



University of Pittsburgh

E-Business Resource Group

Security Guidelines

Revised: 8/5/03

E-Business systems inherently possess a higher degree of risk than mainstream applications, and thus require a greater degree of security. Because of this risk, security should be considered as a fundamental aspect of an e-business system design. The following guidelines for e-business systems are meant to supplement common security practices, as well as existing University policies and procedures related to computer usage and information security. These guidelines are also intended to promote compliance with relevant regulatory laws including the Gramm-Leach-Bliley Act. Please note that while the E-Business Resource Group will assist departments with assessing their project's security and make recommendations; ultimately, each department is responsible for ensuring the security of their e-business system.

Physical Security

- The servers and administrative PCs should be kept in a secure room with restricted access. Be wary of potential access points such as windows, dropped ceilings, large air ducts, and raised floors. Server racks and machine cases should be locked when possible. The room should provide proper environmental conditions and safety for the equipment. Servers should not be placed directly on the floor in case of flooding. An approved fire extinguisher should be kept near the server room.
- Physical security of hard copies and data storage media containing sensitive customer information must be maintained. Windows, doors, and file cabinets should be locked in areas where sensitive information is stored. Where feasible, safes should be used to store especially sensitive data such as credit card information, checks, and currency. Access control to sensitive areas must be maintained and limited to individuals who require access as a result of their job.
- High availability hardware should be used in all e-business servers (e.g. high quality components, redundant storage and power supplies, mirrored servers, error correcting memory, multiple NICs). Uninterruptible power supplies should be used on all servers and tested regularly.
- Backups should be performed on a frequent and regular basis, and the backup media should be kept in a secure location. The backup media should be rotated and moved off-site as frequently as possible.
- Modems should not reside in e-business servers unless absolutely necessary. If a modem is installed, it should be kept powered off or disabled except when needed. For added security, the modem should be configured to utilize features such as automatic call back and data encryption. Firewalls will not protect against attacks by way of the modem.
- To provide more reliable and secure network access, servers and sensitive PCs should utilize switched network ports, not a shared medium such as coaxial cable or a repeated segment. Visible ports and exposed network cabling should not be present in vulnerable or public areas.

Data Storage

- Sensitive information, especially credit card data, should never be stored on the web server. The data collected by the web server should be passed to another physical machine for storage. Ideally, the data collected by an e-business web site should be stored in a location that is not directly accessible to the Internet. Sensitive information should be stored encrypted when possible. Be wary of sensitive data that may be stored in a web server's cache or log files.

- The retention of sensitive information such as credit card numbers should be avoided where possible. Sensitive information should be stored on the minimal number of machines while still maintaining system reliability. Care must also be taken to protect sensitive system data such as private keys.
- Sensitive information should be stored for a minimal length of time. The most sensitive portions of the information should be purged once it is no longer needed (e.g. deleting the customer's credit card number once the transaction has been processed while retaining demographic information).
- Copies of the data stored on the e-business machines must be treated with the same security precautions as the production data. Backup tapes and removable media must be kept in a secure location, and sanitized or destroyed before disposal. Hard copies, such as reports, containing sensitive data should be stored in a secure location, and properly destroyed (e.g. shredded) when no longer required.

Data Transmission

- All transmissions of sensitive information between the web client and the e-business web server should utilize current industry standard encryption (e.g. 128-bit SSL v3 encryption, with a minimum key length of 1024 bits.) Servers should be configured to refuse clients who cannot accept the required level of encryption, although consider providing a link on the site so customers can download the required version of the browser. Usernames and passwords should not be transmitted over the network in clear text. All administrative connections to the web server should also utilize encryption.
- Transmissions of sensitive information between machines other than a client and web server should utilize file encryption such as PGP, and/or utilize a secure communication method such as VPN software, scp, sFTP, or SSH.
- The transmission of sensitive information via e-mail should be completely avoided. If e-mail transmission is necessary, data encryption should be utilized (e.g. PGP, S/MIME). Care must be taken to ensure that e-mail containing sensitive information is not stored, forwarded, or copied to insecure locations or unauthorized accounts. If sensitive information is retained on the mail server, then the mail server should be secured to the same standards as the e-business database server.

System Administration

- All e-business related servers must be hardened. Default installations of operating systems and many applications are rarely configured for ideal security. Minimal services should be running on the servers, and essential services must be properly configured and secured. Keep the least number of ports open on a system necessary for it to function properly, and close or filter traffic on all other ports. The servers should not be used for additional, unrelated applications, or used as a workstation. Patches and updates must be regularly applied, and manufacturers' security recommendations and configurations should be followed. Demo or sample scripts, stored procedures, and applications should be removed when possible. Consider removing or disguising web server banners. Administrators should regularly monitor bug reporting and security sites for relevant security risks, and utilize scanning tools to check for vulnerabilities. All system configuration changes should be logged.
- System administrators must inspect log files (e.g. security, audit, firewall, antivirus) daily for suspicious activity. Investigate repeated login failures, account management events, failed privilege use, policy changes etc. Logs should have defined maximum sizes and retention periods. Administrators should periodically perform self-audits of the e-business systems. Staff should be informed of basic security practices (e.g. locking workstations, strong passwords) and be wary of social engineering attacks. Inquiries regarding customer information should be referred to individuals who have been trained in safeguarding information. Suspicious activity, including suspected intrusions and significant security violations, should

be reported to your supervisor, your department's designated Customer Information Security Officer, University Police, and for cases involving computer security, CSSD. Host and/or network-based intrusion detection systems should be considered as a further security measure.

