

GOOD PRACTICE GUIDE

WEBMAIL

JULY 2007

Abstract

This guide provides some guidance on the advantages and disadvantages of using webmail (namely web based email), either provided corporately or via a public provider, in the context of an organisation that is part of the Critical National Infrastructure. The recommendation of this guide is that webmail use should be restricted where practicable to a webmail service provided by the organisation and that appropriate security mitigation steps set out in the guide should be followed to minimise the vulnerabilities in webmail services.

Disclaimer

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favouring by CPNI. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.

To the fullest extent permitted by law, CPNI accepts no liability for any loss or damage (whether direct, indirect or consequential and including, but not limited to, loss of profits or anticipated profits, loss of data, business or goodwill) incurred by any person and howsoever caused arising from or connected with any error or omission in this document or from any person acting, omitting to act or refraining from acting upon, or otherwise using, the information contained in this document or its references. You should make your own judgement as regards use of this document and seek independent professional advice on your particular circumstances.

Copyright

The material featured in this document is subject to Crown Copyright protection unless otherwise indicated. The Crown Copyright protected material (other than CPNI logo) may be reproduced free of charge in any format or medium provided it is reproduced accurately and not used in a misleading context. Where any of the Crown Copyright items on this site are being republished or copied to others, the source of the material must be identified and the copyright status acknowledged.

CONTENTS

Overview□	2
What is webmail?	3
Basic architecture.....	4
Advantages and disadvantages of webmail for the user.....	4
Advantages and disadvantages of providing a webmail service in the organisation	5
Advantages and disadvantages of allowing access to a public webmail service in an organisation....	7
Generic webmail vulnerabilities	8
Mitigating the risks.....	10
Conclusions....□	11

GOOD PRACTICE GUIDE

WEBMAIL

OVERVIEW

This CPNI Good Practice Guide describes the principal characteristics of webmail, the threats and vulnerabilities of using such systems and provides guidance on managing the risks associated with webmail.

Email communication is critical to business, but it gives rise to increasingly more sophisticated and dangerous threats. Today's users consider email to be a fundamental part of their personal and business communications; they expect access to email at all times and from any location. Web-based email is one of the simplest and least expensive options for email access, and is gaining in popularity as a method of remote mail access, replacing the dial-up solutions of the past. However, webmail brings significant security concerns, and in consequence many organisations refuse to deploy it. This Good Practice Guide sets out some of the threats and vulnerabilities that businesses should recognise when using webmail systems. It also describes the counter-measures that can be used to mitigate most of the security issues. This may take the form of a broader solution to provide a complete email security package.

WHAT IS WEBMAIL?

The term webmail covers all Internet-based email services which can be accessed with only a web browser and an Internet connection. Web-based mail services allow users to access their mailboxes from any computer with an Internet connection, regardless of geographic location.

As an alternative to using a dedicated email client such as Microsoft Outlook, webmail allows users to receive, read, write, send and manage email using a web-based interface. As with all web-based content, a web browser is needed to use these services. The advantages of webmail services are that no software components apart from the browser need to be installed on the client computer, and users are not tied to a particular computer or location to access their email.

By entering the webmail website Uniform Resource Locator (URL) in their web browser's address field, users can then access their webmail account by entering a user name and password. The webmail server software forms a web interface to an email server, which may support common standards such as the Internet Message Access Protocol version 4 (IMAP4) or the Post Office Protocol version 3 (POP3) to access and manipulate emails as well as the Simple Mail Transfer Protocol (SMTP) to send emails.

There are two principal ways in which webmail services are made available. An organisation can either manage a webmail service itself or it can allow individuals to sign up directly for a webmail service offered by a public webmail service provider. Popular webmail service providers include Microsoft (MSN Hotmail), Google email (Google Mail) and Yahoo! Mail. The functionality, for example mailbox size, varies significantly between the different public providers, as does the level of security offered.

