Subject: Secure Remote Audit Log

Submitted by: Tony Panero

File: PSARC/2002/150/opinion.ms

Date: December 4th, 2002

Committee: Ralph Campbell (opinion written by Gary Winiger), James Carlson, Joseph Kowalski, Terrence Miller, Andy Tucker.

Steering Committee:
Solaris Operating Environment Steering Committee
soesc-prodteam@sun.com

Operating Systems and Networking Steering Committee
onsc@sun.com

1. Summary

The project name reflects the original intent of the project and is a misnomer of the project approved. A more appropriate name would not include ''secure.''

This project provides a mechanism to send binary audit data to an alternate and / or secondary destination. The current audit mechanism only allows recording the binary audit data in a file. The alternate or secondary destination is provided for by a plug in to the audit mechanism. This project provides a plug in which sends the binary audit data to a file and one which formats the binary audit data as human readable syslog messages and forwards them to **syslog**(3C) as audit.notice messages. Additionally, it defines the LOG_AUDIT facility for Solaris to correspond with the audit facility defined in RFC 3164 [1].

The structure of this project is such that additional plug ins could be supported by a future project.

2. Decision & Precedence Information

The project is approved as specified in reference [2].

The project may be delivered in a micro or patch release of Solaris.

3. Interfaces

The project exports the following interfaces.

Interfaces Exported		
Interface	Classification	Comments
audit(1M)	Evolving	
auditd(1M)	Evolving	
audit_warn(1M)	Evolving	new ''plugin'' subcommand
audit_plugin(3BSM)	Project Private	**auditd**(1M) SPI interface
audit_binfile(5)	Evolving	**auditd**(1M) plug in to implement the current binary audit trail
audit_syslog(5)	Evolving	**auditd**(1M) plug in to write syslog messages
audit_control(4)	Evolving	new keywords

Interfaces Exported		
Interface	Classification	Comments
auditd.h	Project Private	**audit_plugin**(3BSM) header

The project imports the following interfaces.

Interfaces Imported		
Interface	Classification	Comments
auditsvc(2)	Project Private	See 4.3
audit_control(4)	Evolving	defines which audit paths are active
syslog(3C)	Standard	

4. Opinion

4.1. Not Secure

When this project was initially submitted, it intended to use a secure remote logging protocol. The project could not find an acceptable standard one. It is beyond the scope of the project to create one. Some committee members felt Sun should take a leadership role in defining such a protocol. This led to steering committee advice. Customers requested audit information be available through the syslog protocol. The project investigated the various proposals for ''secure'' syslog and found a lack of focus and movement toward consensus. Combining the customer request for syslog and the goal of remote audit log led to the project as presented.

4.2. Structured syslog Messages

The project proposed to use the syslog protocol [1] to directly write structured audit trail data to remote host formatted as XML compatible with PSARC/2002/377 ''Audit Trail Translation to XML.'' The committee found two major faults with this approach: the direct formatting and transmission over UDP of syslog protocol messages and the precedent of creating structured stable data in syslog. The committee felt strongly that even to imply stability for one class of syslog messages would lead to customer calls for stability of all Sun syslog messages. The project removed its use of XML and created human readable syslog message that extract some significant parts of the audit trail data using **syslog**(3C).

4.3. auditsvc(2) and audit_plugin(3BSM)

This project prompted PSARC/2002/665 ''Audit Interface Reclassification,'' which reclassified **auditsvc**(2) as Project Private. Some committee members expressed concern that the customer(s) who may be using **auditsvc** would have their applications break. The project team pointed out that PSARC/2002/665 only reclassified **auditsvc** and that neither project will actually change the implementation in an incompatible way. **auditsvc** will be announced to be Project Private in the next micro release and its documentation removed in the next minor release.

The known customer(s) reluctantly use **auditsvc** because there has been no alternative to capture the audit data in real-time for analysis. Use of **auditsvc** requires replacing **auditd**(1M). Such replacement is not supported by Sun. This project introduces **audit_plugin**(3BSM) which is intended to replace the need for customer use of **auditsvc** with a more efficient and stable interface. Because **audit_plugin** is a new interface, it is being classified as Project Private. The project intends to offer contracts [3] to use the **audit_plugin** interfaces to the known **auditsvc** users. At the time of a contract is tendered, **audit_plugin** and *auditd.h* will become Contracted Project Private. Once **audit_plugin** is proven it is expected to be promoted to a public interface.

4.4. auditconfig(1M) not getopt(3C) Compliant

A committee member expressed concern with the lack of conformance by **auditconfig**(1M) with **getopt**(3C). This project does not modify this command, rather it only adds notes to the man page. The command syntax is as it was when integrated in 1992. No ARC case can be found for the audit mechanism integrations. The committee concluded that it was outside the scope of this project to change the command to be **getopt** compliant.

4.5. syslog.conf(4) Poorly Worded

A committee member expressed concern with the use of the word ''reserved'' in the **syslog.conf**(4) man page. This project has added new information in a similar syntax to the existing man page. The committee member's concern would have led to an advisory change to the project to reword **syslog.conf**. Instead, the project updated the specification.

5. Minority Opinion(s)

None.

6. Advisory Information

6.1. Need for Secure Remote Logging of Structured Data Protocol

During the investigation of this project, a void was uncovered in the Solaris product line. No secure remote logging protocol is provided in Solaris. The steering committees are advised to fund a project to add to Solaris support for a suitable secure remote logging protocol standard that may be used for recording structured data. Such data might include fault events as well as system level audit data.

7. Appendices

7.1. Appendix A: Technical Changes Required

None.

7.2. Appendix B: Technical Changes Advised

None.

7.3. Appendix C: Reference Material

Unless stated otherwise, path names are relative to the case directory PSARC/2002/150.

1. RFC 3164, The BSD syslog Protocol
   File: final.materials/rfc3164.txt
2. Final Specification
   File: final.materials/*
3. Prototype Contract
   File: final.materials/contract.proto

