High Integrity Systems Journal, 1994. 1(1): p. 83-92

AN INTRODUCTION TO SECURITY IN DISTRIBUTED SYSTEMS

JONATHAN D. MOFFETT
JOHN A. CLARK

DEPARTMENT OF COMPUTER SCIENCE
UNIVERSITY OF YORK
ENGLAND

AUGUST 1993

Abstract

This article considers the security threats that may arise when the computing facilities of an organisation are distributed and highlight ways in which such threats may be countered. Relevant international standards are indicated. The article is intended to be understood by the non-specialist reader.

1 INTRODUCTION

1.1 WHAT IS A DISTRIBUTED SYSTEM?

This article is an introduction to the subject of security in distributed systems. The term **distributed systems** does not have a universally accepted interpretation; in this article a distributed system is one in which several autonomous processors and data stores, supporting processes and/or databases interact in order to co-operate to achieve an overall goal, co-ordinating their activities and exchanging information by means of a communications network.

Figure 1 shows the distributed system of a hypothetical business. The financial department has its own network of clerical workstations with data storage and report printing facilities. This network is linked to production units, some of which may be on remote sites, which have specialist production control processing to perform. there are stores to maintain inventories, sales departments which generate invoices and so on. All these parts communicate with the corporate centre. Their information contributes to corporate planning and their actions to corporate policy. The system is clearly vital to the management of the business and, in consequence, needs to be secured.