The structure and usability of the webmail interface will vary with the webmail product or service used, but many current products and services strive to emulate the functionality and appearance of a dedicated email client. Some features tend to be common to most webmail systems, including anti-

GOOD PRACTICE GUIDE

WEBMAIL

virus support, built-in spam filters and folders for filing email. A less common feature is the provision of a facility to allow webmail users to check their webmail account through any email client¹.

BASIC ARCHITECTURE

Most webmail systems are designed using a multi-tiered architecture. This will usually consist of at least four tiers:

- Client web browser
- Web server
- Webmail software
- Email server

The client web browser is the web interface through which access to the webmail account is obtained. The client web browser may need active scripting enabled (such as JavaScript, Java or Active X) in order to provide a richer user interface. By entering the relevant website URL the user can access their webmail account (subject to authentication). The webmail software then renders the user interface to the email account into web pages formatted in the HyperText Markup Language (HTML)², which then displays the email boxes and the email messages to the user.

The webmail software is also an interface to the underlying email server in terms of translating requests to create, delete and edit emails and email folders. Common webmail software includes Horde Internet Messaging Program, Microsoft Outlook Web Access and SquirrelMail.

These web pages associated with the email account are then sent to the user's web browser by a web server. A web server is an application that accepts requests from client web browsers using the HyperText Transfer Protocol (HTTP) and the HTTP over Secure Sockets Layer (HTTPS), and responds to those requests by serving web pages and handling any errors.

The email server can usually be any email server that supports the open IMAP4 or POP3 standards, but proprietary products and services often have their own webmail software.

Sometimes webmail has a fifth tier in its architecture, namely a database that is used to store configuration details for users and users' address books. While databases of this kind are not always required by the software, they often make the webmail software more efficient.

ADVANTAGES AND DISADVANTAGES OF WEB MAIL FOR THE USER

Users will find that there are a number of advantages of using webmail rather than a dedicated email client. These are limited to functional issues, as the security and legal issues, which are explored later in this Good Practice Guide, depend on whether an organisational or public webmail service is used.

¹ See http://en.wikipedia.org/wiki/Comparison_of_webmail_providers

² Increasingly the eXtensible Markup Language (XML) is being used in computer to computer web interaction, see NISCC Viewpoint 06/2006, <http://www.cpni.gov.uk/docs/VP0606.pdf>

GOOD PRACTICE GUIDE

WEBMAIL

The advantages for the user are:

- a) Email is stored remotely on a server, which means that it is accessible anywhere where there is an Internet connection and a web browser.
- b) Webmail accounts can be set up with the minimum technical competence, and are easy to use. (For organisations, however, technical competence is required to configure the system where the webmail application is a gateway into a corporate system.)
- c) The webmail provider undertakes all administration to maintain the service centrally, including upgrades and security fixes.
- d) The user does not need to install new software (although support for active scripting may be needed).

The disadvantages for the user are:

- a) The webmail interface may not be as easy to use as a dedicated email client and may appear unsophisticated.
- b) The user has to read emails while connected to the Internet; in general they cannot be downloaded and read off-line.
- c) Most emails are usually short, plain text messages of less than 2Kb. With webmail the original email is wrapped in HTML, which can be 40Kb or more. This can bring a significant decrease in speed of use, especially on slow network connections.
- d) Email storage space may be limited (meaning that the user may have to delete email messages). The user is generally unable to keep messages on their local hard drive, though there may be an option to download and save emails. (For organisations, storing data remotely brings confidentiality, availability and data integrity issues, although there are advantages in that it frees server space for the organisation and there is less risk of storing corrupted or virus-infected files centrally.)

ADVANTAGES AND DISADVANTAGES OF PROVIDING A WEBMAIL SERVICE IN THE ORGANISATION

Although there are clear benefits from allowing users to access their email through webmail, there are a number of disadvantages as well. The benefits to the business are:

- a) Having staff able to access their email from a variety of locations may encourage efficient and flexible working and may increase productivity.
- b) Webmail can be secured in transit using standard commercial encryption (namely HTTPS).
- c) There are minimal dependencies on hardware or software. Email can be accessed from a variety of platforms across the organisation. Any device that has a web browser can be used.

