Assuring Post Processed Telemetry Data Integrity
With a Secure Data Auditing Appliance

Jeff Kalibjian, Steven Wierenga
Hewlett Packard Corporation

ABSTRACT

Recent federal legislation (e.g. Sarbanes Oxley, Graham Leach Bliley) has introduced requirements for compliance including records retention and records integrity. Many industry sectors (e.g. Energy, under the North American Energy Reliability Council) are also introducing their own voluntary compliance mandates to avert possible additional federal regulation. A trusted computer appliance device dedicated to data auditing may soon be required in all corporate IT infrastructures to accommodate various compliance directives. Such an auditing device also may have application in telemetry post processing environments, as it maybe used to guarantee the integrity of post-processed telemetry data.

KEY WORDS

Compliance, Audit, Hardware Security Modules (HSM), Federal Processing Information Standard 140-2 (FIPS 140-2), Common Criteria (CC), Federal Information Security Management Act (FISMA), security boundary, key management.

INTRODUCTION

Data auditing devices are increasingly being utilized in corporate IT environments to implement corporate governance and information security controls. Unfortunately, most of these devices are insecure and will be of marginal value to an organization if the data is legally challenged. This is because they are susceptible to possible manipulation by insiders or by outsiders able to gain insider access. Auditing devices could be of great use in telemetry post-processing to guarantee data integrity. However, a next generation secure audit server device would be required to ensure its data integrity features could not be subverted. After reviewing the genesis of data retention compliance and its current impact in on corporate governance; the requirements for secure data auditing will be discussed in relation to securing telemetry post-processed data. An example will be given illustrating how a secure audit server could be used to better secure telemetry post processing and data analysis.

COMPLIANCE OVERVIEW

A number of factors have come together to require rigorous IT compliance in the government, public sector and private sectors. The 9/11 tragedies have resulted in new IT compliance initiatives from industry consortiums (e.g. National Energy Regulatory Commission, NERC) and Federal standards bodies (e.g. National Institute of Standards and Technology, NIST) that deal directly with IT cyber security issues. Revelations of wide-spread corporate fraud in the late 1990's have also resulted in a number of new laws being passed by the Congress that deal with the concept of "compliance" and privacy.

Table 1. Important Federal and State Legislated Compliance Initiatives

Legislated Regulation	Industry	Focus
Sarbanes-Oxley	Public Company Accounting	Information and process integrity
HIPAA	Healthcare	Controlled access
Gramm-Leach-Bliley Act	Financial Privacy	Controlled access
SEC 17A-4	Finance	Information retention
Basel II	Finance	Information and process integrity
21 CFR Rule 11	Pharmaceutical	Information and process integrity
USA PATRIOT ACT	Homeland Security	Information and process integrity
California SB 1386	Financial Privacy	Controlled access

Such laws include Sarbanes-Oxley, and Graham, Leach, Bliley (respectively). Although the legislation is quite complex, a consistent element in both, is the concept of IT resources being utilized to maintain and or protect "un-altered" corporate records or private financial information. Table 1 lists some major state and federal legislated compliance and privacy regulations. Table 2 lists industry initiated compliance mandates. In 2002, Congress also passed the Federal Information Security Management Act [1] to help insure government agencies would also implement cyber compliance principles in their IT operations.

ROLE OF FEDERAL INFORMATION SECURITY MANAGEMENT ACT

The Federal Information Security Management Act (FISMA) specified that:

> "Each Federal agency shall develop, document, and implement an agency- wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source…"

Table 2. Industry initiated compliance mandates.

Industry Initiated Compliance	Industry	Focus
NERC CIP 2-9	Energy Power Generation/Transmission Management Systems Cyber-Security	SCADA/computer security
AGA 12	Gas and Oil Pipeline Cyber-Security	SCADA/computer security
CSMS	US Chemical Industry Cyber-Security	Computer/information security
PCI DSS	Payment Card Industry Data Security Standard	Computer/information security

The FISMA act also called out a special role for National Institute of Standards and Technology (NIST); specifically they were to develop:

- Standards to be used by Federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels.
- Guidelines recommending the types of information and information systems to be included in each category.
- Minimum information security requirements (management, operational, and technical security controls) for information and information systems in each category.

