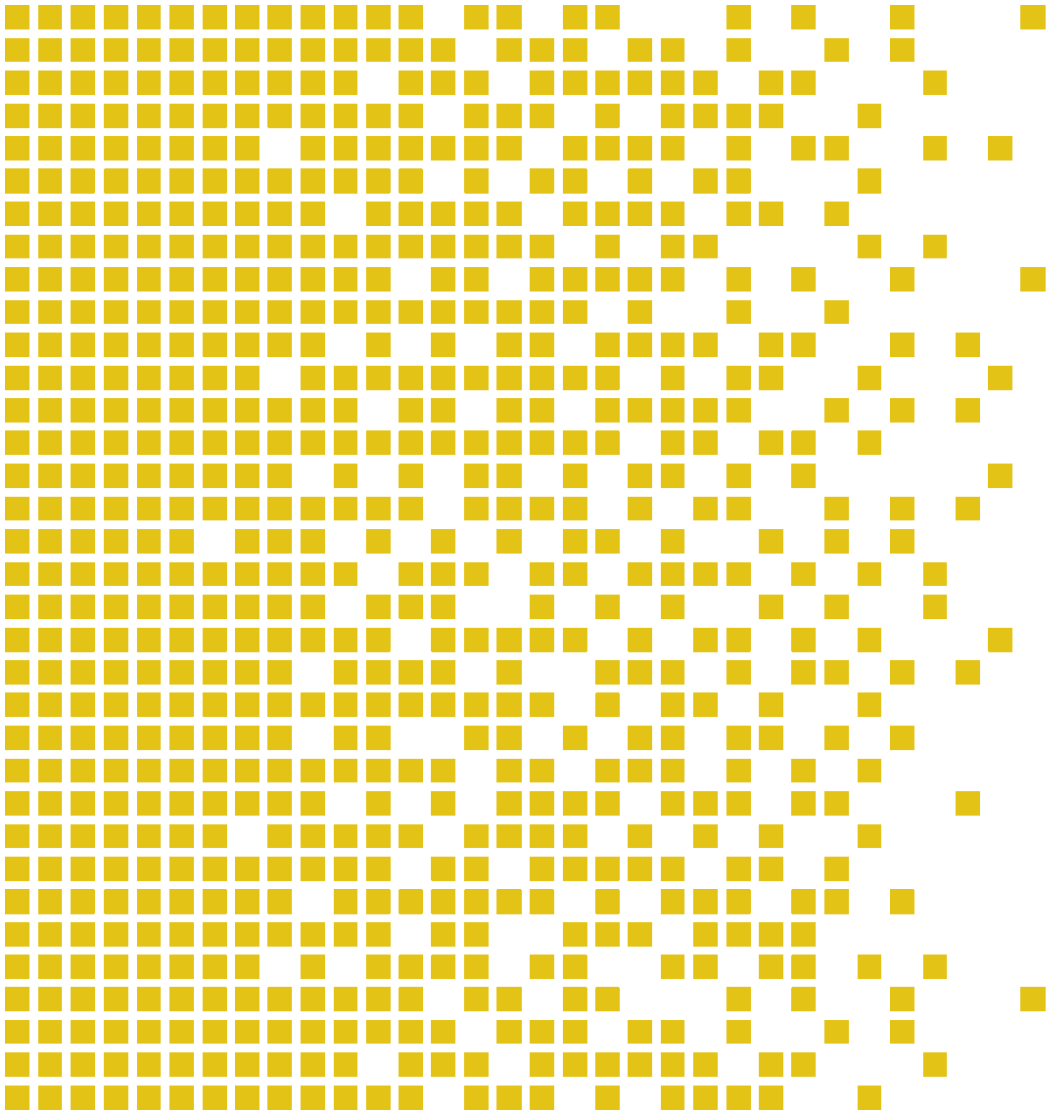
SERTIT-008 CR Certification Report

Issue 1.0 23.02.2010

XOmail Server v14.2.4 running on Windows Server 2003 SP2,including R2, Standard, Enterprise, and Datacenter



SERTIT, P.O. Box 14, N-1306 Bærum postterminal, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party. [*]

[* Mutual Recognition under the CC recognition arrangement applies to EAL 4.]

Contents

1 Certification Statement

Forsvarets logistikkorganisasjon - Investeringsavdelingen (FLO/I) XOmail server is the server component in a military messaging system.

XOmail server version 14.2.4 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 conformant requirements *of* Evaluation Assurance Level EAL 4 for the specified Common Criteria Part 2 conformant functionality when running on the platforms specified in Annex A.