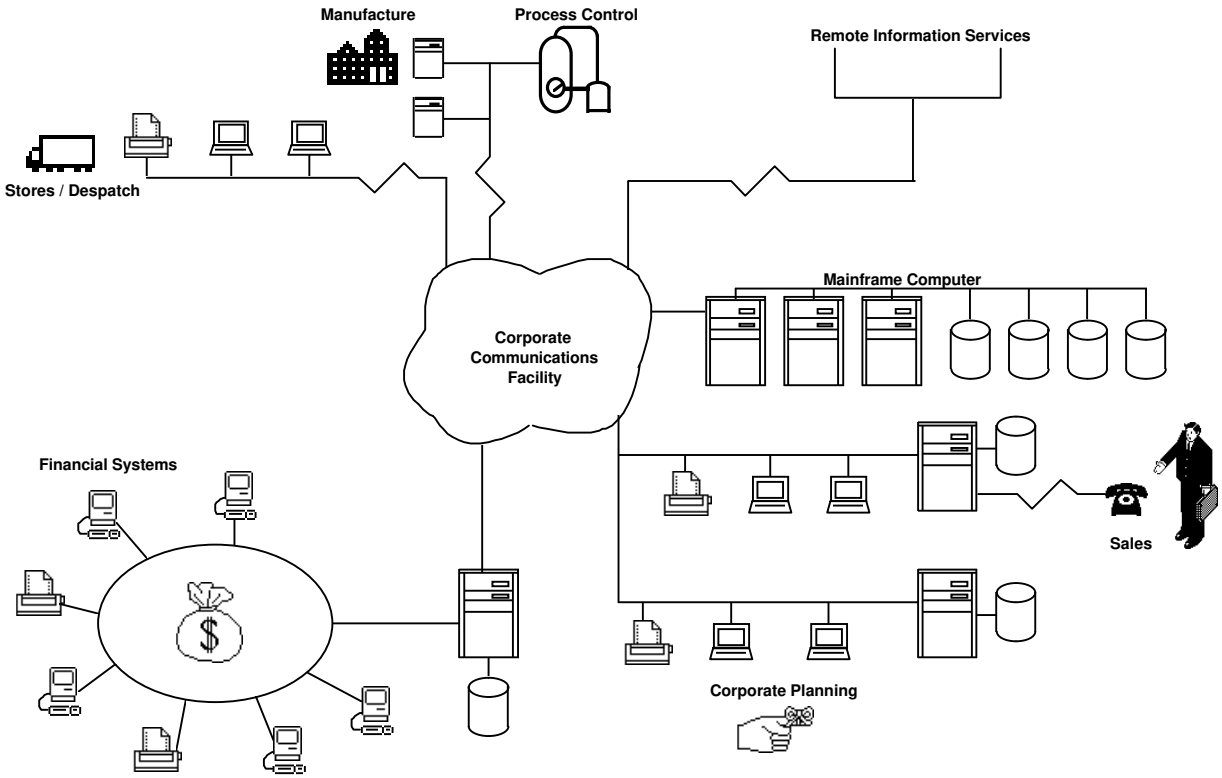

Figure 1 Distributed Computer Systems in a Business

1.2 SECURITY DOWNS AND UPS OF DISTRIBUTED SYSTEMS

1.2.1 Downs

Existing distributed systems are vulnerable to a variety of deliberate and accidental threats. They provide significant opportunities for the introduction of malicious or insecure software, e.g. Trojan horses (programs that apparently perform some useful function but surreptitiously carry out some covert action while running) and viruses (programs that reproduce themselves when invoked). In addition, they provide increased opportunities for hacking and browsing (searching through available data with the aim of uncovering something useful). For many organisations denial of service (rendering a service unavailable) is a particularly important threat. One can easily imagine the losses that might ensue if a company's share dealing network "crashed" in a period of volatile market activity. Equally, systems dealing with emergency calls (e.g. requests for fire, police and ambulance services) must provide uninterrupted service. Such organisations must be vigilant against the malicious attacker.

Some denial of service attacks have been extraordinarily successful. For example, the “Internet Worm” (Spafford, 1988) program propagated itself across several networks, especially in the USA, reproducing itself continuously until it had absorbed all the resources of computers it had invaded and brought them to a halt. An estimated 12000 computers were affected (Stoll, NCSC89) and the cost of recovery was estimated at millions of dollars even though no damage was done to data.

An organisation must also be prepared to meet accidental threats to distributed systems. Components may still suffer random hardware failures, be susceptible to environmentally-caused local disruption (e.g. fire, lightning), or simply fail due to "bugs" in the software they run. An example is the incorrect handling of error reports in electronic mail systems which can cause “mail storms” which swamp the network. This can be caused if a message containing errors is broadcast to multiple sites. If each receiver site reports the error back to the originator and separately triggers off a retry of the entire broadcast, the number of messages grows exponentially until the network halts.

Unprotected systems may be used as an entry point into other inadequately protected but sensitive systems. For example German hackers used unprotected systems as bases from which to probe systematically for security weaknesses in other more sensitive systems, with a surprisingly high degree of success (Stoll, 1989).

The communications network used by distributed components to exchange information may also be subject to malicious or accidental threats, e.g. eavesdropping, recording and replay of messages, and the malicious modification or accidental corruption of messages. In certain cases protection against access to the medium will be impossible (e.g. in the case of satellite radio links). Measures must be taken to render intercepted information unintelligible and to detect which messages originate from a legitimate sender and which do not.

Distribution also adds complications to dealing with the risks. For example, time-lags in respect of reporting security-related information may make it difficult for the security management system to correlate information which, taken together, would indicate a security breach. In addition, in widely distributed systems political, technical, and administrative differences complicate the formation and management of a coherent security policy and make the tracing of security breaches more difficult.

1.2.2 Ups

Distributed systems are not without security benefits. Sensitive data may be distributed across the system; to gain full access to the data an intruder must know where the constituent data components lie and be able to access each of them. In addition, distribution allows the provision of service redundancy helping protect against the failure of an individual service provider.

Security requirements need not necessarily be uniform across a whole system. The environment can be partitioned into separate security domains, each domain reflecting a different aspect of the organisation's policy concerning security. Overall control is obtained either by negotiated security interaction policies between the managers of domains or by a hierarchical structuring of domains with one manager taking responsibility for co-ordinating the interactions of all.

2. SECURITY FRAMEWORK

The objectives of security within distributed systems can be defined at a number of different levels, from a high-level objective such as “to safeguard the organisation's assets” to a low-level one such as “ensure that passwords are changed at least once every month”, with a hierarchy of objectives in between. Each level helps to achieve the objectives of a higher

level. These objectives may be achieved by mechanisms at several different architectural levels within a distributed system.

The International Standards Organisation (ISO) Open Systems Interconnection (OSI) Security Architecture (ISO,7498-2) defines a set of security services based on generally agreed objectives and sets out the options for the architectural levels at which these may be provided. The objectives are described in more detail in the OSI Security Frameworks Review (ISO, 10181-1).

2.1 SECURITY OBJECTIVES

There are three primary security objectives identified by the Security Architecture which apply to both stored data and messages in transit:

- **Confidentiality** - maintaining confidentiality of information held within systems or communicated between them.
- **Integrity** - maintaining the integrity of data held within systems or communicated between systems. This prevents loss or modification of the information due, for example, to unauthorised access, component failures or communication errors.
- **Availability** - maintaining the availability of information held within systems or communicated between systems, ensuring that the services which provide access to data are available and that data is not lost.

