THE JOURNAL OF DIGITAL FORENSICS, SECURITY AND LAW

Journal of Digital Forensics, Security and Law

Volume 2 | Number 4 Article 4

2007

The Design and Implementation of an Automated Security Compliance Toolkit: A Pedagogical Exercise

Guillermo Francia
Computer Security and Forensics Laboratory, Jacksonville State University

Brian Estes
Computer Security and Forensics Laboratory, Jacksonville State University

Rahjima Francia
Computer Security and Forensics Laboratory, Jacksonville State University

Vu Nguyen
Computer Security and Forensics Laboratory, Jacksonville State University

Alex Scroggins
Computer Security and Forensics Laboratory, Jacksonville State University

DOI: https://doi.org/10.15394/jdfsl.2007.1032
Available at: https://commons.erau.edu/jdfsl/vol2/iss4/4

The Design and Implementation of an Automated Security Compliance Toolkit: A Pedagogical Exercise

Guillermo Francia III
gfrancia@jsu.edu
Computer Security and Forensics Laboratory
Jacksonville State University, Jacksonville, AL USA

Brian Estes
bestes83@gmail.com

Rahjima Francia
jima.francia@gmail.com

Vu Nguyen
tienvunguyen@yahoo.com

Alex Scroggins
alex_scroggins@yahoo.com

ABSTRACT

The demand, through government regulations, for the preservation of the security, integrity, and privacy of corporate and customer information is increasing at an unprecedented pace. Government and private entities struggle to comply with these regulations through various means—both automated and manual controls. This paper presents an automated security compliance toolkit that is designed and developed using mostly open source tools to demonstrate that 1) meeting regulatory compliance does not need to be a very expensive proposition and 2) an undertaking of this magnitude could be served as a pedagogical exercise for students in the areas of collaboration, project management, software engineering, information assurance, and regulatory compliance.

Keywords: Information Security, Compliance Toolkit, Forensics, Log Management, Intrusion Detection, Vulnerability Assessment, Sarbanes-Oxley, HIPAA, FISMA, GLBA.

1. INTRODUCTION

The proliferation of federal regulations involving cybersecurity ushered the hottest buzzword in information technology: compliance. These federal

regulations include the Computer Fraud and Abuse Act (last amended in 2001), Computer Security Act (1987), Health Insurance Portability and Accountability Act (1995); Financial Services Modernization Act (also known as Gramm-Leach-Bliley Act (GLBA), 1999), USA Patriot Act (2001; renewed in 2006), Sarbanes-Oxley Act (SOX, 2002), and the Federal Information Security Management Act (FISMA, 2002). The implications of these enactments clearly define the urgent need to meet their requirements. Attached to some of these regulations are fines and prison terms if regulated entities are found to be in non-compliance. Perhaps more importantly, other risks of non-compliance include the public disclosure of key assets, loss of customers, delisting from stock exchanges, damage to brand or company reputation, negative impact to stock price, shareholder lawsuits, and a loss in confidence in key company stakeholders.

Adding to the trouble of compliance is the fact that the requirements of many regulations frequently overlap, leaving businesses with the challenge of sorting out which solutions satisfy which requirements of which regulations. In (Schwartz, 2006), it was reported that Qumas, a vendor of life sciences compliance products, discovered that the processes and policies required by the Food and Drug Administration (FDA) have a lot in common with those required by SOX and the Patriot Act.

As new mandates and legislation are imposed upon businesses, it is becoming increasingly important for companies to find ways to manage the mapping and identification of requirements into easily deployable policies and strategies. However, companies find these to be very expensive undertakings. In 2005, corporate spending on the Sarbanes-Oxley Act compliance effort was estimated to be $6.1 billion (Cognos, 2006). A survey conducted by the Security Compliance Council reveals that an average of 34% of an organization's IT resources are spent on compliance (Perry, 2006). Truly, the expense of compliance is extremely high, and businesses that are unintentionally deploying redundant and unnecessary solutions are only adding to the high cost and frustration of compliance (Kolodgy, 2006). This paper presents an automated security compliance toolkit that is designed and developed using mostly open source tools to demonstrate that meeting regulatory compliance does not need to be very expensive. We developed a compliance matrix that helped us identify the overlapping requirements of four main regulations on each sector of the industry and designed the toolkit based on these common needs.

2. THE REGULATIONS

2.1 The Health Insurance Portability and Accountability Act (HIPAA)

Congress passed HIPAA in 1996. HIPAA is the first federal law to address health privacy in a comprehensive way (Cole, 2006; Swartz, 2003). It requires companies to adopt administrative, physical, and technical measures to protect

the confidentiality, integrity, and availability of certain health information. In addition, the Security section of HIPAA and set of HIPAA regulations known as the Privacy Rule have, for some time, required companies to implement general security measures to protect health information. The Security Rule, under HIPAA, requires companies to create, receive, transmit or maintain health information in an electronic format to meet much more detailed set of security standards than the HIPAA Privacy Rule (Langin, 2004).

