MailGuard Bastion

Security Target (E3)

Table of Contents

Related Documents

[1] Information Technology Security Evaluation Criteria
Commission of the European Communities
Version 1.2, June 1991

[2] Trusted Solaris 2.5.1
SECURITY TARGET
Sun Microsystems Ltd
EC.22740.ST/Issue 6.0

1. Introduction

1.1 Purpose

This document is the security target for the ITSEC evaluation of the MailGuard Bastion. The role of the security target within the development and evaluation process is described in ITSEC (Ref [1]).

1.2 Scope

The content of this document is as defined by ITSEC (Ref [1]) sections 2.4 and E3.2, for a product with a target evaluation level of E3 [ITSEC].

Section 2 is the Product Rationale and identifies the security objectives, the intended method of use, method of use assumptions, environmental assumptions, a list of assumed threats and a summary of security features. Section 3 contains the specification of the required security enforcing functions. Section 4 contains the definition of the required security mechanisms.

1.3 Terminology

This section contains definitions of the technical terms that will be used within this document.

The definition of the following terms can be found in Ref [2] and are not repeated here: *Trusted Process, Mandatory Access Control (MAC), Sensitivity Label, Information Label, Privilege, Authorisation, Role.*

TSOL(E3): Trusted Solaris 2.5.1 - E3 Certified (Sept 98). Trusted Solaris 2.5.1 consists of SUN Solaris 2.5.1 and SUN Trusted Solaris 2.5

Compartmented Mode Workstation (CMW): A trusted workstation that contains enough built-in security to be able to function as a trusted computer. A CMW is trusted to keep data of different security levels and categories in separate compartments.

Label: In a system supporting Mandatory Access Control, a label containing compartment and classification information is assigned to every object or subject in the system.

Compartment: A distinct area of information in a system, implemented by use of labels. The compartment is one component of a sensitivity or information label.

Disjoint Compartments: Two compartments that are incomparable in terms of their labels (neither compartment dominates the other). Access to one compartment does not imply any access to the other.

Firewall: Firewalls are security components used in conjunction with other security hardware and software to provide actively managed channels between networks with differing security policies. Communications are allowed only through specific pre-configured channels. This communication is generally audited and tightly controlled.

Bastion Host: A generic firewall architecture where a single system runs a proxy service which acts as an intermediary in a conversation between two parties on opposing sides of the firewall.

Proxy Service: A proxy service is a service run on a firewall that acts on behalf of a user who is behind the firewall but wishing to communicate past the firewall.

Message Transfer Agent (MTA): A process which collects and delivers messages for mail users, mail-enabled applications and gateways. Usually used in reference to X.400 (P1) messages, for which the term was originally defined

Sendmail: A commonly used SMTP-based MTA.

Simple Mail Transfer Protocol (SMTP): An Internet standard for delivering text based messages across the Internet.

X.400: The messaging protocol defined by ISO (International Standards Organisation) as part of the OSI model (Open Systems Interconnection).

MGB compartment: A CMW disjoint compartment used by the MGB.

Networking compartment: an MGB compartment with a network connection designated for running MTA software.

DMZ compartment: an MGB compartment with no network connection designated for running vetting programs to apply additional checks on all messages passing through the MGB.

The DMZ: The group of all DMZ compartments

1.4 Abbreviations

CMW: Compartmented Mode Workstation

ToE: Target of Evaluation

MGB: MailGuard Bastion

SEF: Security Enforcing Function

MTA: Message Transfer Agent

SMTP: Simple Mail Transfer Protocol

DMZ: De-Militarized Zone

2. Product Rationale

2.1 Introduction

The product rationale allows a prospective purchaser to assess whether the product will help to satisfy his overall system security objectives, and what measures, other than those implemented by the product, would be needed to meet those objectives.

2.2 Intended Method of Use

The MailGuard Bastion (MGB) is intended for use as an electronic mail relay, or messaging firewall, between two networks where one or both networks require complete accountability of all traffic passing through the relay.

The product is particularly intended for use between incompatible, or mutually mistrusting, networks where free exchange of email cannot be permitted and extra controls on message flow need to be enforced at the interface between the two networks. To this end the product offers a protected environment, referred to as the DMZ, into which additional software modules can be plugged to implement the necessary controls on the messages flowing in each direction.