For communication between users and/or programs there are two further primary objectives:

- **Authentication** - authenticating the identity of communicating partners and authenticating the origin and integrity of data which is communicated between them.
- **Non-repudiation** - this is the prevention of a user wrongly denying having sent or received a message. Non-repudiation is important in any situation in which the interests of the sending and receiving parties may be in conflict (e.g. the making or acceptance of a commercial offer or deal).

The secondary security objectives (which lead to the design of services to support the primary ones) identified by the Security Architecture are:

- **Access Control** - providing access control to services or their components to ensure that users can only access services, and perform data accesses, for which they are authorised.
- **Audit Trail** - providing an audit trail of activities in the system to enable user accountability. An audit trail provides evidence of who did what, where and when.
- **Security Alarm** - the detection of occurrences indicating an actual or potential security failure should raise an alarm and cause the system to operate in a fail-safe mode.

The security objectives outlined above are interdependent. For example, authenticated user identities are needed for identity-based Access Control, Non-Repudiation and Audit Trail;

and password-based Authentication requires both Access Control to protect the password file and encryption-based Confidentiality for further protection if the Access Control fails.

2.2 ARCHITECTURAL LEVELS OF SECURITY SERVICES

The ISO Security Architecture identifies the possible communication protocol layers of the Open Systems Interconnection Basic Reference Model (ISO, 7498) at which each security service could be provided. A security service, such as confidentiality, can be applied to communication at different layers in the model but it is not sensible to apply the service at all of the layers. For instance, a user who is obtaining end-to-end confidentiality through encryption at the Presentation Layer, has no need of Link encryption as well (see figure 2). Further standards work will identify appropriate profiles of security services for particular applications.

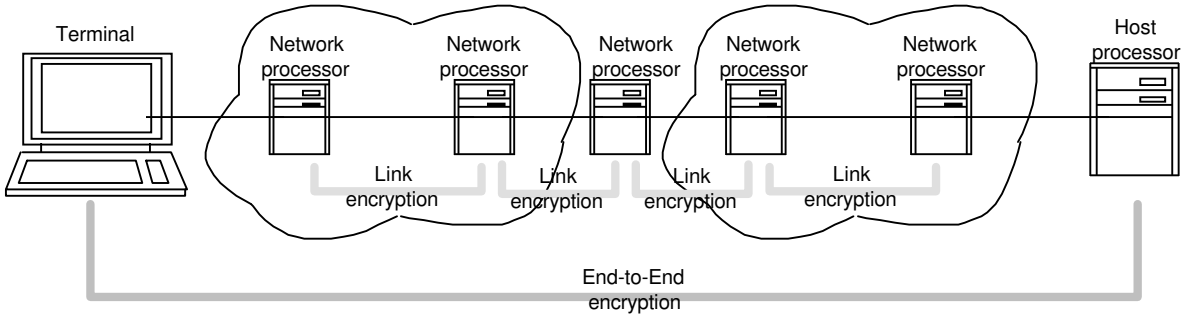

Figure 2 End-to-End vs Link Encryption

3 SECURITY MECHANISMS

A number of different mechanisms are used to achieve security objectives including:

- physical and electronic security of components of the system;
- authentication mechanisms;
- access control mechanisms;
- communication security mechanisms.

They are described briefly here.

3.1 PHYSICAL SECURITY MECHANISMS

Physical security mechanisms are used for protection of equipment and for access control outside the scope of logical access control or encryption. They are necessary for protection against risks such as fire, tempest, terrorist attacks and accidental or malicious damage by users and technicians. Physical security requires a variety of mechanisms:

- Preventive Security - strong construction, locks on doors, fire resistance and waterproofing;
- Detection and Deterrence - movement detectors and door switches linked to alarms, security lighting and closed circuit television;

- Recovery - the provision of a backup site, with alternative computing and communication arrangements, for recovery from disasters.

A basic level of physical security is always necessary even in the presence of logical access control and encryption. In some situations physical protection may be simpler and more secure than a logical solution; for example, by controlling physical access to terminals and personal computers and their data and by storing sensitive data on demountable media. Figure 3 shows a situation where encryption needs to be supplemented by physical line protection if complete end-to-end protection is required. This is necessary because the encryption unit is not an integral part of a secure terminal.

