Although not specifically a capability, care should be taken when configuring the logging infrastructure to account for this threat.

1.2. Capabilities vs. Requirements

Capabilities may or may not be requirements. That is a local determination that must be made by each operator with reference to the policies that they must support. This document, together with RFC4778, will assist network operators in identifying their security capability requirements and communicating them clearly to vendors.

Capabilities are defined without reference to specific technologies.

This is done to leave room for deployment of new technologies that implement the capability. Each capability cites the practices it supports. Current implementations that support the capability are cited.

1.3. Format

Each capability has the following subsections:

- Capability (what)
- Discussion
- Supported Practices (why)
- Current Implementations (how)
- Considerations (caveats, resource issues, protocol issues, etc.)

The Capability section describes a feature to be supported by the device. The Supported Practice section cites practices described in RFC4778 that are supported by this capability. The Current Implementation section is intended to give examples of implementations of the capability, citing technology and standards current at the time of writing. It is expected that the choice of features to implement the capabilities will change over time. The

Considerations section lists operational and resource constraints, limitations of current implementations, trade offs, etc.

2. Functional Capabilities of Log Generating Systems

The capabilities in this section are intended to list testable, functional capabilities that are needed to operate devices securely and meet the obligations of Section 1.1 Security Overview.

2.1. Logging Facility Uses Protocols Subject To Open Review

Capability

The device is capable of providing a logging facility that is based on protocols subject to open review.

Discussion

The use of logging based on protocols subject to open review permits the operator to perform archiving and analysis of logs without relying on vendor-supplied software and servers.

Supported Practices

* Use IETF-defined protocols such as syslog, syslog with reliable delivery, syslog-ng, or SNMP.

Current Implementations

This capability can be satisfied by the use of one or more of syslog [RFC3164], syslog with reliable delivery [RFC3195], TACACS+ [RFC1492], RADIUS [RFC2865], or SNMP [RFC3415].

The current best solution seems to be the following:

* Implement syslog as in .

* Consider implementing syslog with reliable delivery [RFC3195].

* Using SNMP with applicable security controls.

Considerations

None.

2.2. Logs Sent To Remote Servers

Capability

The device is capable of supporting transmission of records of security-related events to one or more remote collection devices. There should be configuration settings on the device that allow selection of destination servers.

Discussion

None.

Supported Practices

* Use multiple collection devices to enhance reliability.

* Use different collection devices to segregate different event sensitivity levels. See Section 2.6.

Current Implementations

This capability may be satisfied by the use of one or more of: syslog [I-D.ietf-syslog-protocol], syslog with reliable delivery [RFC3195], TACACS+ [RFC1492], or RADIUS [RFC2865].

Considerations

This capability is important because it supports individual accountability. It is important to store the security-related events on a separate server to preserve them in case of failure or compromise of the managed device.

This capability also supports analysis. It's easier to run a perl script and insert things into a database on a logging server dedicated to the task than a resource strapped router that may not even have the necessary tools.

Note that there may be privacy or legal considerations when logging/monitoring user activity.

High volumes of logging may generate excessive network traffic and/or compete for scarce memory and CPU resources on the device.

2.3. Ability to Select Reliable Delivery

Capability

The device is able to select reliable delivery of log messages.

Discussion

Reliable delivery is important to the extent that log data is depended upon to make operational decisions and perform forensic analysis. Without reliable delivery, log data becomes a collection of hints instead of a true record of events.

Supported Practices

* Use syslog-ng.
* Use syslog with TLS [I-D.ietf-syslog-transport-tls]
* Tunnel the logging stream over a TCP-based connection.
* Use an out-of-band network to connect critical logging devices to the collection device.

Current Implementations

One example of reliable syslog delivery is defined in I-D.ietf-syslog-transport-tls. Syslog-ng provides another example implementation, although the protocol has not been standardized.

Considerations

Reliable delivery should be used if the path from the log event generator to the collection device transits administrative domains or uses unreliable channels, as it is important that the entire stream of log events is captured.