The product guarantees that each software module embedded within the DMZ has the opportunity to inspect, process and accept/reject each message before the message is forwarded onto the opposing network. Typical modules that could be supported in this manner include virus-scanners, content-filters, sensitivity-label checkers and digital-signature checkers. These modules need not be trusted/evaluated but must be supplied by NET-TEL and must be pre-configured into the product before delivery.

Where beneficial, a perimeter network and packet filters should be used on one or both sides of the MGB to filter out superfluous network traffic and add an extra layer of protection between the two networks being connected.

2.2.1 Method of Use Assumptions

This section indicates some of the procedural measures required to maintain the security of the MGB product. It concentrates on assumptions about the way the product *must be used*, ie installed/configured during start-up, and administered during normal operation. Further assumptions (concerned with environment rather than method of use) are listed in section 2.5 below.

MoU Assumption 1: The pre-delivery procedures (described in the *MGB Pre-delivery Installation and Configuration Guide*) must be followed to install and configure a basic MGB product prior to delivery. These procedures will be semi-automated and will:

1. Define the number and contents of each DMZ compartment [See Note 1]
2. Define the type of MTA required (X.400 or SMTP) [See Note 1]
3. Define all Administration Accounts and Roles [See Note 1]
4. Define/configure the two TSOL network interfaces and associated remote-host details [See Note 1]
5. Install all MGB software and verify CMW labels have been correctly applied.
6. Verify system auditing is enabled and correctly configured
7. Generate an MGB-boot-CD [See Note 2]

[Note 1]. These procedures will take input from an *MGB specification form* (completed by the Customer with help from Sales/Support at or around the point of order).

[Note 2] The MGB-boot-CD will be shipped to the customer by independent means and must be used during post-delivery installation to 'switch on' the product and confirm that the product has not been tampered with during delivery.

MoU Assumption 2: The post-delivery procedures (described in *The MGB System Delivery Guide*) must be followed to complete the MGB installation into its target environment. These procedures will explain how to:

1. Use the MGB-boot-CD to boot the product and verify the installation has not been tampered with during delivery
2. Use TSOL(E3) to generate new passwords for each administration account
3. Physically attach the networks to the MGB and verify the connections are correct
4. Complete a phased start-up of all software and verify each component is functioning correctly.

MoU Assumption 3: The system operation and administration procedures (described in the *MGB Administration Guide*) must be followed during normal day-to-day operation. These procedures will explain how to:

1. reconfigure an administrator account (in the event that one has to be reassigned)
2. reconfigure the remote-MTA details (in the event that one has to be reassigned).
3. disable/enable the software running in one of the DMZ compartments (if this need arises)
4. back-up the system audits and message archives (if configured)
5. use the system audits or message archives to detect a breach of security
6. stop/start the system during normal operation
7. recover the system after abnormal failure

2.3 Security Objectives

The MGB security objectives are as follows:

SO1: The product must provide an electronic mail relay between two networks that guarantees that no network traffic flowing between the two networks (via the MGB) can bypass the MGB software.

SO2: The product must provide a means of applying additional security checks (typically to sanction the export of data, or to enforce additional elements of network policy) on all messages moving between the two networks.

SO3: The product must provide a means of recording an audit trail, or archive, of the messages moved between the two networks.

SO4: If configured to block message flow in one direction, the product must guarantee that electronic mail cannot flow in the direction being blocked.

2.4 Evaluated Configuration

The target of the evaluation (ToE) is the MailGuard Bastion that consists of a pre-installed bundle of software and hardware containing:

1. A SUN SPARC Workstation
2. Two Network Cards
3. SUN Solaris 2.5.1
4. SUN Trusted Solaris 2.5
5. MGB specific software and configuration files

The MGB includes several optional components that must be configured into the product during the pre-delivery installation phase and dictate the exact contents of the product delivered to the customer. Effectively this configuration process results in a number of different versions of the product which, as a group, form the ToE. The configurable components that vary include:

1. The number and content of the DMZ compartments
2. The type of MTAs (X.400 or SMTP) running in the networking compartments
3. The contents of the TSOL(E3) configuration file that defines all CMW labels
4. The contents of the MGB configuration file that defines the message channels through the DMZ compartments.