HIPAA applies "covered entities" as defined in the law. This term includes: healthcare providers, plans, and clearinghouses. Health plans provide or pay for the cost of healthcare. Clearinghouses are entities that process and facilitate information relating to an individual's health, health care, or health care payment. Healthcare providers are doctors, dentists, hospitals, clinics, nurses, medical groups or other providers of medical services that maintain or transmit health information in an electronic form (Langin, 2004). According to HIPAA rules, if an organization provides one of a number of specified services for a covered entity and the service involves disclosing protected health information, it is a business associate. And business associates are directly affected by the HIPAA Privacy Rule. These business associates may include vendors, consultants, lawyers, auditors, clearinghouses, billing firms, and records storage organizations (Swartz, 2003).

2.2 The Federal Information Security Management Act (FISMA)

According to (Nelson, 2006), in the aftermath of September 11, 2001, Congress passed the E-Government Act, which formally recognized the importance of information security to the United States' economic and national security interests. FISMA, title III of the act, requires federal agencies to develop, document, and implement agency-wide information security programs to protect the confidentiality, integrity, and availability of information and systems that support the operations and assets of the agency.

Compliance with FISMA is the law and government agencies are fully accountable for their success in meeting this goal. FISMA is codified in FIPS199, Standards for Security Categorization of Federal Information and Information Systems, which was signed into law December 2003. FIPS 199 defined the requirements to use by Federal agencies in categorizing information and information systems in order to provide appropriate levels of information security. Implemented in March 2006, FIPS200, Minimum Security Requirements for Federal Information and Information Systems, takes the next step. FIPS200 categorizes systems as required by FIPS199 and then selects the appropriate set of security controls from technical guidance documents developed by National Institute of Standards and Technology (NIST) (Nelson, 2006).

FISMA's provisions fall into three major categories: assessment, enforcement, and compliance. The first pertains to determining the adequacy of the security

of federal assets, the second requires that key information security provisions be implemented and managed, and the third established provisions for the management of each agency's information security program and the accountability of each agency for compliance and reporting. In addition, FISMA requires the reporting of significant deficiencies. Agencies must identify and track material weaknesses and report any progress. Using a Plan of Action and Milestones (POA&M), each agency must commit to a schedule of remediation (Qualys Guard Enterprise, 2006).

2.3 The Sarbanes-Oxley Act (SOX)

The Sarbanes-Oxley (SOX) Act of 2002 was enacted by the US Congress mainly to address the crisis brought about by the WorldCom and Enron debacle to the financial markets. The law is ratified to enforce accountability for financial record- keeping and reporting of publicly traded corporations. The CEO and the Chief Financial Officer (CFO) are directly responsible for the completeness and accuracy of their institution's financial reporting and record-keeping systems (PCAOB, 2006; Whitman and Mattord, 2004).

2.4 The Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act, was signed into law in November 1999. The law applies to companies that offer financial products and services to individuals, including banks, insurance companies, mortgage companies, securities brokers, loan brokers, some financial or investment advisors, tax preparers, providers of real estate settlement services, and debt collectors (Dhillon, 2006; Qualys Guard Enterprise, 2006).

2.5 Common Compliance Challenges

Regardless of the regulation, there appears to be a common set of challenges companies experience when faced with compliance. The challenges, which are detailed in (Scalable Software, 2006), are as follows:

- Understanding regulatory mandates.
- Identifying specific requirements.
- Creating a system of control across multiple standards.
- Documenting the compliance auditing approach.
- Collecting and preserving compliance audit evidence.

3. THE COMPLIANCE MATRIX

Our objective in building the toolkit is to be as far reaching as possible. In order to accomplish this objective, we decided on identifying a representative regulation in each enterprise sector and determining shared control objectives.

Thus, we arrived at the following mapping and compliance criterion matrix:

- Public company sector → SOX
- Banking and finance sector → GLBA
- Health care sector → HIPAA
- Federal government sector → FISMA

We found more than the twelve common control objectives that are depicted in Table 1. However, due to time and personnel constraints, we decided to concentrate our development efforts to satisfying the top twelve common control objectives.

CONTROL OBJECTIVES
Document Preservation
Document Disposition/Destruction
Device/Media Control
Media Reuse
Encryption/Decryption
Authentication(2-level)
Transmission Security
Log Management/ Monitoring
Vulnerability Assessment
Intrusion Detection
Report & Benchmark
Message Security

Table 1. The Compliance Criterion Control Objectives

3.1. The Twelve Common Compliance Control Objectives

Group I: Document Control

1) Document Preservation – A system must be in place to gather the document hash digest and create a backup of the document in a

secondary storage device. The hash digest is necessary for future verification and non-repudiation.

2) Device and Media Control – This control requires an accounting and access control system to be in place for all devices and storage media. A secure system must be provided for all media transport.

3) Document Encryption and Decryption – An encryption/decryption system should be utilized for all electronic documents.

Group II: Privacy and Intellectual Property Control

4) Media Reuse – Due to the fact that the media is going to be reused in-house, the requirement of this control is not as stringent as that in the disposition control. This control requires complete document deletion and reformatting of the media involved.