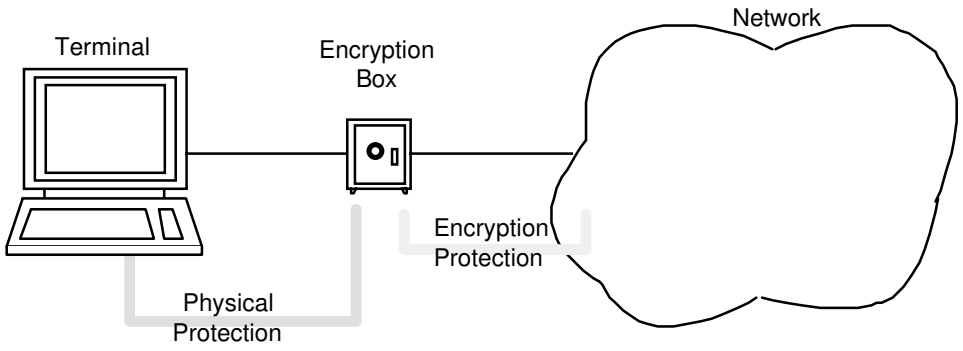

Figure 3 Encryption vs Physical Protection

3.2 ELECTRONIC SECURITY MECHANISMS

There are two aspects of electronic security that need to be considered:

- electronic equipment (VDUs, printers etc.) generally emit electromagnetic radiation. Unless measures are taken to contain such information, an eavesdropper may listen in on these signals to breach confidentiality. Suitably shielded commercial equipment is available and there are also military standards of protection (so-called "TEMPEST" proofing).
- electronic equipment may be affected by both static electricity and electromagnetic interference from other sources, causing it to malfunction in some way.

3.3 AUTHENTICATION

3.3.1. Personal Authentication

The aim of personal authentication in computer systems is to verify the claimed identity of a human user. Mechanisms for personal authentication are based on one or more of the following principles:

- "something you know" - a piece of information known only to the particular user, e.g. a password.
- "something you have" - a magnetic stripe card or 'smart card' containing information unique to the particular user.

- "something you are" - a personal characteristic of the user, e.g. fingerprint, hand geometry, signature, voice pattern) which is unique to the user. Increasingly a user's modus operandi is used as a characteristic (see below).

Passwords are the simplest and cheapest method to implement. They need a number of supportive measures if they are not to be undermined including: regular change by the user, one-way encrypted storage, minimum length and controlled format (such as no dictionary words), limited number of permitted attempts, and logging and investigation of all failures. They can be reinforced by restricting users to logging in at specific physically protected terminals during restricted hours; for example, Payroll clerks may only log on in that capacity using one of the terminals sited within the Payroll Office during normal working hours.

The use of passwords across open communication channels in distributed systems is a particular problem because the password can be discovered by eavesdropping on the channel and then used to impersonate the user. One solution to this is the use of one-time passwords generated by smart cards (see below).

Magnetically coded cards have some advantages over passwords - they cannot be copied so easily and are less easy to forget. However, they also suffer from the potential exposure of their contents in open communication channels. They can also be lost or stolen.

Smart cards offer increased security because they can be programmed to provide variable information. There are several modes in which they can be used for personal authentication. Two of these are:

- One-time password generators which generate a different password each time they are used. One commercial product changes the password every minute. In all cases the computing service must synchronise with the password generator.
- Challenge-response devices. The host sends a challenge number and the smart card has to calculate the correct response.

Smart cards are becoming cheaper and easier to use and they promise to provide a satisfactory way of overcoming the problems of personal authentication in distributed systems. However, any authentication system must cope with the problem of protecting the secure information upon which it is based. This is an aspect of security management (see section 5.1).

Authentication is usually a 'one-off' affair; once a user has been authenticated to the system via a terminal then the system assumes that subsequent input from that terminal is actually from that authenticated user. Of course, in practice users will leave terminals unattended and so a user can come along and pretend to be the original authenticated user. 'Continuous' authentication is now becoming more widely adopted, requiring the user to reauthenticate at periodic intervals or after some period of inactivity. In addition, it as been found that users possess features other than physical characteristics and simple dynamic characteristics (e.g. signature dynamics) that can be used to characterise them. Different users generally have characteristic patterns of computer usage. This enables 'profiles' of user behaviour to be built up over time and these can be compared with current session usage. Behaviour outside

established bounds will cause security management to be alerted. Systems operating on this basis are often referred to as *automated intrusion detection systems*. They provide not only protection against users leaving their terminals but also against masquerading (where intruders may have obtained the authentication credentials of a legitimate user, e.g. seeing a password being entered, and use these to gain access to the system).

3.3.2. Message Authentication

The aim of message authentication in computer and communication systems is to verify that the message comes from its claimed originator and that it has not been altered in transmission. It is particularly needed for EFT (Electronic Funds Transfer). The protection mechanism is generation of a Message Authentication Code (MAC), attached to the message, which can be recalculated by the receiver and will reveal any alteration in transit. See figure 4. One standard method is described in (ANSI, X9.9). Message authentication mechanisms can also be used to achieve non-repudiation of messages.

