4. Security Services

In this section the OSI security services are reviewed as they apply to ISDN. The possibility of extending the services to include additional services from ECMA 138 is also discussed.

4.1 Integrity Service

Integrity services are generally provided for digital data by means of an *Integrity Check Value (ICV)*. The ICV is a field whose value is a known function of all the protected bits in a packet. The ICV is then encrypted with a private or secret key. An intruder can modify a packet and can compute the correct ICV of the modified packet, but cannot then encrypt the ICV. Alteration of the packet can be detected. This provides connectionless integrity. If the ICV covers an appropriate timestamp field, then connection replay attacks can be prevented. The integrity can be extended to full connection integrity by including appropriate sequence number fields within the range of the ICV.

To provide connectionless integrity it is only necessary to encrypt the ICV of a packet. Many packet protocols include a *Frame Check Sequence (FCS)* which is a value computed from all the bits of a packet, used to detect transmission errors. Similarly, many protocols include sequence numbers in each packet, and may use them to detect lost or duplicate packets. Although common FCS's are not ideal ICV's, when packets from such a protocol are encrypted, at a lower layer, then at least a degree of connection integrity is the result. The LAPB and LAPD Data Link layer protocols used with ISDN provide both sequence numbers and an FCS. X.25 provides 3 or 8 bit sequence numbers, which might allow some replay attacks. Security protocols may provide extended sequence number or timestamp protection.

4.2 Non-Repudiation Service

A message may be signed by encrypting the ICV of a packet or message with a private key known only to the originator of a message. If the message contains a date and time, and the recipient checks the time of arrival and keeps a signed copy of the message, then the recipient has non-repudiation with proof of origin.

The purpose of non-repudiation with proof of delivery is to prevent a recipient from falsely denying that he received a message. A form of non-repudiation with proof of delivery can be obtained if the recipient signs the message he receives plus a timestamp and returns that to the originator. While such a mechanism will cover many needs, it is not a complete solution, because the recipient, having seen the message, can decline to confirm its receipt. If electronic communications are to substitute for registered mail, or a process server, then some mechanism which does not require the cooperation of the recipient is required.

Notary mechanisms have been proposed, involving a trusted third party, which delivers the message to the recipient and keeps a copy of the message or a digest of the message. The recipient, having read the message, may, however, falsely claim that the communication line was broken. It may be useful, then, to perform a test of the communication line, requesting a signed acknowledgment prior to sending the data itself. This would be proof that the communications were operational at least immediately prior to sending the message. If, however, a recipient is expecting the equivalent of an unwelcome subpena, the recipient may not respond to the initial communication. Legislation may be needed before non-repudiation services can supplement or replace traditional mechanisms for provable communications.

Non-repudiation is ordinarily considered a layer 7 function, and outside the normal scope of ISDN. However, voice, or facsimile non-repudiation services, may appropriately be considered

ISDN services. Modern digital signal and image processing probably makes it practical, perhaps easy, to make undetectable alterations to any electronic image or voice recording, unless the image is protected by a digital signature. A trusted voice notary service, for example, might be used to produce a signed digital recording of a voice call. Such a recording could not be altered by either of the parties to the call.

4.3 Confidentiality Service

Confidentiality can be assured by end-to-end encryption, physical protection of the entire network, or by secure routing, which ensures that each subnetwork or link through which the data passes is protected by either encryption or by physical means.

Since the cost of physical protection increases with distance, physical protection of the entire ISDN public network is infeasible. Nor is it practical to physically protect long individual communications links. It is feasible to have protected installations, which are closely guarded. This generally requires that all personnel entering the installation be cleared or escorted. While this is expensive and cumbersome, it may be required by the nature of the work done in the installation. In such an environment additional protection is sometimes provided by enclosing communications links in a pressurized shield and detecting the loss of pressure which may accompany any attempt to penetrate the shield.

It is sometimes claimed that fiber optic links are difficult or impossible to tap. While noncryptographic means of protecting fiber communications exist, these means are logically equivalent to link encryption. It is only marginally more difficult to tap fiber links than electrical networks. Security is somewhat improved when particularly vulnerable links, such as terrestrial or satellite microwave links are replaced by optical fiber, but fiber optics by itself does not provide strong confidentiality.