5) Document Disposal and Destruction – This control assumes that the media will be disposed and moved out of the company premises. Thus, a system that will, at the very least, completely obliterate the media or the documents stored in them is required. A simple deletion and formatting system would not be sufficient to meet this control objective.

6) Access Authentication – The minimum requirement of this control objective is the utilization of a two-factor authentication for document access.

Group III: Vulnerability Assessment and Proactive Control

7) Transmission Security – This control objective requires that all electronic document transmissions be made through secure channels such SSL or VPN. Covert transmission mechanisms such as steganography are not acceptable.

8) Log Management and Monitoring – A system that continuously monitors, manages, and rotates log files for the purposes of proactive security checking and record keeping is required by this control. The rotated log files must be properly labeled and stored for possible future audits or forensic investigations.

9) Vulnerability Assessment – This control objective requires that a system and physical vulnerability assessment (VA) should be conducted on a regular basis. Every time a weakness is identified by the VA process, immediate corrective measures must be identified, documented, and implemented by the security team.

10) Intrusion Detection – An intrusion detection system (IDS) is required to be in-place in strategic system locations. A constant monitoring of critical system resources such as the firewall must be in place to

deflect, not only external threats but also, security breaches that may originate from within the perimeter. The IDS provides a mechanism for early detection of security violation and for an appropriate reaction or countermeasure corresponding to such violation.

11) Report and Benchmark – A benchmarking and reporting mechanism is required to a) demonstrate the degree of compliance that was achieved to auditors, b) assist the system administrators in securing new installations and production systems, and c) inform upper management personnel about the status of the company's compliance projects.

12) Message Preservation and Security – The preservation of electronic documents that facilitate communications is a major emphasis found in almost all regulations. The message transmitting tools may include, among others, emails, weblogs, and instant messages (IMs). It is imperative that companies provide tools that collect and preserve them for possible future forensic investigation and analysis.

4. COMPLIANCE FRAMEWORKS AND TOOLS

4.1 IT Governance Frameworks

Despite the complex nature of federal standards and regulations, there are similarities in their basic frameworks. The process of deploying and regularly testing the efficacy of those controls becomes much more efficient if businesses can identify a universal set of those controls that satisfy major frameworks (Kolodgy, 2006). These best practices IT frameworks are excellent guidance tools for compliance and policy development. Examples of these frameworks include COBIT (Control Objectives for Information and Related Technology), ITIL (IT Infrastructure Library), and ISO (International Standards Organization) 17799 (Feldman, 2006).

The COBIT framework comprises of four domain measures of IT products: Planning and Organization, Acquisition and Implementation, Delivery and Support, and Monitoring (ISACA, 2006).

ITIL is a cohesive set of best practices that were drawn from public and private entities worldwide. It consists of a series of books giving guidance on the provision of quality of IT services and on the environmental facilities needed to support IT (ITIL, 2006).

ISO 17799 provides organizations an international standard for information security. The standard is divided into 10 working sections which include, among others, Security Policy, Access Control and Compliance, Asset Classification and Management, Configuration and Vulnerability Management, Business Continuity Management, and Operational Change Control (ISO, 2006).

4.2 Commercial Tools

There is a plethora of commercial compliance tools that are available on the market. Although some of these tools are built around open source software that are available over the Internet, they tend to be very complex and expensive. In order to familiarize the reader about the features of the commercial tools, we briefly describe a few of them in what follows.

Symantec Control Compliance Suite (Symantec 2006). This suite of tools provides regulatory content for SOX, FISMA, HIPAA, GLBA, and Base II. It has 600 out-of-the-box reports which automatically identify potential security threats. Additional features include validation of windows configurations, security audits of networks, monitoring of Windows event logs, and locating users with weak passwords and expired accounts.

Tripwire Enterprise (Tripwire 2006). This tool monitors changes to critical applications such as databases, network configurations, directory services, and file systems. It also provides a facility for audit trails, assessing system damage after an attack, detecting undesirable system changes, and tracking of monitoring devices.

NetIO Risk and Compliance Center (NetIQ 2006). NetIQ provides several solutions for each of the following regulations: SOX, HIPAA, GLBA, and FISMA. In addition, companies that need to get a better control of their security practices may opt for solutions that cover the following standards: ITIL, ISO17799, COBIT, and NIST 800-53.

Qualys Guard Enterprise(QualysGuard 2006). The Qualys Guard has the largest knowledgebase of vulnerability signatures in the industry. It includes tools for network mapping, vulnerability scanning, risk analysis, report generation, end-to-end encryption, and security architecture audits.

4.3. Open Source Tools

The following open source security-related tools are mostly available for download from the Internet and can be utilized to meet control objectives that pertain, but not limited, to vulnerability assessment, encryption, intrusion detection, non-repudiation, log management, authentication, and secure file management and obliteration.

TrueCrypt (TrueCrypt 2006). This is a software system that performs on-the-fly encryption of a storage device volume. The encryption process is done automatically, i.e. without user intervention, before loading or saving the data. The entire file system mounted on that encrypted volume is, by itself, also completely encrypted. Thus, the file property, metadata, link, and free space information are securely encoded. The availability of a wide selection of encryption algorithms makes this tool an excellent choice for meeting the control objectives that require encryption. Figure 1 depicts the Graphical User

Interface (GUI) of TrueCrypt.