Author	Kjartan Jæger Kvassnes Certifier
Quality Assurance	Lars Borgos Quality Assurance
Approved	Kjell W. Bergan Head of SERTIT
Date approved	23.02.2010

2 Abbreviations

C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CAPP	Controlled Access Protection Profile
CC	Common Criteria for Information Technology Security Evaluation
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
CUI	Character-based User Interface
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT/ITSEF	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
HCL	Hierarchical Classification Level (e.g. RESTRICTED)
MMHS	Military Message Handling System
NHC	Non-Hierarchical Category (e.g. CLEAR)
POC	Point of Contact
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
SoF	Strength of Function
SNMP	Simple Network Management Protocol
SPM	Security Policy Model
SP	Security Policy
ST	Security Target
TSC	TSF Scope of Control
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

3 References

[1] Security Target, Forsvarets logistikkorganisasjon - Investeringsavdelingen (FLO/I), XOmail version 14.2 Security Target, Edition: 10-public, 28. April 2009.

[2] Common Criteria Part 1, CCMB-2005-08-001, Version 2.3, August 2005.

[3] Common Criteria Part 2, CCMB-2005-08-002, Version 2.3, August 2005.

[4] Common Criteria Part 3, CCMB-2005-08-003, Version 2.3, August 2005.

[5] The Norwegian Certification Scheme, SD001E, Version 7.0, 28.03.2008.

[6] Common Methodology for Information Technology Security Evaluation, EvaluationMethodology, CCMB-2005-08-004, Version 2.3, August 2005.

[7] Evaluation Technical Report Common Criteria EAL 4 Evaluation of XOmail Server v14.2.4,2009-12-07, ed. 1.1.

[8] 739 20561 ABAA EO XOmail Administrator's Guide

[9] 739 20529 ABAA EO XOmail User's Guide

[10] 712 31897 AAAA DE MHS Security Concept and Design

[11] 712 27734 AXAA EO XOmail Installation and Configuration Guide.

[12] Bell & LaPadula: Secure Computer Systems: Unified Exposition and Multics Interpretation

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of XOmail server version 14.2.4 to the Sponsor, Forsvarets logistikkorganisasjon - Investeringsavdelingen (FLO/I), and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target [1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The version of the product evaluated was XOmail server, version 14.2.4.

This product is also described in this report as the Target of Evaluation (TOE). The developer was Thales Norway AS.

The TOE is the XOmail MMHS server component, with the functionality as defined in Section 4.2.2 of the Security Target[1].

XOmail is a COTS product tailored to information handling and transfer in modern military C4ISR solutions and large organizations.

The TOE consists of the XOmail Server, which is the building block for the messaging infrastructure. The TOE provides a number of APIs, which allow third-party applications to use the messaging infrastructure.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

An overview of the TOE's security architecture can be found in Annex B.

4.3 TOE scope

The scope of the TOE is described in the ST[1], chapter 4.2.2

4.4 Protection Profile Conformance

The Security Target[1] did not claim conformance to any protection profile.

4.5 Assurance Level

The Security Target[1] specified the assurance requirements for the evaluation. The predefined evaluation assurance level EAL 4 was used. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Strength of Function

The minimum Strength of Function (SoF) was SoF-Medium. This was claimed for the *validate security function* that shall be able to verify the integrity of both TSF data and TSF executable code. The validation mechanism produces checksums that must be compared with the developer provided checksums.

4.7 Security Policy

The TOE security policies are detailed in ST[1], chapter 4.3.5.

4.8 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats, OSP's *and assumptions* which these objectives meet and security functional requirements and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

4.9 Threats Countered by the TOE

- Improper administration may result in override of specific security policy.
- An attacker may cause audit records to be lost or modified. Attackers may also cause audit overflow, so that important audit records seemingly disappear.
- The TOE is unable to store audit data or provide necessary audit data to the IT environment, or the audit becomes useless because of the inability to separate important audit records from other records. The latter is the case if the audit is overflowed. The integrity of transmitted information may be compromised due to deliberate or accidental modification.
- An attacker prevents authorised users from accessing system resources via are source exhaustion denial of service attack.
- An attacker introduces information that appears to come from a trusted entity.
- An attacker tries to masquerade as a trusted entity in order to by mistake be trusted with classified information.
- An attacker monitors activities and actions performed on classified information. Such activities and actions include authentication and creating, viewing, modifying and deleting classified information. The monitoring activities can be performed at multiple levels, like screen monitoring or network monitoring.
- A malicious process or user gains access by replaying authentication data.
- A malicious user may gain unauthorised access to an unattended session.
- Unauthorised access to identified assets may occur. Methods of attack covered by this threat are brute force attacks, session hijacking, authentication data cracking, privilege escalation and social engineering.

