Global Information Assurance Certification Paper

Designing the Application Layer Security

Joel B. Cort
September 13, 2000

Introduction

There are several good configuration recommendations available in the industry for hardening the operating system platforms presented in YASSP[1], NT[2] and LINUX[3] among others. These configuration steps provide one piece of the network security solution. They provide the secure platform on which to install an application; however, which additional areas need to be considered when safeguarding the crown jewels of the corporation—applications and data? The design of the application and controls can determine whether data is properly or improperly accessed, created, altered and deleted. This paper will propose—at a high level—additional security controls that should be considered when designing and implementing application security.

Users interact with the application programs at the Application Layer of the TCP/IP and ISO models[4]. The Application Layer is the primary avenue to the data and must be protected as vigorously as other avenues of the operating system (OS) and the lower-layers such as network transport or the physical layers.

Various established industry standard publications referring to application security have provided some of the initial background for these recommendations. The references include the British Standard 7799 (BS7799)[5] and Federal Information Processing Standards (FIPS PUB 73[6]) which may be an excellent starting point for anyone involved in implementing application security.

The security of the application and information includes the technological controls based on business issues and decisions. What are the risks to the business if the information accessed by the application is compromised? Business Risk Analysis (BRA) is important because it can identify and provide knowledge of the threats to the business model and subsequent actions of decision-makers.

Risk Assessment

The risk assessment is a documented analysis of the potential business impact due to compromise of the application or data. An effective risk assessment provides amplifying details clarifying the decision points regarding balancing the cost of implementing security measures vs. accepting the risk posed by a security breach. This information is vital to the organization considering developing and implementing a new application.

The corporate information security policy and the organization's business requirements provide the foundation for performing the risk assessment. Security risk assessments are broad and often complex, and step-by step instructions are beyond the scope of this document; however I will offer a brief overview of the components.

- **Impact level of a security violation on the business:** This analysis is performed to determine if a violation occurred, how much impact would it cause to the business in terms of the value of the information assets of the company.
- **Business accessibility to threats:** Analysis performed to detect vulnerability of the application or how exposed the company may be to threats such as: vandalism, espionage, theft, sabotage or computer fraud.
- **Vulnerability**: Analysis performed to determine what are the specific weaknesses in the current information-handling systems and/or in the business organization, considering physical and logical access, number of system users and technical security compliance.

- **Probability of an asset being subject to a security threat:** Analysis performed to approximate the statistical probability that the identified threat(s) will occur, and at what frequency.

The effective risk assessment fully supports the necessary business decisions required to manage the identified risks. These business decisions typically result in one or a combination of the following outcomes:

- **Acceptance**–of the consequences of a potential security breach without implementing security controls.
- **Mitigation**–Reducing the cost of a potential security breach to an acceptable level by reducing the probability of occurrence through the implementation of controls.
- **Transfer**–Eliminating the potential breach by eliminating the cause of the potential breach.

A detailed description of the risk assessment process is available in the Information Security Management Handbook[7]. The remainder of this document deals with ensuring that the proper security controls have been enabled and designed into the application to mitigate vulnerabilities and risks to the company.

Securing the Application Step by Step

As a security practitioner, my custom and recommendation for improving application security is to follow a layered approach of security controls. The controls are presented in step by step form to manage and mitigate various threats. This information is targeted to application manager and implementers. These steps will ensure that the security controls, policies and practices become standard for the organization and will be enforced. The focus of this outline is at a high-level for clarity of theme (i.e. I will not drill down into specific products or lower layers such as middleware.)

Effective security management practice can be characterized by the preservation of the following standard information security services[8]:

- **Confidentiality**: Ensures that applications and data is accessible to only the users intended and authorized to have access.
- **Integrity**: Guarantees the accuracy of the data.
- **Availability**: Ensures that authorized users have access to the application and the data

when required.

- **Authentication**: Guarantees that the application users are who they claim to be.
- **Non-repudiation**: Proves that the originator of the data and user of the application did perform the transaction.

A. Environment Security

A step by step hardening of the operating system platform (see references 1,2 and 3) prior to introducing the application and its requirements should be completed.

- All measures to control and safeguard the physical environment of the server should be in place with your site's infrastructure and policies.
- Hardening the base operating system first will ensure that the platform environment is secure before any application is installed.
- If the application requires a back-end database such as Oracle, additional time should be spent to configure and harden the database as well.

B. Installation, Configuration Management, and Patches

Next, attention is turned to the maintenance and integrity of the configuration, application software and management of the system.

- This step ensures that a document, such as a logbook, is maintained to record and document the installed software revision level and patches for the application, whether the application is custom designed or a commercial software.
- Any changes and updates are managed and documented through a formal change control process.
- There may also be some legal and financial ramifications if public domain software is in use or required by the application, so it should be dully noted and approved by the management team prior to using in a production mode.

C. Access Control

The following steps ensure that the authorization to access the application is adequately controlled.