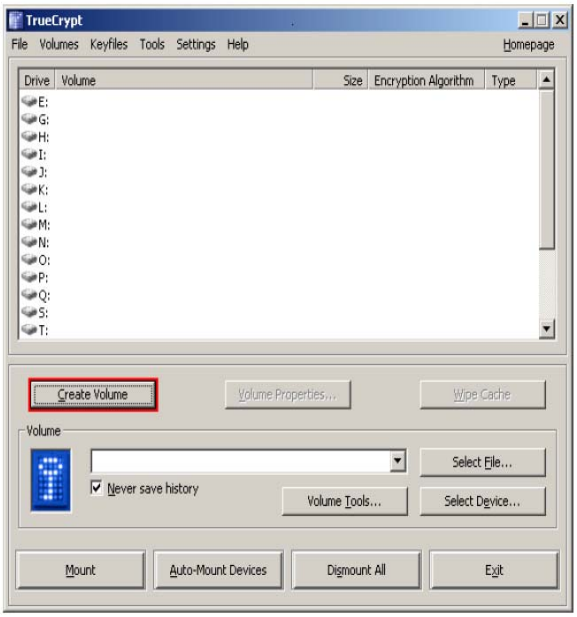


Figure 1. TrueCrypt Graphical User Interface

MS Log Parser Toolkit (Giuseppini and Burnett, 2004). The Log Parser tool first appeared as a utility for testing the logging mechanism of Microsoft's Internet Information Services (IIS). It provided users the ability to retrieve and display all the fields from a single log file in any of the three text-logging formulas supported by IIS. As the tests became more complex, more specifically the filtering of log entries, Microsoft saw an immediate need for a log management tool. Version 2.0 was the first version that was made available outside of Microsoft. MS Log Parser Version 2.2 shipped in January 2005 and is designed and engineered with the vision of helping users achieve their data-processing goals in a simple, fast, and powerful way (Giuseppini and Burnett, 2004). Technically, the tool is not an open source but a free tool that Microsoft shares with the IT community. A snippet of a Log Parser command is shown in figure 2.

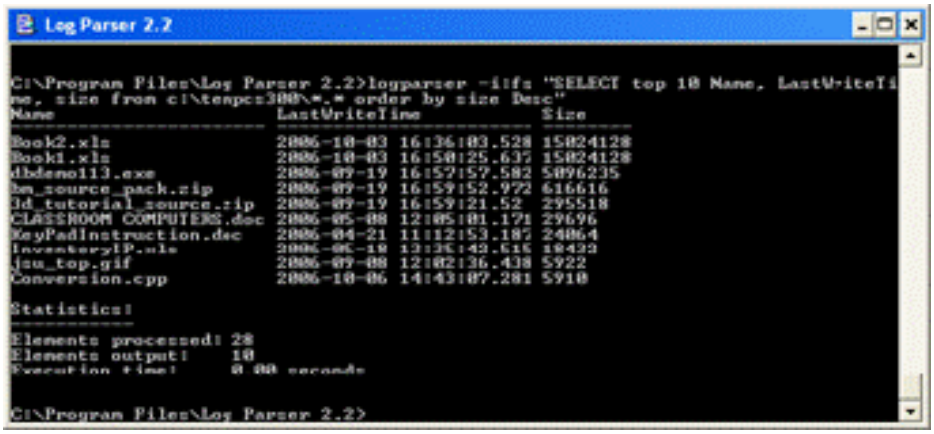


Figure 2. An MS Log Parser Session

Metasploit Framework. This framework provides a complete workbench for writing, testing, and using exploit code. It is, in fact, a solid platform for penetration testing, shellcode development, and vulnerability assessment. The framework is available for multiple operating systems such as Linux, Windows, BSD, and MacOS X. A screenshot of the metsploit framework at work is shown in Figure 3.

Figure 3. A Metasploit Framework Screenshot

OSSEC Host-based Intrusion Detection System (HIDS). This is an open source Host-based Intrusion Detection System which provides basic security and intrusion detection services such as log analysis, integrity checking, rootkit

detection, and time-based alerting. A basic configuration of this system calls for an installation of a server, where reports are being forwarded to and analyzed. The reports originate from multiple clients or agents, which are the stations that need monitoring (OSSEC, 2006).

Center for Internet Security (CIS) Next Generation (NG) Scoring Tool This scoring tool enables users verify the security configuration of systems and network devices for conformance with established benchmarks. In addition it can be used to demonstrate to auditors the system's compliance with the internationally accepted standards for security configuration. The CIS Scoring Tools are host based and produce reports that guide users and system administrators to secure both new installations and production systems (Center for Internet Security, 2006). Figure 4 depicts a snapshot of the questionnaire that is presented to the user for input. Essentially, the questionnaire acts like an interviewer that extracts pertinent system information from the user.

