MANAGEMENT OF SECURE SYSTEMS AND SECURITY WITHIN OSI[1]

Chris J. Mitchell
Computer Science Department
Royal Holloway and Bedford New College
University of London
Egham Hill
Egham
Surrey TW20 0EX
England

[1] This is a minimally reformatted version of the text of 4th June 1990.

1 INTRODUCTION

With the growth in distributed information processing systems, security of information is a requirement of rapidly growing importance. Management of the security infrastructure is one of the most difficult aspects of information security provision. This paper reviews the most important aspects of the security management problem, including the development of security policies. The need for security in multi-vendor systems makes the security problem more difficult, and is forcing the growth of standardised security solutions within the OSI framework. Recent developments in the security standardisation field are reviewed.

The main topics (namely management and standards) are covered in sections 3 and 4 of this paper. Preliminary to these discussions, in Section 2 a brief review of the OSI 7-layer model is given in order to set subsequent remarks in context.

2 THE OSI 7-LAYER MODEL

The aim of Open Systems Interconnection (OSI) is to provide a standardised means of communication between diverse computer systems. As a basis for the development of OSI standards, ISO have developed a Reference Model to partition the problem into discrete layers, and to provide a conceptual framework for understanding the complex problems involved.

The Reference Model has seven layers; from the 'bottom up' they are as follows:

1. Physical Layer
2. Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

The Reference Model specifies the functionality of each layer and the interfaces between adjacent layers. It also defines methods for achieving layer-specific functionality between cooperating computer systems.

The lowest three layers (Physical (1), Data Link (2) and Network (3)) are concerned with the provision of data transmission. The Physical Layer models the interface of a computer system to the physical medium. It includes such aspects as physical connectors and voltage levels. The Data Link Layer provides a framework around data for transmission by the Physical Layer; detection and correction of errors may be performed by this layer. The Network Layer is particularly concerned with routing and relaying. The services offered by the Network Layer to the Transport Layer conceal from it the numbers and types of sub-network that may be involved in the communication.

The Transport Layer (4) operates end-to-end between computer systems and is concerned with Quality of Service. The Transport Layer is responsible for providing the Session Layer with a reliable data transmission service.

The Session Layer (5) assumes reliable data transmission services between computer systems (i.e. end-to-end communications). It occupies the area between the application-oriented upper layers (6 and 7) and the 'real-time' data communication environment. It provides services for the management and control of data flow between two computer systems.
s
The function of the Presentation Layer (6) is to provide a common representation of information whilst in transit between computer systems.

The Application Layer (7) provides the communication-based service to end users. The other six layers of the model exist to support and make possible the activities that take place at the Application Layer.

For further information about OSI see, for example, Henshall and Shaw's book, [6].

3 MANAGEMENT OF SECURE SYSTEMS

3.1 Introduction

We use the term 'management of secure systems' to embrace a broad set of activities relating to the provision of security in information processing and transmission systems. In particular we include all aspects of secure system design, implementation and continuing management. As such, security management is a subject of considerable depth and complexity, and we can only give a brief overview of the main points of the subject here. Before considering certain aspects of the security management process in more detail, we briefly review the security life cycle of a system.

The first part of this cycle (as is true for all system design procedures) is the requirements analysis, which should always precede any system design step. Probably the most important component of any analysis of requirements is an assessment of threats to the system. Security is a meaningless term in isolation; one can only secure a system against a known set of threats. Published methodologies for this analysis exist and are well-used in the computer security field; a well-known example is provided by CRAM.

Apart from the need to meet known threats, there are also possible governmental, legal and standards/interworking requirements. These include such things as specific levels of protection for stored and communicated personal data (e.g. the Data Protection Act) and required levels of assurance that specified services are provided as specified.

Having listed the requirements for the security system, the next step is the definition of security services to meet the perceived threats. Typical security services include: access control (mandatory and discretionary), security audit, user authentication and communications security services such as confidentiality, authentication, integrity and non-repudiation. As well as these explicit services, assurance requirements may necessitate the use of 'pervasive security services' such as the use of trusted hardware.

Next comes the design/implementation step. This involves the selection of appropriate security mechanisms to provide the necessary security services. In practice this usually means the selection of appropriate security products. Apart from selecting products with the appropriate functionality, it will often also be necessary to decide what level of assurance is required that the products provide the claimed services. In the case of government systems this will often be defined by the relevant guide-lines (e.g. in the U.S. by the 'Orange Book', [3]).

Finally there is the major 'continuing management' task, aspects of which include audit, key management and event handling (topics which are covered in more detail below). This includes any necessary changes to the system, which will involve repeating the above cycle.

