Australian Communications-Electronic Security Instruction 33 (ACSI 33)

Point of Contact: Customer Services Team

Phone: 02 6265 0197 Email: assist@dsd.gov.au

HANDBOOK 11

EMAIL SECURITY

Version 1.0

Objectives

1101. This handbook focuses on the functionality and requirements for email security controls. Email security mechanisms on information systems may have some or all of the objectives as follows:

a. To protect the confidentiality of identified information by preventing leakage of information to those without need-to-know .

b. To ensure an appropriate level of sender authentication and non-repudiation.

c. To ensure an appropriate level of email integrity.

d. To protect the availability of the system by controlling access to critical system functions and preventing malicious code based denial of service attacks.

Email Terminology

1102. Electronic mail (Email) has become an essential communication tool for government and business organisations worldwide.

1103. Some of the common terms that are used in this handbook are as follows:

a. **HTML** is the Hypertext Markup Language. HTML is an evolving

standard for creating web pages, and is also used for the transfer of some electronic mail messages.

b. **XML** is the 'Extended Markup Language', and an emerging standard for creating rich content, flexible electronic documents and application interfaces. XHTML is the bridge standard between HTML and XML.

c. A **mail server** is a software tool that receives email messages from either an email client, or another email server, and either routes the message to another server that is closer to the final recipient, or stores the message locally for collection by the final recipient.

d. A **mail client** is a software tool run by an end-user that is able to view email messages and associated attachments. Messages may be presented in raw text, or in some cases HTML or XML.

Mail Client Security

1104. Some mail clients allow users to receive messages formatted in HTML, and will even run Java applets, VBScript, or Active-X controls. As such, your mail client may have similar client-side security risks as identified in **Handbook 10 - Web Security** for web browsers. Software or data files with embedded code (eg macros) that are received as attachments in mail messages and are saved and executed or opened locally may contain malicious code that impacts negatively on the client system. Any executable code downloaded via email, the world wide web, news groups, gopher, or ftp, may contain malicious instructions designed to:

a. Introduce a virus into the organisation.

b. Conduct denial of service attacks.

c. Gain access to otherwise restricted information

1105. Without appropriate controls on the receipt and execution of machine executable code, an organisation may be accepting significant risks to the stability and integrity of their internal network. Controls such as virus checking software may be appropriate for some organisations. More thorough controls may be to remove or quarantine executable content or attachments from email messages using a proxy or firewall solution. For further information on control of malicious software refer to **Handbook 12 - Malicious Software**.

Mail Server Security

1106. Installation of mail server technology creates an access point into an agency's network that can potentially be misused by attackers. A poorly configured or maintained mail server is likely to introduce problems that allow unauthorised remote users to perform actions outside the scope of legitimate activity, impacting on the confidentiality, integrity or availability of the network, hosts and/or users. Examples of such actions include:

a. Flooding a server with large quantities of useless mail so that users find it difficult to access legitimate messages.

b. Retrieve information about the server computer that may allow a potential attacker to target the computer more effectively.

c. Exploit a bug in the mail server, which allows an attacker to execute commands that detrimentally change the system.

d. Exploit a bug in the mail server or other open resource to gain access to email messages before encryption is applied, or after decryption.

e. Use the mail server to distribute virii into the organisation.

f. Use the mail server as a spam relay to forward junk email to other organisations

1107. A mail server is a conceptually simple piece of software, which accepts items of mail for delivery to a named recipient. An extremely simple email server can be implemented with a very small number of lines of code. More complex mail servers run into hundreds of thousands of lines of code.

1108. Complex server components are likely to contain errors, and some of these errors may potentially impact on the security of the server in question. Ensuring that the mail server has the latest recommended security patches will minimise the chances of a successful, well known attack. However, the primary factor in mail server security is the application of sound configuration control and management techniques.

