Annex A
(informative)

Generic Threats

A.1 Introduction

This appendix expands on the generic security threats introduced in

- Unauthorised Modification
- Unauthorised Disclosure
- Unauthorised Use of Resources
- Denial of Service
- Repudiation.

These threats are examined with respect to security vulnerabilities and methods of attack. The objective is to acquaint the reader with the areas of concern and the interdependent nature of the threats.

The term security vulnerabilities refers to the weaknesses in the construction, functionality and operation of information systems that expose them to the accidental or intentional realisation of security threats.

The intentional exploitation of information system vulnerabilities is known as a method of attack. The methods of attack used may vary according to the nature and functionality of the system and its components as well as the objectives and skill of the attacker.

The following analysis mainly concentrates on the vulnerabilities and methods of attack that generally fall within the scope of IT to address.

Copyright © 1994 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

A.2 Unauthorised Modification

With respect to unauthorised modification there are two areas of concern and vulnerability:

- modification of software and hardware
- modification of user, application and system data.

A.2.1 System Software and Hardware Modification

Absence of, or poor system configuration management facilitates the introduction of unauthorised software and hardware components. Such components may accidentally or intentionally contain malfeasant functionality that can damage the integrity of the system. Examples of such attacks are described in the following sections.

Introduction of Malfeasant Software

The common forms of this are:

- *Virus software* : this has the capability of propagating itself and often carrying a payload designed to perform some malicious act.
- *Trojan horse* components: these partially or fully emulate security-relevant software components in order to capture and relay security-sensitive information.
- Security and business-relevant software components containing *trapdoor* functionality:this permits those who know about it to bypass some part of its normal functionality. This category includes the wide range of flaws and undocumented features common to much software.
- Software components designed to perpetrate some malicious or fraudulent act either at some specific time or when signalled to do so: these are sometimes referred to as *logic bombs* . They may be inserted as part of a virus, or be specifically engineered, usually by someone with detailed knowledge of the target system.

Introduction of Unapproved Hardware

Unapproved or unchecked hardware containing hardware and firmware features and functionality that allow existing security mechanisms to be bypassed.

Copyright © 1994 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

A.2.2 Data Modification

The preservation of the integrity of enterprise-sensitive and critical information is usually based on the concepts of well formed transactions. Such well formed transaction models specify the stages in the life cycle of each type of enterprise information. For each stage, whether it be information creation, modification, transmission, or destruction, the well-formed transaction model should capture and define the authorisations and cross checks required to perform the stage.

Vulnerabilities and methods of attack on the integrity of system, user and application data depend on the completeness and correctness of the appropriate transaction models as well as their IT implementation.

A generalisation of the weakness of and attacks on the integrity of system, user and application data is presented in the following sections.

A.2.3 Transmission

Interception and Modification

Information communicated over networks can be intercepted and modified as it passes through weakly defended or uncontrolled links, routers and nodes. The classic example given is the modification, upwards, of the financial amount field of an authorised message requesting a credit to the attacker's account. (This is a somewhat naive example given the level of secondary checking usually accompanying such transactions, but more realistic examples can be envisaged for other areas of integrity-sensitive communications.)

Insertion and Replay

Messages, possibly previously intercepted and modified, are introduced into the communication traffic either as part of a masquerade or fraud attack, or just to damage the integrity and availability of the communication services.

A.2.4 Storage

The integrity of stored data can be accidentally or intentionally compromised in a number of different ways. Many of these result from poor access control facilities. Access control facilities should govern not just who has access to what stored information but also what tools and utilities can be used to access the information. (The more physical ways in which data storage media can be corrupted must be addressed by disaster planning and recovery, although software tools may be used to detect such physical corruption.)

Specifically Targeted Data Modification

As for transmitted data, specific stored data item values can be changed to support a fraud attack or to facilitate the operations of the attacker in some other endeavour.

Copyright © 1994 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

Data Contamination and Corruption

Localised or general corruption of stored data may be either immediately obvious or only discovered after some time. The latter is more insidious as it could be copied into the entire backup archive.

Deletion

The unauthorised removal of sensitive stored data.

Creation and Replacement

The unauthorised introduction or replacement of sensitive information.

A.2.5 Processing

Malfeasant Software

The concern here is in the trustworthiness of the software components used to process sensitive information. Attackers may introduce their own versions of regularly used tools and application components, see malfeasant software above. These can be designed to modify specific instances of data to achieve any one of the range of objectives identified in this appendix.

A.2.6 Modification of System Data

The system and security administration data, and the services used to maintain this system data, determine the current operational configuration of the system. If not adequately protected, system and security management data is susceptible to all of the attacks already described, however, as it is critical to the general preservation of system security, it is explored further here.

