3. Discussion of ISDN and Security

This section provides an introduction to the ISDN and ISDN security.

3.1 Overview of ISDN

At its conception a decade and a half ago, the ISDN was projected to be the universal network which would go everywhere and handle all voice and data applications. Developing one integrated network to serve nearly all voice and data applications was probably never realistic. As ISDN becomes a reality, it is proving to be somewhat less than universal. Nevertheless, it is an important development in the worldwide public network and will considerably extend its utility for data. The digital nature of ISDN also offers an opportunity to provide security services which were previously impractical.

3.1.1 ISDN User Service Interfaces

The ISDN provides digital voice and data services to public network subscribers. Two somewhat different service interfaces are offered by public network service providers:

- *Basic Rate Interface (BRI)*, which provides a single physical line with two independent, circuit switched 64 kbps "*B channels*" and one 16 kbps packet "*D channel*." The B channels may be used for digital voice or to provide a direct digital 64 kbps isochronous channel between computers or other digital devices. Service providers and independent networks will also offer B channel packet services. The D channel is used for signaling, that is to exchange control information between an ISDN terminal and a network switch (for example to set up B channel calls). The B channel also provides packet switched services to users. The ISDN network provides for conversion between the new digital voice services and existing analog terminals, so it is possible to complete a voice call between a digital ISDN terminal and an analog telephone. Up to eight terminals can share one ISDN line in an arrangement called a passive bus. The BRI service is often called "2B + D."
- *Primary Rate Interface (PRI)*, which, in North America, bundles together 23 64 kbps B channels and one 64 kbps D channel (or "23B + D"). It is equivalent to the established T1 1.536 Mbps telephone carrier. The 23 B channels can be independently circuit switched through the network, and each can carry voice or data. The D channel again carries signaling packets (for example to set-up each of the B channels). It may also carry packet switched user data packets. The PRI is primarily used to connect a user Private *Branch Exchange (PBX)* or multiplexor to the public network. In the world outside North America, the PRI is usually 30 B channels plus 1 D channel (30 B +D).

At the present time the ISDN services are just becoming available from network services providers. They are expected to be widely available by the mid 1990's. There will be a transition period of more than a decade while the ISDN gradually supplants the present analog service. There are a number of texts which provide a detailed introduction to ISDN [STAL 89], [VERM 90], [BOCK 88].

3.1.2 Historical Perspective

The conversion of the analog telephone network to a digital network has been under way for about 30 years. Digital computers proved to be first a flexible way to control and add new features to otherwise conventional analog switches. Digital trunks provided a means of carrying signals without adding noise as lengths were extended. By 1980 advances in digital semiconductor components made all digital switches advantageous.

By the mid 1970s it was apparent that new standards would be required for the interworking of the emerging digital networks and the CCITT began the process of developing the Integrated Serviced Digital Network. The CCITT operates on a 4 year cycle in issuing its recommendations. By 1980 the general architecture of ISDN we know today had been defined by CCITT, specifically the basic circuit switched 64 kbps B channel and the bundling of two B channels with a 16 kbps packet for out-of-band signaling, into the fundamental 2B + D service. The concept of primary rate service at higher rates (1.536 Mbit/s in North America and 2.048 Mbit/s in Europe) and various user interfaces (S and T interfaces) and Network terminations (NT1, and NT2) were well established.

The 1984 CCITT recommendations provided the basis for the first commercial ISDN products. In general, however, they were not sufficient for interworking of products from different vendors. The refinement and completion of the recommendations continued in 1988, improving interworking, but products based on the 1988 recommendations still fall short of the goal of full interworking of terminals with switches from different vendors.

In the mid 1970s when the ISDN was conceived, international telephony was largely characterized by national *Postal, Telephone and Telegraph (PTT)* government monopolies. That is, one government agency typically controlled all national communications services. Competition for network switching equipment was generally limited to one or two national suppliers (except in third world countries without an electronics industry). In the United States there was not a PTT, however one large regulated private company, AT&T,* dominated long distance and local telephone service, as well as the manufacturing of switching gear and terminals. Although about half the local lines in the country belonged to smaller independent companies, AT&T effectively provided the technical standards for the entire nation.