1109. Some simple operating system configuration mechanisms can be used to reduce the effectiveness of potential attacks against your server. Many of the controls are operating system specific, but can be broadly grouped into the following categories:

a. **Privilege reduction**. Running the mail server as a non-privileged user, which has limited access to system resources.

b. **File system limitation**. Ensuring that the user that runs the mail server has limited access to the host file system. On Unix machines, this may imply that the server runs in a 'chroot' environment - with access only to the mail spool directory and appropriate configuration files at runtime. For Windows NT servers, this may imply restricting the user's group memberships to a very limited subset, and setting access controls to severely limit file system access for those groups.

c. **Limited interactive system access**. Removal of non-administrative users from the computer that runs the mail server further decreases the risk of any mail server level access controls being circumvented, and may reduce the requirement for strong global file system access controls or comprehensive auditing.

d. **Email filtering**. Using an automated or manual process to filter virii,

executables or other content from incoming or outgoing email messages. This may require the position of an external mail relay with this capability on the email path to/from the server.

e. **Regular system maintenance**. Many of the vulnerabilities associated with email programs have been related to the release/patch level of the mail server program and have been identified and fixed by subsequent releases.

1110. Standard Simple Mail Transfer Protocol (SMTP) mail servers do not require any form of authentication when sending mail. As such, unless digital signatures, encryption or similar technologies are implemented on top of SMTP, forging electronic mail is a very simple process. Unless the content is significantly out of character, a forged email that appears to originate from a trusted associate is almost indistinguishable from a legitimate message.

1111. Volumes of unsolicited email may intentionally or unintentionally comprise a denial of service attack against your mail server. Users may not be able to simply distinguish legitimate email messages from the mass of 'junk mail', and as such, productivity losses, or failure of critical hardware or software due to mail volume, may be experienced. Some unsolicited incoming electronic mail messages may actually contain information that is in violation of the organisational security policy, or perhaps compromise the organisation's legal obligations, such as pornography, inappropriate material, or virii.

1112. Password authentication for mail servers is susceptible to the same problems that plague normal operating system passwords, such as:

a. Network interception and replay.

b. Exhaustive password attempts.

c. Dictionary attack if the attacker has access to the mail server configuration files.

1113. Additional security assets such as firewalls or screening routers, and content filtering systems may limit exposure to such attacks.

Mail Server Auditing

1114. Audit logs produced by the mail server can be advantageous both from a security point of view, and for usage statistics. Enabling audit in a mail server is similar to enabling operating system audit (see **"Audit and Log Analysis" of Handbook 13 - Intrusion Detection and Audit Analysis**) - it is not worth configuring unless a tangible plan for the data is produced. Managing audit logs is a non-trivial task that usually requires ongoing maintenance and monitoring:

a. File systems need to be watched to ensure that disk space does not fill, and therefore contribute to a denial of service situation.

b. Audit information needs to be protected by access controls so that it cannot be easily read or overwritten. Streaming audit logs to a separate

system or write protect media is a mechanism that could be employed.

c. Audit information needs to be archived to offline storage, or removed from the file system when no longer required.

d. Audit analysis software needs to be acquired, installed, and run according to an agreed schedule.

e. The results of audit analysis need to be distributed to those who have a need to know, with the capability to recognise anomalous events. Anomalous events need to be followed up.

1115. The auditing of a mail server can result in significant benefits to the organisation, which may include:

a. Logs that can identify the source of some hacking attempts or denial of service attacks.

b. Logs that can pinpoint problems with your mail server configuration.

c. Usage statistics that can identify when an upgrade of network bandwidth is likely to be required.

1116. A site that wishes to guard against denial of service attacks that attempt large volumes of connections to the mail server with the goal of filling the file system of the local machine may wish to consider locating the audit logging facility on a physical or logical disk device that is separate from the disk on which the primary operating system is located. If this is not possible, a form of automatic log rotation may be appropriate.

Data Integrity

1117. Normal Internet SMTP mail does not offer integrity, authentication or non-repudiation services. Some mail clients will respond to a 'return receipt' request, but this feature is optional for mail clients and implementation is not guaranteed. Most clients that allow return receipts will also ask the recipient for confirmation before sending a delivery receipt.