CAUTION: The use of reliable delivery is heavily debated within the logging and security communities as errors encountered when reliably logging can cause the log generator to repeatedly attempt to deliver the log message in turn causing a denial of service or deadlock condition. It may be desirable to use a rate-limiting

features in syslog senders or for the logger of a message to have the option to either not log more messages or cease its own

operation. This document does not specify which options to use.

2.4. Ability to Remotely Log with Privacy

Capability

The device is capable of delivering log data stream to the collection device in a confidential manner.

Discussion

While syslog *could* provide this capability, it has many security issues and by itself does not address issues from the threat model. See the security considerations section of RFC3164 for a list of issues. Syslog with reliable delivery provides solutions to most/all of these issues, however at the time of this writing there are few implementations. Other possible solutions might be to tunnel syslog over a secure transport, but this often raises difficult key management and scalability issues.

Supported Practices

* Log data tunnelled within IPSec or SSH.
* Use syslog-ng.
* Use security services supplied by SNMP [RFC3414]

Current Implementations

There is no common implementation of this capability.

Considerations

Delivering log data across untrusted streams or including

sensitive data in a event data may require additional countermeasures to protect the data. This concern should not be addressed lightly.

ISPs are fully aware that there is no security with syslog but IPSec is considered too operationally expensive and cumbersome to deploy. Implementations of syslog such as Syslog-ng and stunnel could be used for better authentication and integrity protected solutions. Physical security and access controls are important in

the prevention of unauthorized access and modification of logs.

2.5. Ability to Log Locally

Capability

The device is capable of logging data locally on the device itself into non-volatile storage.

Discussion

Logging of failed authentication attempts to local non-volatile storage is critical as it provides a record of events if the device gets isolated from its authentication interfaces or an attack overwhelms the console interface. Local logging is also important for viewing information when connected to the device and it provides some backup of log data in case remote logging fails.

Local logging also provides a way to quickly view logs relevant to one device without having to sort through a possibly large set of logs from other devices at the collection device.

Supported Practices

* To conserve space, only failed device logins and network connectivity issues are logged locally.

Current Implementations

One example of local logging would be a memory buffer that receives copies of messages sent to the remote log server.

Another example might be a local syslog server (assuming the device is capable of running syslog and has some local storage).

Considerations

Storage on the device may be limited. High volumes of log messages may quickly fill the available storage, in which case there are two options: new logs overwrite old logs (possibly via the use of a circular memory buffer or log file rotation) or

logging stops.

2.6. Ability to Log Different Severities to Different Destinations

Capability

The device is capable of specifying different severity levels of log message to be delivered to different collection destinations.

Discussion

A network of multiple devices may generate a significant amount of log data. The ability to send critical log messages, for example a root login, to a specific destination device will enhance the ability of the network operator to notice the critical event.

Supported Practices

* Email critical event notices to a continuously monitored mailbox.

* Send critical event notices to a separate log collector that scrolls received messages upon a large display in the NOC.

Current Implementations

There are no common implementations of this capability.

Considerations

The use of multiple collectors will incur maintenance and reliability issues. In some cases, multiple filters watching a single collection point may be more efficient than using multiple collectors.

2.7. Ability to Log to Multiple Destinations

Capability

The device is capable of allowing log message to be delivered to multiple collection destinations.

Discussion

All ISPs have multiple syslog servers - some ISPs choose to use separate syslog servers for varying infrastructure devices (i.e., one syslog server for backbone routers, one syslog server for customer edge routers, etc.). This duplication provides a backup mechanism to see what is going on in the network in the event that a collection device 'forgets' to capture syslog messages if its CPU is busy.

Supported Practices

* Use multiple log servers to enhance reliability.

Current Implementations

Most ISPs use multiple, sometimes geographically diverse, log collectors.

Considerations

None.

2.8. Ability to Maintain Accurate System Time

Capability

The device is capable of maintaining accurate, "high resolution" system time.

Discussion

Accurate time is important to the generation of reliable log data. Accurate time is also important to the correct operation of some authentication mechanisms.

The ability to correlate network events from different devices is directly related to the accuracy of the log timestamps. If a time line cannot be constructed, the event logs and forensic data are useless.