ISDN, as originally conceived, dealt largely with the interfaces between terminals and the network, and with the international services to be transferred across network boundaries, but not with the interconnection of switches within the network. ISDN defined interfaces with customer premisses equipment, not network trunk interfaces. The market for terminals was seen as broadly competitive, requiring standards, but not the market for switches or network trunks. Standardization of services was required to permit their transportation across (usually international) network boundaries. The internal organization of national networks was seen as not subject to standardization, and the interfaces between national networks could even be accomplished in a case by case manner, if the services were standardized.

Security, except as it is improved by the out-of-band D channel signaling, was not considered in the development of the ISDN standards.

The situation has changed. In the United States AT&T has been broken up into seven regional operating companies and one long distance and manufacturing company. Two other significant companies contend for long distance business, and the long distance carriers compete with the regional companies to interconnect large accounts within the territories of the regional companies. An apparatus of standards committees has partially replaced the technical standards setting function of AT&T. Only local residential and small business service remains a monopoly, reflecting the high cost of the copper twisted pair local distribution plant. Even this monopoly

---

* Certain commercial organizations are identified in this publication. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology.

may be subject to challenge in the next decade by cable TV operators and cellular telephone networks.

Other parts of the world are moving in the same direction, introducing competition and privatizing national telephone systems. Moreover, a number of companies have built large private networks to serve their needs. The largest of these has 8 million km of cable and connects 300 mainframe computers, 2,000 minicomputers, 300,000 computer terminals and 250,000 telephones [ECON 90].

Traditional telephone carriers are also being forced to compete with mobile telephone systems. The cellular mobile telephones market over the past decade has been the big new growth area in telephony. Emerging standards for digital mobile cellular telephony will further enhance the capacity of these networks. It is not unthinkable that residences might be served by cellular radio telephone service, perhaps greatly reducing the cost of the local plant. Unprotected broadcast telephone service is, of course, easily intercepted.

There has been an increase in competition between central office switch vendors and a consolidation of that business. At the same time, within networks, the diversity of switching equipment is increasing as traditional exclusive ties to vendors are cut. To compete, network service providers need alternative switch suppliers.

There is now a stronger need for standards affecting the internal aspects of ISDN networks, including internal network security (that is to protect the integrity of the network itself and to protect service providers against fraud, rather than to protect the security of user communications). With more diversity in the networks, there may also be more exposure to security vulnerabilities. Moreover, as the number of networks proliferates, the need for security standards between networks increases. When one monopoly service provider served a nation, internal network security could be treated as an internal concern of that supplier and not properly the subject of standards. When that monopoly is replaced by many competing but interoperating networks, many aspects of network security can only be dealt with via broadly accepted standards. A detailed consideration of this important subject is beyond the scope of this document.

Another consequence of the breakup of national monopolies is that it reduces any possibility of the user simply relying on the public network to provide secure communications, even within one nation. Whatever network security standards there may eventually be, there will be too many independent service providers for users to rely on the "public network" to provide him with strong, consistent security. While it may be possible for network service providers to offer some security features and services, it will not be practical to simply secure the link to the network switch and then rely on the network thereafter. Users who wish secure end-to-end communications will have to rely on user to user protocols and standards. This report focuses on the user-to-user protocols and the services which will be needed to support them.

3.1.3 ISDN Principles & Goals

The original principles of the CCITT ISDN standards are outlined in CCITT Recommendation I.100. They are:

a) the standardization of services offered to subscribers, so as to enable services to be internationally compatible;

b) the standardization of user-network interfaces so as to enable terminal equipment to be portable (and to assist in a);

c) the standardization of network capabilities to the degree necessary to allow user-to-network and network-to-network interworking and to achieve a) and b) above.

Terminal portability and the ability to transport services internationally were the major goals. To those ends user-network interfaces, services and capabilities are standardized. While network capabilities are standardized, internal network interfaces are not included in this list, and portability of network switching or transmission equipment between networks was not a goal.