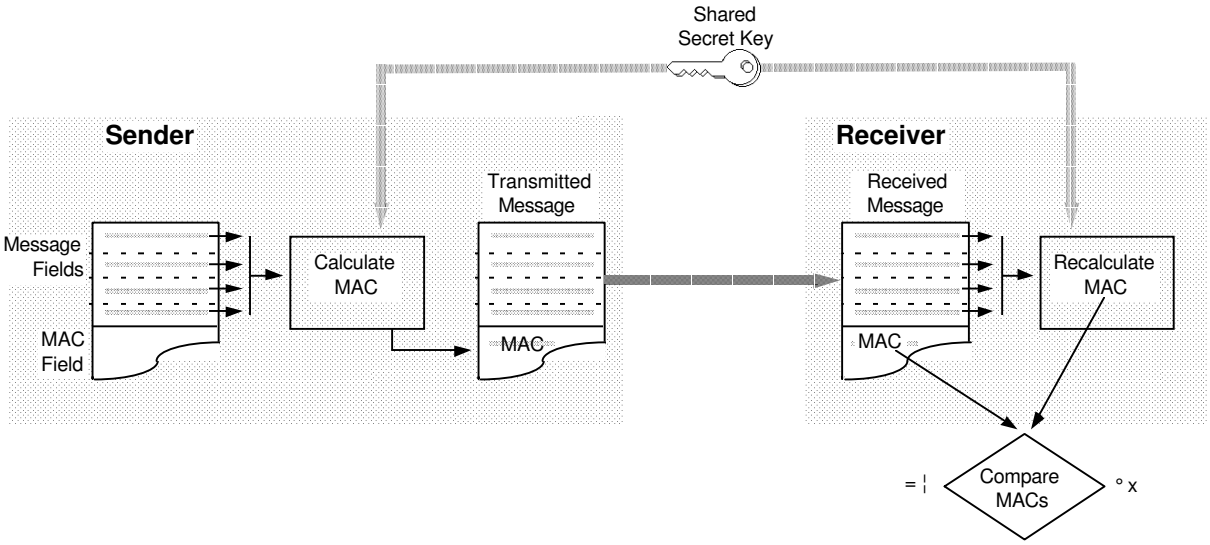

Figure 4 Message Authentication Code (MAC)

3.4 LOGICAL ACCESS CONTROL

Logical access control has to be used when physical access control is impossible, as is the case in multi-user systems. A model for logical access control is provided by a Reference Monitor, which intercepts all access attempts and allows them only if the access is authorised. Otherwise the access is blocked, an error message is returned to the user and appropriate logging and alarm actions are taken.

There are two main forms of logical access control: mandatory access control, based upon fixed rules; and discretionary access control which permits users to share and control access. The recommended discretionary access control approach is Identification/Authorisation. The system ensures that the identities of users are authenticated when they log on, and the

Reference Monitor makes a decision based on access rules which relate the user, the entity being accessed, and the operation the user is attempting to carry out.

There are two main implementations of discretionary access control rules:

- An Access Control List (ACL) is attached to the target entities, defining the users who are authorised to access them and the operations which they can perform;
- Users obtain authenticated Capabilities which act as tickets authorising them to access defined resources.

Many personal computing systems only provide access control based upon file passwords. For general purpose use these are inappropriate for the purpose; the number of passwords a user needs to remember is increased (worse when we wish to grant different modes of access) and there are difficulties when applications need to access objects (are passwords stored as part of the application?). Management of access becomes difficult: there is no real way of knowing who has knowledge of the password for a file and changing of the password necessitates a distribution of the password to all authorised parties by some means. Since periodic password changing is desirable a significant administrative overhead may be incurred.

Similarly, profiles present an inferior means of implementing discretionary access controls. A profile is a list of objects a particular user may access together with the modes of access he/she is allowed to each of those objects. determining who has access to a particular object requires searching every such profile - a highly inefficient task.

Another (and more plausible) method uses "protection bits" where a bit mask is associated with groups of bits indicating the accesses allowed for particular user groups - typically the file owner, a specific group of users and the 'rest-of-the-world'.

3.5 COMMUNICATION SECURITY MECHANISMS

There are two main mechanisms in ensuring communication security, in addition to physical protection of the lines and equipment: encryption, and traffic padding.