Supported Practices

* The time is derived from NTP which is generally configured as a flat hierarchy at stratum-1 and stratum-2 servers to have less configuration and fewer maintenance issues.

* Each router is configured with one stratum-1 peer both locally and remotely.

Current Implementations

This capability may be satisfied by supporting the Network Time Protocol (NTP) [RFC1305], Simple Network Time Protocol (SNTP) [RFC4330], or via direct connection to an accurate time source.

Considerations

System clock chips are inaccurate to varying degrees. System time should not be relied upon unless it is regularly checked and synchronized with a known, accurate external time source (such as an NTP stratum-1 server). Also note that if network time synchronization is used, an attacker may be able to manipulate the clock unless cryptographic authentication is used.

2.9. Display Timezone and UTC Offset

Capability

The device is capable of displaying and logging system time in a timezone or offset from Universal Time Coordinated (UTC).

Discussion

None.

Supported Practices

* The log timestamps include a timezone indicator like "-05:00".

Current Implementations

Many devices support this capability.

Considerations

Knowing the timezone or UTC offset makes correlation of data and coordination with data in other timezones possible. Bob is in Newfoundland, Canada which is UTC -3:30. Alice is somewhere in Indiana, USA. Some parts of Indiana switch to daylight savings time while others do not. A user on Bob's network attacks a user on Alice's network. Both are using logs with local timezones and no indication of UTC offset. Correlating these logs will be difficult and error prone. Including timezone, or better, UTC offset, eliminates these difficulties.

Notice that a physical location may have different offsets from UTC during a year as summer time, daylight savings time, or other local customs are applied.

2.10. Default Timezone Should Be UTC

Capability

The device is capable of using UTC for its default timezone for display and logging. The device may be capable of supporting a mechanism to allow the operator to specify the display and logging of times in a timezone other than UTC.

Discussion

Knowing the timezone or UTC offset makes correlation and coordination in other timezones possible.

Supported Practices

* The timezone offset can be entered as part of configuration of a device.

Current Implementations

Bob in Newfoundland (UTC -3:30) and Alice in Indiana (UTC -5 or UTC -6 depending on the time of year and exact county in Indiana) are working an incident together using their logs. Both left the default settings, which was UTC, so there was no translation of time necessary to correlate the logs.

Considerations

None.

2.11. Log Entries Must Be Timestamped

Capability

By default, the device should be capable of generating timestamps on all log messages, accurate to within a second or less, and including a timezone. The device should be capable of disabling the generation of timestamps.

Discussion

Accurate timestamps are necessary for correlating events, particularly across multiple devices or with other organizations. This applies when it is necessary to analyze logs.

Supported Practices

* Each entry into the log file contains a time value.

Current Implementations

This capability may be satisfied by writing timestamps into syslog messages.

Considerations

It is difficult to correlate logs from different time zones. Security events on the Internet often involve machines and logs from a variety of physical locations. For that reason, UTC is preferred, all other things being equal.

2.12. Log on Exception or Identified Event

Capability

The device is capable of generating log entries on exceptions (e.g., failures) or event matching (e.g., generate a log entry if an event happens) via a configurable value.

Discussion

Traditionally, log events are generated on exceptions, such as failures or errors. Often this is not sufficient as a network operator cannot tell if an attacker failed to log into a device once, or failed once and then succeeded on the second try. Devices should be configurable to allow for log messages on failures, successes, or everything.

Supported Practices

* Log all login events to a device but have only the collection device alert on failures.

* Log successful device configuration changes since one must be aware of all modifications on some types of devices.

Current Implementations

Some ISPs put in passive devices to see routing updates and withdrawals, so that they do not rely solely on the device for log files.

Considerations

None.

2.13. Logs Contain Untranslated IP Addresses

Capability

The device is capable of NOT using the DNS name of the log message generating device in event messages and logs. The device will use the IP Address of the log message generator in its logs.

Discussion

Although sometimes less obtuse than DNS names, IP address assignments tend to be more stable than DNS entries. If an operator is trying to correlate a historical event, the DNS name may have been changed from that used at the event. To ease this confusion, the IP address of the source of the action that caused the log event should be retained in the log entry.