GOOD PRACTICE GUIDE

WEBMAIL

- d) Webmail can bring resilience in the event of an incident if the office webmail is available to staff outside of the office environment.

The disadvantages of offering a webmail service are:

- a) Webmail can in some circumstances be used to bypass the security of the client computer as dedicated email clients usually have their own anti-spam functions and are linked to the anti-virus scanner. Care needs to be taken that security checks are performed on the email server.
- b) Webmail uses web browser functionality, such as HyperText Markup Language (HTML), to create and read mail messages. HTML presents security problems because messages formatted in HTML can hold active content, such as JavaScript and links to other objects on the Internet. Malicious JavaScript could, for example, prompt the user to re-enter their password, which is then sent to the attacker, or it could be used to direct the user's web browser to a web page which contains an exploit. As JavaScript can be embedded in messages in various ways, filtering of these active contents is often difficult. The use of plain text email is recommended, but often HTML cannot be de-activated and the user may be required to read all webmail messages in HTML.
- c) A significant drawback if the webmail service is outsourced is that webmail security is under the control of the webmail provider. Unless it is stipulated contractually, the organisation may not know where in the world the server is located or what level of security is used by the service provider to ensure that the server and its contents remain secure. Without adequate security practices, anyone could gain access to the server and therefore access to the user email content, or be able to gain control of, or infect with malicious code, the server through which the webmail service is accessed. The security of the server is critical to the safe operation of webmail service, and the organisation, without putting in place some risk mitigation steps, could be exposed to numerous threats, including Trojans, viruses, identity fraud etc.
- d) The organisation's data could be stored on computers it does not own (remote users' computers for example) unless a policy is enforced that it can only be accessed from computers owned by the organisation.
- e) Web browser vulnerabilities have been used as a common attack vector in the past. Many electronic attacks do not only use technical means but trick users to click on links in emails (including URLs).
- f) Providing webmail to users increases the external attack surface of the organisation. Web applications tend to have a high vulnerability rate. By taking advantage of weaknesses in application code, attackers can crash or compromise email defences and servers. This allows the attackers to gain access to the network infrastructure where they can access messages or accounts, and exploit workstations and servers to launch attacks on other areas of the organisation. A compromised webmail system may allow attackers to gain access to sensitive emails, steal corporate digital certificates, encryption keys and other confidential information. Legitimate users may even be impersonated by hackers who send email messages from the users' accounts.

GOOD PRACTICE GUIDE

WEBMAIL

The disadvantages identified above can be countered to a large extent by complete security policies, stating, for example, that the organisation's data can only be accessed from computers owned by the organisation. These policies will need to be supported by technical security measures such as the use of virtual private networks to the office for all communications (from remote users or from remote sites) - which could of course be via the use of HTTPS to a web server owned by the organisation (although IPSEC is the norm because it encrypts more parts of the network packets, and so less is visible to potential attackers)³.

Access to the webmail service should not require the user's computer to accept active content, such as Java, JavaScript and ActiveX. Users can defend against HTML malicious code by using webmail clients which do not automatically download and display HTML, images or attachments, and by configuring their clients not to display these by default and by requiring emails to be displayed in plain text format.

The use of strong authentication methods, such as mutual (i.e. client and server) certificate-based authentication in HTTPS or challenge-response mechanisms (which is available as an HTTP authentication method)⁴, are also recommended. Since webmail is a type of web application, the guidance on authentication and encryption in NISCC Briefing 10/06 'Secure web applications'⁵ should also be consulted.

ADVANTAGES AND DISADVANTAGES OF ALLOWING ACCESS TO A PUBLIC WEBMAIL SERVICE IN AN ORGANISATION

Whereas the provision of organisational webmail may be justified in business terms, allowing users to access public webmail services has far less to be said in its favour. The only apparent benefit is:

- a) If the access is for personal use only, webmail may help maintain work/life balance and keep staff happy.

