

TNO Defence Research

TNO Physics and Electronics Laboratory

Oude Waals TD 921906
2507 AK The Hague
P.O. Box 96
2500 JG The Hague
The Netherlands

Fax +31 70 328 09 61
Phone +31 70 326 42 21

TNO-report
FEL-92-B225

copy no.

28

title

Secure Open Systems
An Investigation of current Standardisation Efforts for
Security in Open Systems

AD-A263 575



author(s):

P.L. Overbeek

TDCK RAPPORTCENTRALE

Frederikkazerne, gebouw 140
v/d Burchlaan 31 MPC 16A
TEL. : 070-3166394/6395
FAX. : (31) 070-3166202
Postbus 90701
2509 LS Den Haag

date:

June 1992

classification

title : unclassified
abstract : unclassified
report text : unclassified

DTIC
APR 26 1993
D

All rights reserved.
No part of this publication may be reproduced and/or published by print, photoprint, microfilm or any other means without the previous written consent of TNO.

In case this report was drafted on instructions, the rights and obligations of contracting parties are subject to either the 'Standard Conditions for Research Instructions given to TNO', or the relevant agreement concluded between the contracting parties.
Submitting the report for inspection to parties who have a direct interest is permitted.

TNO

no. of copies :

no. of pages : 28 (excl. RDP and distr. list)

no. of appendices : -

All information which is classified according to Dutch regulations shall be treated by the recipient in the same way as classified information of corresponding value in his own country. No part of this information will be disclosed to any party.

Netherlands organization for applied scientific research

TNO (before a Research consists of the TNO Physics and Electronics Laboratory the TNO Pure Mathematics Laboratory and the TNO Institute for Perception



93 4 26 117

93-08818



The Standard Conditions for Research Instructions given to TNO, as filed at the Registry of the District Court and the Chamber of Commerce in The Hague shall apply to all instructions given to TNO.

report no	FEL-92-B225
title	Secure Open Systems An investigation of current standardisation efforts for security in open systems
author(s)	P.L. Overbeek
institute	TNO Physics and Electronics Laboratory
date	June 1992
NDRO no	-
no in pow '91	709.2
Research supervised by	D.W. Fikkert, H.A.M Luijff
Research carried out by	P.L. Overbeek

=====
A-1

ABSTRACT (unclassified)

This paper outlines the achievements of standardisation in the area of secure open systems. Security in open systems is a special problem since each element in an open system (hardware, networks, operating systems, databases and other applications) must be able to offer security in co-ordination with other elements.

First, a new view on requirements for security is presented. Security requirements are studied from different angles: openness, organisational structures, the value of information and services, social structures and security of the system itself.

Next, the results of our investigation of current standardisation initiatives in the area of technical security in open systems are presented. Main conclusions are:

- 1 None of the initiatives addresses all requirements for secure open systems.
- 2 None of the initiatives gives a solid basis for co-ordination of security between the elements of the open system.
- 3 All initiatives disregard the security functionality that is needed to map normal organisational structures and responsibilities.
- 4 Technical security ignores the needs for security that stem from society.

- 5 The basic security functionality in the system described in the initiatives, is rather divergent and sometimes conflicting. An emphasis is put on prevention, other security measures are neglected to a large extent, and, if addressed at all, they lack structure.
- 6 There is a lack of integration between application security, operating system security and network security. Therefore, an architecture for security functionality is needed that crosses the borders of applications, operating systems and networks.

In the last section a simple model for security in open systems is presented. The aim of this model is to provide a reference framework for the discussion of security in an open systems environment. The building block approach in open systems is underlined: what is to be provided where, and how will the pieces fit together.

This study has been performed as part of the PhD-project SEDIS (Securable Distributed Information Systems). This project aims at a better understanding of and contribution to security in distributed information systems.

This paper is presented at the IFIP/Sec '92 "8th International Information Security Conference and Exhibition", 27-29 May 1992, Singapore.

rapport no : FEL-92-B225
titel : Veilige 'Open Systemen',
Onderzoek en analyse van de huidige standaardisatieactiviteiten voor
beveiliging in 'Open Systemen'
auteur(s) : Ir. P.L. Overbeek
instituut : Fysisch en Elektronisch Laboratorium TNO
datum : juni 1992
hdo-opdr no :
no in rwp '91 : 709.2
Onderzoek uitgevoerd o l v : D.W. Fikkert, ir. H.A.M. Luijff
Onderzoek uitgevoerd door : Ir. P.L. Overbeek

=====

SAMENVATTING (ongerubriceerd)

Dit rapport beschrijft de stand van zaken op het gebied van de standaardisatie voor technische beveiliging in open systemen. Beveiliging in open systemen is bijzonder omdat de elementen van een open systeem (hardware, netwerk, besturingssysteem, applicaties) in onderlinge afstemming en samenhang de noodzakelijke beveiliging moeten bieden.

Allereerst wordt een nieuwe visie op beveiligingseisen gepresenteerd. Beveiligingseisen worden bestudeerd vanuit verschillende invalshoeken: beveiligingseisen die specifiek zijn voor *open* systemen, beveiligingseisen die voortkomen uit maatschappelijke relaties, beveiligingseisen die voortkomen uit de organisatie en de -structuren, beveiligingseisen die zich richten op de bescherming van de waarde van de informatie en de -diensten en de beveiligingseisen voor de veiligheid van het systeem zelf.