Supported Practices

* Include the source IP address in all log messages.

* Although a corresponding DNS name is useful, DNS lookups can be slow and consume resources.

Current Implementations

Most devices include the source IP in event logs

Considerations

A failed network login should generate a record with the source address of the login attempt, but the Source addresses may be spoofed. Network-based attacks often use spoofed source addresses so they should not be completely trusted unless verified by other means. Having accurate timestamps in the logs increases the chances that the use of an address can be correlated to an individual.

2.14. Logs Contain Records Of Critical Security Events

Capability

The device is capable of generating a log event for at least the following events:

* authentication successes

* authentication failures
* session termination
* authorization changes
* configuration changes
* device status changes

Discussion

The main function of any of these log messages is to see what the device is doing, as well as to try and ascertain what certain malicious attackers are trying to do.

Typically, the data logged will contain the source and destination IP addresses and layer 4 port numbers as well as a timestamp.

Supported Practices

* Examples of events recorded include: user logins, bad login attempts, logouts, user privilege level changes, configuration commands issued by privileged users, and system startup/ shutdown events.

Current Implementations

Most devices crudely support this capability.

Considerations

This list is far from complete. Note that there may be privacy or legal considerations when logging/monitoring user activity or personal information.

This is an important capability because it supports individual accountability and auditing as well as forensics. See section 4.5.4.4 of Site Security Handbook [RFC2196].

2.15. Logs Contain Records of General Security Events

Capability

The device is capable of generating a log record for all other security related events including filtering (or ACL) exceptions, routing protocol state changes, all device access (regardless of authentication success or failure), all commands issued to a device, and all routing events (boot-up/flaps).

Discussion

The main function of any of these log messages is to see what the device is doing as well as to try and ascertain what certain malicious attackers are trying to do.

Typically the data logged will contain the source and destination IP addresses and layer 4 port numbers as well as a timestamp.

Supported Practices

* Examples of events recorded include: ACL matches, filtering exceptions, and individual configuration commands issued by users.

Current Implementations

Most devices crudely support this capability.

Considerations

This list is far from complete. Note that there may be privacy or legal considerations when logging/monitoring user activity or personal information.

This is an important capability because it supports individual accountability and auditing as well as forensics. See section 4.5.4.4 of the Site Security Handbook.

2.16. Logs Do Not Contain Senstitvie Data

Capability

By default configuration, the device is capable of excluding sensitive data such as passwords, plaintext cryptographic keys, and sensitive configuration information, from all audit records including records of successful or failed authentication attempts.

Discussion

A user may make small mistakes in entering a password such as using incorrect capitalization ("my password" vs. "My Password"). Event logs are traditionally dispersed widely so unexpected events

will be noticed. Unauthorized access to event logs that contain these mistakes may compromise more than just the network devices as most users do not have independent passwords for every system.

Supported Practices

* Login failure log messages include the failed username, timestamp, and source IP address, but not the password used.

Current Implementations

Access control and authorization requirements differ for accounting records (logs) and authorization databases (passwords). Logging passwords may grant unauthorized access to individuals with access to the logs. Logging failed passwords may also give hints about actual passwords. See section 4.5.4.4 of Site Security Handbook.

Considerations

There may be situations where it is appropriate/required to log passwords, such as when performing real-time attack analysis. Caution is advised in these rare circumstances.

Even with that caution, there's a remaining risk with logging user names, since many users accidentally type in their password for the username. One way to mitigate this risk is to log only usernames that actually do exist but this adds considerable complexity to a logging system and might allow a different attack vector.

2.17. Devices Should Log Every Message

Capability

Devices should be capable of being configured to either log every

event (possibly with operational degradation) or to drop events due to congestion. If used, the drop capability should be configurable as described in 2.18

Discussion

Many devices implement logging as an afterthought with the device dropping log messages or failing to log critical events when the device is "busy." This behaviour makes forensic analysis difficult, if not impossible. Devices should be configurable to not drop log events. The goal is to be able to enable or disable this feature at times when collection of log messages may trump operational stability.

Supported Practices

* Use multiple logging devices and collectors to capture enough extra messages if one collector is not powerful enough to recreate a full log.