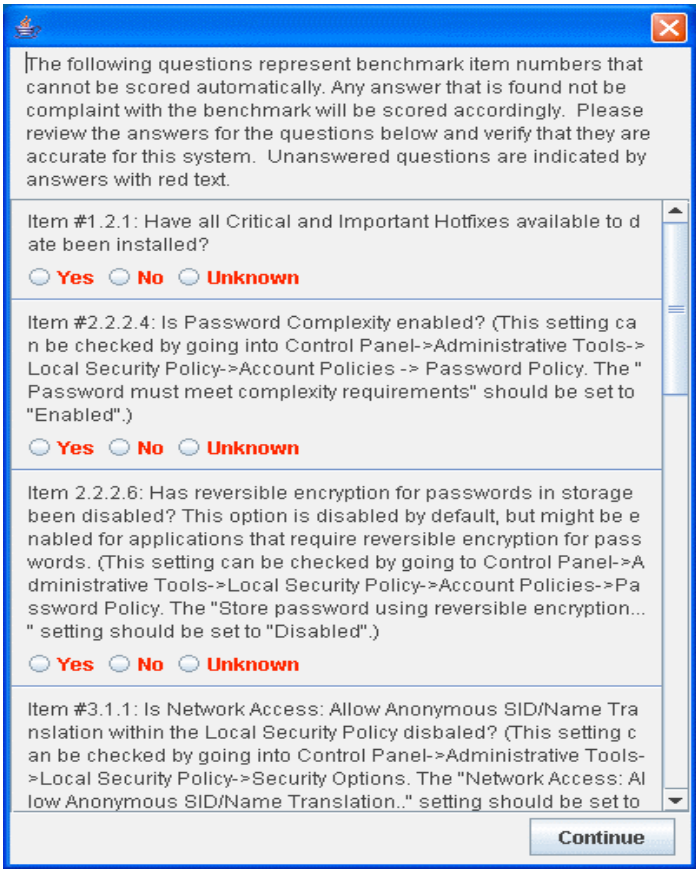
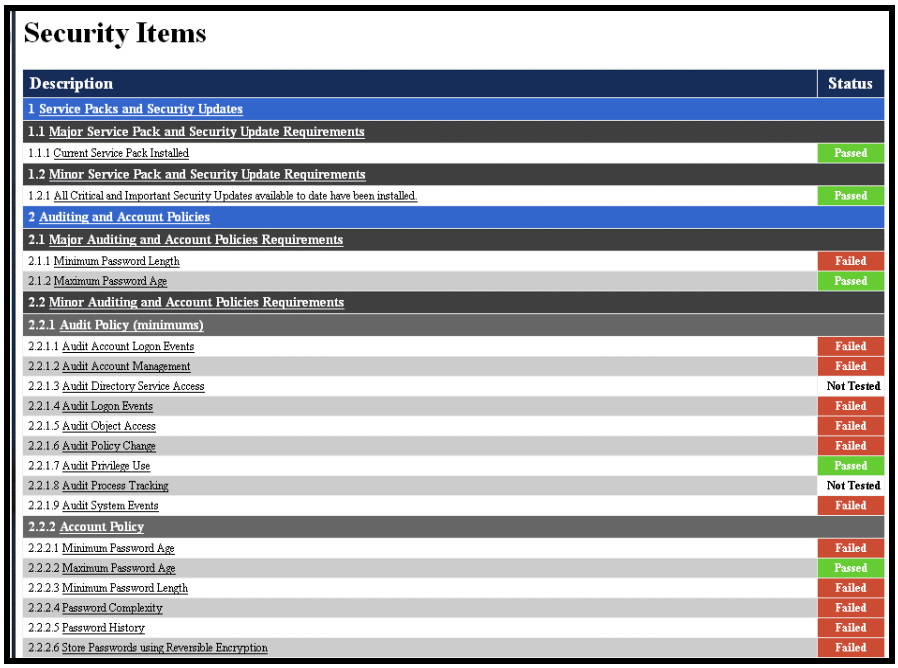


Figure 4. The NG Tool Questionnaire

Figure 5 displays the section of the benchmark report which shows the status of each security item. An item labeled with the status "Failed" is non-compliant with the benchmark recommendation; a "Passed" status indicates meeting or exceeding the benchmark; a "Not Tested" status indicates that the item is either having a benchmark value which not defined or is too subjective to have a recommended value. Figure 6 is a portion of the Benchmark Summary Report. It shows the actual score garnered and the maximum score possible for each item.