It is interesting to note how many of the components of system security management have close parallels in other system management activities (such as system accounting and system configuration). Indeed, much of security management can be considered as one part of the system management function. However, the system management itself will often need to be secured, placing some security functions at a different level.

3.2 Security domains and policies

When designing a security system it is fundamentally important to define the scope of the system and to lay down the criteria underlying its operation. The terms security domain and security policy are widely used to describe these concepts. More precisely, the OSI security architecture, ISO 7498-2, [9], defines a security policy as 'the set of criteria for the provision of security services'. A security domain is then simply the scope of a single security policy.

In the context of the system security life-cycle defined above, the definition of the security policy will be in response to the initial requirements analysis, and will dictate both the security services to be provided and how they should be applied. It will also indicate how the continuing security management process should function. Most threats involve the notion of authorised and unauthorised behaviour, e.g. access to data and resources. A generic security policy given in ISO 7498-2, [9] is as follows:
Information may not be given to, accessed by, nor permitted to be inferred by, nor may any resource be employed by, those not appropriately authorised.
The way in which authorisation is given distinguishes various types of policy.

The OSI security architecture distinguishes between two types of security policy, namely identity-based security policies and rule-based security policies. An identity-based policy is based on the identities and/or attributes of users and resources being accessed. A rule-based policy is based on global rules imposed on all users; these rules typically rely on a comparison of the sensitivity of resources with attributes belonging to users wishing to access them. There is a further distinction to be drawn between administration-imposed and dynamically-selectable security policies (c.f. mandatory and discretionary access control services).

3.3 OSI security management

Clause 8 of ISO 7498-2, [9], defines security management as the control and distribution of information for use in providing security services and mechanisms and reporting on security services, security mechanisms and the occurrence of security-related events. Thus the distribution of access rights information to enable an entity to make a connection is part of security management.

ISO 7498-2 also introduces the concept of a Security Management Information Base (SMIB) as a store for all security-relevant information needed for security management. Conceptually, although not necessarily in practice, this SMIB will be part of the Management Information Base (MIB). In a distributed system each end system will often need to carry local security information to enable it to enforce the prevailing security policy; thus the SMIB will often be distributed over the end systems. SMIBs may take a large variety of forms, e.g.
* tables of data;
* files;
* data or rules embedded within software and/or hardware.

ISO 7498-2 identifies four different categories of OSI security management activity:
* system security management,
* security service management,
* security mechanism management, and
* security of OSI management.

We now consider each of these aspects in turn.

System security management is concerned with management of the security aspects of the entire system. Typical activities include:
* security policy management;
* interaction with other OSI management functions (e.g. accounting, fault management, configuration, etc.);
* interaction with security service management and security mechanism management;
* event handling management (e.g. reporting of apparent attempts to violate system security, modification of thresholds used to trigger event reporting, etc.);
* security audit management (see 3.4 below);
* security recovery management (e.g. maintenance of rules used to respond to security violations, security administrator interactions, etc.);
* access control policy management.

Security service management is concerned with management of particular security services, e.g. confidentiality, authentication, etc. Typical activities include:
* selection of the security mechanism(s) to be used to provide a requested security service;
* negotiation of available security mechanisms.

Security mechanism management is concerned with the management of individual security mechanisms (which, in turn, provide security services). Typical security mechanisms include:
* key management (see 3.5 below);

* encipherment management (e.g. establishment of cryptographic parameters, cryptographic synchronisation, etc.);
* access control management (e.g. distribution of security attributes including passwords, updates to access control lists, updates to capabilities lists, etc.);
* data integrity management;
* authentication management (e.g. distribution of identifying information such as passwords);
* traffic padding management (maintenance of rules to be used for traffic padding, where such rules might include: pre-specified data rates, specific lengths for messages, etc.);
* routing control management (typically involving the definition of links which are secured or trusted with respect to particular criteria);
* notarisation management (e.g. distribution of information about notaries, interaction with notaries, etc.).

Security of OSI management is concerned with the security of the management functions themselves, and the security of communicated management information. For example, this will include provision for the protection of the MIB, and for security of communications between parts of a distributed MIB.

3.4 Security audit

Security audit is defined in ISO 7498-2, [9], as 'an independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in control, policy and procedures'. This process usually makes use of a security audit trail, defined as 'data collected and potentially used to facilitate a security audit'.

Security audit management is one of the system security management activities defined above. and includes:
* the selection of events to be logged and/or remotely collected;
* the enabling/disabling of audit trail logging of selected events;
* the remote collection of selected audit reports;
* the preparation of security audit reports.