Vervolgens worden de resultaten van dit onderzoek naar de standaardisatie-initiatieven op het gebied van de technische beveiliging in open systemen gepresenteerd. De belangrijkste conclusie zijn:

- 1 Geen van de standaardisatie-initiatieven dekt alle beveiligingseisen voor open systemen.

- 2 Geen van de initiatieven biedt voldoende basis voor de afstemming van beveiliging tussen de elementen van een open systeem.
- 3 Geen van de initiatieven biedt functionaliteit voor het representeren van normale organisatie-structuren, taken en verantwoordelijkheden in een systeem.
- 4 Geen van de initiatieven biedt aandacht aan de beveiligingseisen die voortkomen uit maatschappelijke relaties.
- 5 De elementaire beveiligingsfunctionaliteit in de verschillende initiatieven is zeer divergent en soms strijdig met de benadering in andere initiatieven. De nadruk ligt op functies voor preventieve beveiliging. Andere vormen van beveiliging worden grotendeels genegeerd en, als ze al aandacht krijgen, dan is dat op een ad hoc, ongestructureerde wijze.
- 6 Er is te weinig samenhang tussen beveiliging in applicaties, het besturingssysteem en het netwerk. Daar voor is een beveiligingsarchitectuur nodig die de grenzen van applicaties, besturingssysteem en netwerk overstijgt.

In het laatste deel van deze publicatie wordt een eenvoudig model voor beveiliging in open systemen gepresenteerd. Het doel van dit model is om een referentie-kader te bieden voor de discussie over beveiliging in open systemen. In dit model wordt de 'bouwsteen' benadering benadrukt: welke beveiligingsfunctionaliteit moet waar geboden worden en hoe is de samenhang tussen de verschillende beveiligingsfuncties.

Dit onderzoek is uitgevoerd als onderdeel van het promotieonderzoek SEDIS (Securable Distributed Information Systems). Dit project beoogt inzicht te verwerven in, en bij te dragen aan beveiliging in gedistribueerde informatiesystemen.

Dit onderzoek is gepresenteerd op de "8th International Information Security Conference and Exhibition (IFIP/Sec '92)", 27-29 mei 1992, Singapore.

CONTENTS

	ABSTRACT	2
	SAMENVATTING	4
1	INTRODUCTION	7
1.1	Security	7
2	SECURITY REQUIREMENTS REVISITED	9
2.1	Organisation and Security Requirements	9
2.2	Requirements for security of services and information from the perspective of owners and users	10
2.3	Requirements for security imposed by society	10
2.4	Implications for the security requirements for the system	11
2.5	Summary of security requirements	11
3	INITIATIVES IN THE AREA OF SECURE OPEN SYSTEMS	13
3.1	Major initiatives	13
3.2	Other initiatives	14
4	RESULTS OF THE INVESTIGATION	16
4.1	Fulfilment of Security Requirements	16
4.2	How do different initiatives fit together?	18
4.3	Summary of conclusions from this investigation	20
5	A COMMON UNDERSTANDING OF SECURE OPEN SYSTEMS: THE FIRST STEP	21
5.1	An open system	22
5.2	A simple model for security in open systems	22
5.3	Conclusion	24
6	ACKNOWLEDGMENTS	25
7	ACRONYMS	26
8	REFERENCES	27

1 INTRODUCTION

Currently, there is a drive towards *open systems*. There is no agreed definition of what an *open* system should be. Regrettably, it shares this with many terms in high-fashion information technology. During the mid-eighties, *open* was equivalent to Open Systems Interconnection (OSI) [5]. Later on the discussion focussed on UNIX as an *open* operating system. Just a few years ago, the development of standard interfaces between applications and (proprietary or 'closed') operating systems gave us a new view on *open-ness*. A hardware architecture is said to be *open* when its interfaces are available to all interested parties. Recently, the so-called fourth-generation languages were introduced. The suppliers claim that these languages enable the development of *open* software, which means software that is independent of, say, a specific database management system.

Thus, *open* appears to be a moving target. In general, the following relate to *open*:

- Properly defined interfaces, services and protocols.
- The availability of these definitions to third parties.

Following the literature, the term *open* is used in this paper in combination with elements of a system like hardware, networks, operating systems, databases and other applications.

1.1 Security

The elements of an *open* system must not only be able to coexist with one another but should also be able to benefit from one another and offer a concerted "value added" effort. This also implies the co-ordination of security between the elements of an *open* system and consistency of security within an element.

It must be assumed, and this is not specific to *open* systems, that the information-technology infrastructure is shared with unreliable and unpredictable participants (computers, networks, users and software). Currently, information flow is not restricted to one specific computer system or network and not even to any specific application. Information security must secure the information at all times and ubiquitously. Therefore all information flow also must be secure. In order to achieve this in an *open*-systems environment, all elements of the *open* system must seamlessly fit together: standardisation is essential.

This paper outlines the achievements in the area of secure open systems. First, requirements for secure open systems are discussed. Next, the results of our investigation are presented. This investigation concentrates on technical security. In the last section a simple model for security in open systems is presented. The aim of this model is to provide a reference framework for the discussion of security in an open systems environment.

2 SECURITY REQUIREMENTS REVISITED

In this section, the security requirements for (open) information systems are studied from different angles. First, security requirements that come from organisational considerations are discussed. Next, the security requirements for information and services in the system are addressed, seen from the perspective of the users. These perspectives are chosen in such a way that all relationships that influence the security requirements for a system are covered.