The present goals of network service providers have undoubtedly evolved and are much broader. One principle, not stated by I.100, but undoubtedly implicit in ISDN from the very beginning, is that ISDN is compatible with the preexisting analog/digital telephone system and interoperates with it over a long transition period. A corollary to this principle is that ISDN must preserve the large investment in copper twisted pair distribution loops, that is it must operate over them. They are one of the principle assets of network service providers.

Another goal is to provide end-to-end digital connectivity. Although computer data traffic is a small part of the overall network load, it is a fast growing part. Facsimile, traffic, also digital, is growing very rapidly. The digital B channel service provides about a 4:1 improvement over the data rates which can ordinarily be achieved over analog voice circuits.

Integration of access and service is implicit in the name. One unified access method is defined for a variety of services and features. Customers can request the services they require on a call by call basis.

While terminal interfaces (the S and T interface points - see sec. 5.1.4 and fig. 11 below) were standardized by CCITT, the network interface was explicitly not defined. In the spirit of keeping the network itself relatively unconstrained by ISDN standards, a network provided termination (NT1) converted the network interface to the terminal standard at the user premises. Each network might theoretically have its own interface. In the United States, this has been overturned by the FCC, and a standard for the U interface has been defined. Neglecting differences in connectors, however, the S and T interfaces remain consistent.

Interchangability of network switching equipment and communications links has become a goal of the service providers. Network service providers need the advantage of multiple equipment suppliers to be able to offer competitive prices and services to their customers. This change in emphasis may not yet be fully reflected in the present CCITT ISDN standards, but it is the focus of much service provider activity. Indeed the present emphasis is more on installing the ISDN infrastructure in the network switching plant and internal operation of the public network than in broadly offering ISDN services to users.

3.1.4 Reference Models for ISDN and the Relationship to OSI

The Reference Model for Open Systems Interconnection was briefly described in section 4.1 above. Figure 1 above illustrates the seven layer OSI protocol stack. As noted above, the OSI protocols are peer-to-peer protocols, and the vertical interfaces are defined only as logical service primitives. An observer on the interconnection medium will see a series of nested encapsulated PDUs, with the PDU of each layer encapsulated in those of its lower neighbor.

An Application layer PDU can be both fragmented into multiple lower layer packets and encapsulated as many as eight or more times (including sublayers). Opening and closing sessions or connections also generate exchanges of packets on the physical medium. While the resulting

packet exchanges can be complex, OSI is a very simple and powerful paradigm. Its major goal is broad interconnection of open systems, not high efficiency. OSI expects to be able to reliably get packets across many successive concatenated dissimilar networks. While quality of service parameters may be specified, OSI makes few performance guarantees, is in no sense "real time" and there is no concept of synchronism in OSI.

ISDN has a different original paradigm. Although a packet D channel service is provided for signaling, which can also be used for user to user packet services, and various packet networks may be accessed through the circuit switched B channel, ISDN is first a circuit switched network. The fundamental service is a 64 kbps, isochronous, full duplex, circuit switched, 8-bit byte aligned, point to point B channel. It offers a modest and unvarying delay and a constant data rate. Provided that the rate is adequate, then it is suitable for real time applications and telemetry. Furthermore, because of the pervasive nature of the telephone network, if ISDN becomes universal in the telephone system, then these B channel circuits become available on demand from nearly anywhere direct to nearly anywhere else. We can go end to end, from terminal equipment to terminal equipment, anywhere, on what amounts to a single link.