There is a wide range of options available to the attacker as to how to exploit vulnerabilities in this area. Some of these are reasonably direct, obvious and detectable; others are more subtle, insidious and less easily detected. Examples are given in the following sections.

User Account Modification

Unauthorised access to user account or profile data and services can be used to:

- Create unauthorised user accounts.
- Increase or decrease the privileges and authorisations assigned.
- Discover and use redundant user accounts.
- Remove active user accounts.

Communication Configuration Modification

Unauthorised access here can be used to create or modify communication addressing and routing parameters at different levels of communication service in order to open up new channels and even redirect communication.

Copyright © 1994 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

Changing Clocks

There is an increasing number of security mechanisms that are dependent on correct time synchronisation. An attacker who manages to falsify a system clock may well succeed in defeating these mechanisms.

System Service Modification

More generally, inadequately controlled access to system administration and management services can be exploited by an attacker to perform disclosure, modification and denial of service acts.

A.3 Unauthorised Disclosure

There is a variety of ways in which the confidentiality and privacy of information within information systems can be compromised. The vulnerabilities to unauthorised disclosure threats occur in the following areas.

A.3.1 Transmission

Eavesdropping

Sensitive information transmitted over local and particularly wide area networks is liable to eavesdropping at diverse points in the layered communication services and networks. The term *sniffer* is used to cover a component designed for eavesdropping. Typically a sniffer is placed at some strategic point in the communication services from where it can observe and report sensitive transmitted information, for example user ids and passwords.

Traffic Analysis

In certain cases the frequency, volume, origin and destination of messages is considered to be confidential information. An attacker may discover such information through the analysis of communication traffic flow.

A.3.2 Storage

Copying

Information, as variously stored, can be subject to unauthorised copying using any one of the many IT techniques and tools for reading and producing copies of stored information.

Garbage Searching

A sometimes overlooked vulnerability arises in the tendency within all levels of information system services to make transient copies of information as it is processed and transmitted. These copies often take the form of large internal buffers or temporary files occupying reusable *garbage space*. Thus an attacker may use the electronic equivalent of garbage collection and analysis.

Copyright © 1994 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

A.3.3 Processing

Malfeasant Software

As for unauthorised modification, attackers may introduce their own versions of regularly used tools and application components. These can be designed to capture and relay the sensitive information they process.

Electromagnetic Radiation

If not adequately shielded, computers, terminals and electronic communication equipment radiate electromagnetic signals which can be picked up at distances varying according to the strength of the signal. With the appropriate equipment, the displayed, processed or transmitted information can be reconstructed.

A.3.4 Indirect Disclosure Vulnerabilities and Attacks

There are more derived classes of confidential and private information that are subject to indirect and subtle forms of attack. Examples are given here to ensure that they are included in the future development of X/Open security guidelines.

Aggregation

Sensitive information may be deduced through the assembly of less sensitive information. For example, this could be achieved by the unauthorised construction of a detailed description of an individual by aggregating the parts of the description from different sources.

Deduction

The very fact that certain data is being held on a system or database may be considered to be sensitive information. Although unauthorised direct access to this data may be effectively prohibited its presence can sometimes be deduced from the responses to carefully constructed searches.

Listening

Microphones and voice recording services are features recently introduced on some workstations. It appears that in certain cases the default configuration of these services permits other users, possibly remotely, to turn voice recording on without there being any visible indication to the owner of the workstation. This disclosure vulnerability is included here to indicate the ever widening range of disclosure weaknesses in modern information systems.

Copyright © 1994 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

A.4 Unauthorised Use of Resources

Unauthorised use in its widest context includes the theft of hardware and software resources. Although schemes and mechanisms for the electronic tagging of physical computer assets are emerging, addressing these is not currently within the scope of the Framework. Similarly software licence management is outside the current scope.

Within scope are the vulnerabilities to the unauthorised use of systems and the services they offer. Weaknesses in the control of access to these resources can then lead to disclosure, modification, repudiation and denial of service attacks. The converse is also true, in particular disclosure and modification vulnerabilities can facilitate unauthorised use attacks.

A.4.1 Discovery and Use of Authentication Credentials

Identification, but principally, authentication credentials are used to establish the authenticity of authorised users and other entities, such as systems and their component services, and even hardware. In many cases mutual authentication is needed to counter masquerade by either party.

With respect to entity authentication credentials, the main area of vulnerability lies in poor measures governing use, selection, renewal, and safe transmission and keeping of these credentials.

Where entity authentication credentials are used, the receipt, passing (sometimes over dubious long haul networks) and storage of authentication credentials may be liable to the attacks described below. Discovered authentication credentials may then be used to masquerade as the entity by reusing the credentials or replaying them over the network.

