Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Application Security, Information Assurance's Neglected Stepchild - A Blueprint for Risk Assessment

In this paper we will focus on how to properly assess the security of application software. When executed correctly and to the appropriate level of detail, an application system audit is an objective evaluation of an organization's ability to prevent, detect and recover from information system failures. Byproducts of that assessment are a set of recommendations to ensure that assets are protected according to company, federal, state and local regulatory policies and a system security plan which is a blueprint for actio...

Copyright SANS Institute

Author Retains Full Rights

AD

Title:	Application Security, Information Assurance's Neglected Stepchild - A Blueprint for Risk Assessment
Submitted by:	Ted Mina
Version:	1.2e
Certification:	GIAC Security Essentials – Baltimore, MD May 18-20, 2001
Submission:	Original

© SANS Institute 2002, Author retains full rights.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Application Security, Information Assurance's Neglected Stepchild
A Blueprint for Risk Assessment

A conversation between the Chief Executive officer and the Chief Information Officer at Hypothetical.com corporation:

CEO: "How secure are our computer systems?"

CIO: "They are perfectly secure. We have a stateful packet filtering firewall appliance with a tried and true policy configuration. Our corporate web and mail servers are deployed in a DMZ. All incoming e-mail attachments are scanned for viruses and our mail server is configured to prevent third party relaying. Our dial up users are authenticated via one time use passwords and we war-dial all corporate phone numbers every month to check for modems left on in answer-mode. Any file written on any computer in our organization is checked for known viruses. The virus scanning software is centrally maintained and attack signatures updates are forced daily. We run a packet analyzing network intrusion detection system running on its own server 24 X 7. [1] We have hardened all of our Unix and Windows NT servers by removing all known operating system installation and configuration vulnerabilities. All internal access to the Internet is through a network address translating proxy server. Our Security policy is signed by every user and reviewed every 3 months. Our 128-bit encrypted network passwords are required to be eight characters that must include at least 2 non-alphanumerics and must be changed each month."

CEO: "So why were we late last week in transmitting our payroll information to the third party service provider who does the gross to net calculation and produces our paychecks? That cost us thousands of dollars in "hot" processing fees and expedited overnight check delivery to our 42 locations, not to mention that all of our direct deposits were made 24 hours late"

CIO: "Well, we had to upgrade our client software for that system and due to cost containment measures we had one of our people do it instead of hiring an outside consultant. She had never done anything like that before, there were several things missing from the upgrade documentation and it didn't go so well. She had to spend hours on the phone with the vendor's support group in order to get it up and running at all. Then, just as we were about to let the users into the system at 5:00PM, she clicked on the wrong icon on the payroll server and started a 3 hour vendor supplied database maintenance process that could not be interrupted.

CEO: "The order entry system in our consumer sales division was down for 2 days last month. We were unable to take phone orders for hours until someone located order forms and then our phone lines were tied up while the sales reps

[1] Northcutt, Chapters. 1 & 2

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

were filling out the forms. Orders that were placed on our web site are just plain GONE! Again, thousands of dollars in profit and customer goodwill, GONE!

CIO: “Application Development updated the order entry system executables first thing in the in the morning and didn’t find out until that afternoon that the new code was corrupting the system’s data integrity. Then they spent a day trying a code fix, which was also incorrect and just made matters worse. The system didn’t get brought back up until the executable and database directories were restored by Tech Support from prior to the introduction of new code.”

CEO: And finally, why is it that the water main rupture that flooded our basement data center five days ago has been dealt with, but most of our applications are still down?”

CIO: “Well, actually, our backup server was underwater and was completely destroyed. And, ah, we had not upgraded the software in well, quite a while, and we could not find the install disks and when we called the vendor for a new copy…”

CEO: “Yes, and…?”

CIO: “They said that the new version of the software, which is all they have available, will not read our old backup tapes.”

CEO: “You are **soooo** fired!”

Exaggerated? Yes. Impossible, no. Most of the incidents above were based on an actual event known to the author. The point is: So much time, effort, publicity and just plain “hype” is devoted to protecting corporate information assets against outside threats that outages due to human frailty are often neglected altogether. System failures due to poor planning, lack of knowledge or faulty design are just not sexy. It should be obvious that it is far easier for one disgruntled, vengeful or just plain klutzy employee with a system user ID to wreak havoc than it is for the most skillful hacker to intrude from outside the organization. In the author’s nearly 20 years as an computer systems consultant, natural disasters and man-made blunders have caused the most severe system outages that he has encountered.