* Use less complex local logging to collect every event as a backup to remote log message omissions.

* Use creative aggregation techniques to capture the essence of every log message but not the overhead of repeated logging, as some versions of the syslogd implementation do when they report "same message received 5 times" instead of logging all five instances.

Current Implementations

Most current implementation use multiple logging devices and caution the user when enabling full logging features.

Considerations

Improper configuration or implementation of this capability may open a device, network, or logging infrastructure to a self-inflicted denial of service attack. With that caution, there are also times when the collection of every log message is important for short time periods.

2.18. Log Drop Policy Should be Configurable

Capability

The device is capapable of being configured to drop log messages due to message volume or storage space constraints. The device should be configurable to either: a) stop logging to all devices, b) drop the oldest log messages, or c) stop logging to the local device, when the local logging device is full.

Discussion

All log devices experience a time when there are more log messages being generated than the system can handle or the local log storage becomes full. Depending on the situation, the operator may want to stop local logging as they are rectifying the logging component, an re-enable it when the many-log-message activity is completed.

A serious concern is to not allow the logging system to be totaly disabled for extended periods of time.

Supported Practices

* Disable local logging to conserve log device resources and use the remote log messages to rectify the situation.

* Disable local logging to retain the initial log messages of the event and use the remote log messages for operation.

* Drop old log messages and retain a full log record at the remote log message collector.

* Stop logging to all devices as troubleshooting progresses and re-enable logging at the return to normal operations.

Current Implementations

Some syslog implementations implement a subset of this capability; other implementation perform quite poorly.

One implementation possibility is to use a Unix-style syslog privilege mechanism, where log messages are divided into categories. Each category has the drop capability so low-value messages could be dropped while still delivering or recording security critical messages to the collection devices.

Considerations

Improper configuration of this capability may cause the complete loss of log messages, which should be considered a serious event.

An administrator or privileged account may be required to configure this capability. Conversely, the log message collector could run monitoring to raise an alarm if log messages are not received periodically from critical devices.

This capability could be extended to include a time-out period such that if a device would restart logging if it was disabled for more than a certain time period.

2.19. Local Log Storage Notification

Capability

The device is capable of notifying remote log collectors if the local log storage device is in danger of complete exhaustion.

Discussion

A remote log message collector may be unaware that the local log storage device is nearly full and will stop accepting more log

message relatively soon. The log device should generate a notification of some type to the remote log collectors so they are aware of the fact. Since most operators perform analysis on the remote copy of log messages, the operator would at least be aware that they should rectify the situation

Supported Practices

* Send a message to the remote log collectors when the local storage device is 95% full.

Current Implementations

Some versions of syslog can be configured to provide this capability.

Considerations

How the log device determines the right threshold (i.e. 95% vs 85%) to send out the notice and whether said notice is also captured in the local storage is expected to be vendor specific.

2.20. Syslog-specific Capabilties

The predominant logging mechanism within network infrastructures is BSD-syslog and its variants. With such widespread use, this section identifies capabilities specific to syslog.

2.20.1. Configurable Facility Values

Capability

The device is capable of allowing for the selection of the syslog facility number via configuration.

Discussion

A network operator may have many similar devices in their network. The ability to segregate different severity events by the strategic use of the syslog facility number is extremely useful.

Supported Practices

* Authentication log entries are marked at a different facility code to allow for easier segregation at the event collector.

Current Implementations

Some devices support this capability via a configuration variable.

Considerations

None.

2.20.2. Configurable Destination UDP Port

Capability

Devices are capable of allowing for the configuration of the destination syslog UDP port number.

Discussion

In large logging environments, spreading the load amongst multiple receiving daemons is a useful optimization. This capability also allows operators to differentiate between different device

functions very easily, for example all backbone router log to port 512 and all access router log to port 513.

Supported Practices

* Send all backbone routers log to port 512 and all access router log to port 513.

Current Implementations

Some devices support this capability via a configuration variable.

Considerations

None.

2.21. SNMP-specific capabilities

Another common logging mechanism uses the notification messages of the Simple Network Management Protocol [RFC3411].