Trojan Horse
Trojanisation of some part of the identification and authentication functions.

Eavesdropping
Interception when passed over local and wide area networks.

Accessing the Credential Store
Discovery of authentication credentials by access to their stored representation. Here, even though the credentials may be stored encrypted, poorly selected credentials may be liable to brute force decryption attacks.

A.4.2 Acquisition of Authorisations

As already identified under unauthorised modification of system data, an attacker can exploit weaknesses in the protection of authorisation information to acquire further authorisations and thus access services and information beyond that normally allowed to them. For example, in UNIX-like systems there are a variety of ways in which an attacker can acquire *root* or *superuser* authorisations.

Copyright © 1994 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

A.5 Denial of Service

Information system vulnerabilities to denial of service and availability threats abound. They include areas of obvious concern such as:

- dependency on continuous power supply and communications links
- system hardware component reliability
- system software component reliability.

These are generally well recognised areas of system availability management and planning. The establishment of disaster strategies and plans, and the regular taking and securing of backup copies of sensitive information, is appreciated by most and practised by many. Apart from physical events and acts the accidental or intentional denial of service can be caused by:

Unreliable Software
This is the most common cause of denail of service.

Malfeasant Software
Many of the types of malfeasant software attack can be used to destroy or cripple a service.

Swamping
The availability of a system or service to authorised users can be severely reduced by flooding it with requests. Swamping may also overwhelm the system or service by exhausting the storage associated with it.

Of concern to information system security are attacks that aim to disable some part of the existing security mechanisms. By taking advantage of the fact that on failure, either the system or some security relevant service, does not fully recover to a secure state, an attacker may bypass the normal defences.

A.6 Repudiation

Repudiation attacks are predicated on the existence of some measures for making users and other entities accountable for their business-sensitive or security-sensitive actions. There are two such general mechanisms:

Audit logging
This is the recording each action and the identity of the responsible entity in an audit trail.

Sealing and Signing
This is the binding the identity of the responsible entity to information produced by the action.

The often quoted example of the latter case is the binding of digital signatures to electronic mail messages. In both cases additional information such as location, context and particularly time is usually recorded.

Copyright © 1994 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

Attacks on such measures and mechanisms are levered off more basic attacks.

Masquerade
The use of the identity of another entity hide the true responsibility.

Audit Trail Modification
The breaching of the access controls to the audit trail and changing or deletion of all or only relevant audit records.

Malfeasant Software
The use of unauthorised software to perform the operation and to omit or falsify the record or signature.

A.7 Lack of Awareness and Utility

To put things in perspective, currently the most common vulnerabilities arise from the lack of awareness of information system security concerns, needs and practices by the users and owners.

There is often failure clearly to assign to users and administrators responsibility for information security. Addressing this falls outside the scope of X/Open specifications. However, the concept of security domains, as described in does provide a useful way of establishing boundaries of security responsibility and jurisdiction.

There are system security awareness and utility issues that do fall within the scope of the framework. They are summarised in the following sections:

Awareness

Not knowing in sufficient time that a system has been attacked or that its security has been compromised. The vulnerabilities arise from inadequate measures for detecting and reporting attempted or successful attacks. Damage limitation and control is obviously dependent on timely detection and warning.

Utility

Even though strong security measures may have been deployed, if these are difficult to use and manage, then their effectiveness is significantly diminished.

From the users' point of view, if the security behaviour of the system appears to impede normal operational efficiency, they are encouraged to find ways round the system's security.

The effectiveness and utility of system and security management are currently one of the greatest areas of vulnerability within distributed systems. Lack of facilities that allow large, heterogeneous distributed systems to be easily managed almost guarantees that they are riddled with vulnerabilities.

Copyright © 1994 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.

A.8 Assessment of Threats, Vulnerabilities and Risks

Security threat and risk assessment is typically an iterative process applied at each level: enterprise, information system, information sub-system and IT service. Simply, the assessment steps are:

- Identify what assets have to be protected against which threats.
- Determine the vulnerabilities which can manifest these threats.
- Estimate the risks of these vulnerabilities being exploited.
- Where the risks are unacceptable, identify and specify a set of countermeasures to the threats with the aim of reducing the vulnerabilities and associated risks to acceptable levels.

The information system security concerns (risk weighted threats and vulnerabilities) may vary from one enterprise to another. The proposal here is to use functional profiles to generalise these concerns.

However, in the X/Open specification for each of the major functional areas of IT the list of threats, vulnerabilities and methods of attack, given above, should be interpreted and adapted to the context and functionality of each area and component.

Copyright © 1994 IEEE. All rights reserved.
This is an unapproved IEEE Standards Draft, subject to change.