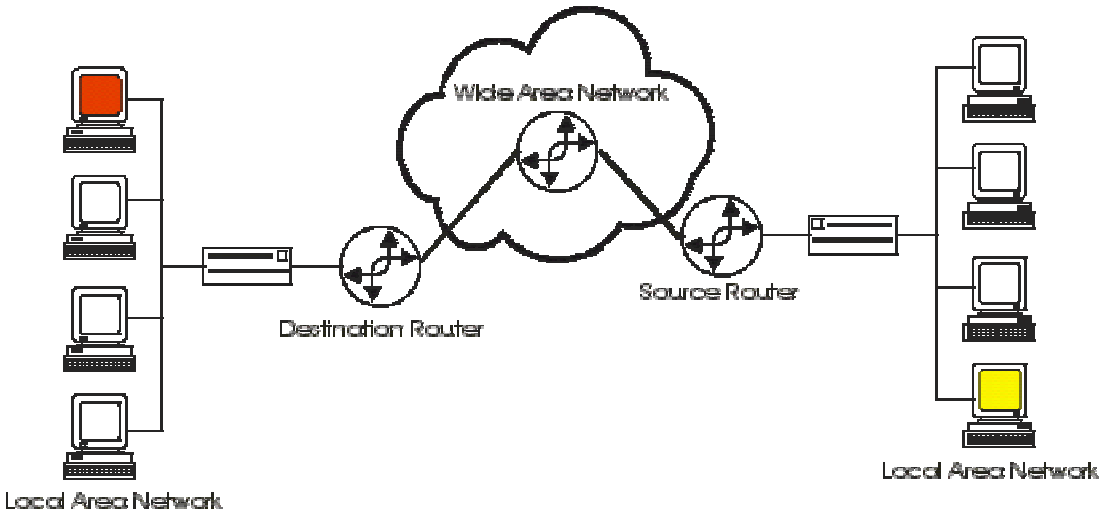
1118. The integrity of a mail message and its delivery can be enhanced by using digital signatures, encryption, hash exchanges, or a combination of these techniques. Encryption and digital signatures are discussed below. A hash exchange is a system whereby an original email mathematical signature is delivered to the recipient via another mail message or an alternative delivery mechanism. The mathematical signature of the received message is generated, and compared with that of the original message. If a match is obtained, the recipient can have more confidence that the message has not been modified in transit.

1119. Sender integrity issues are also of concern. Standard SMTP mail servers do not require any form of authentication when sending mail. As such, users who

either have access to the sender's mail client, or have knowledge of the SMTP protocol, can easily impersonate a legitimate user.

Data Confidentiality

1120. Unless appropriate encryption technology is in use, information that is sent over a network can be intercepted and analysed at any point between the client computer and the remote recipient. Modern networks are structured in such a way that information usually passes through several network 'hops' to get from source to destination. In the following diagram, if a user on a machine on the right wishes to send an email to a user on a machine on the left, there are several places where the communication can be intercepted.



1121. The communication between source and destination can be potentially intercepted by:

a. Any user who has physical access to the source or destination laptop or desktop computer. A user who has physical access to the source computer can consult the 'Sent' or 'Inbox' files maintained by most mail clients to examine incoming or outgoing mail.

b. Any user who has logical read-access to the mail spool owned by the sender or recipient. Some mail servers function as a mail holding area for a number of users. File system access controls should be configured to limit users to only those mail boxes for which they are authorised.

c. Any user on the source or destination local area network. A local area network usually operates in 'broadcast' mode. Each station 'shouts' over the network so that the destination host, or any network devices that create a path to the network host, can 'hear' it.

d. The administrator of the source or destination router
The source router is responsible for creating a network path between the source machine and the destination machine, and as such carries the communication.

e. The administrators of any intermediate network devices such as routers or firewalls.
On an intranet, some level of trust can be safely assigned to the network devices on your network, and those staff that are performing administration tasks. The Internet however, is a dynamic system that will re-route communications in response to degraded traffic flow or service interruption. The source machine has very little control over which path communications will flow, and as such, cannot guarantee the integrity of administrators at each network device along the path from source to destination.

1122. Encryption technology is one of the more effective mechanisms to provide data confidentiality between source and destination in an Internet or public wide area network environment. Encryption is discussed later in this handbook and in **Handbook 9 - Cryptographic Systems**. Whether or not encryption technology is employed between sender and receiver, messages are usually stored unencrypted in the Inbox of the recipient's computer, and in the Sent folder of the sender's computer. Physical security incidents such as theft of a laptop, or leaving a PC unattended in an insecure location, can therefore impact upon data confidentiality. The attacker may not be able to intercept the messages in transit, or may not be able to decrypt the messages, but accessing the mail at either the source or destination may be a viable alternative.