It should be noted that, with the exception of the message archiving program, the software running in all DMZ and networking compartments will be shown to be security-irrelevant and will not require evaluation.

2.5 Environmental Assumptions

This section indicates the remaining personnel, physical and procedural measures required to maintain the security of the MGB product. It concentrates on assumptions about the Environment rather than Method of Use. Note that the TSOL(E3) environmental assumptions (as listed in Ref [2] section 2.4) also apply and are not repeated here.

E1 The system running the MailGuard Bastion must be kept in a physically secure environment which meets or exceeds the environmental security requirements of both attached networks.

E2 Physical access to the system should be restricted to the nominated personnel who require access for core administration purposes.

E3 No other applications will be installed or run on the MailGuard Bastion

E4 All access to the system will be via console only. Remote login/management will be disabled.

E5 All non-essential software packages will be removed from the system.

E6 The MGB administration roles defined during installation will not be added to or modified in any way and all administration accounts will be managed in strict accordance with the procedures laid down in the MGB documentation.

E7 If either or both of the networks being connected has a specific archiving policy the MailGuard Bastion will be archived according to the stricter of the policies which is in place. The system running the MailGuard Bastion itself is to be treated as though it is a member of the more strictly controlled network, should there be a difference between the two being connected.

2.6 Assumed Threats

The assumed threats for the MailGuard Bastion are as follows.

T1: A network based attacker attempts to establish an independent network connection across the MGB that bypasses the MGB software.

T2: A network based attacker overruns one or both of the MTAs and then attempts to use the established MTA network connection(s) to bypass the remaining MGB software.

T3: A local or network-based attacker attempts to modify or overrun the MGB mechanisms that ensures all email passes through each of the DMZ compartments defined by the MGB configuration, and thus enable email to bypass one or more of the DMZ modules.

T4: Local or network-based attack attempts go undetected allowing an attacker to slowly learn the weaknesses of the product and, through a trial-and-error process, eventually defeat the security objectives.

T5: A locally based attack by an unauthorised user to the system, or abuse of trust/privilege by an authorised user.

T6: A deliberate or accidental attempt by a network user to send an email message in the wrong direction across the MGB when the MGB is configured to support message flow in one direction only.

T7: An IP 'spoofing' attack, where a network user on one network attempts to make a connection to the MTA running in the wrong (ie. opposing) networking compartment by using a source IP address of a host based on the opposing network.

2.7 Summary of security features

The primary security features of the MailGuard Bastion are:

- An electronic mail (X.400 or SMTP) messaging gateway between two networks connected to, and separated by, the MGB.
- Archiving of all messages passing through the MGB (optional)
- A plug-in interface that allows additional software checks to be applied to each message as it passes through the MGB. This mechanism can be used to apply import/export sanctions, to or enforce additional elements of network security policy such as (but not limited to) virus scanning, content filtering, filtering based on sensitivity labels or digital signature verification.
- Separate channels for managing the message flow in each direction (allowing differing export sanctions and/or network policy to be applied in each direction)
- Administrator identification and authentication, along with system-auditing, provided by TSOL(E3).

3. Security Enforcing Functions

Philosophy of Design

The MailGuard Bastion consists of several software sub-systems, each responsible for a particular activity. Like most networking applications the networking sub-system represents a large and complex component of the product which, due to its size, complexity and exposure to the network is particularly vulnerable to attack. Networking products are thus particularly difficult to assure at a security level.

The MailGuard Bastion acknowledges this difficulty and takes the view that the networking sub-system (ie. MTA) is inherently untrustworthy. The primary aim of the design is thus too sufficiently isolate each network connection such that the correct operation of the MTA is not relevant to the security objectives, and thus its functions can be classed as security irrelevant.

To this end the MGB uses TSOL(E3) domain separation to provide several secure compartments for running the various software components of the MGB. Two of these compartments are connected to the network (one network connection per compartment) and run the MTAs (X.400 or SMTP). The remaining compartments (DMZ) are used to channel email messages between the two MTAs and to run additional software checks on the messages as they pass through.

The contents of all compartments, and the configuration of the MGB messaging sub-system (that controls the message channels between compartments) is pre-configured into the system prior to delivery.

SEF1: Domain Separation

The MGB product shall use domain separation to separate trusted and untrusted components of the product and to protect the security-enforcing functions of the product.