- The application must provide an authorization mechanism for authorized users to control access to classified or sensitive application objects.
- Access must be limited to those objects required by the application.
- Access to computing resources and networks by customers, vendors, business partners, etc. is limited or restricted to only the essential functions.
- All application interfaces, such as legacy feeds, LAN, WAN, Internet and remote access must be identified, documented and diagrammed. Documentation must be kept current

as the system and application evolves.

- User access is limited to what is required to perform the task at hand. The application should be designed to grant minimum privileges to the application or system for users.
- To safeguard the access to the data, the application software should launch an automatic screen lockout feature or the client workstation has a screen saver mechanism enabled that requires a password during idle periods.
- The tracking of repeated logon attempts is an essential component in detecting system attacks. The application software must contain a feature to detect and prevent repeated logon attempts and/or password guessing due to a brute force attack. After a number of attempts to access an application with user ID and incorrect password combination, a mechanism exists to disable the specific user ID account for a time period.
- When the successful access to the application is obtained, an informative banner is displayed telling the user that this application is proprietary and restricted for company business use. The banner should provide appropriate legal language to protect the corporation in a court of law.
- The application should not establish a connection to an external resource without being reviewed and approved.
- No dial-out routed or permanent routed connections are established from an application to other systems or networks without being reviewed and approved.
- Dial-in access and remote access is permitted only to authorized access points. Dial-in access points use two-factor authentication mechanism.
- Communication paths to external networks are limited to approved firewall gateways.

D. Account Policy

The following considerations are related to granting user accounts, and subsequent authentication to authorize application use and data access. Implementation of these steps may vary due to site-specific security policies.

- Users are authenticated using a unique user ID and password before accessing applications, database objects, and data.
- Database or applications cannot operate without entering a valid user password.
- Database or application user account maintenance (additions, deletions, cancellations, and changes) conforms to the processes established for managing system users.
- User accounts are only granted to justified users and such authorization is documented.
- Application passwords must be hard to guess and contain a minimum of *six* alphanumeric characters. (or whatever is appropriate with your site security policy.)
- Expiration of passwords will be required (i.e. expires every *30* days, depending on the site security policy.)
- Reuse of password must be aged to enforce changes. (depending on the site security policy.)

- All passwords stored electronically are encrypted.

E. Auditing

Auditing the application serves the dual purpose of monitoring the dynamic system to provide continuous availability and provides forensic information in the event the system has been attacked or otherwise compromised.

- Audit controls are implemented, which help monitor system activities through regular observation of activity logs and records.
- Application audit trails and logs are in place to track all relevant information and meaningful activity and identify who, when, where and what.
- The audit trail/log must be guaranteed not to be falsified or examined by unauthorized auditors.
- The application does not continue operation if the logging mechanism fails. If you are unable to tell what activities have taken place then the integrity of the application is at stake.
- System and audit logs are reviewed and monitored regularly and provide suitable alarms for capacity monitoring when thresholds are passed.
- Application audit logs may be sent to alternate logging resources to be stored and tracked.
- Audit logs should reside on a trusted server.
- Logs are kept for a suitable amount of time for auditing purposes.
- Application logging includes login failure, failed object access, and failed function access as well as successful logins.
- Support personnel are educated on appropriate response and escalation of security incidents.

F. File System Security

The following checks address the integrity of the file system and the classification of the data. Data changes depending on circumstances. Senior executives must recognize the value of their organization's data and take action to ensure that they protect it[9].

- The installation of the application and any other software and data originated and is received from trusted sources.
- Host Intrusion Detection Software (IDS) may be required to ensure file integrity.
- Data is classified by the data owners in accordance with your company's data classification rules. Identifying and classifying confidential information helps establish legal ownership rights and provides a tool for protecting valuable information[10].
- The application manages, displays, and stores classified information in a manner

consistent with your company's data policy.

- Classified data is identified by the application with proper markings.
- Data classification level is always displayed on the screen when these data are displayed, or at a minimum, a banner or splash on the first screen indicates the data classification level for the information displayed by the application.
- Reports or other printed classified data always displays the classification markings.
- If encryption is used to store classified data, the encryption methods are consistent with any required export restriction.
- Encryption keys are not hardwired or stored in cleartext. The application is coded to decrypt on demand rather than store cleartext.
- All classified or other sensitive information exchanged over the Internet is encrypted.

G. Backup and Recovery

There are volumes of information available on data backup and recovery. The following steps are presented with the data *and* application in mind.

- Application files and data may be backed up separately from the operating system and user data for speed and efficiency. Considerations are given to application specific backup/restore procedures and requirements. Backup procedures and requirements are documented by Business/Application Owners.
- All security mechanisms are retained in backups. All security requirements for storage are also on backup media. "Security mechanisms" refers to all encryption/encrypted text, files, passwords as well as file privileges and role restrictions. A file system must retain the permissions and configuration on the rebuilt system identical to the original system. The security requirements for storage may extend to properly labeling and identifying the data classification on the backup media (CD, diskette, tape etc.)
- All storage locations for classified data are identified in the backup and recovery plan.
- All backups of classified data are labeled with the classification markings.
- Periodic tests of backup data recovery from media are performed by the support team, as documented in the application backup and recovery plan.