3.5 Key management

This aspect of security management is fundamental to provision of any cryptography-based security services, since keys are necessary for the provision of any such services. Key management is 'the generation, storage, secure distribution and application of keys in accordance with a security policy', [9].

As defined by ISO 7498-2, key management forms part of security mechanism management and involves:
* generation of suitable keys at intervals commensurate with the level of security required;
* determination, in accordance with access control requirements, of which entities should receive a copy of each key;
* distribution of keys in a secure manner.

3.6 Assurance

We conclude this discussion of security management by briefly reviewing the issue of assurance. When designing or assessing a security system there are two fundamental considerations; first the functionality of the system (i.e. what security services it provides and what types of security policy it can support), and second the level of assurance that this functionality operates correctly.

As an example consider an access control system on a 'typical' conventional mini-computer operating system of the early 1980s. Most likely it allows users to specify what type of access is permitted to their own files (e.g. owner only access, group access or universal access). Thus this system has a certain level of access control functionality. However, on many such systems of the recent past (and even some current systems), many loopholes exist which allow users to circumvent the access control mechanisms and gain unauthorised access to files. These loopholes exist for many reasons, including deliberate design and simple error. Thus, the claimed functionality is of low value, since there is no assurance as to how well the claimed functionality operates.

This concept was taken up by the U.S. Government sponsored work on providing standards for computer security, which resulted in 1985 and 1987 in the Orange and Red Books, [3], [22]. The Orange Book lists criteria which computer systems must satisfy in order to reach one of six security levels: C1 (lowest), C2, B1, B2, B3, A1 (highest). For each level there are two sets of criteria which a system must satisfy, one containing functional requirements and the other assurance requirements. The former contains things such as requirements that a B1 system should offer Mandatory Access Control (MAC) facilities. The latter ranges from informal requirements on testing for low levels, to requiring (for A1 systems) that there exists a formal proof that the top level specification meets the security policy (also formally specified).

The Red Book, [22], is the U.S. National Computer Security Center 'Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria'. This U.S. Government standard is intended to supplement the previous Orange Book. The Red Book interprets the Orange Book requirements for network products, and therefore enables designers of network products to obtain the same security level 'ratings'. In terms of functionality, relatively little is required. Indeed, obtaining Red Book certification does not specifically require the provision of any cryptographic services. The main areas in which the Red Book requires special functionality are security label transfer and audit. For example, for B1 certification the main functional requirement is the secure transfer of security labels from one machine to another.

Following on from this work, various European countries have defined their own national standards for computer security. In the U.K. draft standards exist which follow a somewhat different approach to that of the Orange Book. The same level structure exists, but these levels specify solely assurance requirements, omitting any specific functionality. Whilst the U.S. standards are intended primarily for use in government

purchase specifications, the European work is for more general commercial use.

It is clear that having a sensible level of assurance in claimed security functionality is almost more important than the functionality itself. Using incorrectly designed and/or poorly implemented security systems can be a greater risk than using completely insecure systems.

4 OSI SECURITY ACTIVITIES

The work of the main international standards committees involved in work on security for OSI (i.e. ISO, CCITT and ECMA) can be divided into three main parts:
* First there is work on underlying security techniques, such as: cryptographic algorithms, modes of operation for cryptographic algorithms and peer entity authentication mechanisms.
* Second there is more general work describing how these techniques may be used to provide security in both OSI applications and various layers of the OSI model, such as: the OSI security architecture, Lower and Upper Layer security models and various security frameworks.
* Third there is work on specifying how security should be provided in specific OSI applications, as typified by the security elements in the 1988 version of the CCITT X.400 Recommendations, [1].

We now summarise each of these three main areas of activity.

4.1 Security techniques

Within ISO, work on techniques for security, in particular on cryptographic techniques, has been primarily focussed within ISO/IEC JTC1/SC20 and its successor, SC27. Outside ISO, other work has proceeded within ANSI and the NBS (in the U.S.A.). This work can be conveniently divided into three areas: algorithms (e.g. encryption functions, digital signature functions), peer entity authentication protocols and key management.

4.1.1 Algorithms

After the failure of attempts to standardise specific encryption algorithms, it was decided that ISO would change tack. Instead, it has been decided to adopt the idea of an international register of algorithms, through which any encryption algorithm can be given a standardised identifier. The draft proposal ISO DP 9979, [18], caters for registering proprietary algorithms, the details of which may remain confidential to their owners. An international standard, ISO 8372, [10], specifying modes of use for an arbitrary 64-bit block cipher algorithm has also been produced. A successor to this standard, in the form of a draft proposal, ISO DP 10116, [19], generalises this further to specifying modes of use for an N-bit block cipher algorithm.