Encryption is one of the most important techniques in computer and communications security. Encryption transforms (enciphers) plain text into ciphertext, which is impossible to read, and decryption transforms it back again into readable plain text (deciphers it). Cryptography is a very powerful technique. Algorithms such as the Data Encryption Standard (DES) are easily available, simple to use, and provide a high degree of protection against threats to the confidentiality and integrity of communications.

Encryption can be used for several purposes: the prevention of eavesdropping; the detection of message alteration; and, in conjunction with the use of unique message identities, the detection of message deletion and replay.

Traffic padding is the insertion of dummy messages on the line to ensure that there is a uniform level of traffic at all times. The aim is to prevent an eavesdropper from gaining information due to the very existence, frequency and destination of messages. It is mainly of interest in a military level of security.

1. Link or End-to-end Encryption

Encryption may be used on individual links or on an end-to-end basis. Link encryption only covers the communication links, and the information is "in clear" at each communication processor. By contrast, end-to-end encryption is carried out directly between the initiating and target systems. An intermediate level is network encryption, where encryption spans an entire network, but not the gateways between networks. In all cases where encryption is carried out by a separate hardware unit, the link between the terminal and the unit is not covered by encryption, and physical protection is required in addition.

2. Encryption Algorithms

There are two main types of encryption:

- Secret key encryption, which uses a single secret key shared between sender and receiver. See figure 5.
- Public key encryption, which uses a related pair of keys. One key is publicly available and may be used to encrypt messages, while the other key is secret, known only to the receiver, and may be used to decrypt messages. See figure 6.

Secret key encryption is available in a number of proprietary algorithms, and in the Data Encryption Standard (DES) which is an American, but not an international, standard. The DES is described in a number of text books (Davies & Price, 1989). The DES algorithm is available in software and also in hardware as a semi-conductor chip, providing higher performance. The chip is subject to export restrictions from the USA, and the hardware is therefore not suitable for multi-national applications. Any secret key algorithm suffers from key management problems, because of the need to transport secret encryption keys securely. There is a standard method of key management, described in (ANSI, X9.17), which covers: key generation and distribution; protection of the key management facility; and protocols for the cryptographic service.

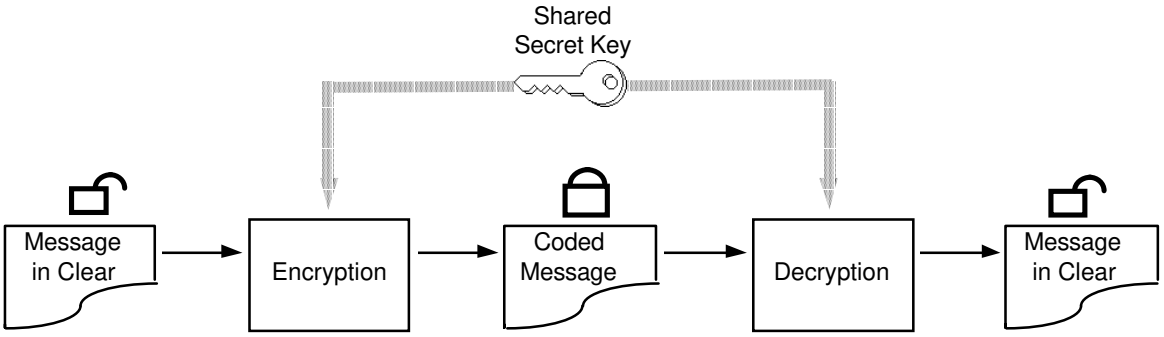

Figure 5 Secret Key Encryption

The most widely accepted method of public-key encryption is the RSA algorithm (Rivest, Shamir, & Adleman, 1977). Its performance speed is much poorer than the DES algorithm, but key management is easier because there is no need for secrecy of the key used by the sender. Some mixed-mode systems use RSA for key distribution and DES for message security, thus gaining many of the advantages of each method.