The security requirements for *open* information systems are not different from those of other information systems. The difference between open and other systems is in the implementation of the requirements. An open system may consist of many elements (hardware, networks, operating systems, databases and other applications). Each element in an open system must be able to offer security in concert with other elements.

2.1 Organisation and Security Requirements

2.1.1 Security must fit the organisational structure

Each employee performs one or more roles (or: functions) in the organisation. He has been assigned tasks and responsibilities by the management of that organisation. Managers must be able to control the tasks for which they are responsible. For this, they need management information about these tasks. Management tasks are special since they influence the tasks and responsibility assignments directly. Examples of management tasks are: definition of new tasks, authorisation of tasks to employees, auditing of the continuation of the assigned tasks, modification of task definitions, reassignment of tasks, termination of tasks and withdrawal of responsibilities.

The security offered by the information systems used by an organisation must fit the security requirements of that organisation. Therefore, it must be possible to express the employees' responsibilities and tasks in the real organisation in these information systems.

2.1.2 Representation of roles in a system

The 'real life' roles are to be translated into roles in the system.

- An employee is represented in the system by one or more processes acting on his behalf (sometimes these processes are somewhat misleadingly called 'the user').

- Tasks are performed using services offered by the system. To enable an employee to perform his tasks, he is allowed (or constrained) to use certain services offered by the system. Through these services, he is able to access information.
- Responsibilities are translated into rights and duties in the system.
- Task management implies that, using a management service, rights and duties to perform services are (re-)assigned to employees. The progress of the tasks may be checked by means of a management service, giving aggregated task information.

2.2 Requirements for security of services and information from the perspective of owners and users

Information and services are valuable and therefore need be secured. Their value is largely determined by the well known properties *confidentiality*, *integrity* and *availability*. Information security also must reflect the needs of the organisation. Therefore, the relative value of the information to the organisation must be taken into account when security measures are selected. Security measures are most commonly subdivided into organisational, technical, physical and procedural security measures. Another approach is to look at a chain of security measures that address a (possible) breach of security (a *security event*). We have identified six types of measures. First, the occurrence of an event can be excluded or prevented by *preventive* measures. At the same time, the possible loss resulting from an anticipated event can be minimised by *reductive* measures. When an event has occurred, it must be discovered. This is done by *detective* measures. *Repressive* measures stop the continuation or recurrence of an event, thus reducing losses. Next, the information and services are restored as well as possible by *corrective* measures. Finally, it is worthwhile to *evaluate* the effectiveness of the security measures.

2.3 Requirements for security imposed by society

All organisations are part of social structures and are influenced by external relations. Examples are relations with: shareholders, management of the holding company, external accountants or auditors, judiciary, (for banks:) the national central bank, external users (clients, suppliers) and relations with the people that are registered. These are all external parties that are involved in the way an organisation handles its information systems. The resulting demands will impact the security requirements for the information systems.

Examples are:

- External clients may demand *anonymity*, while the service-providing organisation needs accountability (specifically billability).
- In supplier/purchaser relations, *proof of transactions* might be required.
- Many countries have legislation which regulates the *privacy* of information, implying technical security, amongst others. Privacy is an aspect both for the registrees as well as those using the system (to what extent is it permissible to analyse the activities of employees?). Note that privacy encompasses both confidentiality and integrity of personal data.
- In many cases information about the information system itself and the security of the information system is required by external parties. This may concern the *proof of proper functioning* of the system (does it offer the correct figures?) and proof of certain activities (will the audit file be usable to provide *legal proof* of an action?).

2.4 Implications for the security requirements for the system

One of the key issues to security as seen from the system is that the system does not (have to) trust its users *a priori*. Furthermore, the system must be able to maintain its own security to some extent. Therefore, the system has to control the use of services (which might be trusted by the system or not). In doing so, access to information as well as other services is controlled. Every security-relevant action is mapped against the assigned rights and duties of the user. The scope of what a security-relevant action is depends on the *granularity* in the system, i.e. the definition of what can/must be managed as a whole, seen from the stand-point of security. The granularity is determined by the units of information that can be managed individually (data field, record, file, database, filestructure, etc.) as well as the active entities that can be distinctly managed in the system (e.g. processes, applications, services, 'pipes').

By controlling all security-relevant actions, the system is able to maintain a safe situation. In doing so, it is also able to secure itself, which is essential for continuation of the secure situation.

2.5 Summary of security requirements

In the next section the results of our investigation of current standardisation initiatives in the area of secure open systems are presented. Each of the identified initiatives is studied using the following check-list to see which security requirements are addressed.

Security requirements regarding openness:

- An open system may consist of many elements (hardware, networks, operating systems, databases and other applications). It is required that each element in an open system is able to offer security in co-ordination with other elements.

Security requirements that stem from organisational considerations:

- It must be possible to represent organisational structures and the users' real-life tasks and responsibilities in the system. Considerations are: the representation of an employee in the system; the mapping of tasks to services by which information can be accessed and/or handled; the mapping of responsibilities to rights and duties in the system; the mapping of management tasks to services in the system.