In addition to data confidentiality, a good deal of work has also been done within ISO (and other standards bodies) concerning standardising algorithms for message authentication, integrity checking and digital signature. A draft international standard now exists, ISO DIS 9797, [14], for a data integrity mechanism. Two standards proposals exist relating to digital signature algorithms. The first is a draft proposal, ISO DP 10118, [20], specifying possible methods for computing hash functions for digital signatures. The second is a proposal for a signature algorithm for 'short' messages, ISO DP 9796, [13].

4.1.2 Peer entity authentication

In parallel with the current work within ISO on algorithms, efforts have also been made to standardise the protocol exchanges involved in performing party-to-party authentication. This has resulted in drafts for a multi-part standard, ISO DP 9798-n (n=1,2,3,...), [15], [16], [17].

4.1.3 Key management

ISO work on key management is at an early stage of development. Three draft documents exist, entitled: Cryptographic mechanisms for key management: Part 1: Key management overview, Part 2: Key management using secret key techniques and Part 3: Key management for public key register. It is likely to be some time before any of these documents emerge as Draft Proposals, since at the moment none of them are any where near completion. The general ISO work on key management will need to take account of earlier work in this area, in particular that undertaken for the financial community, where ANSI and ISO standards already exist.

4.2 Using security mechanisms

Within ISO, the questions of how and where within the OSI model security mechanisms are to be used falls primarily within the scope of SC21/WG1, together with the layer and application specific Working Groups of SC6 and SC21. Work in this area can be divided into three parts, namely: security architectures and models, security frameworks and layer specific standards.

4.2.1 Security architectures and models

To date, the main achievement in this area has been the production of the OSI Security Architecture, ISO 7498-2, [9], in 1988. This document covers a number of important topics, including: standardised definitions of security terminology and security services, a guide to the relationship between security services and mechanisms, an indication of which security services are relevant to which layers of the OSI model and a short introduction to security management.

Subsequent to the production of this standard, work has started within SC21 and SC6 on two security models: a Lower Layer Model (relevant to OSI Layers 1-4) and an Upper Layer Model (relevant to OSI Layers 5-7). These models are intended as general guides to the insertion of security

facilities into the relevant layers of the OSI model. Work on these two models is at an early stage and has not yet reached DP status.

In parallel with these activities, security facilities are under consideration both within the ISO Open Distributed Processing group (SC21/WG7) and the CCITT's Distributed Applications Framework (DAF) activity. Finally we briefly mention the ECMA work in this area. ECMA have produced a technical report entitled Security in Open Systems - A Security Framework, [4] and have also produced a draft for an ECMA standard entitled Security in Open Systems: Data elements and service definitions, [5]. These documents are likely to be most significant in terms of the influence they have over subsequent ISO standards and CCITT Recommendations. They have particular relevance to the provision of access control services in distributed systems.

4.2.2 Security frameworks

Another recently inaugurated work topic within ISO/IEC JTC1/SC21 covers the 'security frameworks'. This projected six-part standard will give a framework for the provision of particular security services in distributed systems. The six parts will cover the following topics:
Part 1: Authentication Framework
Part 2: Access Control Framework,
Part 3: Non-repudiation Framework
Part 4: Integrity Framework
Part 5: Confidentiality Framework
Part 6: Audit Framework

In addition there will be a Part 0, giving a general introduction to the six security frameworks. All these documents are at an early stage of development, although it is hoped to progress Parts 1 and 2 to DP status within the next few months.

4.2.3 Layer specific standards

Apart from the Upper and Lower Layer Security Models, a number of other drafts are in existence covering the provision of security services in specific layers of the OSI model. An ISO standard exists, ISO 9160, [11], specifying how security should be provided in Layer 1 (Physical). Within IEEE 802.10, work is progressing on standardising the provision of security in LANs, [7], [8]; the proposed security functionality all resides in Layer 2 (Link). The U.S. SDNS work (now being progressed by NIST) has resulted in two documents, [23], [24], specifying how security should be provided in Layers 3 (Network) and 4 (Transport).

4.3 OSI application layer security

We now very briefly consider the effort that has been devoted to providing standardised security solutions for specific OSI applications.

The 1988 version of the X.500 CCITT Recommendations on Directory Services, [2], and their corresponding ISO draft standards, [12], include means to use the Directory Service to provide key management and peer-entity authentication through storage of user public keys in the

directory. The 1992 versions of these Recommendations are also expected to contain detailed provisions for access control to directory entries.