4.10 Threats Countered by the TOE's environment

- An attacker may cause audit records to be lost or modified.
- An attacker may try to replace parts (or the complete) TOE with a malicious version.
- An attacker block authorised users from system resources via a resource exhaustion denial of service attack.
- The TOE is installed and/or configured in a manner that undermines security.
- Unintentional or intentional errors in design of the XOmail may occur. Such design flaws includes inability to adequately separate information based on SP, HCL or NHC and inability to associate correct security attributes with the users.
- The developer has failed in implementing the TOE in a secure manner, failed in implementing the TOE according to the design, or deliberately planted backdoors, Trojans or similar.
- A malicious user may gain unauthorised access to an unattended session.

4.11 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.12 Environmental Assumptions and Dependencies

The following assumptions are assumed to exist in the environment:

- All administrators know how to administer the TOE in a secure manner.
- Administrator personnel review audit logs on a regular basis.
- Administrators or developers will not intentionally compromise the TOE security
- Proper disposal of authentication data and associated privileges is performed after access is removed
- The network connections used between separate parts of the TOE and for external communication are protected from unauthorised disclosure and modification
- Administrators and users notify the proper authority of any security issues that impact their systems
- The hardware on which XOmail runs is protected from unauthorised physical modification
- The hardware on which XOmail runs is located where only authorised personnel have access

- The TOE runs on a CAPP evaluated OS with EAL4 or higher
- All users know how to use the TOE in a secure manner

4.13 IT Security Objectives

The TOE IT security objectives in the XOmail ST are as follows:

- The TOE maintains information related to previous attempts for a user to establish a session
- The TOE uses its internal secure database (SS), as well as OS audit mechanisms for recording any security related information
- The TOE provides an automatic logout mechanism for the Mail Client and the CUI
- The TOE provides means for restricting access to administrative commands for each user or group of users
- The TOE provides means for recording administrative commands
- The TOE ensures Discretionary Access Control by controlling access to resources based on the identity of users and groups of users
- A user is identified and authenticated before given access to classified information
- The TOE ensures that information is labelled with the correct human-readable label when exported out of TSC
- The TOE provides a locking mechanism that makes it possible to prevent users from logging on, even if they have a valid account
- The TOE allows administrators to effectively, accurately and securely manage the TOE and its security functions
- The TOE ensures Mandatory Access Control by controlling access to resources based on security clearance of users and resources
- The TOE allows authorised security administrators to specify the security clearance of users and resources
- The TOE provides secure messaging functions
- The TOE will ensure preservation of a secure state in the event of a secure component failure
- A reference monitor ensures that a SFP implemented by a TSF cannot be bypassed.
- The TOE ensures that no entity can block other authorised entities from accessing resources
- The TOE ensures secure reuse of resources
- When template "Permit" flag is set, only administrators with the same, or a more privileged level can associate users with that template

- The TOE assigns each user to a specific role
- The TOE database performs a self-test during start-up
- Those responsible for the TOE will ensure that the product is configured such that only the group of users for which the system was accredited may access the system, and furthermore that each individual user is assigned a unique user identification
- The OS will perform auditing as specified in CAPP
- A user is identified and authenticated before given access to the OS that the TOE runs on
- Those responsible for the TOE will ensure that networks that are used for communication between separate parts of the TOE and for external communication are protected
- The TOE environment will ensure that TOE administrative network traffic can be separated from other TOE network traffic

4.14 Non-IT Security Objectives

- Those responsible for the TOE will ensure that administrators of the system are trustworthy
- Those responsible for the TOE will ensure that the TOE is installed, managed and operated according to the TOE guidance documentation
- Those responsible for the TOE will ensure that security relevant components of the TOE are protected from physical attack that might compromise the IT-security

4.15 Security Functional Requirements

The TOE provides security functions to satisfy the following Security Functional Requirements (SFRs):

- Security alarms FAU_ARP.1
- Audit data generation FAU_GEN.1
- User identity association FAU_GEN.2
- Potential violation analysis FAU_SAA.1
- Audit review FAU_SAR.1
- Restricted audit review FAU_SAR.2
- Protected audit trail storage FAU_STG.1
- Action in case of possible audit data loss FAU_STG.3

- Prevention of audit data loss FAU_STG.4
- Subset access control FDP_ACC.1
- Access control functions FDP_ACF.1
- Export of user data with security attributes FDP_ETC.2
- Complete information flow control FDP_IFC.2
- Hierarchical security attributes FDP_IFF.2
- Import of user data with security attributes FDP_ITC.2
- Full residual information protection FDP_RIP.2
- Authentication failure handling FIA_AFL.1
- User attribute definition FIA_ATD.1
- Timing of authentication FIA_UAU.2
- Multiple authentication mechanisms FIA_UAU.5
- Timing of identification FIA_UID.2
- User-subject binding FIA_USB.1
- Management of security attributes FMT_MSA.1
- Static attribute initialization FMT_MSA.3
- Management of TSF data FMT_MTD.1
- Specification of Management Functions FMT_SMF.1
- Security roles FMT_SMR.1
- Fail secure FPT_FLS.1
- Manual Recovery FPT_RCV.1
- Automated recovery FPT_RCV.2
- Function recovery FPT_RCV.4
- Non-bypassability of the TSP FPT_RVM.1
- Complete reference monitor FPT_SEP.3
- Inter-TSF basic TSF data consistency FPT_TDC.1
- TSF testing FPT_TST.1
- TSF-initiated termination FTA_SSL.3
- TOE session establishment FTA_TSE.1