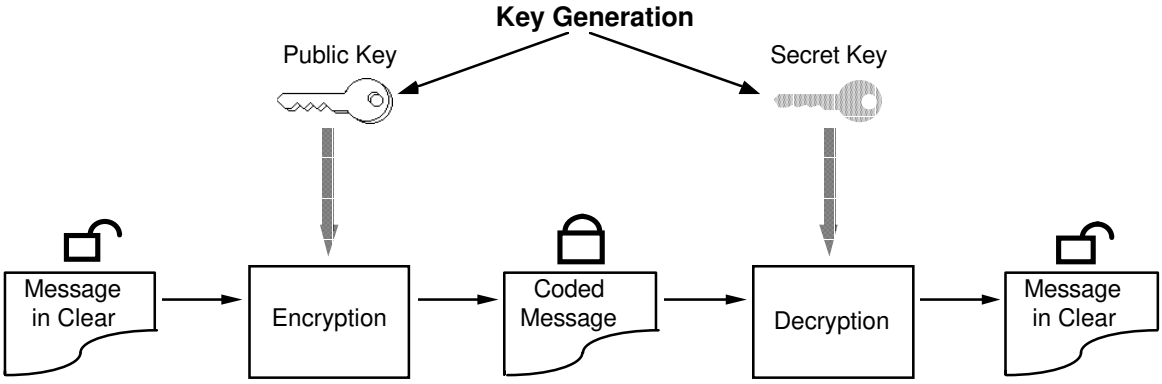

Figure 6 Public Key Encryption

4. SECURITY STANDARDS

There are three main categories of security standards which concern distributed systems. The first are standards related to the security of individual computers, which have been in existence for some time, and are quite mature. The second are standards for the protection of communication transmission and remote authentication. These too are quite mature. The third, still under development, are those which integrate computer and communication security standards to provide distributed systems security standards.

The standards do not generally prescribe physical or procedural mechanisms, nor do they prescribe risk management or risk assessment procedures or requirements for their use. These are all necessary elements to be considered and resolved for the resources that comprise the whole distributed system. Therefore, although security standards are an important support to distributed system security policies, they have to be viewed in the context of an overall security policy which uses other measures as well.

4.1 COMPUTER SECURITY STANDARDS

The USA Department of Defense Trusted Computer System Evaluation Criteria (TCSEC - the Orange Book) (Department of Defense (USA), 1985), deals with access control to individual systems. It defines a number of possible levels of trust which may be placed in a system, ranging from the certified high security of the A1 level down to a low level of informally defined security at the C1 level. It is commonly used as a means of indicating the level of security required or supplied in computer systems.

Access control is divided by this standard into two categories: mandatory and discretionary access control. The former enforces policies which are built into the design of the system and cannot be altered except by installing a new version of the system. An example is the policy that in multi-layer security systems data cannot be read by a user with a lower security classification than has been assigned to the data. Discretionary access control mechanisms are defined as those which allow users to specify and control sharing of resources with other users. For example the C2 level discretionary access control policy is defined as requiring mechanisms which ensure that information and resources are protected from unauthorised access and that access permission is only assigned by authorised users.

The Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria (Department of Defense (USA), 1987) (the Red Book) extends the criteria of the Red Book to networks. It is chiefly concerned with the security criteria to be met when accessing remote hosts.

The Orange and Red Books are now quite old and have always been more oriented to military type security than to commercial security. A standards effort which is now under way is the Information Technology Security Evaluation Criteria (ITSEC) (CEC, 1991). This is a joint undertaking by the UK, Dutch, French and German governments. Its aim is to take into account the needs of commercial users and improve on the Orange and Red Books by separating concerns about security levels from the way in which the security is evaluated. In the UK, the Department of Trade and Industry and the Communications-Electronics Security Group have established the UK IT Security Evaluation and Certification Scheme (CESG, 1991) which evaluates and certifies products using the criteria of ITSEC. Similar efforts are under way in other countries.

4.2 COMMUNICATION SECURITY STANDARDS AND ENCRYPTION

1. Transmission Security

Transmission security standards are mainly concerned with encryption methods. One algorithm in particular has been the subject of standards efforts: the DES algorithm for secret key encryption which is an American, but not an international, standard. On the other hand, the RSA algorithm for public key encryption is the subject of USA patents. It has become a de facto standard for public key cryptography but because of its patented status is not currently defined as a national or international standard. These two algorithms have been described briefly in section 2.5.2, above.

Encryption depends for its strength upon the security of the hardware which is used, and (BSI, 86/67937) describes standards for the Physical Security of Cryptographic Equipment.

The basic standard for DES is (NBS, 46), supplemented by (ANSI, X3.92). There are supplementary standards describing its Modes of Operation (NBS, 81) and Guidelines for Installation and Use (NBS, 74). The management of keys in banking applications is described in (ANSI, X9.17), but this standard is rather generally expressed and would apply to other applications also. A detailed discussion of DES standards is in (Davies & Price, 1989).

2. Authentication Standards

A number of standards have been developed for banking applications for peer-to-peer communication and message authentication. They too are quite general in format and could be used for other purposes. They include (ANSI, X9.19) for Message Authentication and (ANSI, X3.118) for personal authentication using a Personal Identification Number (PIN).