NIST ROLE IN SECURITY COMPLIANCE

Since 2002, NIST has complied with the FISMA request and published six specifications to aid government agencies in securing their IT infrastructures. The publications will aid government entities in categorization of information and information systems, risk assessment, security planning, security implementation, and security verification. The documents are summarized in Table 3.

Table 3. Elements of the US Information Security Program

NIST Standard	Category	Document ID	Description
FIPS 199	Information Categorization	SP 800-60	Defines categories of information and information systems according to levels of risk for confidentiality, integrity, and availability; maps information types to security categories
FIPS 200	Security Selection and Implementation	SP 800-53	Management, operational, and technical controls (i.e., safeguards and countermeasures) planned or in place to protect information and information systems
	Risk Assessment	SP 800-30	Analyzes the threats to and vulnerabilities of information systems and the potential impact or magnitude of harm that the loss of confidentiality, integrity, or availability would have on an agency's operations and assets
	Security Planning	SP 800-18	Documents the security requirements and security controls planned or in place for the protection of information and information systems
	Verification	SP 800-37 SP 800-26 SP 800-53A	Measures the effectiveness of the security controls associated with information systems through security testing and evaluation
	Authorization	SP 800-37	The authorization of information systems to process, store, or transmit information, granted by a senior agency official, based on the effectiveness of security controls and residual risk

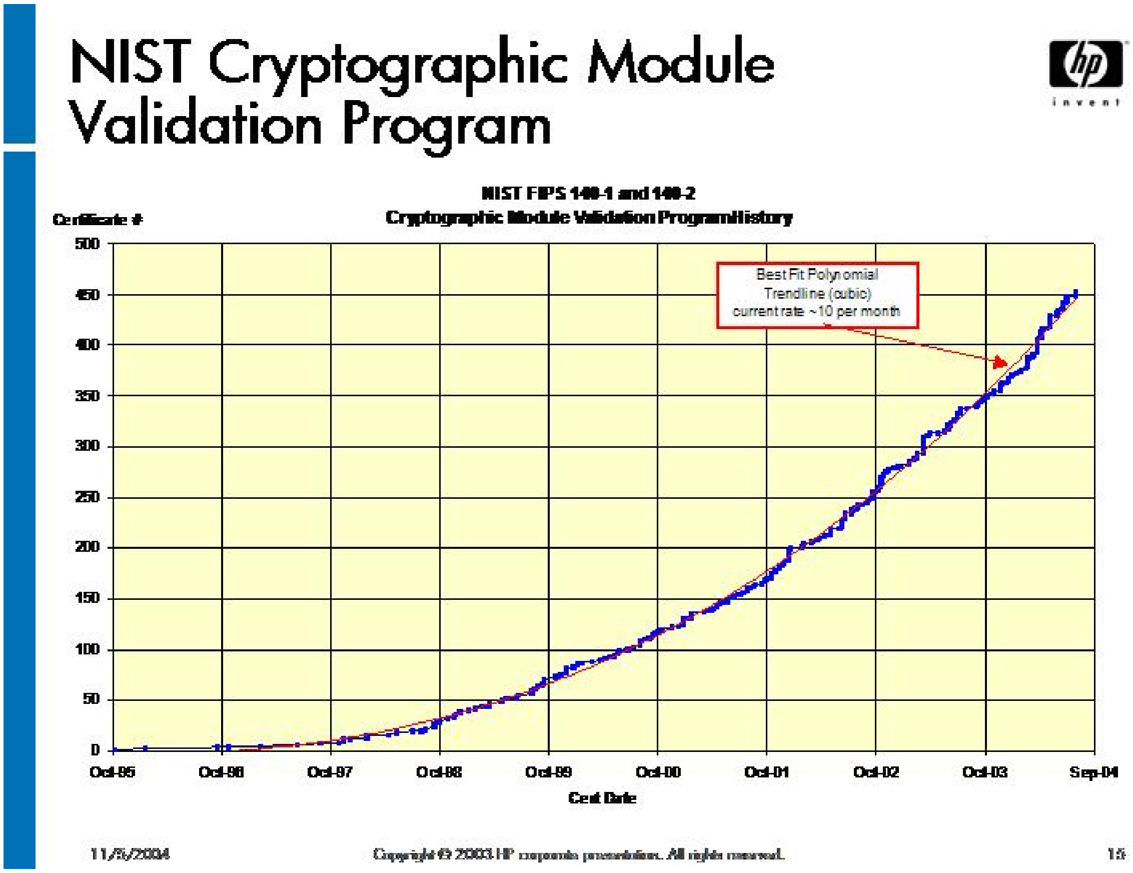
Of particular importance is FIPS 200 (SP 800-53) [2]. This document requires that agencies utilize FIPS 140-2 [3] certified hardware to secure cryptographic keying material and security processes. It also specifies rigorous auditing methodologies recommended for application to critical IT computers in enterprise networks

