

Introduction

1. The following guidance is intended for departmental and company security officers within the UNIRAS constituency for securing web sites against an untrusted user community. In the case where a web site is managed for the department or company by an Internet Service Provider (ISP), the departmental or company security officer should ensure as far as possible that the ISP has procedures in place to comply with the department's or company's web site security policy and to meet the following specific recommendations for securing the department's or company's web site. It is also strongly recommended that the application and maintenance of those procedures is checked on a regular and frequent basis by qualified security consultants such as those accredited under the CHECK service.

Background

It needs to be stressed that most successful attacks on web sites are made possible by misconfiguration of the web server and failure to install security patches. The guidance in the sections below aims to provide advice on correct configuration and patch application.

1. The Briefing assumes that the department or company has a web site security policy in place and procedures for enforcing that policy. The guidance in this Briefing is designed to inform such security policies and procedures from a technical perspective. Physical and personnel measures will also be required to ensure that the web server environment is secure, but these are beyond the scope of this Briefing.

2. Further advice on protecting UK Government connections to the Internet can be found in CESG Infosec Manuals M and P and in CESG Infosec Memorandum No. 13. Details of how to obtain these documents can be obtained from the CESG web site, www.cesg.gov.uk.

3. The security of a web site is determined by the security of the following:

- The security of the web server application
- Remote web server administration (not addressed here)
- The security of the operating system of the web server computer
- The security of the local area network of the web server computer
- The security of "backend" (eg database) applications supporting the web server
- The security of the authoritative domain name server for the web server network

4. In this Briefing each area of security will be considered in turn with recommendations for each. All of the recommendations should be followed if good web site security is to be achieved.

5. This Briefing presupposes that the web server is open to an untrusted user community and does not address the possibility of trusted users accessing or maintaining the web site remotely. Most web servers provide remote file and directory authentication for such purposes, although the types and use of such authentication are beyond the scope of this Briefing.

The security of the web server application

1. A web site is hosted by a web server. A web server is an application that accepts requests from client web browsers in the hypertext transfer protocols (http and https) and responds by sending web pages and other content to the client web browsers.

2. These web pages can be manually generated by a web page designer or they can be automatically generated. Automatically generated pages may use interpreted scripting languages such as perl or python to produce the web pages in the common gateway interface (cgi) format, or they may use proprietary server side programming extensions such as Microsoft's Active Server Pages (ASP). Web server security therefore splits into 2 further areas:

- The security of the web server application itself
- The security of any cgi scripts or server extensions

3. For the security of the web server itself, guidance is available in CESG Infosec Manual P. The following steps are recommended:

a. As with any application, ensure that you monitor UNIRAS Briefings and commercial sites such as bugtraq (www.securityfocus.com) on a regular and frequent basis and install any security patches relevant to the version of the web server that you are using. The web site vendor's web site should also be able to provide instructions on installing the patches and their coverage of vulnerabilities.

b. When configuring the web server, ensure that any access controls that can be set within the web server application are set appropriately on all directories under and including the root directory of the web as follows:

- i. Ensure that no web directories or files within the web directory structure are modifiable or writable by anyone other than the web server administrator.
- ii. Access to web pages should be read only for web users, although the web user will need permission to execute scripts or programs used to generate web pages dynamically.
- iii. Web users should not be able to list the contents of directories.
- iv. No access should be granted to other directories or programs in the web directory structure unless there is an explicit need.

v. **No access should be granted to the web server executable or to the web server configuration files.**

vi. No access should be granted above the root of web server directory structure.