The best defensive weapon against all threat areas: external or internal, intentional or accidental, is the Information Assurance audit. A comprehensive Information Assurance audit will cover all aspects of a firm’s Information Technology operations ranging from assessments of network server vulnerability to physical plant security and disaster recovery planning. In this paper we will focus on how to properly assess the security of application software.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

When executed correctly and to the appropriate level of detail, an application system audit is an objective evaluation of an organization's ability to prevent, detect and recover from information system failures. Byproducts of that assessment are a set of recommendations to ensure that assets are protected according to company, federal, state and local regulatory policies[2] and a system security plan which is a blueprint for action in the event of system failure that is specifically tailored to the organization's capabilities and limitations.

The Audit Process

1. **Identify the Auditor** - The audit starts with retaining an outside consultant. The use of an outside professional ensures objectivity and independence that should prevent the examination from being biased. An experienced consultant will have insight based on exposure to many different kinds of systems in many different kinds of businesses. This type of skill and knowledge is required to correctly judge the sensitivity and vulnerability of software applications.

2. **Charter the Audit** - The auditor will conduct an initial meeting with the client company's senior IT management that is sponsoring the project to establish and document the responsibility, authority and accountability[3] for the audit. The charter will also specify the scope of systems to be examined, set expectations for the results of the assessment and set a general timeframe for the completion of the audit. The scope will vary depending upon the size of the client's company and the nature of their business. It could be limited to, for example, the systems with largest user base, the systems that have experienced the most outages, systems with external user interfaces or it could include all major (i.e. non-office desktop) application systems. It is also important to state what is not in scope, i.e. that accounting or cash handling procedures will not be inspected, etc.

3. **Inventory the Systems** - The next step is to review all existing documentation and meet with appropriate management in order to create an inventory of computer software systems that will be examined. At this meeting the system security plan roles that identify key personnel responsible for the operations and security of each system can be fleshed out.

4. **Interview Custodians** - This step in the process is the most time consuming and tedious. It involves scheduling and conducting interviews with custodians (owners and administrators) of the various systems that are in the scope of the audit. The auditor should prepare a questionnaire that can be forwarded to the custodians prior to the meeting to save time. Among the objectives of the interview are:

[2] Marchany, pg. 5
[3] Information Systems Audit and Control Association. "Audit Charter".

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Determine the primary business purpose of the system	Determine the physical deployment of the system
Identify the technical platform (hardware and software)	Evaluate the sensitivity of the system's data
Identify existing backup and recovery procedures	Identify system testing and new software migration procedures
Evaluate the quality of system and user documentation	Evaluate the quality of the process for training new users
Understand the system's built-in security	Identify all third party reporting tools used on the system's data
Identify interfaces with other in-house or external systems	Review process for removing terminated users from the system

A "walkthrough" of the system should also be scheduled at this time. For larger organizations the auditor may require assistants to aid in conducting interviews and system walkthroughs.

5. **Conduct a System Walkthrough -** The walkthrough should consist of the auditor physically witnessing the following actions being performed by a custodian:

System startup	System Administrator login
System shutdown	System Administrator logout
Normal user login	Demonstration of the most frequent transactions performed using the system.
Normal user logout	Internal system backup (if any)
Data import/export functions	Report creation (both periodic and ad hoc)

The auditor should also perform a "hands on" navigation of the system in order to review all system functions available to users and administrators that may not be known or frequently used.

6. **Prepare the Report** - For each application system in the scope of the audit, prepare a report consisting of the following sections: (Please see Appendix A: Sample Application Security Assessment Report)
   - A description of the purpose, deployment cost and general technical characteristics of the system, including a description of any security measures that are built into the application.
   - An assessment of the sensitivity of the information contained in the system. Data sensitivity can be rated in three categories[4]:

[4] Fisher

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

    - Confidentiality – To what extent does this data have to be protected from public access and unauthorized disclosure? Are there laws governing the privacy of this data?
    - Integrity – What impact would unauthorized, accidental or malicious modification of this data have?
    - Availability – What consequence would result if this data was not accessible on a timely basis?
- An evaluation of Backup and recovery procedures. They should, at a minimum be rated as:
    - Good - Multiple recovery paths are available
    - Adequate – At least one reliable recovery path exists
    - Inadequate – Recovery path is unreliable or non-existent
- Vulnerability analysis – This is where the insight and judgement of the auditor is critical to assigning an accurate rating value of high, medium or low. A brief explanation that justifies the rating should accompany each evaluation. The system's vulnerability to threats should scored in the following areas[5]:
    - Programming error – damage to the system caused by an error introduced by applying poorly tested or incorrect program code.
    - Environmental failure – damage to the system due to external uncontrollable elements such as power failure, fire, flooding, etc.
    - Hardware failure – damage resulting from memory, CPU, disk, telecommunications line or other device loss
    - Internal intentional misuse – damage caused by dishonest, disgruntled, vengeful or other malicious users of the system
    - Internal accidental misuse – damage caused by poorly trained or unskilled users, a poorly designed interface or an overly complex or cumbersome process.
    - External misuse – frivolous or malicious damage by hackers, professional criminals, terrorist groups, hostile governments or competitors.
- Recommendations for Improvement – These are specific protective measures that should be taken to address the vulnerabilities identified in the previous section. The recommended actions should be based on an economically acceptable level of risk balanced by the overall value of the system.
- System Security Plan –This document lists the names and contact information for each person assigned to a security role for the system. This section also lists intrusion detection procedures that should be proactively used to detect a system failure. Finally it contains a detailed step by step recovery plan to be followed in the event of a system failure. The security roles are:
    - Internal Owner: The manager who is accountable for the work performed by the system.