Security requirements that regard the value of information:

- Information and services are valuable and therefore need be secured. Their value is determined by the properties confidentiality, integrity and availability.
- The security measures must reflect the value of the information. In the chain of security measures that address a possible security event we recognise measures that aim at prevention of an event, reduction of the consequential losses of an anticipated event, detection, repression and correction of a security event and evaluation of security events.
- It is required that users can trust the system.

Requirements for security imposed by society:

- All organisations are part of social structures and are influenced by external relations. This will result in consequential security requirements for the information systems. Examples are: anonymity, accountability, proof of a transaction, privacy, proof of proper functioning and legal proof.

Security requirements for the security of the system:

- The system must be able to maintain its own security. Therefore, the system must be able to control every security-relevant action (involving services or information). The granularity in the system is a yardstick for what should be a security-relevant action. Security information is needed about the information in question, the assignment of rights and duties concerning the identified user, the service and the information as well as security information about other ongoing activities in the system.

3 INITIATIVES IN THE AREA OF SECURE OPEN SYSTEMS

For the purpose of this investigation a considerable amount of documents was studied. First an inventory of ongoing standardisation activities in the area of security took place. Many sources were used for this inventory, most notably [13] and [4]. Next, all documents that offered or supported (part of) an architecture for security in open systems were studied, varying from provisional drafts to definite international standards.

The study showed that there is a tremendous amount of effort going on in the area of security. Nevertheless, there is only a limited number of activities that address, directly or indirectly, open systems. These are briefly introduced in the following section. The initiatives, in as far as they are not generalised, are grouped in the following areas: applications, operating systems and networks.

3.1 Major initiatives

3.1.1 Application area

In the area of security offered by applications, more or less in cooperation with the operating system, many initiatives are taking place. The most important initiatives are:

- The "Framework for Secure Open Systems" is produced by the ECMA [12]. This framework addresses the requirements and concepts for the provision of security in open distributed systems. Although the approach is suitable to be applied more generally, the security services are merely focussing on the applications.
- Security in OSI applications is primarily addressed by the OSI and the CCITT. Applications like Electronic Data Interchange (EDI) [3], The Directory (X.500) [9] and Message Handling Systems (MHS) [8] provide interfaces to add security services at a later stage.
- The Trusted Database Interpretation (TDI) [14] of the Trusted Computer System Security Evaluation Criteria (TCSEC) is developed by the American National Computer Security Center (NCSC). The TDI focuses on security in applications in general and database management systems in particular.

3.1.2 Operating Systems

- Evaluation criteria for security in operating systems are defined in the Trusted Computer System Evaluation Criteria (TCSEC) [2]. The TCSEC has been produced by the DoD / NCSC (Department of Defense / National Computer Security Center). The TCSEC contains different sets of evaluation criteria for security which in practice work as design criteria. It has had, and still has, a tremendous impact on the security of operating systems.
- The development of the Portable Operating System Interface for Computer Environments (POSIX) [12] has been driven by the Institute of Electrical and Electronics Engineers (IEEE). The POSIX initiative aims at defining a standard interface set for applications. This interface set is to be offered by the operating system. The purpose of the Security Interface of POSIX is to define a standard interface for applications that require a secure environment.

3.1.3 Networks

- Most important for security in networks is the Open Systems Interconnection (OSI) Security Architecture [6]. It describes security services, mechanisms and the recommended placement of these within the OSI layers.
- For security in networks the NCSC has developed the Trusted Network Interpretation (TNI) of the TCSEC [15].

3.1.4 General

- Four European countries, France, Germany, The Netherlands and the United Kingdom, are harmonising criteria for the evaluation of security in information technology products. The result of this effort is the Information Technology Security Evaluation Criteria (ITSEC), a framework for the evaluation of technical security [7]. The development of the ITSEC is supported by the Commission of the European Communities.

3.2 Other initiatives

Initiatives of other organisations also have been studied. These initiatives either not address technical security at an architectural level or use an approach that is derived or adopted from one of the initiatives mentioned above.

The work of the following groups was studied: ISO JTC1 SC27 "Security Techniques", CCITT Subgroup VII/Q19 (security framework for distributed applications), ISO JTC1 SC21 "Information Retrieval, Transfer and Management for OSI" (security models, frameworks and management), ISO TC 68 "Banking and Related Financial Services" (standards for security for

inter-bank communications), ISO JTC1 SC18 "Text and Office Systems" (security in the Office Document Architecture), the IEEE 802.10 program "Standard for Interoperable LAN Security" (LAN security in the lower OSI layers), NATO (NATO OSI Security Architecture), Massachusetts Institute of Technology Athena project (Kerberos), the Open Software Foundation, the X/Open group, the USA Open Implementors Workshop, the Independent European Programme Group (PCTE), the European Telecommunications Standards Institute and, finally, the European Workshop for Open Systems.

4 RESULTS OF THE INVESTIGATION

This paper can only give a brief presentation of the results of this investigation. The full report is available as [10]. Firstly, the possibility to fulfil the security requirements with one of the initiatives studied is discussed. Secondly, the relations between the initiatives are discussed as well as the possibility for a coexistence of different approaches in one system. Finally, it is discussed which combinations may be mutually beneficial and may offer a good basis for secure open systems.

4.1 Fulfilment of Security Requirements

Security requirements regarding openness:

For their security, the elements of an open system depend on each other to a large extent. None of the initiatives provides a solid basis for the distribution of security functionality between the elements of an open system (networks, operating systems, databases and other applications). Also missing is the possibility to exchange security information between the elements of the open system. From this, it follows that an element of an open system has no knowledge of the provision of security in its environment. This is a serious problem since most of the elements of an open system are unable to provide the required security by themselves.