H. Security Monitoring

These considerations are related to the final, deployed application. The operating system and application have now been hardened. The consideration now is whether or not there are ports and "back-doors" that may have been overlooked.

- Security monitoring software has been obtained to run a scan on the system vulnerability. Scan levels can be configured from light to heavy by the operator depending on how vulnerable or the level of risk a system has.

- A security compliance scan should be performed on the system at least every six months or whenever new software or configuration changes occur.
- Security monitoring can also include the monitoring of the host intrusion detection software.

I. Data Integrity

The following components need to be implemented to ensure integrity of the data and the application process.

- Authentication and authorization are performed prior to loading any classified data.
- All database or application software posts data with a message displaying the level of information classification.
- Applications run at the minimum authorization level to accomplish their purpose. Whenever possible, applications do not run with system level (root) privileges.
- Applications do not allow users to perform functions that are not specific to that application.
- Application access controls are in place to provide the least privilege necessary for users to perform their business function.
- Final compilations are done with all debugging mechanisms and backdoors removed prior to deployment.

J. Disaster Recovery and Business Continuity Planning

Finally, there are volumes of information emphasizing disaster recovery (DRP) and Business Continuity Planning (BCP). These steps really depend on the site and plans for business continuity so this will be addressed I a general overview. The following steps are presented with the data and application in mind. Most of the information and decision originate as a result of the risk assessment. The value of a particular application and its data may receive different levels of importance based on the criticality to the business.

- Ensure that critical Application files and data have been backed up and the backups are reliable. Also ensure that the operating system and the configuration settings are also backed up and well documented, so that the entire system can be rebuilt from this media.
- Depending on the business criticality an alternate computing environment may be available to continue the operation of the application. Ensure that the same security controls and mechanisms are in place and managed at the alternate site.
- Ensure that the change control process, (as it relates to the security of your application) is in place and followed at the alternate site, even during the havoc of an emergency operation.
- Document your plan as it pertains to your application and the required data to operate.

(The assumption is that the telecom folks have done their part on routing to the alternate site.)

- All storage locations for classified data are identified in the DRP.
- The DRP has been tested and validated in a live environment to ensure that what is documented works.
- Ensure that the security controls are in affect, after the primary operations have recovered from the disaster, at all sites involved.
- Have a lessons-learned session and document all findings after going through such exercises to improve the entire process.

Conclusion

This paper presents a review of tested controls that should be implemented or designed into an application to provide a good level of assurance that the application is secured. The application security offers one half of the whole solution, the second half also must be implemented: a hardened platform upon which the application will reside. Again, this is a high level review and, it must be obvious, additional granularity can be configured as well as additional controls and enhancements. I have stepped the reader through a layered security control approach to protect the "crown jewels" and proposed an operational framework to provide security in the Application Layer.

References

[1] Chouanard, Jean, YASSP: Yet Another Solaris Security Package, July 20, 2000, Xerox Corporation URL: http://yassp.parc.xerox.com

[2] Windows NT Security Step by Step, Version 2.15,Copyright © 1999 by the SANS Institute, July 30, 1999.

[3] Securing LINUX Step by Step, Version 1.0, Copyright © 1999, 2000 by the SANS Institute.

[4] Conorich, Douglas G., Internet Security: Securing the Perimeter, Chapter 5, Pg. 87; Information Security Management Handbook, 4th Edition, Tipton, Harold F., and Krause, Micki, Copyright © 2000 by CRC Press LLC.

[5] British Standard 7799 Parts 1 and 2 (BS 7799), BDD/2 - Information Security Management, BSI-DISC, URL: http://www.c-cure.org/fbs7799.htm, Email: c_cure@bsi.org.uk, Tel 020 8995 7799.

[6] Federal Information Processing Standards Publication 73 (FIPS PUB 73) Guidelines for Security of Computer Applications, Washington, DC. GPO, June 1980.

[7] Ozier, Will, Risk Analysis and Assessment, Chapter 15, Pg. 247; Information Security Management Handbook, 4th Edition, Tipton, Harold F., and Krause, Micki, Copyright © 2000 by CRC Press LLC.

[8] Stackpole, Bill, Application-Layer Security Protocols for Networks, Chapter 10, Pg. 164; Information Security Management Handbook, 4th Edition, Tipton, Harold F., and Krause, Micki, Copyright © 2000 by CRC Press LLC.

[9] Cohen, David, Cohen, Lance, The Unrecognized Risks of Data, Copyright © 1998 by MEMCO Software Inc., MEMCO Software 12 East 49th Street, 32nd floor New York, NY 10017 USA.
URL: http://www.ca.com/etrust/, (formerly www.memco.com) Phone: 800-862-2602, 212-888-6200.

[10] Fine, Naomi, Confidential Information ownership and classification: Legal and Practical Considerations, Copyright © 1999 by Computer Security Institute, Presentation from Pro-Tec Data
URL: http://www.pro-tecdata.com, Email: nfine@pro-tecdata.com.