4.16 Security Function Policy

The TOE has an information flow security function policy defined in FDP_ACF.1, FDP_ETC.2, FDP_IFC.2, FDP_ITC.2, FMT_MSA.3, FPT_SEP.3, FDP_ITT.1.

Details of the security function policy is described in Annex B

4.17 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[6].

SERTIT monitored the evaluation which was carried out by the Norconsult EVIT (ITSEF). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR)[7] to SERTIT 2009.12.07. SERTIT then produced this Certification Report.

4.18 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3 [4]. These classes comprise the EAL 4 assurance package.

Assurance class	Assurance components

Configuration Management	ACM_AUT.1	Partial CM automation
	ACM_CAP.4	Generation support and acceptance procedures
	ACM_SCP.2	Problem tracking CM coverage
Delivery and operation	ADO_DEL.2	Detection of modification
	ADO_IGS.1	Installation, generation and start-up procedures
Development	ADV_FSP.2	Fully defined external interfaces
	ADV_HLD.4	Security enforcing high-level design
	ADV_IMP.1	Subset of the implementation of the TSF
	ADV_LLD.1	Descriptive low-level design
	ADV_RCR.1	Informal correspondence demonstration
	ADV_SPM.1	Informal TOE security policy model
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Life Cycle support	ALC_DVS.1	Identification of security measures
	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT.1	Well-defined development tools
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: high-level design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_MSU.2	Validation of analysis
	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.2	Independent vulnerability analysis

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[7] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

All assurance classes were found to be satisfactory and were awarded an overall "pass" verdict.

5.2 Delivery

The developer's delivery and operation procedures ensure that the TOE is not compromised during transfer and installation, and ensures that the integrity of the TOE medium and operational server is verified with use of checksums (the checksums and installation CD is delivered by the developer in 2 separate deliveries). On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised during delivery.

5.3 Installation and Guidance Documentation

Using Perl extensions, XOmail supports automated installation. This module is used for installation only, not for operational use.

Installation procedures are described in detail in XOmail Installation and Configuration Guide[11]

5.4 Misuse

There is always a risk of intentional misuse of the system or misconfigurations that could possibly compromise classified information, but with the extensive use of administrators monitoring received alarms, security cleared personnel and regular security audits is the risk mitigated.

Administrators should follow the guidance [8] and[10] for the TOE in order to ensure that the TOE operates in a secure manner. The guidance documents adequately describe all possible modes of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively administer and use the TOE's security functions, and to detect insecure states.

5.5 Vulnerability Analysis

The developer's vulnerability analysis identifies potential exploitable vulnerabilities, and describes if and what assumptions and environmental security measures that covers the specific potential vulnerabilities. The evaluators' assessments of potential exploitable vulnerabilities in the TOE have been addressed by the developer, and the TOE in its intended environment should be resistant to attackers with a low attack potential.

The TSF with a SOF-claim is resistant against known attacks at the given time of evaluation, but this could change in the future as computers become more powerful and attack techniques become more sophisticated. However the algorithm utilized by the TOE (SHA-256) should be sufficient for many years to come.

5.6 Vulnerability analysis

The developer's vulnerability analysis, ref. MHS Security Concept and Design Part II, incorporates the risk associated with SNMP. The developer provided a rationale describing the potential vulnerability of using the Microsoft SNMP Agent, and included a potential exploitable vulnerability in the SNMP traps Denial of Service (DoS). The evaluator consider SNMP vulnerabilities and other potentially exploitable vulnerabilities not to be exploitable by an attacker possessing low attack potential, in the TOE's intended environment.

5.7 Developer's Tests

The developer's test documentation shows that the TOE is methodically tested against the functional specifications. The developers test specification are directly linked with its corresponding functional specification, and passing one test shows that that specific functional specification works according to the documentation.

The depth and coverage analysis shows that the developers' tests cover all TSF, and that the TOE has been extensively tested against its functional specification. The developer's testing results lead either to a test is passed, or the test is failed and an error report is created for that error.

The results show that the developer testing requirements is extensive and that the TSF satisfies the TOE security functional requirements.

5.8 Evaluators' Tests

The independent testing performed by the evaluators focused on the different TSFs, and the retesting tested approximately 25% of the developer's TSF specific tests. The testing performed by the evaluator focused on verifying key aspects of the TSF, and the retesting focused on the main functionality of the security functions.