Security Items

Description	Status
1 Service Packs and Security Updates	
1.1 Major Service Pack and Security Update Requirements	
1.1.1 Current Service Pack Installed	Passed
1.2 Minor Service Pack and Security Update Requirements	
1.2.1 All Critical and Important Security Updates available to date have been installed.	Passed
2 Auditing and Account Policies	
2.1 Major Auditing and Account Policies Requirements	
2.1.1 Minimum Password Length	Failed
2.1.2 Maximum Password Age	Passed
2.2 Minor Auditing and Account Policies Requirements	
2.2.1 Audit Policy (minimums)	
2.2.1.1 Audit Account Logon Events	Failed
2.2.1.2 Audit Account Management	Failed
2.2.1.3 Audit Directory Service Access	Not Tested
2.2.1.4 Audit Logon Events	Failed
2.2.1.5 Audit Object Access	Failed
2.2.1.6 Audit Policy Change	Failed
2.2.1.7 Audit Privilege Use	Passed
2.2.1.8 Audit Process Tracking	Not Tested
2.2.1.9 Audit System Events	Failed
2.2.2 Account Policy	
2.2.2.1 Minimum Password Age	Failed
2.2.2.2 Maximum Password Age	Passed
2.2.2.3 Minimum Password Length	Failed
2.2.2.4 Password Complexity	Failed
2.2.2.5 Password History	Failed
2.2.2.6 Store Passwords using Reversible Encryption	Failed

Figure 5. Status of Security Items

Active@KillDisk. This freeware demo tool (a professional version is available at minimal cost) is used to completely delete information bits from a disk. The standard system commands found in most operating systems such as delete, format, and fdisk are simply inadequate in completely erasing the files on a disk. Furthermore, Active@KillDisk conforms to four international standards for clearing and sanitizing data. These standards are: US DOD 5220.22-M, German VISTR, Russian GOST p50739.95, and Gutmann method. The only drawback is that the software needs to be loaded on a bootable floppy disk to be operable.

Benchmark: Windows XP Professional Benchmark
Profile: SP2 Legacy Domain Member
Scan Time: 10/09/2006 18:06:13

Description	Items		Score	
	Passed	Failed	Actual	Max
1 Service Packs and Security Updates	2	0	20.000	20.000
1.1 Major Service Pack and Security Update Requirements	1	0	10.000	10.000
1.2 Minor Service Pack and Security Update Requirements	1	0	10.000	10.000
2 Auditing and Account Policies	12	12	10.774	20.000
2.1 Major Auditing and Account Policies Requirements	1	1	5.000	10.000
2.2 Minor Auditing and Account Policies Requirements	11	11	5.774	10.000
2.2.1 Audit Policy (minimums)	1	6	0.357	2.500
2.2.2 Account Policy	1	5	0.417	2.500
2.2.3 Account Lockout Policy	3	0	2.500	2.500
2.2.4 Event Log Settings – Application, Security, and System Logs	6	0	2.500	2.500
2.2.4.1 Application Log	2	0	0.833	0.833
2.2.4.2 Security Log	2	0	0.833	0.833
2.2.4.3 System Log	2	0	0.833	0.833
3 Security Settings	20	22	5.667	20.000
3.1 Major Security Settings	1	3	2.500	10.000
3.2 Minor Security Settings	19	19	3.167	10.000
3.2.1 Security Options	19	11	3.167	5.000
3.2.2 Additional Registry Settings	0	8	0.000	5.000

Figure 6. Summary of the Benchmark Report

System iNtrusion Analysis & Reporting Environment (SNARE). This is an open source tool that allows the collection and forwarding of Windows event logs to a remote audit event collection facility, the SNARE microserver (InterSectAlliance, 2006). An enterprise version of the microserver is available as a commercial product which is fully supported by the IntersectAlliance Company. SNARE, which is an Intrusion Detection System (IDS) for Windows, allows system and security administrators full access and remote control of the application through a web browser. The application uses intelligent agents to automate the collection and reporting of log data. The SNARE agent tool is also available for Solaris, AIX, IRIX, Unix, and Fedora Linux operating systems. A SNARE Event Window graphical user interface is shown in Figure 7.

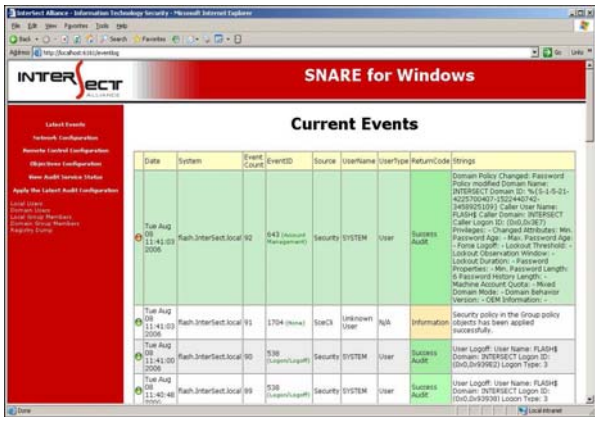


Figure 7. A SNARE Event Window

5. THE AUTOMATED COMPLIANCE TOOLKIT

The philosophy behind the design and implementation of the automated compliance toolkit is simplicity and affordability. The three-tier design of the system provides flexibility to adapt new technologies and future expandability. Figure 8 depicts the system architecture of the toolkit.

The following section is a brief description of each subsystem.

Subsystem 1: The Device and Media Control Subsystem. The function of this subsystem is to provide the necessary services to be able to properly secure and document the transfer of storage media. Additional services that are afforded by this subsystem are media reuse, document and media disposal and destruction, and document preservation and non-repudiation. . The open source tools that are used in creating this subsystem are TrueCrypt for media encryption and non-repudiation, Eraser for media reuse and destruction, mySQL database for media cataloging and tracking.