The disadvantages are as follows:

- a) Even if access is for personal use only, the employer could still be legally liable for abusive or illegal emails (and attachments) sent by their staff at the workplace.
- b) If webmail is used for business purposes, it may breach the acceptable use policy with the web service provider.
- c) Staff could bypass internal security policies on emailing business documents using the organisation's email infrastructure.
- d) Confidential organisational data could be stored on mail servers belonging to third party organisations.
- e) Webmail services have not been independently evaluated. (This could be overcome by putting such services through an independent evaluation to assess information assurance)

⁴ See NISCC Viewpoint 03/06: Virtual Private Networks, <http://www.cpni.gov.uk/docs/VP0306.pdf>

⁵ See RFC 2671, www.ietf.org/rfc/rfc2617.txt

⁶ <http://www.cpni.gov.uk/docs/secureWebApps.pdf>

GOOD PRACTICE GUIDE

WEBMAIL

standards, such as the CSIA Claims Tested (CCT) Mark Scheme, which is a UK government quality market for IT security products and services.)

In light of these disadvantages, any organisation wishing to allow its staff access to webmail services should consider the risks very carefully. CPNI's recommendation is not to allow access to public webmail services from the workplace or any logical extension of it.

GENERIC WEBMAIL VULNERABILITIES

Webmail is a specific example of a web application. The vulnerabilities in webmail are typical of those for any web application, while recognising the possible five tiers of webmail, namely:

- Web browser vulnerabilities (for example, active scripting objects with buffer overflows, cookie identity disclosures)
 - o Active scripting objects (such as Active X controls) are executable programs that are run on the user's computer to provide an enhanced web browsing experience. Downloading untrusted active scripting objects or using built in programs that have vulnerabilities (such as buffer overflows, see below) can lead to compromise of the user's computer.
 - o Session cookies are files containing information about the user's web session. The webmail server records this information in a text file and stores that file on the user's hard drive. The session cookie may contain authentication information along with the usual data about the last URL viewed by the user. Problems can arise when the user logs off. If the user does not close his or her browser or the webmail system does not erase the session cookie stored, an attacker can log in to the webmail system by guessing the session identifier contained in the cookie or locally by using the cached cookie. (It is also possible to set cookies on a user's computer by using cross-site scripting if the user visits a vulnerable web site. See below for an introduction to cross-site scripting.)
- Web server vulnerabilities (for example, buffer overflows, directory traversal, cross site scripting)
 - o Buffer overflow attacks involve sending overly-long commands that overwrite server memory, either crashing the system or executing the attacker's arbitrary code in the context of the web server process. The result is server compromise or denial of service.
 - o Directory traversal allows attackers to access restricted directories, execute commands and view data outside the normal web server directory. Attackers use directory traversal to try to access restricted web server files outside of the web server's root directory. As a result, attackers might view restricted files or execute commands on the web server, leading to a compromise of the web server.

GOOD PRACTICE GUIDE

WEBMAIL

- o Several webmail servers have had cross-site scripting vulnerability flaws exploited. These open the door to phishing scams, account hijacks and other attacks. Cross-site scripting attacks allow script injection into vulnerable but trusted web pages by malicious web users, with the malicious content being embedded in a URL. If the user then follows that URL, the malicious data is sent to the web application, which in turn creates an output page to the user's browser, rendering (i.e. executing) the malicious content. The user is, however, normally unaware of the attack, and assumes the data originates from the trusted web server itself, leading the user to believe this is valid content from the website.
- Webmail software vulnerabilities (for example, not checking that an HTTP request does not cause an error in the email server)
- Email server vulnerabilities (for example, being able to access email folders belonging to other users)
- Database server vulnerabilities (for example, Structure Query Language (SQL) and script injection vulnerabilities)
 - o SQL injection is the injection of database commands into a web request with the aim of executing the commands on the database server that underlies the web application.