DEPARTMENT OF DEFENSE ALSO WEIGHS IN

While the US military and intelligence organizations have always utilized the equivalent FIPS 140-2 Level 3 or 4 computer hardware ("Type 1 Cryptographic Devices") to secure sensitive voice/data communications; since July 1, 2002, the DOD Information Insurance Implementation, Number 8500.2, requires all purchased computer software to be Common Criteria [4] evaluated.

UNDERSTANDING THE IMPORTANCE OF FIPS AND COMMON CRITERIA

The National Institute of Standards and Technology (NIST) has established a Federal Information Processing Standard (FIPS) that specifies the security requirements within a system protecting sensitive information pertaining to cryptographic operations. The standard defines four increasing levels of security; namely,



NIST Cryptographic Module Validation Program

11/5/2004 Copyright © 2003 HP corporate presentation. All rights reserved. 15

Figure 1. FIPS 140-2 product certification is accelerating rapidly.

- Level 1 defines the lowest level—no specific physical security mechanisms are required however one “approved” NIST cryptographic algorithm (e.g. DES) or security function must be utilized. The software and/or firmware components of the cryptographic module may be executed on a general purpose processor that has an un-rated operating system.

- Level 2 adds a requirement of physical tamper evidence (e.g. tamper evident coatings or seals on containers housing the electronics). It also specifies role-based authentication for security officer interaction with the cryptographic module (e.g. for key loading, etc.). If software and/or firmware components implement the cryptographic capabilities, they may be executed on a general purpose processor, but the OS on the processor must be rated at CC EAL-2 or its equivalent.

- Level 3 requirements include all Level 2 requirements, but add constraints to minimize threat of data compromise. This usually takes the form of data zeroization circuitry. It also requires identity-based authentication for security officers needing to access the processor system. Any software/firmware cryptographic functionality provided by a general purpose processor, requires an OS on that processor rated at CC EAL-3.

- Level 4 is the highest standard and requires physical security that detects and responds to all unauthorized attempts at access. In addition to Level 3 features, Level 4 provides for zeroization even when environmental conditions such as temperature, voltage, are exceeded. Level 4 also requires an operating system rated at CC EAL-4 or higher if software or firmware is utilized to implement cryptographic functionality

It is desirable to have FIPS 140-2 ratings of Level 3 and above on systems that are protecting critical information or processes, particularly from potential insider threats.

The security worthiness of software is usually evaluated with the Common Criteria metric. In Common Criteria evaluation a set of security requirements and specifications, otherwise known as a Protection Profiles (PP) and Security Targets (ST), are developed for a software system referred to as the Target of Evaluation (TOE). Common Criteria is an ISO standard (15408) and has seven increasing Evaluation Assurance Levels (EAL).