However, some of the initiatives (most notable: the ECMA Framework) suggest the concept of *security domains* (a technically bounded group of manageable entities to which a single security policy applies) on a per-element basis. This concept may be a suitable basis to offer services for the exchange of security information and distribution of trust between the elements of the open system. Moreover, the TDI introduces the concept of TCB subsets. TCB subsets enable the local provision of security in the operating system or in an application.

Requirements for information security that stem from organisational considerations:

None of the initiatives addresses relations between the tasks of an employee in real life and his/her work using the system (whether the system is stand-alone or in a network). The same holds for the mapping of real-life responsibilities to the system.

All the initiatives completely disregard the security functionality that is needed to map normal organisational structures and responsibilities.

Demands from society for information security:

None of the initiatives acknowledges security requirements that stem from relations with society. Services for privacy, legal or other proof of correct functionality and anonymity are not considered (an exception is DAF-security which identifies a need for anonymity).

Technical security seems to ignore the needs for security that stem from society.

Basic security functionality in the system

Authentication

- Authentication of users is commonly done on a per-computer-system basis (limited to one operating system at one end system). Authentication that can be used over more computer-systems in a network only is addressed in the approaches of the ECMA Framework and Kerberos. Authentication that can be used both in operating systems and applications is addressed in the TDI.
- Many of the initiatives disregard the need for authentication of active entities other than users (applications, services, processes). The need for authentication of passive entities (entities that are being accessed) is disregarded as well. The ECMA Framework is an exception to this.

Management

None of the initiatives offers a structured approach to the management of security information. Only OSI provides a mechanism for the management of security information in its Management Framework.

The properties of information

- Confidentiality is present in all initiatives.
- Integrity is addressed in most of the initiatives. Some of the initiatives suggest an approach that may be applicable to others as well (e.g. basing access-control-decisions on the triplet USER/APPLICATION/INFORMATION).
- Availability is not regarded as an important issue (except by the TNI).

Security measures

- Prevention is the starting point for security in all initiatives.
- Reduction is scarcely addressed and if at all, in an unstructured way.
- In most initiatives detection is synonymous with audit which is always *post factum* and often belated.
- Repression is hardly addressed and if addressed at all, it is incomplete and in an unstructured way.

- Correction is addressed by some of the initiatives, but not in a structured way and with insufficient detail.
- Evaluation is not addressed at all.

From the above it can be concluded that emphasis is put on prevention and that other security measures are neglected to a large extent, and, if addressed, they lack structure.

Mutual trust

The users of the system have no means to assure themselves of the proper behaviour of the system. In most cases, the system does not have to trust its users. Some of the initiatives assume that this unbalanced situation is corrected by physical and organisational security measures. In most of the initiatives this problem is disregarded.

4.2 How do different initiatives fit together?

The initiatives are sorted on the specific aspect they address: application security, operating systems security and network security. In most systems these are all needed together. It is discussed which initiatives do and do not fit well in one system. In some cases, the initiatives take conflicting approaches, in others, a combination of approaches might be of mutual benefit. First, it is noted that the ITSEC is not listed below. The ITSEC is a general framework for the specification of security provisions in a TOE. Therefore, it does not show a specific relationship with any of the initiatives, nor does it conflict with any of them.

Application-dependent security

Some standards for applications offer hooks to add security functionality at a later stage. The placement of these hooks restricts the security services that can be offered.

All the applications studied are OSI-oriented. However, there is no relation between the security offered by these applications and the security that is available through the OSI Security Architecture (fortunately, there is no conflict either).

Application-dependent security might easily conflict with the TCSEC approach. Firstly, the security functions that are offered via the hooks of the (non-trusted) applications lie partly outside the Trusted Computing Base (TCB, the bounded group of all security-enforcing functions). The TCSEC approach demands that all security-enforcing functionality should be inside the TCB. Secondly, and even more important, OSI applications may cause uncontrolled information flow and frustrate the TCSEC Formal Security Policy (or relaxed versions thereof that can be found in other initiatives).

Applications and Operating System or Networks

The ECMA approach conflicts in many aspects with the TCSEC approach. To name the most important ones: the TCSEC needs a Trusted Computing Base where the ECMA approach chooses distributed security based on cryptographically protected credentials. Secondly, the ECMA Facilities do not offer the TCSEC 'control objectives'. Thirdly, the ECMA approach offers freedom of choice of a security policy whereas the TCSEC imposes the Bell - LaPadula policy.

The TDI offers an integrated approach to security in applications and the operating system. Some of the concepts of the TCSEC, on which the TDI is built, had to be extended. It is not easy to extend the TDI approach to networks. The TDI does not match the OSI SA.

The POSIX Security Interface matches with the TCSEC in many aspects. Nevertheless, the POSIX Security Interface collides with the TCSEC in the enforcement of privileges without using the mediation of the TCB-enforcing functions. The POSIX Security Interface offers (even) less security services than the TCSEC and does not offer all of the control objectives of the TCSEC. Network security is not addressed at all by the POSIX Security Interface.

None of the initiatives shows a clear relation to the TNI approach.