Encryption will be the principal mechanism for ensuring confidentiality in wide area networks such as ISDN, because its cost does not scale with distance. Encryption can be located at any layer of the OSI model and provide both confidentiality and (often in combination with an integrity check value and/or appropriate message sequence numbers) integrity services. Perhaps most important, it can provide end-to-end confidentiality and integrity through otherwise insecure channels, without any change to the network.

Encryption algorithms are conventionally broken down into two general classes:

- *symmetric* or *secret key* algorithms, in which both parties share the same secret key. Examples include the DES [FIPS 46] and the *Fast Data Encipherment Algorithm FEAL-8* [MIYA 88]. These algorithms can be computationally efficient, and the DES has been studied for more than a decade without publication of successful attacks, leading to some confidence in their basic security. The greatest difficulty symmetric key algorithms is the difficulty of managing the secret keys.
- *Public key* algorithms, which use both a public and a private key. In the most general case plaintext enciphered with the public key can be recovered only by use of the private key and vice versa. In some cases the algorithms simply allow two parties to securely negotiate a secret key over a nonsecure link. The *Diffie-Hellman* algorithm [DIFF 76] and the *Rivest, Shamir, Adleman (RSA)* algorithm [RIVE 78] are probably the best known algorithms published to date. These two algorithms, as do several other algorithms, require the exponentiation of large numbers, a computationally intensive process, which limits their speed. Breaking these two algorithms is believed

(but not proved) to be respectively equivalent to two intensively studied difficult problems in mathematics, the discrete logarithm problem and factoring large numbers.

Both symmetric key and public key cryptography can be combined on one system, using each to best advantage. For example, one experimental X.25 cryptographic system uses the Diffie Hellman algorithm to derive a common secret DES session key, and uses the RSA algorithm for authentication and signatures.

4.4 Authentication Service

The framework for Directory authentication is ISO/IEC 9594-8, while a draft OSI Authentication Framework [JTC1 1] provides a draft authentication framework for OSI. The Directory application (X.500) provides a repository for attributes (information) about named objects in a *Directory Information Base (DIB)*. The Directory will provide a digital signature mechanism, which will allow users to verify information placed in the DIB by a *Certification Authority* , including the public keys of users. The main security feature of the Directory is to provide a secure mapping between users and their public keys.

The draft OSI Authentication Framework provides a broad overview of authentication and outlines a number of schemes for authentication. It defines two classes of authentication, Class 1, which provides protection against disclosure of authentication information, but is vulnerable to replay attacks, and Class 2, which provides assurances against replay and masquerade attacks. Class 1 mechanisms require encryption or one-way hash functions. Class 2 functions require unique numbers and challenges as well as encryption or one-way hash functions.

A one-way hash function transforms data in a way that is not reversible. A one-way hash function is easy to compute but difficult to invert. Given the output of the hash function it is not practical to compute an input value which results in that output.

ISO/IEC 9594-8 defines two classes of authentication, *simple authentication* and *strong authentication.* Simple authentication procedures rely upon a secret password known to the user. The name and password of user A are transferred to B, possibly with a timestamp and random number. The passwords may be protected by a one-way hash function. In a simple protected authentication, for example, A sends B an authenticator consisting of a timestamp, a random number, A's distinguished name, all in the clear, and a protection parameter generated with a one-way function from the first three parameters plus A's secret password. B then accesses a local copy of A's password to generate the protection parameter, which it compares to the protection parameter received from A.

Simple authentication is most useful for access to local systems and equipment. Where access is restricted to ISDN TE or services, a simple user authentication process is appropriate. Simple authentication is less useful in the more general case, where A wishes to be able to authenticate to any B through the ISDN network. B must either have A's protected key, requiring that B be trusted by A, or some third party trusted by both A and B, with knowledge of the secret key, must be invoked to check the authentication.

Strong authentication requires the use of public key cryptography. Public key algorithms used for strong authentication have the property that $X_p \bullet X_s = X_s \bullet X_p$, where X_p and X_s are the encipherment functions using the public and secret keys, respectively. A certification authority produces *certificates* for users which include the distinguished name of the user, the validity dates of the certificate and the public key of the user. The certificate is protected by the *digital signature* of the certification authority. That signature contains a summary of the certificate

produced by a one-way hash function and enciphered with the secret key of the certification authority. The encipherment ensures that the certificate cannot be forged.