Subsystem 2: The Encryption Subsystem. This subsystem is used for the encryption and decryption of files. The open source, TrueCrypt, is adopted for the intended purpose of this subsystem.

Subsystem 3: The Authentication Subsystem. This subsystem is designed and implemented using two-factor authentication. The first factor requires a strong password while the second factor is a 512-bit soft-token that is randomly generated and stored in portable USB memory stick. The authentication subsystem is used to validate the users of the compliance toolkit.

Subsystem 4: The Vulnerability Assessment Subsystem. The Metasploit Framework and the Log Parser tool are complementary instruments that are used to build this subsystem.

Subsystem 5: The Intrusion Detection Subsystem. This Intrusion Detection subsystem utilizes the open source IDS tools, SNARE and OSSEC. In the both of the SNARE and OSSEC configuration schemes, a server is deployed using a Windows host and a number of system data collection agent tools are installed in client hosts running Fedora Linux, Solaris, and Windows.

Subsystem 6: The Message Preservation Subsystem. The primary objective of this subsystem is to facilitate the preservation of electronic documents that are used in business and personal transactions. The open source tools that are used in creating this subsystem are TrueCrypt for message encryption, decryption, and non-repudiation, mySQL for record cataloging and tracking, and WinZip for file compression.

Subsystem 7: The Log Management Subsystem. The MS Log Parser is our

primary tool in this subsystem. We built an automated data management process of log rotation, preservation, and retrieval using the .Net Framework and the Log Parser. In addition, the logs are maintained for traceability and accountability in order to comply with the auditing requirements of multiple regulations.

Subsystem 8: The Report and Benchmark Subsystem. This subsystem is built primarily with the Center for Internet Security (CIS) Next Generation (NG) Scoring Tool. The purpose of this subsystem is to verify the security configuration of systems and network devices for conformance with established benchmarks. Reports that are generated by this tool will be used as instruments to document partial or full compliance with federal and state regulations.

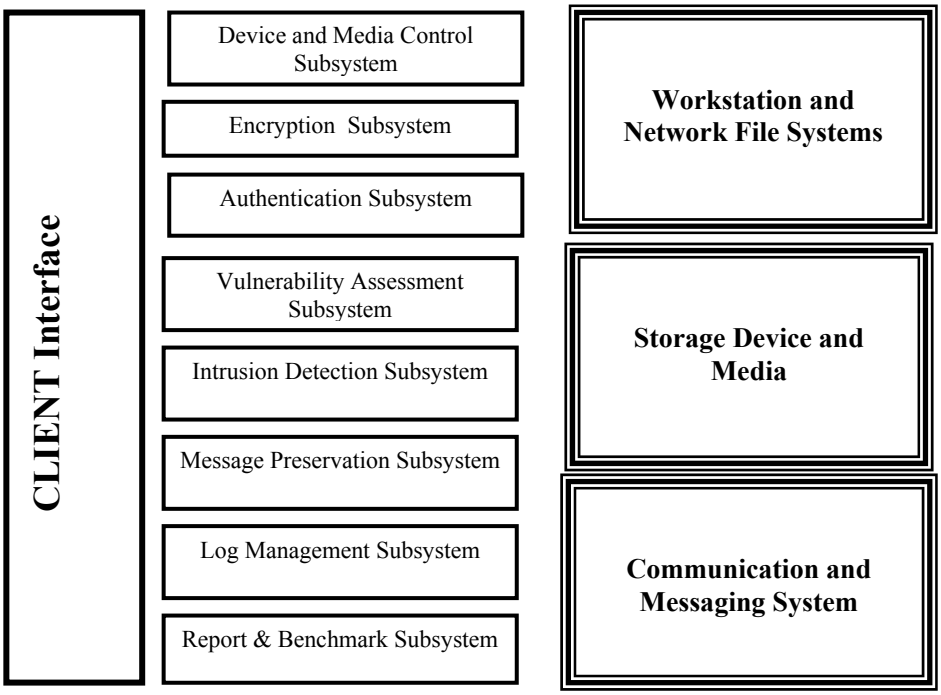


Figure 8. The Compliance Toolkit's System Architecture

A mapping of the control objectives, which were identified earlier, with the toolkit subsystems is shown in Table 2. The mapping illustrates which subsystems satisfy each control objective.

Toolkit Subsystem **Control Objective**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Document Preservation	✓					✓	✓	✓
Document Disposal and Destruction	✓						✓	✓
Device/Media Control	✓							
Media Reuse	✓							
Encryption/Decryption	✓	✓						
Authentication(2-level)			✓					
Transmission Security	✓	✓						
Log Management And Monitoring	✓						✓	
Vulnerability Assessment				✓				
Intrusion Detection					✓			
Report & Benchmark								✓
Message Security						✓	✓	

Table 2. Mapping of Objectives with Subsystems

6. ACKNOWLEDGEMENTS

This project is partially funded by a grant received from the Faculty Research Council at Jacksonville State University. The opinions expressed herein are those of the authors and are not necessarily of the University.