[5] Russell and Gangemi, Chapter 1

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Application Administrator: This is the functional user who has day to day operational responsibility for the system. This role is also responsible for adding new system users, disabling terminated users and configuring internal access groups if the system contains its own internal security.
- Security Administrator: This is the person responsible for ensuring that this system and its users comply with the organization's overall security policy.
- Application Technical Support: This is the programmer, developer or system integrator that is responsible for addressing any software issues associated with this application such as installation, configuration, troubleshooting, enhancements and upgrades.
- Network Technical Support: This is the network engineer responsible for ensuring access to this application over the network.
- Database Technical Support: This is the data administrator who is responsible for ensuring availability of the third party database management system used by the application system, if any.

7. **Present the Report** – This is the culmination of the Audit. Once again, depending upon the size and nature of the client's business this presentation could range from an small informal meeting to a "High Ceremony". It is a good idea to have a preliminary presentation of the results made to the project's sponsor so that any glaring, critical or otherwise embarrassing security flaws can be addressed immediately.

Some Practical Tips from the Field

Recommendations do not have to be complex - Many recommendations are nothing more than common sense suggestions. However, an outside auditor has the advantage of reviewing the systems anew and is not constrained by pre-existing corporate thinking patterns. Consider the example, given in the beginning of this paper, of the systems engineer who inadvertently started a long running, non-cancelable database maintenance process by clicking on the wrong desktop icon. The desktop on the server had an icon to start the process and one to view the log generated by the process. Viewing the log was a frequent function. An unattended process scheduler normally started the maintenance process itself at night. Therefore, there was no reason to have the icon to manually start the process on the desktop. It was removed and the threat of that specific accidental failure occurring again was greatly reduced.

See it for Yourself - The auditor must also insist upon personally examining the systems that he or she is assessing. At one client who operated their own cafeteria, the systems director declared that the point of sale systems were password protected and therefore secure. The walkthrough of the cafeteria systems was held during lunchtime, their busiest period and the system startup

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

and login process could not be demonstrated. The auditor insisted upon coming back after the cafeteria was closed and having the manager go through the startup procedure. It was then discovered that the system was in fact password protected, but when prompted by the software for the password, the operator entered it by pressing a programmable key that was hand lettered with a “P”. If the auditor had accepted the director’s word instead of insisting upon a first hand examination, this severe security breach would have gone undetected.

Good change control is essential - It is impossible to over emphasize the importance of good configuration management. Configuration management can be defined as the control of a software change as it is promoted along the migration path from initial testing to production implementation. A variety of factors affect the steps that constitute an appropriate migration path. The size of the organization, the complexity of the change, whether the system is in-house written and maintained or a third party package maintained by a vendor all affect the structure of the migration path. A configuration control tool can be a complex series of third party packages or a simple set of forms and a published procedure. Whatever the actual implementation is, the most important implication for application security is that the control system must contain checkpoints that ensure adequate, realistic testing and a quick and easy process for backing out software changes that have unintended results.

© SANS Institute 2002, Author retains full rights.

Appendix A: Sample Application Security Assessment Report

Fundraising System Security Assessment

This purchased package records donor information, pledges and donations for capital and operating fund raising campaigns. The system contains data on over 6000 donors.

The system is based on the DataPie database and is a client server deployment with software on each workstation as well as the dedicated SERVER1 network server. Vendor B's reporting software is used as the back-end reporting tool. A gift detail report listing all checks received is sent to the Accounting system for posting on a daily basis.

The application contains sophisticated multi-level access control to menu items as well as field level security.