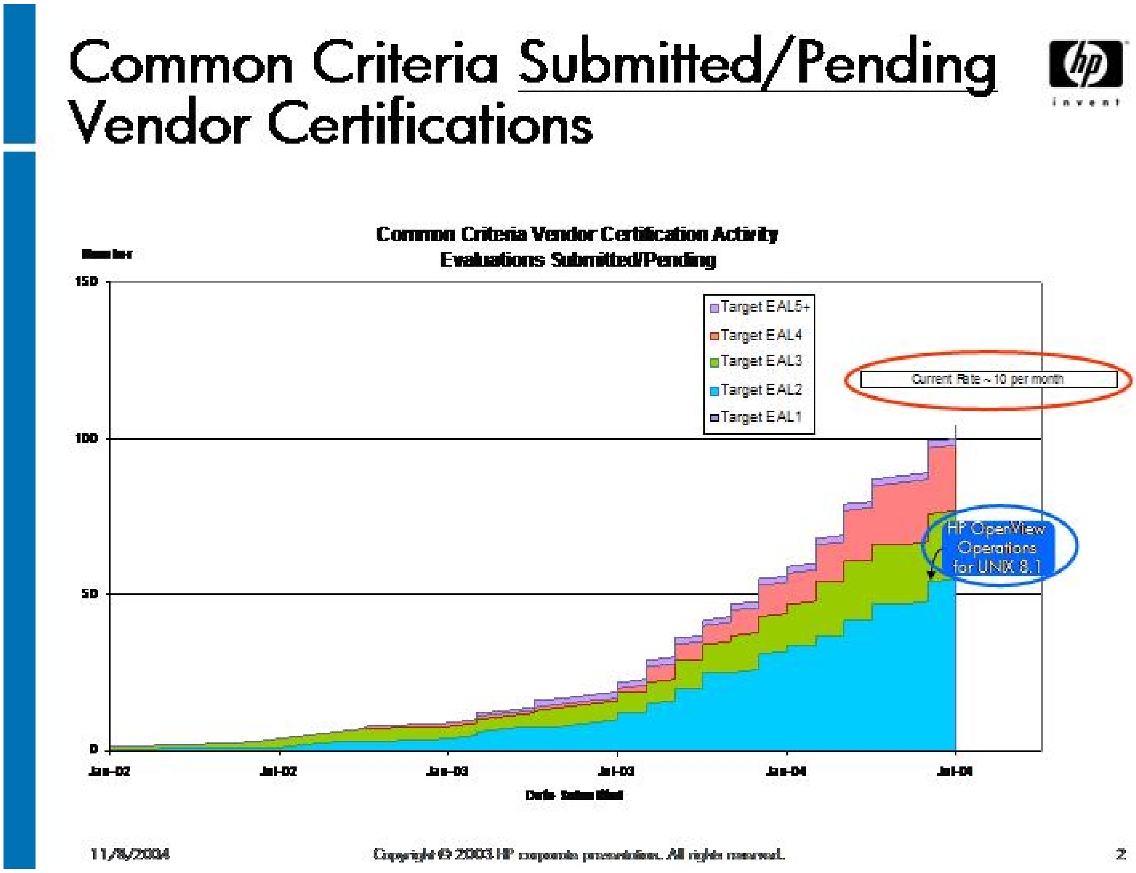
- EAL - 1 – Functionally tested. Evaluation of TOE is done with respect to the customer documentation. Used when threats to security are not considered serious and only some confidence of correct operation is desired.

- EAL - 2 – Structurally tested. Evaluation of TOE is done with respect to developer design information and test results. Used when developers or users require a low to moderate level of independently assured security.

- EAL – 3 –Methodically tested and checked. Evaluation of TOE is done at design stage. Used when developers or users require a moderate level of independently assured security.

- EAL – 4 – Methodically designed, tested, and reviewed. Used when developers or users require a moderate to high level of independently assured security.

- EAL – 5 – Semiformally designed and tested. Rigorous commercial development tools and specialty security design techniques to design and implement TOE. Used when developers or users require a high level of independently assured security.



Common Criteria Submitted/Pending Vendor Certifications

11/8/2004 Copyright © 2003 HP corporate presentation. All rights reserved. 2

Figure 2. Common Criteria certification submissions are steadily rising.

- EAL – 6 – Semiformally verified design and tested. Security engineering techniques applied to an advanced development environment. Used when developers or users are developing applications deployed in high risk situations protecting valuable assets.

- EAL – 7 – Formally verified design and tested. Advanced security engineering and development techniques that can be rigorously mathematically modeled and analyzed. Used for applications deployed in extremely high risk environments protecting large value assets.