7. CONCLUSION AND FUTURE PLANS

We have presented a compliance toolkit that was designed and built using open source software. As the toolkit evolved, we discovered more features are immediately realizable using minor tweaks of the system parameters. In doing so, we covered more control objectives that we have not anticipated during the design phase. Such features include, among others, security policy auditing, log data warehousing and mining, visual data analytics, and configuration change control. Although the toolkit was designed and implemented to be a proof-of-concept

variety of a viable commercial instrument, it has the capability to partially meet the compliance requirements of most regulations. We are confident that we have achieved our stated goal at the onset, i.e. to demonstrate that meeting regulatory compliance does not need to be a very expensive proposition. Most importantly, we have demonstrated that providing students with a meaningful pedagogical exercise on the areas of collaboration, project management, software engineering, information assurance, and regulatory compliance is feasible and worthwhile.

The future plans for this toolkit are

1) to continuously enhance its features to cover more control objectives,
2) to add an intelligent agent component that will automate most of the data collection processes and alert functions, and
3) to study the feasibility of configuring the entire toolkit in a stand-alone embedded appliance system.

8. REFERENCES

Center for Internet Security (2006), "Next Generation Scoring Tool," http://www.cisecurity.org. Access date: October 01, 2006.

Cognos (2006), "IT's Critical Role in SOX and Regulatory Compliance," http://www.cognos.com/pdfs/whitepapers/wp_its_critical_role_in_sox_and_regulatory_compliance.pdf?mc=-web_ns_cpp_it_0830, August 30, 2006.

Cole, K. (2006), "HIPAA Compliance: Role Based Access Control Model," http://www.giac.org/practical/Kenneth_Cole_GSEC.doc, August 30, 2006.

Dhillon, G. (2006), Principles of Information Systems Security, Wiley Publishing Inc., New York.

Feldman, Johnathan (2006), "Don't Get Burned," Network Computing, September 28, 2006.

Giuseppini, G. and Burnett, M. (2004), Microsoft Log Parser Toolkit, Syngress, Rockland.

IntersectAlliance (2006), "Guide to SNARE for Windows 2.5." http://www.intersectalliance.com/resources/Documentation/Guide_to_SNARE_for_Windows-2.5.pdf, October 11, 2006.

ISACA (2006), "COBIT Framework," http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981, October 06, 2006.

ITIL (2006), "IT Infrastructure Library (ITIL)." http://www.itil.co.uk, October 06, 2006.

ISO (2006), http://www.iso.org/iso/en/commcentre/pressreleases/archives/2005/Ref985.html, October 06, 2006.

Kolodgy, C. (2006), "Optimizing Your IT Controls Environment for Compliance with Multiple Regulations," http://eval.veritas.com/mktginfo/enterprise/white_papers/ent-whitepaper_idc_bindview_policy_manager_2005.en-us.pdf, August 30, 2006.

Langin, D. (2004), "HIPAA Security Provisions: Is Your Network Ready for a Physical," TripWire, pp.1-12.

Nelson, M. (2006), "Complying with the Federal Information Security Management Act," TripWire, pp.1-6, 2006.

NetIQ (2006), "NetIQ Compliance Solutions," http://www.netiq.com/solutions/regulatory/default.asp, October 10, 2006.

OSSEC (2006), "OSSEC Host-based Intrusion Detection System," http://www.ossec.net/en/home.html, October 10, 2006.

Public Company Accounting Oversight Board (PCAOB) (2006), "Sarbanes-Oxley Act of 2002", http://www.pcaobus.org/rules/Sarbanes_Oxley_Act_of_2002.pdf, October 15, 2006.

Perry, C. (2006), "Compliance Control," Processor, Vol# 28, Issue#30.

Qualys Guard Enterprise (2006), http://qualys.com/products/qgent, October 10, 2006.

Qualys, Inc. (2004), "FISMA Compliance: Making the Grade," http://www.qualys.com, October 01, 2006.

Qualys, Inc. (2006), "Making Gramm-Leach-Bliley Security Compliance Fast & Easy," http://www.qualys.com/glba, October 10, 2006.

Scalable Software (2006), "Reducing the Cost of IT Compliance: Streamlining the IT Compliance Life Cycle," http://www.scalable.com/media/whitepapers/wp_Reducing_Compliance_Costs.pdf, October 13, 2006.

Schwartz, E. (2006), "The Compliance Headache," InfoWorld, 12.

Swartz, N. (2003), "What Every Business Needs to Know About HIPAA," The Information Management Journal, 26-34.

Symantec (2006), "Control Compliance Suite," http://www.symantec.com/Products/enterprise?c=prodinfo&refId=1482, October 08, 2006.

Tripwire Enterprise (2006), http://www.tripwire.com/products/enterprise/index.cfm, October 08, 2006.

TrueCrypt (2006), "TrueCrypt 4.2a," http://www.truecrypt.org/, October 10, 2006.

Whitman, M. and Mattord, H. (2004), Management of Information Security, Course Technology.