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that XOmail server version 14.2.4 running on Windows Server 2003 SP2, including R2, Standard, Enterprise, and Datacenter meets the specified Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 4 for the specified Common Criteria Part 2 conformant functionality, in the specified environment, when running on platforms specified in Annex A.

SERTIT has also determined that the TOE meets the minimum SoF claim of SOF-Medium given above under Section 4.6 "Strength of Function Claims".

6.2 Recommendations

Prospective consumers of XOmail server version 14.2.4 should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A.

Annex A: Evaluated Configuration

TOE Identification

The TOE is uniquely identified as:

XOmail Server version 14.2.4

TOE Documentation

The supporting guidance documents evaluated were:

- ST[1]
- Administrator's Guide[8]
- User's Guide[9]
- MHS Security Concept and Design[10]
- Installation and Configuration Guide[11]

TOE Configuration

The following configuration was used for testing:

The TOE test-bed consisted of three virtual machines connected together in a LAN and running in VMware Workstation 6.5. The virtual machines run Windows Server 2003 with SP1 in a Common Criteria EAL4 evaluated configuration. The machines are configured with the aid of "Windows Server 2003 SP2 Security Configuration Guide" version 3.0 and runs with the baseline (required settings) configuration. There where though some practical exceptions to the configuration:

- Prevention of automatic installation of device drivers is deactivated (allowing for use of USB-sticks in the test-bed).
- Minimum password length is reduced to 2 (instead of 8), and password complexity is turned off.
- Password protected screen-saver was deactivated.
- Generation of administrative alert messages when the audit log is full is deactivated.

The virtual Server 1 runs Active Directory (AD), DHCP and DNS, and Server 2 and Server 3 are members of the same AD domain.

For penetration testing the same configuration was used.

Annex B: Security Policy Model

About the Description of the XOmail Security Policy Model

The XOmail Security Policy model consists of the Bell-LaPadula based model for access control [12].

Management security policy and system integrity policy is not modelled.

The XOmail security policy for access control is based on the Bell-LaPadula security model which is a formal security policy model. The XOmail security policy for access control will be described using the terminology and concepts found in the Bell-LaPadula security model.

Tailoring of XOmail Security Policy

XOmail is designed to support a range of national and organisational security policies for multi-level secure systems. The Security Target for XOmail version 14.2 [1] shows how XOmail will support Norwegian and NATO security policies including the security policies for access control. However, XOmail may also be tailored to support other security policies for access control.

Note that a given implementation of XOmail may simultaneously support several security policies for access control (e.g. Norwegian security policy and NATO security policy).

Elements in the XOmail Security Policy for Access Control

The elements described in this section are used by the security mechanisms to enforce and support the security policy for access control.

Subjects

Subjects are active entities. They initiate requests for operations on objects. Subjects represent external users (e.g. human beings, or other entities (e.g. processes related to OSI communication or ACP127 communication). Each subject is associated with a security clearance and a unique identifier. These are used by the XOmail security mechanisms to verify access rights to objects. Subject representation is closely related to execution domains.

Each existing subject is associated with:

- The UID of the user it represents.
- A unique identity that identifies it among all other subjects, including subjects with the same UID.
- Sensitivity label.

Objects

Objects are passive entities. They are created and manipulated by subjects. Objects are represented as stored information within the system. Each object is associated with a sensitivity label, which is used by the security mechanisms to control

subject's rights to manipulate objects.

Sensitivity Label (SL)

Any subject and object security level is expressed by a sensitivity label. The sensitivity label for subjects and objects are used by the security protection mechanisms to grant subjects access to manipulate objects.

Each subject sensitivity label contains:

- A Subject Maximum Clearance (SMC)
- A Subject Current Clearance (SCC)
- A set of Subject Privilege Flags (SPF)

Each object sensitivity label contains:

- An Object Current Classification (OCC)
- An Object Maximum Clearance (OMC) (optional, only used for some object types)
- An Object Minimum Clearance (OLC) (optional, only used for some object types)
- A set of Object Privilege Flags (OPF)

Each of the clearance (SMC, SCC, OMC and OLC) and classification (OCC) attributes consists of these different information parts:

- Hierarchical classification level (HCL)
- Non-hierarchical categories (NHC)
- Security policy identifier (SP)
- Type (i.e. clearance or classification)

HCL contains the hierarchical classification value for the subject/object, and is used when evaluating access (MAC), e.g. NATO UNCLASSIFIED or NATO RESTRICTED.

NHC contains the non-hierarchical category values for the subject/object, and is used when evaluating access (MAC), e.g .CRYPTO SECURITY or EXCLUSIVE.