The certificate is not secret and can be contained in the Directory without protection and be freely distributed. Because it is signed it cannot be forged or altered without knowledge of the certification authority's secret key. Any user knowing the public key of the certification authority can check the validity of the certificate. Two users, A and B, may not share the same certification authority. However, the certification authority for each may contain certificates for other certification authorities through which it is possible to construct a *certification path* between A and B. A certification path forms a logically unbroken chain of trusted points between two users who wish to authenticate. When A authenticates to B, B obtains A's public key from A's certificate. A produces an authentication token message containing the certification path from B to A, and a signed portion consisting of a timestamp, a non-repeating number and B's name. B can obtain the public key of A from the certification path and decrypt the signature which can only be produced using A's secret key. A two-way strong authention requires B to return an authentication token including the random number from A in the signature. An alternative three-way authentication allows the timestamp to be dispensed with.

ISO/IEC 9594-8 provides a directory foundation upon which ISDN authentication may be built. ISDN users may be bound to a specific TE, in which case the necessary authentication processes, keys and passwords may be stored in the TE. Access to the TE may be physically controlled, the user may authenticate to the TE (typically with a password and simple authentication), or possession of a physical token may be required for authentication of the user to the TE, which then authenticates to remote TEs. In this mode ISDN places no additional constraints on normal OSI authentication.

ISDN users, however, are frequently not bound to a specific terminal. They wish to be able to use any ISDN telephone terminal and authenticate from it. In the absence of a better authentication service for terminals, the Calling Line ID supplementary service will be used for authentication. This service, while useful to businesses (for example, to automate the retrieval of customer records when a call is received), is not a reliable means of authentication of individuals and is objectionable to some in that as implemented it is often automatic and involuntary. Moreover, individuals wish access to services from any terminal, not simply their home telephone.

Today, when ordinary telephones are used for remote access to services requiring some form of authentication, an account number and a password or *personal identification number (PIN)* of some kind is usually entered through the keyboard. An intruder tapping the communications link immediately learns the password. A different password is required by each user. Since passwords should be memorized, so that they cannot be stolen, they are usually only a few digits and an individual can only memorize a few frequently used passwords.

Many specialized transaction terminals now use standardized plastic magnetic stripe cards. These may be calling cards, bank cards or travel credit cards. These cards can be read with readers built in terminals, and may be augmented by requesting a password or PIN. These cards at present are widely used as authentication tokens for a variety of commercial transactions. When used through the telephone network without a special reader, the number of the card is either stated verbally, or entered through the telephone keyboard. When used without a reader the number is stated verbally, or entered through the keypad.

Cards can be stolen and numbers obtained by employees of businesses when the cards are used. The cards are vulnerable in that they can easily be copied. While card transactions are routinely

checked via the public network against lists of valid and stolen card numbers, fraud is widespread. Many individuals find it expedient or necessary to carry several different bank, credit, travel and calling cards. Each may have its own unique PIN. Individuals, unable to memorize several different PINs, write them down and carry them, allowing both the PIN and card to be stolen.

"Smart cards," which contain integrated circuits on a small card somewhat similar to a credit card in size offer the prospect of strong personal authentication. Haykin [HAYK 88] provides an introduction to smart card technology, which is evolving rapidly. The authentication card would be issued by a certification authority to a person and might include a certificate signed by the authority, giving the privileges of the person, and perhaps containing personal identification information, or even an image of the person. The person's private key would be stored on the card and the card would be designed to prevent it from being read directly. Logic to perform a one way hash function to check a personal password might also be contained on the card.

If a standard for such cards were adopted, interfaces to the cards could be built into ISDN terminals and other equipment, such as personal computers, requiring user authentication. The card could be used as an unforgable authentication token. If personal identification information were included in the certificate, then sales personnel could compare the user with the information. As further a check against stolen cards, the user might be required to furnish a password to activate the authentication.

While universal, standardized strong personal authentication would make a dramatic contribution to ISDN security, the topic transcends ISDN and the communications industry. It involves the financial, banking, retail and service industries, and has profound social implications. An authority (or multiple authorities) must be recognized to issue certificates. A widespread standard for strong personal authentication could be a major social issue and could easily be viewed as a sort of national identity card.