The 1988 versions of the X.400 CCITT Recommendations, [1], include a variety of security features making it possible to provide a variety of security services for electronic mail. For a general discussion of these security features see, for example, [21].

In parallel with the general growth in interest in EDI (Electronic Data Interchange), there has also been a very rapid growth in concern regarding the security of EDI messages. For those EDI messages transmitted using X.400 networks, use of the X.400 security features may be sufficient. However, for EDI messages sent by other means, or where security services are required which cannot be provided using the X.400 features, EDI may need to be enhanced to incorporate security elements. This is an area of current debate.

REFERENCES

[1] C.C.I.T.T. Recommendations X.400, X.402, X.407, X.411, X.413, X.419, X.420, Message handling systems, C.C.I.T.T. IXth Plenary Assembly, October 1988.

[2] C.C.I.T.T. Recommendations X.500, X.501, X.509, X.511, X.518, X.519, X.520, X.521, The Directory, C.C.I.T.T. IXth Plenary Assembly, October 1988.

[3] DoD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria, December 1985.

[4] ECMA TR/46, Security in open systems - A security framework, ECMA, July 1988.

[5] ECMA Draft Standard, Security in open systems - Data elements and service definitions, Output of the 11th (Bristol) meeting, ECMA/TC32/TG9, June 1989.

[6] J. Henshall and S. Shaw, OSI explained, Ellis Horwood (Chichester), 1988.

[7] IEEE P802.10A/D1, Standard for Interoperable Local Area Network (LAN) Security (SILS), Part A - The Model, Draft of December 9th 1989.

[8] IEEE P802.10B/D1, Standard for Interoperable Local Area Network (LAN) Security (SILS), Part B - Secure data exchange, Draft of December 9th 1989.

[9] ISO 7498-2, Information processing systems - Open systems interconnection - Reference Model - Part 2: Security Architecture, International Organization for Standardization, 1988.

[10] ISO 8372, Information processing - Modes of operation for a 64-bit block cipher algorithm, International Organization for Standardization, 1987.

[11] ISO 9160, Information processing - Data encipherment - Physical layer interoperability requirements, International Organization for Standardization, 1987.

[12] ISO/DIS 9594-1, 9594-2, 9594-3, 9594-4, 9594-5, 9594—6, 9594-7, 9594-8, Information Processing Systems - Open systems interconnection - The Directory, International Organization for Standardization, 1988.

[13] ISO/3rd DP 9796, Data cryptographic techniques - Digital signature scheme giving message recovery, International Organization for Standardization, 1989.

[14] ISO/DIS 9797, Data cryptographic techniques - Data integrity mechanism using a cryptographic check function employing an n-bit algorithm with truncation, International Organization for Standardization, 1988.

[15] ISO/DP 9798-1, Information processing systems - Data Cryptographic techniques - Peer entity authentication mechanisms, Part 1: general model for peer entity authentication mechanisms, International Organization for Standardization, ISO/IEC JTC1/SC27 N18, 1989.

[16] ISO/DP 9798-2, Information processing systems - Data Cryptographic techniques - Peer entity authentication mechanisms, Part 2: Peer entity authentication mechanisms using a secret key algorithm, International Organization for Standardization, to appear.

[17] ISO/DP.2 9798-3, Peer entity authentication mechanisms, Part 3: Peer entity mutual authentication mechanisms using a public key algorithm, International Organization for Standardization, ISO/IEC JTC1/SC27 N25, 1989.

[18] ISO/DIS 9979, Data cryptographic techniques - procedures for the registration of cryptographic algorithms, International Organization for Standardization, 1988.

[19] ISO/DP 10116, Information processing - Modes of operation for an N-bit block cipher algorithm, International Organization for Standardization, 1988.

[20] ISO/2nd DP 10118, Information Technology - Data encryption - Hash-functions for digital signatures, International Organization for Standardization, 1989.

[21] C. Mitchell, D. Rush and M. Walker, 'CCITT/ISO standards for secure message handling', IEEE Journal on Selected Areas in Communications 7 (1989) 517-524.

[22] NCSC-TG-005, Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria, National Computer Security Center, July 1987.

[23] SDN.301, SDNS Secure Data Network System, Security Protocol 3 (SP3), Revision 1.5, 15th May 1989.

[24] SDN.401, SDNS Secure Data Network System, Security Protocol 4 (SP4), Revision 1.3, 2nd May 1989.