Operating System and Network

The TCSEC addresses end systems and not networks. OSI addresses networks and not end systems. It is clear that these two must be fitted together, given the fact that they will have to coexist in one system since both operating system security and network security are needed. From this report it is concluded that there may be a possibility in the combination of the reference monitor databases and the local part of the SMIB.

The TNI approach aims at offering network security but it does not offer a clear connection with the end systems security (which is the TCSEC-environment).

4.3 Summary of conclusions from this investigation

None of the initiatives addresses all security requirements for secure open systems. Some of them provide a good starting point, especially those that do not exclude additional security services. Some initiatives fit better together than others.

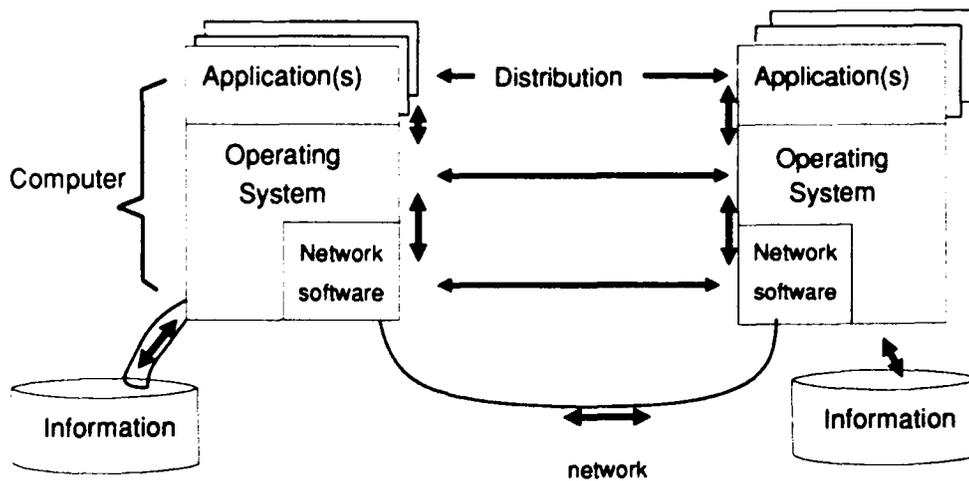
The most promising starting point for a basis for secure open systems is the combination of the standards of ECMA and OSI SA, including the use of supporting standards (like X.500 and Kerberos). The problem of integrating application and operating system security must be solved (the TDI TCB subset may provide a suitable mechanism).

It is concluded that there is a lack of integration between application security, operating system security and network security. For the purpose of integration of security, an architecture for security functionality and interfaces is needed that crosses the borders of applications, operating systems and networks.

5 A COMMON UNDERSTANDING OF SECURE OPEN SYSTEMS: THE FIRST STEP

One of the conclusion of our investigation is that none of the initiatives gives a solid basis for coordination of security between the elements of the open system (networks, operating systems, databases and other applications).

In our view, it would prove beneficial to develop a common understanding of what is required to provide security in open systems. Later in this section, we present a simple model for security in open systems, as a first step.



The horizontal arrows represent communication between peers at the same abstraction level. The communication concerns distribution of information and/or services. There is no direct communication between peers, except at the lowest level. The vertical arrows denote the actual route of the flow.

Figure 1: Elements of an open system

5.1 An open system

Figure 1 shows the elements of an open system. Applications offer the services that present and give access to information for the users. The applications have access to the information via the operating system. Also, communication with other applications takes place via the operating system. The operating system hides configuration and manufacturer dependent characteristics from the applications (and the users). The abstraction level is different from that of the applications in the sense that the operating system does only handle 'structured data' without knowing its meaning. The network is one of the configuration specific characteristics that is hidden by the operating system. The network can be seen as a common configuration specific element of the connected operating systems.

5.2 A simple model for security in open systems

Communication between applications is based upon a peer-to-peer relation. The security of this communication must also be based on this peer-to-peer relation. These peer-to-peer relations also exist between communicating operating systems and between communicating network entities. Security based on peer-to-peer relations is called *horizontal security*, since it is having the same level of abstraction.

Generally, there is no *direct* communication between peers. Two applications can only exchange information through the operating system and devices, possibly using the network. So the communication takes place through several layers. The security that is needed to secure the communication between the layers is called *vertical security*. *Vertical security* is a prerequisite for *horizontal security*.

Note that, whatever form of technical security, some minimal physical security will always be needed.

Horizontal security requires security between communicating applications, as well as security between communicating operating systems and security between communicating network entities. Vertical security implies that security between application and operating system, as well as security between operating system and the network must be defined.

The figure 2 shows security domains in an open system. A security domain is defined as a technically bounded group of manageable entities to which a single security policy applies. Each domain is defined to encompass exactly one element of an open system.

This straightforward model provides a basis to discuss the following issues:

- 1 Security functionality and management may be available *in* each domain. A suitable starting point is to identify the granularity of the entities that can be managed individually within the domain.
- 2 Security functionality may be needed between peer-domains. This is the horizontal security.
- 3 The 'higher' domains require security functionality from the 'lower' domains.
- 4 The 'lower' domains must be able to notify to the 'higher' domains the security functionality they can offer.