Domain Separation is a Type B mechanism provided by TSOL(E3).

SEF2: Network Separation

Each of the networks (of the two permitted) that connect to the MGB shall be connected to a networking compartment that is not connected to any other network.

To illustrate, imagine two networks (INNERNET and OUTERNET) and two compartments (INSIDE and OUTSIDE). All call attempts from remote hosts on INNERNET shall be associated with and handled by compartment INSIDE. All call attempts from remote hosts on OUTERNET shall be associated with and handled by compartment OUTSIDE.

SEF3: Assured message handling

The transfer of messages between compartments, and thus across the MGB, shall be managed by a trusted messaging sub-system. This sub-system shall be the only additional product component, over and above TSOL(E3), that has sufficient privileges to move data between compartments.

SEF4: Assured message channels

The messaging sub-system (and its configuration files) that controls the movement of messages between compartments shall guarantee that there shall be no more than one channel for **successful** message flow through the DMZ (and thus across the MGB) in each direction. The messaging sub-system shall guarantee that the channel cannot be bypassed or short-cut.

Note, there maybe several channels used for **unsuccessful** message flow (that terminate in an inner DMZ compartment or return a message to the network compartment it originated from). These channels are acceptable provided they do not interfere with the channels set-up for **successful** message flow.

A channel is defined by the number and order of DMZ compartments that each message will be forced to pass through by the messaging system. All channels for a particular MGB installation shall be pre-configured into the product (and verified) prior to delivery.

SEF5: Acknowledged message processing

The messaging sub-system that controls the movement of messages between compartments shall guarantee that no message can leave a DMZ compartment without some form of acknowledgment (from a process running within the compartment) that the message has been detected and processed.

SEF6: Message archives

If configured, all messages entering the DMZ of the MGB shall be archived. A copy of every message shall be saved to an archiving spool directory.

SEF7: System Auditing

The TSOL(E3) System Auditing shall be used to record (at least) the date, time and originating process/user details of the following events:

- Console logon/logoff events
- All administrator actions
- Any security-critical events generated by the security-enforcing components of the product.

SEF8: Administration Access Control

At least two MGB administration roles shall be defined and used, one for administering the trusted components of the MGB and one for the untrusted components. Access to all MGB administration accounts, and thus the product, shall be protected by a password which is generated by the TSOL(E3) password generator. The TSOL(E3) algorithms for password generation and authentication are a type A mechanism.

4 Security Mechanisms and Evaluation Level

4.1 Required Security Mechanisms

The ToE relies on TSOL(E3) for domain separation. This is a Type-B mechanism.

The ToE relies on TSOL(E3) for password encryption and authentication. The algorithms used by TSOL(E3) for this purpose constitute a Type-A Mechanism.

4.2 Strength of Mechanisms

The ToE will be configured such that all passwords must be generated by TSOL(E3) hence the claimed strength of mechanism for the password encryption and authentication algorithms is *High*. See Ref [2], section 4.2.

4.3 The Target Evaluation Level

The target evaluation for the product is E3 [ITSEC].

Appendix A: Suitability

This appendix discusses how the assumptions and the technical measures (SEFs) work together to counter the identified threats and thus support the Security Objectives.

The method of use assumptions support the SEFs by guaranteeing that the freshly installed state of MGB is secure (meets all objectives), and also by defining what activities can be performed on the MGB once in operation, including procedures for how to complete those activities safely. The environmental assumptions support the SEFs by providing and maintaining a stable environment in which the SEFs can operate safely and consistently.

A 'Y' in the table below indicates a positive counter against the threat labelled at the top of the column. The threats are detailed in section 2.6 of this document.

	T1	T2	T3	T4	T5	T6	T7	
SEF1:	Y	Y	-	-	-	-	-	Domain Separation
SEF2:	Y	-	-	-	-	-	Y	Network Separation
SEF3:	-	Y	Y	-	-	-	-	Assured message handling
SEF4:	-	Y	Y	-	-	Y	-	Assured message channels
SEF5:	-	-	Y	-	-	-	-	Acknowledged message processing
SEF6:	-	-	-	Y	-	-	-	Message Archiving
SEF7:	-	-	-	Y	-	-	-	System Audits
SEF8:	-	-	-	-	Y	-	-	Administration Access Control