SP identifies the classification security policy defining the meaning of HCL and NHC. Different values for SP may be used for creating non-overlapping sets of HCL and NHC combinations. SP is used when evaluating access (MAC), and in addition controls the presentation of HCL when sensitivity labels are mapped to/from textual (human-readable) representations..

The value set for SPF is:

- Subject is trusted (ST)
- Subject is un-trusted (SU)

The value set for OPF is:

- Object is multi-level (OM)
- Object is single-level (OS)

Access Control List (ACL)

An ACL is associated with each object controlled by the DAC mechanisms. The ACL is used to state access rights to objects in terms of the UID the subject represents. An ACL contains a set of Access Control Elements (ACE). Each ACE consists of the following information elements:

- Subject set identifier (SSI)
- Access privileges (AP)

An SSI identifies a user, a set of users, a user group or a set of user groups. AP defines the actual access rights for the selection of users given.

The AP value set is:

Symbol	Access type	Meaning
R	Read access	(observation)
W	Write access	(alteration)
E	Execute access	(no observation, no alteration)
(none)	No access	

Execution Domains

Execution domains are the essential building blocks used to construct a software environment for enforcing the security policy.

The execution domain is an abstraction for an execution environment where Kernel functions, Trusted functions or other functions can execute under the full control of the TCB. A single execution domain will contain either TCB module(s) or non-TCB module(s), but never both types. All communication between execution domains is completely controlled by the TCB. However, within a specific non-TCB execution domain the TCB has no such influence.

XOmail Security Mechanisms

The security mechanisms described in this section enforce the security policy for access to and operations on objects. These mechanisms are implemented partly by the OS and partly by trusted XOmail functions.

Mandatory Access Control (MAC)

MAC implements the procedures for how to treat classified information. It implements access rights according to hierarchical classification (HCL), non-hierarchical category (NHC) of information, and security policy (SP). For MAC evaluation, SP is handled in the same way as the NHC.

The MAC mechanism ensures that subjects cannot read information for which they are not cleared, i.e. the subject SL must dominate the object SL ("ss-property"

according to [12]). MAC also ensures that no information can be written to a "lower" level, i.e. the object SL must dominate the subject SL ("*-property" according to [12]).

Discretionary Access Control (DAC)

The DAC mechanism uses an object's access control list (ACL) to state a subject's discretionary access rights to the object. The DAC differs from MAC in that it is based on user identities instead of security labels, and the actual access rights may be specified by the object's owner.

Different types of access are defined in section 0. The DAC mechanism use of an ACL is best described by an example:

Subject	Ident	Access	
user_1	group_1	RW	user_1 in group_1 has Read and Write access
ALL	group_1	R	All other users in group_1 have Read access
ALL	ALL	(none)	No other users/groups have access

Note that the ACL is conceptually always sorted with the ALL specification at the end of the list. The DAC mechanism scans the list from top to bottom, and uses the first matching ACL element to decide the access.

Interaction of MAC and DAC

The MAC and DAC represent two different access control mechanisms. These are both invoked when a subject attempts to access an object. It is important to note that MAC evaluation produces a "resulting permitted access" for that attempted access, which is a subset of an underlying access permission structure enforced by DAC. Because some of the subject attributes of MAC are dynamic by nature, this access mode is computed every time such an access is requested.

Authentication

The authentication mechanism is used to assure the correct relation between system users and their internal representation as subjects, i.e. to associate a user with the correct UID.

User access to the authentication mechanism is the only access that is not controlled by the XOmail access control mechanisms. That is, anyone who is physically able to access a logon device may try to log on to the system.

Audit

The audit mechanism is used for the registrations of security related events that occur during system operation. It is an aid for the system security administrator to reconstruct security related event sequences that have occurred in the past.

Audit registrations will be initiated from TCB modules where the events occur. All registrations are reported to a common audit function, which is responsible for the storage of audit information. Access to audit information is restricted to specially authorized users.

The CLEAR Policy

Communication of information between different MMHS servers requires the use of a communication channel. Each of these channels is classified either as "Secured" or "Unsecured". Communication of classified information normally requires use of a Secured communication channel.

The use of the CLEAR security policy will allow the communication of classified information by using unsecured communication channels.

This implies reclassification of information, and possibly downgrade to a lower classification level. This is because the original classification of a CLEAR-ed message is removed when sending the message, and at the receiving MMHS server is set to a predefined fixed security level.

The CLEAR policy is implemented by a trusted function, and is available only for subjects explicitly given the CLEAR privilege.

A separate CLEAR category value in the NHC part of the sensitivity label for subjects permits a subject to use the CLEAR policy. The same category value used in the object security label defines the object as CLEAR-ed. Only subjects with the CLEAR privilege are allowed to CLEAR an object.