A rather complex reference model has been defined for ISDN [I.324]. It was derived from the OSI model and is illustrated in figure 7. This model is primarily useful for circuit switched B channel connections. With seven layers and three planes, it is somewhat difficult to follow. The front, or user, plane, represents the circuit switched B channel. Except in the end terminals, this plane never rises above the Physical layer. The second, or control plane, deals with signaling and control of switching. This is defined between *customer premises equipment (CPE)* and the network by the Q.931 [T1.607] [Q.931] signaling protocol, which is a layer three protocol. Between the public network switches this function is performed by the *Signaling System Seven*

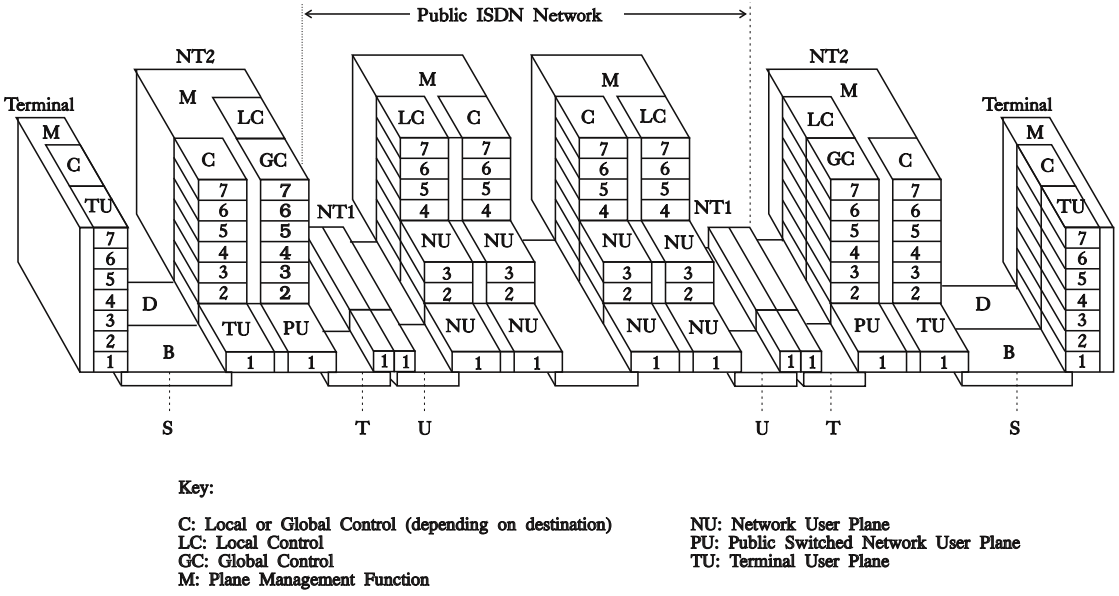


Figure 7 - ISDN Protocol Reference Model.

(SS7) protocol. The rear, or management plane, is concerned with the management of the network.

In OSI systems the management function is usually conceived as an application layer function with special access to the internals of each of the layers. There is no concept of a separate out of band signaling path for network control, all control is an in band function of either the *System Management Application Process (SMAP)* or peer layer management protocols.

Some general texts on ISDN attempt to decompose the model of figure 7 into a single plane, or separate single planes for the B and D channels, and make the model appear more OSI-like (*e. g.*, [STAL 89], [BOCK 88]). By isolating separate functions, these models may be somewhat easier to understand. Figure 8 is typical of such models, illustrating two separate stacks for the packet D channel and the circuit switched B Channel.

This model is more easily understood, but ISDN does not map into the OSI model in an entirely satisfying way. OSI is defined in terms of peer-to-peer protocols, while ISDN is defined primarily in terms of interface points and highly asymmetric protocols between a terminal and the network defined at those points. In ISDN peers do not talk directly to peers, at least in most cases.

There are two fundamentally different modes of operation in ISDN, corresponding to the circuit switched B channels and the packet D channel. The circuit switched B channel roughly corresponds to the front, or "user" plane of the model shown in figure 7, and the packet D channel corresponds roughly to the middle or "control" plane.