Further details of these types of vulnerability can be found in other NISCC papers, including:

- NISCC Briefing 10/06: Secure Web Applications⁶
- NISCC Briefing 05/06: The Phishing Guide⁷
- NISCC Briefing 13/06: The Pharming Guide⁸
- NISCC Good Practice Guide 09/04: Guidance on mitigating the Security Risks of SQL Injection Attack⁹
- NISCC Good Practice Guide 02/04: Spam Mitigation Techniques¹⁰
- NISCC Good Practice Guide 05/03: Configuration and Use of Web Browsers¹¹
- NISCC Good Practice Guide 01/03: Understanding Database Security¹²
- NISCC Good Practice Guide 03/02: Guidance on securing Web Sites¹³

⁶ <http://www.cpni.gov.uk/docs/secureWebApps.pdf>

⁷ http://www.cpni.gov.uk/docs/phishing_guide.pdf

⁸ http://www.cpni.gov.uk/docs/pharming_guide.pdf

⁹ <http://www.cpni.gov.uk/docs/re-20041101-00962.pdf>

¹⁰ <http://www.cpni.gov.uk/docs/re-20040227-00102.pdf>

¹¹ <http://www.cpni.gov.uk/docs/re-20030801-00725.pdf>

¹² <http://www.cpni.gov.uk/docs/re-20030110-00721.pdf>

¹³ <http://www.cpni.gov.uk/docs/re-20020530-00478.pdf>

MITIGATING THE RISKS

The papers mentioned above describe common vulnerabilities in the technologies relevant to webmail, and provide mitigation advice on those vulnerabilities. However, here are the key points:

- Use a specific web browser build, standard across the organisation, to limit the exposure to publicly known vulnerabilities
- Do not browse with administrator privilege
- Keep all of your software up to date (including web browsers and server software)
- Use anti-virus and anti-spam tools on your email server and on the client computers
- Disable active scripting for untrusted sites if you can
- Use a web proxy server (load balanced if necessary) for all outbound web traffic and analyse traffic (see below on content checking)
- Use a specific web application firewall to check contents and to identify potential attacks and potential misuse
- If you operate your own webmail infrastructure, consider deploying a protective layer around the infrastructure with a reverse web proxy used as a hardened server. A reverse proxy will also help reduce the load on the webmail server as pages can be cached on the proxy server. Be sure to analyse traffic
- Block traffic you do not expect with a boundary firewall
- Use IPSEC or HTTPS to encrypt the webmail session, and use strong methods of authentication. Strong methods of authentication, such as one-time passwords and two factor authentication mechanisms, should be implemented as part of a corporate webmail deployment
- Consider terminating your virtual private network at your external firewall so that the content can be checked.
- Use a network-based intrusion detection system on the Internet content network segment to support the web firewall and content checker. The intrusion detection system can be used to detect known exploits unique to webmail, including buffer overflows, directory traversal, path obfuscation and malformed HTTP requests.

As far as denying access to public webmail providers is concerned from within the organisational boundary, there are a number of web proxy servers which will block access to web sites based on their URL or their network (i.e. IP) address. It would also be possible to block the IP addresses on the Internet facing firewall; and some firewalls have their own web proxies built in, enabling URL based web site blocking from the firewall.

GOOD PRACTICE GUIDE

WEBMAIL

The use of an HTTPS virtual private network has a great deal to commend it. For added security, it is often combined with HTTP basic authentication (i.e. username and password). Form based and challenge/response (digest access) authentication are also supported by HTTP, but since they are not commonly implemented with HTTPS, if their use were preferred, they should be implemented across an IPSEC virtual private network.

It is also important that any users of webmail are educated to exit the webmail service with the log off button or similar so that others cannot access the account from the client computer.

CONCLUSIONS

The recommendation of this Good Practice Guide is that webmail use should be restricted where practicable to a webmail service provided by the organisation. The disadvantages of allowing users to access public webmail services significantly outweigh the benefits.