1123. An additional risk to data confidentiality known as 'cascading carbon copy' exists for electronic mail messages. An original message distributed to one or more recipients often includes a wider recipient distribution in any replies due to the practice of 'info-ing' concerned parties. If the originator is not vigilant and aware of the full distribution, replying to the response may include a wider than intended distribution.

1124. Pro-active scanning of an organisation's outgoing mail content may be required in situations where information leakage is a significant concern. Trade secrets, intelligence material, budget data, or similar information that has a high damage potential if released outside the organisation may require a lexical scan of outgoing electronic mail messages. This strategy also requires rigorous configuration of internal mail systems to ensure that message labelling is reliably implemented.

Encrypted Transactions and Public Key Infrastructure

1125. To overcome the problems associated with lack of authentication of email, a digital signature can be attached to prove the identity of the source. Public Key certificates can also service other requirements including confidentiality and integrity. Keys and client certificates may be stored in a number of different configurations:

a. Within a user's home directory, relying on operating system access controls to determine access to the digital certificate, and providing a single-sign-on facility to a site's user base for access to the normal

operating system desktop and email signature and encryption.

b. Within a user's home directory, but protected using password-based authentication over and above the normal operating system access controls.

c. Within a directory server, and optionally protected using additional password authentication.

d. On magnetic media for ease of transport, and optionally protected by additional password-based authentication.

e. On a smart card, and optionally protected by additional password or biometric authentication.

1126. Physical security issues aside, the items above are ranked approximately in order of security. More intrusion detection and access control management is required for each level in order to attain a similar level of assurance. For example, significant auditing and access control would be required to bring home-directory based certificate storage to the same assurance level as a smart card protected by biometrics.

Government Public Key Authority

1127. In late 1997, the Government decided to take the lead in the development of a national framework for the authentication of users of electronic online services. The National Office for the Information Economy (NOIE) was charged with ensuring that a strategy be in place so that the Government can make optimal use of Public Key Technologies (PKT) for electronic transactions. The Government Public Key Authority (GPKA) has been established to manage the evaluation and accreditation for organisations and individuals who wish to participate in the delivery of public key technologies and associated evaluation services for government use.

1128. The GPKA will recognise two levels of Certification Authority accreditation: Entry Level Accreditation and Full Accreditation. Entry level accreditation requires (in part) policies and practices on how services will be implemented, and a commitment to have the public key products certified to EAL4 (see **Handbook2 - Evaluated Products**). Full accreditation involves satisfactory completion of the Entry Level requirements, and completion of the product evaluation. Details on the certification standards and related issues can be found at the Gatekeeper web site, at **www.gpka.gov.au**.

Grades of Email Server and Client Security

1129. The following email security grades have been included to assist in determining the level of effort that should be allocated to the task of securing mail clients and servers. They are not definitive, and when implementing security should therefore be used as a guide only. Implementation of email security will vary from organisation to organisation, depending on the outcomes of a risk assessment.

a. **Grade 0**

Mail Servers

i. Regular application audit to ensure mail client and server software is upgraded with the latest security patches.

ii. Mail servers are set to run as a user with minimal file system or operating system privileges.

iii. Operating system access controls should be configured to allow users to access only those mail archives for which they are authorised.

Users and Mail Clients

i. Users to be informed of the risks associated with email security, particularly with reference to attachments and integrated web browser capabilities.

b. **Grade 1**

Mail Servers

i. Regular application audit to ensure mail client and server software is upgraded with the latest security patches.

ii. Mail servers are set to run as a user with minimal file system or operating system privileges.

iii. Operating system access controls should be configured to allow users to access only those mail archives for which they are authorised.

iv. Audit is configured on all mail servers, and rotated nightly to assist with problem diagnosis and repair.