Security Level Transformation

During their lifetime MHS messages may be converted between different format representations. Within XOmail several different formats exists, i.e. the ACP127 format, the STANAG 4406 formats (including DMP), the Internet Mail format, and the XOmail internal storage format. The value set for security classification for such a message, i.e. the OCC part of the message sensitivity label, need not be the same for the three different format representations.

There shall exist a predefined and unambiguous way to transform the security label between these representations. This transformation must be performed by a trusted function. The transformation must correctly handle cases with syntactical or semantic errors in a security label, and cases where a security label cannot be represented in the target format. These shall result in the transformation not taking place, with a subsequent failure in message processing.

Command Attributes

All administrative commands have attributes associated with them. The command attributes specify how execution of a command shall be handled. Supported attributes are:

- Verify
  The administrator must verify the executed commands. The command execution is not performed until the command is verified within a given period of time.
- Re-authenticate
  The administrator must re-authenticate within a given period of time before the command can be executed.
- Double check
  Two administrators must perform the same command within a given period of time for the command to be executed.
- Log
  Every execution, both successful and unsuccessful, will be logged. Three levels of logging are supported: none, normal and detailed. Log level may be configured on a per command basis. Means for reviewing the command log is provided in XOmail Admin.

Command attributes are configured per server, and applies to all administrators on the server.

Command Access

The set of security attributes that are associated with each authenticated user contains a list of all administrative commands available for that specific user. Commands that a user is not explicitly granted access to are unavailable for the user.

Analysis of guidance documentation – misuse (AVA_MSU.2)

Security Function	Documents	Analysis
SF.AUDIT ▪ Message operations ▪ Message reception and transmission ▪ Administrator commands ▪ Login attempts ▪ User lockout ▪ Command access changes ▪ System failures ▪ Self tests and self test results ▪ Start-up and shutdown of the XOmail server	Installation and Configuration Guide: No impact.	A user cannot affect which alarms or events that are recorded. Hence, there is no risk of misuse.
	Administrator's Guide: Describes how to enable/disable auditable Administrative commands, Describes how to ▪ Interpret alarms, ▪ modify alarm descriptors ▪ access and analyse log entries ▪ configure other audit mechanisms (Ch 6 Server, 14 Alarms, 18 Day-to-Day administration, 19.10 Security Audit, App A Alarm Descriptors)	
	User's Guide: No impact.	
SF.AUTHENTICATION	Installation and Configuration Guide: Describes configuration of single-signon	The authentication mechanisms cannot be disabled. Hence, there is no risk of misuse.
	Administrator's Guide: Describes management of users and administrators (Ch 9 Users).	
	User's Guide: No impact.	

Security Function	Documents	Analysis
SF.AUTO_LOGOUT	Installation and Configuration Guide: No impact. Administrator's Guide: Describes how to adjust the automatic logout interval. (Ch 7 Clients) User's Guide: No impact.	Any configuration of this security function will be recorded as audit records. The security function cannot be disabled. Hence, there is no risk of misuse.
SF.CLASSIFICATION_TAG	Installation and Configuration Guide: No impact. Administrator's Guide: Describes configuration of the XOmail Guard (Ch 19.8 Secure Guard). User's Guide: No impact.	Any configuration of this security function will be recorded as audit records. Users may deliberately or accidentally violate policy (e.g. use incorrect security labels). This may be discovered by inspection of audit records, or user or department journals.
SF.CLEAR	Installation and Configuration Guide: Describes how an administrator may change the CLEAR handling policy. (Ch 9.11 Security labels) Administrator's Guide: Describes the CLEAR policy. (Ch 19.1, Ch 19.4, App C.4)	Authorised users may deliberately violate organisational security policy by sending classified messages as CLEAR when there is no operational need. All messages will be journalled and the message operation

Security Function	Documents	Analysis
	User's Guide: No impact.	will logged. Security administrators may violate organisational security policy be giving CLEAR authorization to a person who according to the organisations policy should not have this authorization. Adminstrator actions will be recorded as audit records.
SF.COMMAND_ACCESS	Installation and Configuration Guide: No impact. Administrator's Guide: Describes how security administrators may grant command access to other administrators (Ch 9.1.8 Commands). User's Guide: No impact.	Any configuration of this security function will be recorded as audit records. Command access cannot be granted to non-administrators. Users cannot bypass this security function. Hence, there is no risk of misuse.
SF.COMMUNICATION_SECURITY	Installation and Configuration Guide: No impact. Administrator's Guide: Describes setup of system unit security (Ch 11 System Units).	Users cleared to send CLEAR messages may bypass this policy. Users may deliberately violate organisational security policy by marking messages