Data sensitivity	Hi	Med	Low	Comments
Confidentiality		**X**		While donor information is not highly confidential and no credit card numbers are stored in the system, there is no reason to allow free access to this information.
Integrity	**X**			This system contains financial transaction data. Unauthorized or accidental modification of this data could result in lost revenues.
Availability	**X**			This is a major source of revenue for the organization. Loss of pledge and payment data would have a major financial impact on the organization. Loss of donor information would require a major expenditure of time and effort to recover and re-enter.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

	Good, multiple recovery paths	Adequate, single recovery path	Inadequate	Comments
Backup and Recovery	X			Has internal "export" capability Uses standard system recovery (see Network Backup and Recovery

Vulnerability of Failure due to:	Hi	Med	Low	Comments
Programming error:		X		Software updates are periodically received from the vendor. Due to introduction of software errors as a result of applying these updates in the past, the updates are applied only on an "as needed" basis. There is no backout or testing capability and vendor support is considered to be unsatisfactory.
Environmental Failure:			X	Normal risk level
Hardware Failure:			X	Normal risk level
Internal Intentional Misuse:		X		While the system does have good internal access controls, it uses a publicly available common database platform. An unauthorized user with network access to the server, could potentially access the stored data.
Internal Accidental Misuse:			X	The system is well organized and formal classroom training is available from the vendor.
External Misuse:		X		While the system does have good internal access controls, it uses a publicly available common database platform. If an intruder gained network access to the server, they could potentially access the stored data.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Specific Recommendations:

Create and maintain a list of all files on both the workstation and the server that constitute this system so that files to be restored during recovery may be identified.

Locate and document the location of application install disks. Keep them in a secured area.

Appoint a backup application administrator to act in the application administrator's absence.

Isolate the remotely accessed database files onto a separate folder on the server.

Create a network user group (FUNDRAISER) for users of this application and give it appropriate network and directory permissions.

Create a permanent hard copy "master" list of donors and keep it in a secure area.

At an appropriate point in each find raising campaign, create a permanent hard copy list of donor pledges and keep it in a secure area.

Shred all documents containing financial data when done using them.

Implement and enforce strong internal access control measures:

- Require each user to have a unique internal user ID.
- Require a password of at least 6 characters
- Require passwords to be changed by the user every month

Log on to the system as a user and ensure that users do not have administrative capabilities such as password modification, menu item and field privilege control, etc. Only the System Administrator user ID should have these privileges.

Using the system's internal capability, the Application Administrator should make a periodic export of all system data to serve as an alternate recovery path.

Shut down the NT Server service for this application prior to the nightly backup to ensure the integrity of all files.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Fundraising System Security Plan

Role	Assignee
Internal Owner:	Director of Finance John Doe Office: 410-555-1212 Cell: 443-555-1212 Home: 410-555-1212
Application Administrator:	Financial Associate Joanne Doe Office: 410-555-1212 Cell: 443-555-1212 Home: 410-555-1212
Backup Application Administrator:	None at this time
Security Administrator:	Director of Network Systems Jane Doe Office: 410-555-1212 Cell: 443-555-1212 Home: 410-555-1212
Application Technical Support:	Really Good Software, Anytown, USA (800-555-1212) site ID: 123
Network Technical Support:	Director of Network Systems Jane Doe Office: 410-555-1212 Cell: 443-555-1212 Home: 410-555-1212
Database Technical Support:	Director of Network Systems Jane Doe Office: 410-555-1212 Cell: 443-555-1212 Home: 410-555-1212

Intrusion Detection Procedures:

Application Administrator should track and periodically review gift detail reports for unusual donation patterns or amounts.

Security Administrator or staff should review Event Viewer security log on SERVER1 for successful/failed access to database files semi-weekly.

Security Administrator or staff should review the DataPie access log semi-weekly.

System Recovery Procedures:

1. Application Administrator obtains system file list and contacts Network Technical Support.

2. Application Administrator and Network Technical Support decide which files from which dates to recover.

3. Network Technical Support locates backup tape containing the needed files.

4. Network Technical Support uses Backup Software to recover files on the Server.

Or:

1. Application Administrator obtains an internal export file and imports it into the application.

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

References:

Marchany, Randy. Course Book: Understanding & Auditing Information Systems. SANS Institute, March 2000, 26-29

Russell, Deborah and Gangemi, G.T., Sr.Computer Security Basics. O'Reilly and Associates. 1st edition 1991.

Icove, David, Seger Karl and VonStorch, William. Computer Crime. O'Reilly and Associates. August 1995

Northcutt, Stephen. Network Intrusion Detection An Analyst's Handbook. Indianapolis. New Riders Publishing. 1999

Information Systems Audit and Control Association. "Standards for Information System Auditing". Undated. URL: http://www.isaca.org/standard/enstandard.pdf

Information Systems Audit and Control Association. "Audit Charter". May 1999. URL: http://www.isaca.org/standard/guide17.pdf

Fisher, Jim. "Concept Presentation for ESWG on the ECS Security Risk Management Plan". April 1999.
URL: http://esdis-it.gsfc.nasa.gov/SECURITY/PRES/RISK/Sld001.htm

B. Fraser, ed."RFC 2196 Site Security Handbook". Sept. 1997
URL:http://www.faqs.org/rfcs/rfc2196.html

© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 26th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**