Users and Mail Clients

i. Users to be informed of the risks associated with email security, particularly with reference to attachments and integrated web browser capabilities.

c. **Grade 2**

Mail Servers

i. Regular application audit to ensure mail client and server software is upgraded with the latest security patches.

ii. Mail servers are set to run as a user with minimal file system or operating system privileges.

iii. Operating system access controls should be configured to allow users to access only those mail archives for which they are authorised.

iv. Audit is configured on all mail servers, and analysed for general intrusion attempts, or attempts to circumvent mail server controls. Audit logs are either rotated, or migrated to offline storage depending on results of risk assessment.

v. Mail proxy configured to virus check all incoming messages.

vi. Digital Signature and Encryption technology is available to users who wish to send mail messages with enhanced security - Public Key encryption based on x.509 certificates is used between sender and recipient to enhance data confidentiality. Cryptographic services evaluated as per **Handbook 9 - Cryptographic Systems** and **Handbook 2 - Evaluated Products**.

Users and Mail Clients

i. Users to be informed of the risks associated with email security, particularly with reference to attachments and integrated web browser capabilities.

ii. Users' mail clients are configured to reject all Java and Active-X in attachments.

d. **Grade 3**

Mail Servers

i. Regular application audit to ensure mail client and server software is upgraded with the latest security patches.

ii. Mail servers are set to run as a user with minimal file system or operating system privileges.

iii. Operating system access controls should be configured to allow users to access only those mail archives for which they are authorised.

iv. Audit is configured on all mail servers, and analysed for general intrusion attempts, or attempts to circumvent mail server controls. Audit logs are either rotated, or migrated to offline storage depending on results of risk assessment.

v. Mail proxy configured to virus check all incoming messages.

vi. Digital Signature and Encryption technology is available to users who wish to send mail messages with enhanced security - Public Key encryption based on x.509 certificates is used between sender and recipient to enhance data confidentiality. Cryptographic services evaluated as per **Handbook 9 - Cryptographic Systems** and **Handbook 2 - Evaluated Products**.

vii. Operating system accounts on the mail server are restricted to administrative users only.

Users and Mail Clients

i. Users to be informed of the risks associated with email security, particularly with reference to attachments and integrated web browser capabilities.

ii. Users' mail clients are configured to reject all Java and Active-X in attachments.

iii. Users' mail clients configured to reject all JavaScript and Cookies if determined appropriate by risk assessment.

iv. Application extensions to mail clients are evaluated by qualified system security staff if determined appropriate by risk assessment.

v. Laptop or other portable computing devices are purged of sensitive messages before leaving a secure area.

e. **Grade 4**

Mail Servers

i. Regular application audit to ensure mail client and server software is upgraded with the latest security patches.

ii. Mail servers are set to run as a user with minimal file system or operating system privileges.

iii. Operating system access controls should be configured to allow users to access only those mail archives for which they are authorised.

iv. Audit is configured on all mail servers, and analysed for general intrusion attempts, or attempts to circumvent mail server controls. Audit logs are either rotated, or migrated to offline storage depending on results of risk assessment.

v. Mail proxy configured to virus check all incoming messages.

vi. Mail proxy configured to scan outgoing message for sensitive information leakage.

vii. Digital Signature and Encryption technology is available to users who wish to send mail messages with enhanced security - Public Key encryption based on x.509 certificates is used between sender and recipient to enhance data confidentiality. Cryptographic services evaluated as per **Handbook 9 - Cryptographic Systems** and **Handbook 2 - Evaluated Products** .

viii. Operating system accounts on the mail server are restricted to administrative users only.

ix. Mail servers forced by the operating system to use a virtual root - a subset of the computer's file system from which the mail server cannot escape.

x. Mail proxy configured to strip all attachments from incoming mail messages.

Users and Mail Clients

i. Users to be informed of the risks associated with email security, particularly with reference to attachments and integrated web browser capabilities.

ii. Users' mail clients are configured to reject all Java and Active-X in attachments.

iii. Users' mail clients configured to reject all JavaScript and Cookies if determined appropriate by risk assessment.

iv. Application extensions to mail clients are evaluated by qualified system security staff if determined appropriate by risk assessment.

v. Laptop or other portable computing devices are purged of sensitive messages before leaving a secure area.