- c. Do not assign access control override privileges to the web user as these can be abused by attackers to turn off access control.
 - d. Enable logging on the web server so that all web server activity is logged. This should be analysed on a regular and frequent basis by the department or company IT security officer for events indicative of an attack, for instance attempts to run non-existent scripts. The web server log should also contain all attempted and established connections, error messages, remote authentication attempts, all scripts run and any access control violations for files and directories under access control of the web server.
4. For the security of cgi scripts and server extensions, the following steps are recommended:
- a. Remove all sample scripts installed with the server.
 - b. Disable any server directives or extensions that enable scripts to run operating system level commands on the web server computer (eg for a UNIX environment, Server Side Includes).
 - c. Ensure that a competent person, preferably a qualified security professional (eg a CHECK consultant or a CLAS consultant), checks all scripts that are used on the web server to ensure that they validate input to allow only expected types and lengths of input data and produce error messages otherwise. Care should be taken that special characters and empty values are treated adequately. Escapes to an operating command shell should never be permitted.
 - d. If possible, store all scripts in the same directory and forbid execution of scripts outside this directory.

The security of the operating system of the web server computer

1. The security of the web server is only as good as the security of its environment. If the operating system is configured securely, the damage that a malicious web user could do will be restricted to what can be obtained with the web user privileges.

2. For the security of the operating system of the web server computer, guidance is available in CESG Infosec Manual P. The following steps are recommended:

- a. When selecting an operating system, a high level of security will be obtained by:
 - i. selecting an operating system has been evaluated against a security standard for discretionary access control, recognised by the UK Government which includes an independent check of the security enforcing source code (eg ITSEC E3 F-C2 or Common Criteria EAL4 with the Controlled Access Protection Profile); and
 - ii. configuring the operating system to run in its evaluated configuration.

Microsoft Windows NT 4.0 Service Pack 3 meets this standard using the NTFS file system, as do a number of UNIX operating systems. See the IT Security Evaluation and Certification Scheme web site, www.itsec.gov.uk, for details. The use of a certified operating system providing mandatory access control (ITSEC F-B1 or Common Criteria Labelled Access Protection Profile) that separates the user file and process space into levels or compartments will provide even greater security in the web server environment if the web server is run as an unprivileged user in its own compartment.

- b. As in the case of the web server, ensure that you monitor UNIRAS Briefings and commercial sites such as bugtraq (www.securityfocus.com) on a regular and frequent basis and install any security patches relevant to the version of the operating system that you are using. The operating system vendor's web site should also be able to provide instructions on installing the patches and their coverage of vulnerabilities.
- c. Ensure that the web server runs with the least privilege needed. The web server should not run as an administrator (including the web server administrator) or superuser (if applicable). In a UNIX environment if superuser privileges are needed to bind to the http port, the binding should be run as the superuser using a set user id process and all subsequent processes should be run as an unprivileged web user.
- d. Do not assign discretionary access control or mandatory access control override privileges to the web user as these can be abused by attackers who manage to gain web user privilege.
- e. To ensure that the web server is an unprivileged user, restrict access for the web server user to files and directories relevant to the web server application (which may be the directory structure under the web server root). Check the permissions on all other files and directories on the web server to ensure that the web server cannot gain access to any executables or data files that are not needed.
- f. If the web server directory structure is not virtual (ie the directories exist within the operating system environment), ensure that access controls are set appropriately on all files and directories relevant to the web server application:
 - i. Ensure that no web directories or files are modifiable or writable by anyone other than the web server administrator.
 - ii. Access to web pages should be read only for web users, although the web user will need permission to execute scripts or programs used to generate web pages dynamically.
 - iii. Web users should not be able to list the contents of directories.
 - iv. No access should be granted to other directories or programs relevant to the web server application unless there is an explicit need.
 - v. No access should be granted to the web server executable or to the web server configuration files.
- g. In a UNIX environment, it may be beneficial to security to run the web server with a redefined root directory using the *chroot* command. In this case do not have any symbolic links to files outside the directory structure that includes directories under the redefined root directory.

h. Enable logging on the operating system so that security relevant activity is logged. This should be analysed on a regular and frequent basis by the department or company IT security officer for events indicative of an attack, for instance attempts to access files without the correct permissions. All error messages, application startup and shutdown, attempted remote application logins, and changes in file permissions should also be logged.

i. The web server should be run as a dedicated web server. To decrease the risk of misconfiguration remove all unnecessary executables (including compilers and utility programs) and network services from the web server computer.

j. Remove all unnecessary users accounts from the server and implement passwords for the remaining accounts that are hard to guess and accord with the department or company security policy for password generation and use. If applicable, please refer to CESG Compusec Memorandum No. 8 on password management for CESG advice to UK Government.