Security Function	Documents	Analysis
	User's Guide: No impact.	with an inappropriate security label. All messages will be journalled and the message operation will logged. Any configuration of this security function will be recorded as audit records.
SF.DAC	Installation and Configuration Guide: Describes adding users to the OS (Ch 3.1.3 and Ch 3.2.1).	Any configuration of this security function will be recorded as audit records. A user may deliberately violate organisational security policy by granting an unauthorised existing XOmail user read access to his own journal.
	Administrator's Guide: Describes system management, including users (Ch 9 Users, Ch 9.6.4 Security), administrators (Ch 9.1.1 Main, Administration Access), departments (Ch 9.6.2 Access, 10.1.3 Access, Ch 10.4.3 Access) and system units (Ch 11).	
	User's Guide: Describes how users may grant other users read access to his own journal (Ch 4.6 Security).	
SF.DB_SELF_TEST	Installation and Configuration Guide: No impact.	There are no configuration options for this security function,

Security Function	Documents	Analysis
	Administrator's Guide: Describes self-test behaviour and how to handle XOmail alarms (Ch 18.7 Alarms, App A Alarm Descriptors).	and the security function cannot be disabled. Hence, there is no risk of misuse.
	User's Guide: No impact.	
SF.EXECUTION_DOMAINS	Installation and Configuration Guide: No impact.	There are no configuration options for this security function, and the security function cannot be disabled. Hence, there is no risk of misuse.
	Administrator's Guide: No impact.	
	User's Guide: No impact.	
SF.LABEL_TRANSFORM	Installation and Configuration Guide: No impact.	There are no configuration options for this security function, and the security function cannot be disabled. Hence, there is no risk of misuse.
	Administrator's Guide: Describes error handling (App A Alarm Descriptors).	
	User's Guide: No impact.	
SF.LABELLING	Installation and Configuration Guide: No impact.	There are no configuration options for this security function, and the security function cannot be disabled. Hence, there is no risk of misuse.
	Administrator's Guide: Describes error handling (App A Alarm Descriptors).	
	User's Guide: No impact.	

Security Function	Documents	Analysis
SF.LOCK	Installation and Configuration Guide: Describes how to configure the maximum number of times a user can enter an illegal user/password-combination before the account is locked.	An administrator may deliberately or by mistake unlock users that should not have been unlocked. Such modifications will be recorded to audit records.
	Administrator's Guide: Describes automatic and manual locking of users (Ch 7.3 Passwords, Ch 7.5 Automatic network disconnection, Ch 9.6 Users).	
	User's Guide: No impact.	
SF.MAC	Installation and Configuration Guide: Describes configuration of the maximum security clearance for an XOmail Server installation (Ch 5.1 XOmail Server).	The system may be installed with an inappropriate maximum security clearance. Security administrators may violate organisational security policy by granting users, departments or system units a security clearance that is higher than it should be, based on actual personnel security clearance, or
	Administrator's Guide: Describes setting security labels for various parts of the system and configuration of how labels from other message servers are handled (Ch 9.1.9, Ch 9.6.4, Ch 9.7.6, Ch 10.1.6, Ch 10.4.6, Ch 11.2.2, Ch 11.4.3, Ch 11.5.3, Ch 19 and App C4).	

Security Function	Documents	Analysis
	User's Guide: Describes how to set the security label for a new message, and how to change the security label of a message draft (Ch 7.3 Create a message, Ch 11.6.1 Change the security label).	network accreditation. Users may intentionally violate MAC on messages they already have access to, by copying information to new a message and setting a different security label. Any configuration of this security function and all user message operations will be recorded as audit records.
SF.ROLES	Installation and Configuration Guide: No impact.	There are no configuration options for this security function (the commands available to each role cannot be configured), and the security function cannot be disabled.
	Administrator's Guide: Describes how to grant administration access (Ch 9.1 User Templates)	
	User's Guide: No impact.	
SF.SECURE_STATE_RECOVERY	Installation and Configuration Guide: No impact.	There are no configuration options for this security function, and the security function cannot be disabled. Hence, there is no risk of misuse.
	Administrator's Guide: Describes error handling and alarms (Ch 21 Troubleshooting, App A Alarm Descriptors).	
	User's Guide: No impact.	

Security Function	Documents	Analysis
SF.SUBNET_RESTRICTION	Installation and Configuration Guide: No impact.	This security function is disabled by default. Configuration of this security function is recorded to audit records.
	Administrator's Guide: Describes how to restrict which hosts clients may log in from (Ch 9.1 User Templates, Ch 9.6 Users, Ch 10.1 Department Templates, Ch 10.4 Departments).	
	User's Guide: Comments that a user may be unable to access to his mailbox or a department because of a subnet restriction (Ch 3.2.1, 5.2 and 10.2).	
SF.VALIDATE	Installation and Configuration Guide: Describes how to validate the installation media and the integrity of an operational server (Ch 5.1.3).	The administrators may deliberately violate policy by not performing the validation procedures.
	Administrator's Guide: No impact.	
	User's Guide: No impact.	