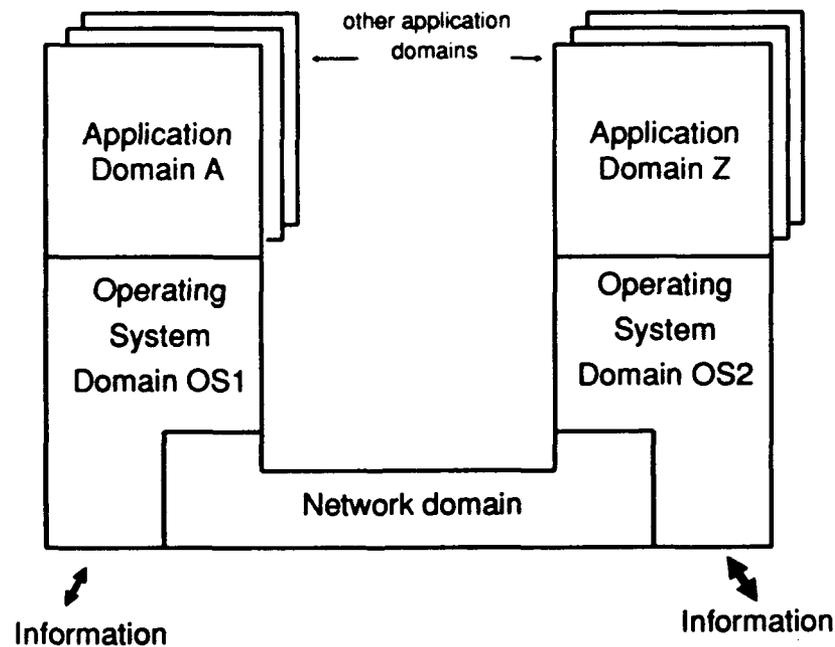


Figure 2: Security domains in an open system

5 The integrity of a domain may be depending on the security that is offered by a 'lower' domain. To secure the 'lowest' domains, some physical security may be required.

As input for the first issue the list of requirements given in section 2.5 can be used. Issues 2 to 4 ask for properly defined interfaces, services and protocols (similar to OSI).

In our view, it should be possible to group domains together to make super-domains. This may lead to client-server domains (a combination of peer domains). In the same way a sub-domain may be defined, e.g. a partition of the network. Finally, it is foreseen that non-technical security domains, e.g. the group of employees of a department, will 'interface' with the technical domains.

5.3 Conclusion

The aim of this model is to provide a reference framework for the discussion of security in an open systems environment. The five issues in the previous paragraph underline the building block approach in open systems: what is to be provided where, and how will the pieces fit together? The model is kept simple and details are avoided at this time of the discussion. By doing so, we hope that this model will help in bringing back the discussion of the provision of security in open systems to more manageable proportions.

6 **ACKNOWLEDGMENTS**

The author wishes to thank prof. dr. I.S. Herschberg, J. Heijnsdijk (Delft - University of Technology) and H. Luijff (TNO Physics and Electronics Laboratory) for their valuable support in the preparation of this paper.

7 ACRONYMS

The following acronyms are used within this paper.

CCITT	Comité Consultatif International Télégraphique et Téléphonique
DAF	Support Framework for Distributed Applications
DoD	USA Department of Defense
ECMA	European Computer Manufacturers Association
EDI	Electronic Data Interchange
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organisation for Standardisation
ITSEC	Information Technology Security Evaluation Criteria
JTC	Joint Technical Committee
LAN	Local Area Network
MHS	Message Handling Systems
NATO	North Atlantic Treaty Organisation
NCSC	USA National Computer Security Center
NIST	National Institute for Standards on Technology
NOSA	NATO OSI Security Architecture
OSI	Open Systems Interconnection
POSIX	Portable Operating System Interface for Computer Environments
SC	Sub Committee
SILS	Standard for Interoperable Local Area Network Security
SMIB	Security Management Information Base
TC	Technical Committee
TCB	Trusted Computing Base
TCSEC	Trusted Computer System Evaluation Criteria (Orange Book)
TDI	Trusted Database Interpretation (Grey Book)
TNI	Trusted Network Interpretation (Red Book)

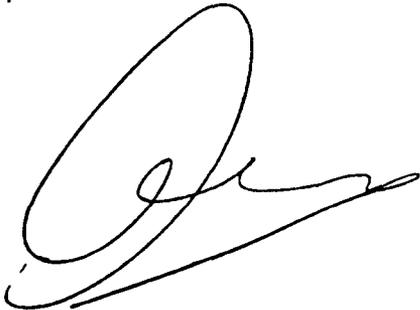
8 REFERENCES

- 1 DAF: Security, CCTTT Support Framework for Distributed Applications (DAF), DAF: Working Document on Security, version 4, May 1989
- 2 Department of Defense Trusted Computer System Evaluation Criteria, DoD 5200.28 STD. (TCSEC or Orange Book), December 1985
- 3 Electronic data interchange for administration, commerce and transport (EDIFACT), ISO 9735:1988
- 4 Guide to Open System Security, ISO/IEC JTC1/SC21 N6765, February 1992
- 5 Information Processing Systems - Open Systems Interconnection - Basic Reference Model, ISO 7498:1984
- 6 Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture, ISO 7498-2:1988
- 7 Information Technology Security Evaluation Criteria, ITSEC version 1.2 (provisional), ISBN 92-826-3004-8, June 1991
- 8 Message Handling Systems, CCITT Recommendation X.400-X.430 (1988)
- 9 Message Oriented Text Interchange Systems (MOTIS), ISO/IEC DIS 10021, May 1988
- 10 Secure Open Systems - An Investigation, Overbeek P.L., December 1991, available as TNO Report FEL-91-B293
- 11 Security in Open Systems - A Security Framework, ECMA TR/46, July 1988
- 12 Security Interface for POSIX, IEEE P1003.6/D7, August 1990
- 13 Taxonomy for Security Standardisation, CEN/CENELEC Security Group, CSecG/49/90, (also available as SC27 N173 and JTC1 N1040), September 1990
- 14 Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria, (TDI or Grey Book), USA National Computer Security Center, April 1991, NCSC-TG-021, library no. S235.625
- 15 Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, (TNI or Red Book) NCSC-TG-005, lib.nr. S228,526 Version 1, July 1987