The security of the local area network of the web server computer

1. The web server environment extends from the web server computer to its local area network and to the internet or intranet environment.

2. For the security of the local area network of the web server computer CESG Infosec Manuals M and P and CESG Infosec Memorandum No. 13 provide guidance on firewalls, internet connectivity and possible network architectures to UK Government. The following web server specific steps are recommended:

a. Install a firewall between the web server computer local area network and the internet to handle all traffic to and from the internet or intranet. For web traffic the firewall should deny all unnecessary incoming services and should offer http and possibly https (X.509 digital certificate compliant Secure Socket Layer over http) for commercial standard IP encryption of web traffic as uninitiated incoming connections. Http should be proxied to provide initial validation of the web page request. DNS should be allowed outbound on an unprivileged port to request DNS lookups and should listen on that port for responses. It is recommended that a certified firewall is used. For details of certified firewalls see the IT Security Evaluation and Certification Scheme web site, www.itsec.gov.uk.

b. Isolate the web server computer on its own network segment. This may be as a stand alone network or on a DeMilitarised Zone (DMZ) that has restricted access to the internal network and in particular to any database server that are used to store sensitive information. If a company does not have a DMZ, the use of a non-routable IP protocols (eg NetBEUI for Microsoft Windows computers) between the web server and the internal network could be considered. (Note that NetBIOS over TCP/IP should not be made available on Microsoft Windows computers.)

c. Enable logging on the firewall so that security relevant activity is logged. This should be analysed on a regular and frequent basis by the department or company IT security officer for events indicative of an attack, for instance attempts to access services with known vulnerabilities. As noted in CESG Infosec Manual P, successful/denied connections, error messages, multiple access attempts and access to insecure ports should be logged.

The security of "backend" applications supporting the web server

1. Any supporting "backend" applications (eg databases) should be stored on another computer. Care needs to be taken that the web user account can only perform a specified set of actions on the "backend" applications so that the security of those applications is not unduly compromised. For example, if a database application is used as a read-only source to web users, the web user account should have read only access, while if the database is updated by the web user account via web forms, the web user should be restricted to database update queries. This could be performed by a database application which provides access control by query type and data object (such as database and table) within the database application.

The security of the authoritative domain name server for the web server network

1. It is possible to change the IP address associated with a web site address (URL). When this is done maliciously it is known as DNS poisoning. DNS poisoning can be achieved in a number of ways (see also CESG Compusec Manual N):

a. by exploiting a buffer overflow in the DNS implementation and altering the DNS databases;

b. by spoofing the response to a query from a legitimate DNS server by guessing its response identifier;

c. by exploiting a vulnerability in versions of some older DNS implementations that allows a DNS server to upload DNS records relating to a domain for which it is not authoritative; or

d. by spoofing an authoritative DNS server.

2. To prevent this type of DNS poisoning, the web address registration authority should if possible upgrade the DNS version to the latest version and apply all relevant security patches. DNS server administrators should also if possible configure their servers to check DNS records obtained from an authoritative DNS server by comparing them with those taken from another authoritative server. Authoritative master primary DNS servers should be protected by a firewall. Zone transfers should be restricted from master primary DNS servers to designated slave DNS servers, which preferably should be within the perimeter protected by a firewall. It is recommended that the web server administrator confirm with the administrator of the authoritative DNS server that the protective measures identified above have been taken.

3. It is also possible for DNS poisoning to be performed manually. This type of DNS poisoning is discussed in detail in UNIRAS Briefing 045/00, but the basic security issues are as follows. The web address registration authority for the domain that includes your web server may receive bogus requests to alter the IP address associated with the web site URL, by email for example. The departmental or company security officer should satisfy himself or herself that the registration authority has adequate security measures in place to ensure the authenticity of any changes to the IP addresses in their domain. Examples of reasonably secure authentication schemes are digitally signed emails, challenge-response password authentication over the telephone and a recognised signature on official company notepaper.