- Strong passwords must be used for all user and system accounts. Enable passwords at multiple layers (e.g. BIOS, network login, database). Unattended machines should be kept locked with a password-protected screensaver. Inactive or unnecessary accounts should be disabled or removed. Default passwords, commonly known system accounts, or compromised passwords should be removed or changed immediately. Strong passwords should:
 - Have sufficient length to hinder brute force attacks (e.g. seven or more characters)
 - Be changed on a frequent, regular basis (e.g. every 45 days)
 - Be unique and not repeatable for a number (e.g. 10) of changes
 - Be locked out after a number (e.g. 3) of failed login attempts
 - Not consist of dictionary words, proper nouns, or personally identifiable names or numbers (e.g. person's name, computer name, SSN, phone number, birth date)
 - Make use of mixed case and non-alphabetic characters where possible
 - Be known only by the user responsible for the account
- Minimal system privileges should be granted to users and services, and file systems should restrict access to sensitive data. Rights should be granted on an as-needed basis. The use of privileged accounts should be kept to a minimum. Separation of duties should be implemented as feasible. Ordinary user accounts should not be created on the e-business servers unless they are essential.
- Servers and sensitive PCs should run antivirus software which is updated on a frequent basis. Machines involved in the transmission or storage of sensitive information should reside behind a firewall or utilize router ACLs/IP packet filtering to restrict access.
- Disaster recovery and business contingency plans should be developed which include the definition of what constitutes a disaster, procedures of what should be done to recover from various failures, and how business will resume. The plan should be tested and periodically reevaluated. Backups and test restores should be performed on a frequent and regular basis. The backup and recovery process, including recovery point and time objectives, should be documented and tested on a regular basis. Consider how you will handle service interruptions or a denial of service.

Application Development

- Strong user authentication (e.g. username/password, digital certificate) should be used with web-based systems. Unique user identification and passwords should be used and enforced by the application before each transaction. Passwords should not be visible or retrievable online. IP addresses should not be considered reliable authentication for sensitive information. Consider the use of personal digital certificates or tokens for stronger authentication.
- All user transactions should be logged with user ID, transaction type, data, time stamp, etc. Avoid logging unnecessary sensitive information. Care should be taken to ensure partial transactions do not occur in case of error or disruption of service. Consider how to handle non-repudiation issues and fraudulent transactions.
- Sensitive information should never be stored on the web server. Sensitive information should not be stored in persistent cookies. Cookies should not be considered a reliable authentication mechanism for sensitive information (e.g. reading a customer's user ID from a cookie without password authentication). The acquisition of unnecessary sensitive information should also be avoided, such as storing customer social security numbers only for use as a primary key in the database.

- Ensure that no sensitive information, including login dialog, is being transmitted over the web without encryption. Session keys should automatically expire after a short period of time (e.g. five minutes). Care should be taken to ensure that session ID algorithms are strong enough to avoid prediction or duplication of IDs. HTML pages should prevent encrypted files from being cached on the client via Meta tags.
- The transfer and display of credit card numbers or other sensitive information should be kept to a minimum. Credit card numbers should not be retrievable online. Applications should only display a small portion of the credit card number after it is initially entered by the user. Changes and deletions of the stored credit card number should be allowed without revealing the original number.
- Source code must be kept in a secure location. Store scripts and applications in separate directory from mainstream content, or on a separate application server when possible. Programs and sensitive information should not reside in an area that can be indexed or readable by the public. Shield appropriate HTML pages from search robots with Meta tags or through dynamic content. Do not store scripting executables (e.g. Perl) in the CGI-Bin area. Do not store development tools such as compilers on production servers.
- Many ways exist for unauthorized users to run code of their choosing on servers. All data provided by the user should be filtered and validated by several criteria (e.g. ranges, lengths, authorization, invalid characters) on both the client and server side to avoid buffer overflows. Avoid use of UNIX shell scripts where possible. Avoid programs that create temporary files to avoid possible system race conditions. Likewise, CPU time limits should be placed on scripts and applications.
- Ensure that all applications use proper HTML and coding to avoid incompatibilities, system crashes, and possible security risks. Mobile code should be signed to allow compatibility with secure clients. Consider how to handle clients who refuse or restrict the use of potentially insecure features such as cookies, Java, and ActiveX. Avoid use of relative paths when referencing commands or files. Avoid use of the “put” HTTP method; use the “post” method instead.
- Imbedded scripts, cookies, “hidden” fields, search features, code comments, error messages, and URL lines can reveal sensitive information, programming structure, and possible security holes. Return codes should be checked and handled. Care should be taken to ensure that information sent to the browser does not reveal excess information about the system’s architecture, data validity, or any sensitive information. Do not transmit unnecessary parameters.
- Online content and program modifications should follow an established change control procedure with testing. Test results should be retained. All code should be reviewed by multiple competent developers. Content should be inspected to avoid copyright or trademark infringements, defamatory statements, or privacy infringements. After consultation with the Office of General Counsel, consider posting a copyright notice, legal disclaimer, and/or privacy statement on the web site for added protection. Broken or orphaned links should be removed or corrected.
- Applications and modifications should be thoroughly tested before being placed online. Use tools to check for common errors such as buffer overflows and code syntax. The access of the application from various browsers must be tested for compatibility. The system should be tested for reliable service under projected production loads and stress conditions.