D.W. Fikkert
(project manager)

H.A.M. Luijff
(supervisor)



P.L. Overbeck
(author)

REPORT DOCUMENTATION PAGE

(MOD-NL)

1 DEFENSE REPORT NUMBER (MOD-NL) TD92-1906	2 RECIPIENT'S ACCESSION NUMBER	3 PERFORMING ORGANIZATION REPORT NUMBER FEL-92-B225
4 PROJECT/TASK/WORK UNIT NO 20555	5 CONTRACT NUMBER -	6 REPORT DATE JUNE 1992
7 NUMBER OF PAGES 28 (excl RDP & distr.list)	8 NUMBER OF REFERENCES 15	9 TYPE OF REPORT AND DATES COVERED FINAL
10 TITLE AND SUBTITLE SECURE OPEN SYSTEMS AN INVESTIGATION OF CURRENT STANDARDISATION EFFORTS FOR SECURITY IN OPEN SYSTEMS		
11 AUTHOR(S) OVERBEEK P.L.		
12 PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) TNO PHYSICS AND ELECTRONICS LABORATORY, P.O. BOX 96864, 2509 JG THE HAGUE, THE NETHERLANDS		
13 SPONSORING/MONITORING AGENCY NAME(S) TNO PHYSICS AND ELECTRONICS LABORATORY, P.O. BOX 96864, 2509 JG THE HAGUE, THE NETHERLANDS		
14 SUPPLEMENTARY NOTES		
15 ABSTRACT (MAXIMUM 200 WORDS, 1044 POSITIONS) THE ACHIEVEMENTS OF STANDARDISATION IN THE AREA OF SECURE OPEN SYSTEMS ARE OUTLINED. SECURITY IN OPEN SYSTEMS IS SPECIAL SINCE EACH ELEMENT IN AN OPEN SYSTEM (HARDWARE, NETWORKS, OPERATING SYSTEMS AND APPLICATIONS) MUST BE ABLE TO OFFER SECURITY IN CO-ORDINATION WITH OTHER ELEMENTS. A NEW VIEW ON REQUIREMENTS FOR SECURITY IS PRESENTED. SECURITY REQUIREMENTS ARE STUDIED FROM DIFFERENT ANGLES: OPENNESS, ORGANISATIONAL STRUCTURES, THE VALUE OF INFORMATION AND SERVICES, SOCIAL STRUCTURES AND SECURITY OF THE SYSTEM ITSELF. NEXT, THE RESULTS OF THE INVESTIGATION OF CURRENT STANDARDISATION INITIATIVES IN THE AREA OF TECHNICAL SECURITY IN OPEN SYSTEMS ARE PRESENTED. ONE OF THE CONCLUSIONS IS THAT THERE IS A LACK OF INTEGRATION BETWEEN APPLICATION SECURITY, OPERATING SYSTEM SECURITY AND NETWORK SECURITY. AN ARCHITECTURE FOR SECURITY FUNCTIONALITY IS NEEDED THAT CROSSES THE BORDERS OF THESE ELEMENTS OF AN OPEN SYSTEM. IN THE LAST SECTION A SIMPLE MODEL FOR SECURITY IN OPEN SYSTEMS IS PRESENTED TO STIMULATE THE DISCUSSION OF SECURITY IN AN OPEN SYSTEMS ENVIRONMENT. THE BUILDING BLOCK APPROACH IN OPEN SYSTEMS IS UNDERLINED: WHAT IS TO BE PROVIDED WHERE, AND HOW WILL THE PIECES FIT TOGETHER. THIS STUDY HAS BEEN PERFORMED AS PART OF THE PHD-PROJECT SEDIS (SECURABLE DISTRIBUTED INFORMATION SYSTEMS). THIS PROJECT AIMS AT A BETTER UNDERSTANDING OF AND CONTRIBUTION TO SECURITY IN DISTRIBUTED INFORMATION SYSTEMS. THIS PAPER IS PRESENTED AT THE 8 th INTERNATIONAL INFORMATION SECURITY CONFERENCE AND EXHIBITION (IFIP/SEC '92), 27-29 MAY 1992, SINGAPORE.		
16 DESCRIPTORS INFORMATION SYSTEMS SECURITY DISTRIBUTED NETWORKS STANDARDISATION	IDENTIFIERS	
17a SECURITY CLASSIFICATION (OF REPORT) UNCLASSIFIED	17b SECURITY CLASSIFICATION (OF PAGE) UNCLASSIFIED	17c SECURITY CLASSIFICATION (OF ABSTRACT) UNCLASSIFIED
18 DISTRIBUTION/AVAILABILITY STATEMENT UNLIMITED	17d SECURITY CLASSIFICATION (OF TITLES) UNCLASSIFIED	