4.3 OSI SECURITY STANDARDS

Network security was not a primary concern when the Open Systems Interconnection (OSI) effort first got under way in the late 1970s. However there is now a series of ISO standards under development which aim to add security to OSI. The standards define the security

services which the partners in a communication could agree upon, and the protocols to be used in setting up a secure interaction.

The security services which may be required for the communication facilities have been defined in the ISO 7498-2 Security Architecture (ISO, 7498-2). The protocols for their provision are still largely under development and are not yet available in OSI products.

The security services described in the Security Architecture are described in more detail in a series of Security Frameworks which are currently in production. They will eventually appear as International Standards 10181-1 to 10181-8. The planned framework parts are:

1 Overview - a general introduction (ISO, 10181-1);
2 Authentication;
3 Access Control;
4 Non-repudiation;
5 Integrity;
6 Data Confidentiality;
7 Audit framework;
8 Key management.

Many other standardisation efforts have security implications, and therefore have security-related standards, e.g. in the areas of OSI Directory, OSI Systems Management and Electronic Data Interchange (EDI). Several similar and related efforts are in progress, including profiles to describe the security characteristics of selected applications.

FURTHER READING

INFORMATION SECURITY

Caelli, W., & al (1991). *Information Security Handbook*. MacMillan.

Denning, D. E. (1982). *Cryptography and Data Security*. Addison-Wesley.

DISTRIBUTED SYSTEMS

Sloman, M., & Kramer, J. (1987). *Distributed Systems and Computer Networks*. Prentice-Hall 1987.

Tanenbaum, A. S. (1988). *Computer Networks* (2nd ed.). Prentice-Hall International, Inc.

DISTRIBUTED SYSTEMS MANAGEMENT

Langsford, A., & Moffett, J. D. (1992). *Distributed Systems Management*. Addison-Wesley.

COMPUTER NETWORK SECURITY

Davies, D. W., & Price, W. L. (1989). *Security for Computer Networks*. John Wiley.

Muftic, S. (1989). *Security Mechanisms for Computer Networks*. John Wiley.

REFERENCES

ANSI X3.118 (1984). *Personal Identification Number - PIN Pad*. American National Standards Institution.

ANSI X3.92 (1981). *Data Encryption Algorithm*. American National Standards Institution.

ANSI X9.17 (1985). *Financial Institution Key Management, (Wholesale)*. American National Standards Institution.

ANSI X9.19 (1986). *Financial Institution Retail Message Authentication*. American National Standards Institution.

ANSI X9.9 (1986). *Financial Institution Message Authentication, (Wholesale)*. American National Standards Institution.

BSI 86/67937 (10 Dec 1986). *Physical Security of Cryptographic Equipment*. British Standards Institution.

CEC (1991). *Information Technology Security Evaluation Criteria (ITSEC): Provisional Harmonised Criteria; Version 1.2* (Report No. Office for Official Publications of the European Communities, Luxembourg.

CESG (1991). *UK IT Security Evaluation and Certification Scheme. Description of the Scheme* (Report No. UKSP 01, Issue 1.0). Communications-Electronics Security Group, Room 2/0804, Fiddlers Green Lane, Cheltenham GL52 5AJ, UK.

Davies, D. W., & Price, W. L. (1989). *Security for Computer Networks*. John Wiley.

Department of Defense (USA) (1985). *Department of Defense Trusted Computer System Evaluation Criteria* (Report No. DOD 5200.78 - STD).

Department of Defense (USA) (1987). *Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria* (Report No. NCSC-TG-005 version 1). Technical Guidelines Division, National Computer Security Center (USA).

ISO 10181-1 (1991). *Open Systems Interconnection - Security Frameworks - Part 1: Overview*. International Standards Organisation.

ISO 7498-2 (1988). *Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture*. International Standards Organisation.

NBS 46 (Jan 1977). *Data Encryption Standard*. National Bureau of Standards, US Department of Commerce.

NBS 74 (April 1981). *Guidelines for Installation and Use of the Data Encryption Standard*. National Bureau of Standards, US Department of Commerce.

NBS 81 (Dec 1980). *Data Encryption Standard Modes of Operation*. National Bureau of Standards, US Department of Commerce.

Rivest, R., Shamir, A., & Adleman, L. (1977). A Method for Obtaining Digital Signatures and, Public-Key Cryptosystems, MIT Laboratory for Computer Science, memo LCS/TM82.

Spafford, E. H. (1988). *The Internet Worm Program: An Analysis* (Report No. CSD-TR-823). Dept of Computer Sciences, Purdue University, West Lafayette, IND 47907-2004.

Stoll, C. (1989). *The cuckoo's egg: tracking a spy through a maze of computer espionage*. New York: Doubleday.