It is desirable to achieve CC ratings of at least 4 and above for systems protecting critical information and processes.

A process of PP and ST definition feed into the development, evaluation, and operation of the TOE. This represents a continual process of feedback and evaluation that eventually leads to the implementation and evaluation of the secure software system utilizing varying levels of sophistication in software security design and development. While ideally this occurs starting at the requirements phase, it is economically feasible to retrofit existing designs with Common Criteria methodology and achieve up to EAL-4 ratings. This is why EAL-5 and above ratings are more desirable, because it implies a rigorous design and implementation of security features; while the EAL-4 rating may simply imply an “after the fact” documentation re-creation.

The reason why both NIST and the DOD are advocating FIPS and CC certifications for deployed computer based solutions requiring security is because they are the best, objective, measures of a how well both computer hardware and software have been architected and implemented to protect information. Industry sees this trend, and Figures 1 and 2 graphically depicts the movement of commercial FIPS and CC certified products.

ROLE OF CRYPTOGRAPHY IN SECURING COMPUTER SYSTEMS

The threat model for all computer systems has four elements

- External threats introduced into the computer system. Examples of this would be viruses or malicious scripts.
- Internal threats: misplaced trust. This includes overloading privileges onto the Administrator role and allowing the Administrator to exercise their privileges without dual control.
- Attacks against the operating system or applications running on the operating system. This can include replacing known operating system resources with compromised ones, or attacking the memory partition an application is running in.
- Internal and external data snooping. This might involve access to sensitive data residing in CPU registers or main memory via fault dumps or Logic State Analyzer (LSA) access to system bus activity.

Securing a computing system involves introducing cryptographic technology, preferably in secure hardware boundaries, that provides privacy, authentication, and authorization services for the operating system and applications running on that operating system.

PUBLIC SECTOR IMPACT

Public sector has also been affected by 9/11. Public sector entities such as electric, gas, oil, water, and telecommunications utilities have been designated as “Critical National Infrastructure.” That is, their continued smooth operation is critical to the economy and overall well-being of the United States. In order to assure these organizations make their IT infrastructures resistant to terrorist actions, the government is encouraging (via the threat of federal legislation) industry trade groups to establish their own best practices guidelines for securing IT infrastructure. A number of these self policing guidelines call out NIST certifications like FIPS 140-2. An example of this is the American Gas Association (AGA) trade group. This trade group is comprised of organizations that operate and own pipelines that natural gas and oil flow through. Their AGA 12 guidelines specifically call on the use of FIPS 140-2 certified hardware to manage cryptographic keys that are used in securing the Supervisory

Control and Data Acquisition (SCADA) systems that control the pipelines. Another trade group that is taking a proactive stance in defining their own IT security standard is the North American Electric Reliability Council (NERC). In cooperation with the Department of Energy, NERC has specified eight cyber-security guidelines (known as the NERC Critical Infrastructure Program (CIP) 2-9) they recommend power generation, transmission and distribution entities adopt to protect their SCADA and IT systems. Although it doesn't specifically call out FIPS 140-2 or Common Criteria, many of the guidelines can be addressed with the aid of systems with these certifications.

INSIDE THE MANDATES

Cyber compliance mandates specify processes, procedures and technologies entities must employ to not only insure their computer networked infrastructures are secure, but guarantee root cause analysis of anomalous events can be performed. The former implies establishing computer security policies that detail the use and deployment of firewall, intrusion detection, intrusion prevention, and authorization/authentication solutions. The later implies sophisticated audit and logging technologies to insure transaction records of application and operating system activities can be archived and reviewed. The use and deployment of firewall, intrusion, and authentication appliances to secure networked infrastructures is well known. Deploying secure auditing technologies to monitor and review transactions is less common and will be examined for application in an enterprise reducing and analyzing telemetry data.