4.5 Access Control Service

Access control in the context of a communication network such as ISDN is not quite as complex as it is in the context of distributed computer systems, since a network does not store data beyond that required for its operation. There are three principal access control concerns for ISDN security:

- Network access
- Terminal or CPE access
- Access to network data bases

The ISDN access control issue is, is the user authorized to use the network or a particular network service? For example, is the user authorized to place a long distance call, an international call, or, perhaps, a secure call? In the case of an installation with ISDN PBX, the PBX can enforce user access control checks. While standards are not necessary for such services in PBX's, without them terminal interchangability might be poor. The simplest solution is to bind the access privileges to the terminal. This changes the access control problem to one of controlling access to terminals.

In the context of the public network, the problem is more complex. There is no good personal authentication standard. It is reasonable to expect that service providers might eventually offer some sort of password protection for specific services. This would probably not provide strong protection, but might, for example, suffice to prevent children from making long distance calls or

from calling 900 numbers. Indeed it is possible that carriers may be forced by PUCs or legislation to provide some sort of access control, particularly in the context of controlling access to sexually oriented 900 services.

Terminals can have both inward and outward access controls. With outward access controls the issue is, may the user place a particular type of call (based upon its service class or destination) from the terminal? With inward access controls the issue is, is the caller authorized to call this terminal?

Outward access controls can be readily built into terminals, with or without standards. Some sort of token or password may be required to use a terminal. If this is done, and there is some sort of authentication of the terminal to the switch, or if it is physically difficult for an intruder to exchange his terminal for a controlled terminal on a particular line, then network access controls based on binding privileges to specific lines may be extended to the user layer. Even if there are no network access limitations on a line, a terminal with built in access controls may prevent use of that terminal by unauthorized individuals.

Inward access controls require standards. The only present useful standardized ISDN service is the Calling Line ID supplementary service. Terminals (or PBX's) could refuse to accept calls from any number other than those specifically authorized. This should be thought of more as a screening mechanism than a strong access control, since it is not built upon strong authentication.

Control of access to the network databases (including databases maintained by PBXs) is vital. The subject is complex and largely beyond the scope of this report. Databases containing records of calls are confidential and unauthorized users must be prevented from accessing them. Databases maintained for routing and the management or maintenance of the network must be protected from unauthorized modification. An intruder might either modify them to perpetrate a fraud (for example by deflecting calls from their proper destination) or to disrupt the operation of the network.

Effective access control requires effective authentication. The primary need, then, to enable access control, is standards for effective authentication. If a standard system for strong personal authentication were adopted, for example using smart card technology, identification and authentication could be separated from privileges, or provision could be made to bind all privileges in one card. Including privileges (*e. g.*, a credit limit of a certain amount) with authentication in one card would simplify exercising those privileges, since no check with any remote authority would be required. However, since privileges may change rapidly, it would be more secure to separate privileges from authentication, and maintain them in a secure database. ECMA 138 proposes such a mechanism for Privilege Attribute Certificates.

4.6 Security Services From ECMA-138 for ISDN

In addition to the five security services of ISO 7598-2, it is useful to consider extending the services for ISDN to adopt concepts introduced in ECMA 138. As stated in section 4.2 above, ECMA 138 deals with Authentication and Access Control in the broad context of distributed computer systems. ECMA 138 articulates the concept of a Privilege Attribute Certificate (PAC) as well as a Security Attribute service and an Interdomain service, which provide an approach to addressing Access Control and Authentication.

ECMA expands the Directory Certificates, used only for public keys, to PACs which contain additional security attributes. ECMA 138 does not consider the X.400 Directory to be suffi-

ciently secure for PACs. ECMA 138 also considers interworking between different security domains and postulates a Security Attribute Service, which maps or translates attributes for labelled objects and an Interdomain Service, which is trusted to translate PACs between domains and reseal them.

In general, ECMA go well beyond what is ordinarily thought of as communications security. However it has application to two specific problems in ISDN:

- ISDN network database access control, which in a public network is a serious and difficult problem.
- Interdomain security interworking, which is also a serious concern for a public network. It is also essentially a research subject at this point, in any general context.

ECMA 138 also explicitly recognizes that, to maintain security, security information must be collected and defines a Security Audit Information Service. This service automatically records security-related events. For example any access or attempt to access the databases maintained by the network itself is a security-related event. In principle, any use of the network is potentially security-related, however privacy concerns will require that suitable criteria be developed for screening the events to be recorded in a public network, and only the time, parties and network services utilized will probably be recorded (which are needed for billing as well).