2.21.1. Read-only Operations Supported

Capability

The device is capable of disabling SNMP write operations to the device.

Discussion

Since SNMP is used as a management protocol in addition to its logging functionality, the ability to disable operations that would change the device operations should be supported for those devices that aren't using the management functions.

Supported Practices

* Disable SNMP write operations.

Current Implementations

Some devices support this capability via a configuration variable.

Considerations

None.

2.21.2. Restrict Sources of SNMP Queries

Capability

The device is capable of restricting the IP addresses that can query the SNMP interface for event data.

Discussion

Since event data can educate an adversary, devices should be able to only send event data ("responses") to certain, configured IP addresses, not any system that interrogates them. See [RFC3413].

Supported Practices

* Configure devices to only accept SNMP requests from authorized addresses.

Current Implementations

Some devices support this capability via a configuration variable. It may also be implemented using packet or traffic filtering to the device. See [I-D.ietf-opsec-filter-caps].

Considerations

None.

2.21.3. Only Return Specific Data to Requestor

Capability

The device is capable of delivering specific managed object data (e.g., values linked to a specific OID) instead of returning all event data for the device (e.g., an entire OID subtree).

Discussion

Since event data can educate an adversary, devices should be able to only send specific event data instead of returning all the data in every query. See [RFC3415].

Supported Practices

* Queries request specific OID values instead of dumping the entire MIB. This practice reduces event data volume in addition to attaining security.

Current Implementations

Most devices support this capability.

Considerations

None.

3. Security Considerations

Security capabilities of network devices is the subject matter of this entire memo. The capabilities listed cite practices in [RFC4778] that they are intended to support. RFC4778 Also defines the general threat model, practices, and lists justifications for each practice.

4. IANA Considerations

There are no IONA actions required by this document.

5. Informative References

[I-D.ietf-opsec-filter-caps]
Morrow, C., "Filtering and Rate Limiting Capabilities for IP Network Infrastructure", draft-ietf-opsec-filter-caps-09 (work in progress), March 2007.

[I-D.ietf-syslog-protocol]
Gerhards, R., "The syslog Protocol", draft-ietf-syslog-protocol-21 (work in progress), June 2007.

[I-D.ietf-syslog-transport-tls]
Miao, F. and M. Yuzhi, "TLS Transport Mapping for Syslog", draft-ietf-syslog-transport-tls-10 (work in progress), May 2007.

[RFC1305] Mills, D., "Network Time Protocol (Version 3)", RFC 1305, March 1992.

[RFC1492] Finseth, C., "An Access Control Protocol, Sometimes Called TACOS", RFC 1492, July 1993.

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

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC3164] Lonvick, C., "The BSD Syslog Protocol", RFC 3164, August 2001.

[RFC3195] New, D. and M. Rose, "Reliable Delivery for syslog", RFC 3195, November 2001.

[RFC3411] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.

[RFC3413] Levi, D., Meyer, P., and B. Stewart, "Simple Network Management Protocol (SNMP) Applications", STD 62, RFC 3413, December 2002.

[RFC3414] Blumenthal, U. and B. Wijnen, "User-based Security Model (ISM) for version 3 of the Simple Network Management

Protocol (SNMPv3)", STD 62, RFC 3414, December 2002.

[RFC3415] Wijnen, B., Presuhn, R., and K. McCloghrie, "View-based Access Control Model (CACM) for the Simple Network Management Protocol (SNMP)", STD 62, RFC 3415, December 2002.

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

[RFC4330] Mills, D., "Simple Network Time Protocol (SMTP) Version 4 for IPv4, IPv6 and OSI", RFC 4330, January 2005.

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

[SP800-92] Souppaya, M. and K. Kent, "Guide to Security Log Management", FIPS 800-92, April 2006.

Authors' Addresses

Patrick Cain
The Cooper-Cain Group, Inc.
P.O. Box 400992
Cambridge, MA 02140
U.S.A.

Phone: +1 617-848-1950
Email: pcain@coopercain.com

George Jones
Port111 Labs.

Email: gmj3871@pobox.com

Full Copyright Statement

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

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