SECURITY IMPLICATIONS FOR AUDITING

Auditing computer transactions/events is not new----performing those auditing actions in a secure in a reliable manner is. When data is received by the auditing device it should be over a private and authenticated channel. After receipt of data, the audit device should time-stamp (with the time coming from a secure time source) and digitally sign the information before it is archived into a database. The device should be administered using dual control concepts and privilege minimization roles to prevent one person from being able to subvert established auditing polices. Finally, the audit device itself should be FIPS 140-2 and Common Criteria certified to assure that cryptographic keys and processes employed cannot be compromised.

COMPLIANCE IMPLICATIONS FOR POST PROCESSING AND ANALYSIS

A compliance product for telemetry would not only record post processing actions taken on the original telemetry product, but also note who has accessed any of the derivative telemetry data. Figure 3 illustrates a system that might be employed to monitor these activities. Client systems that allow analysts to examine/reduce telemetry data will require X.509 digital credentials be verified by a centralized audit server. A secure TLS or IPSec protocol could be utilized to ensure the integrity and privacy of analyst client

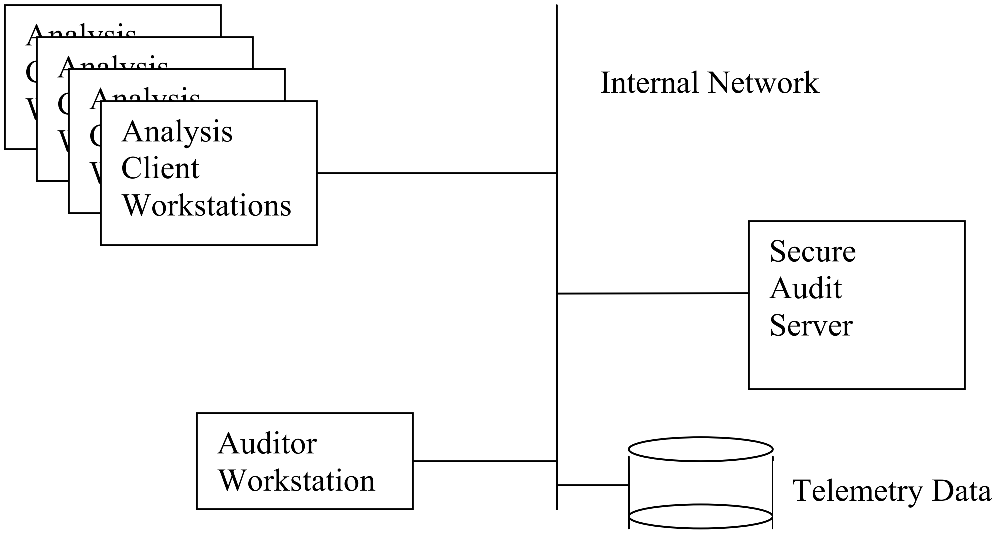


Figure 3. Secure audit infrastructure for telemetry data.

workstation-central audit server interactions. Every time data is accessed, or new data is generated the client workstation must contact the central audit server to record the transaction events. When data is received by the Audit Server it is digitally signed and time-stamped, to insure the audit data cannot be subsequently tampered. Typical information that might be archived would include the action on the telemetry data taken, the time the action was taken, and the user who initiated the actions. At certain intervals internal auditors would be given access to the central audit server so they might review actions that have been taken to insure they are consistent with internal company policies. Automated review processes could also be run on the audit server to review actions in real-time. Alert notices could be sent out to appropriate personnel when anomalous behavior was detected. Due to the sensitivity of the operations performed in the audit server, its security must be robust. It should be both FIPS 140-2 and Common Criteria certified. Client workstations should also have a robust security framework at least encompassing a FIPS 140-2 certified key handling system.

SUMMARY

Legislated and industry mandated compliance has become a reality. Since the value of the decisions made based on telemetry data is high-----multi-billion dollar programs may be cancelled or approved based on the analysis done on the telemetry data, it makes sense to consider deploying FIPS 140-2 and Common Criteria certified compliance technologies, like secure auditing, to monitor the integrity of telemetry post processing and analysis activities.

REFERENCES

[1] http://csrc.nist.gov/policies/FISMA-final.pdf

[2] http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf

[3] http://csrc.nist.gov/cryptval/

[4] http://www.commoncriteriaportal.org/