In normal operation a TE uses the D channel for signaling. Using an asymmetric protocol usually called *Q.931*, the TE sends packets to the network switch to which it is attached to set up

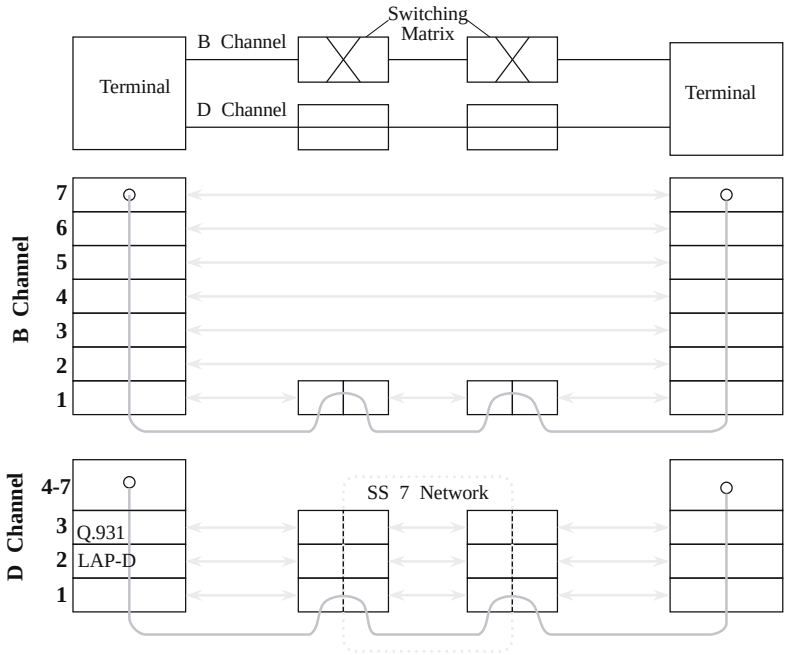


Figure 8 - ISDN Circuit Switching Protocol Model.

a circuit connection on the B channel. The network uses another somewhat similar protocol, SS7, to communicate between network switches, or separate networks, and the destination switch sends Q.931 packets to the destination TE. Q.931 packets which effectively go from TE to TE are translated into SS7 packets while they cross the network. Other Q.931 packets are generated by the network switches and sent to the TEs.

If the destination TE accepts the call, then a B channel connection is established between the two TEs. Actual data transfer, be it data or voice, normally takes place on the B-channel.

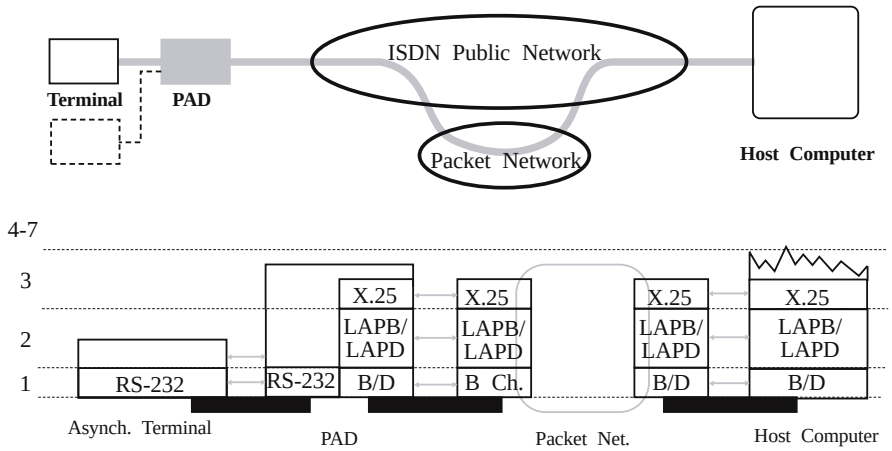
In recent years, there has been a trend to increase the integral user-to-user packet data functionality of the ISDN. The use of the ISDN as a user-to-user packet network is hardly represented in figure 7, and not at all in figure 8. Two methods of sending data in packets over the D channel are defined. One incorporates a user-to-user field in SS7 packets packets and sends those packets through SS7 along with call setup and other signaling. Although user-to-user signaling is defined in ISDN, service providers have been reluctant to offer the service. The other mechanism routes D channel packets to a separate packet handler and packet network rather than using the SS7 network.

When the B channel is to be used for packet data, the B channel is circuit switched to a packet handler. Although the service providers will purport to provide B channel packet services as a built-in feature of their ISDN, there is logically no difference from a circuit switched connection to a packet handler provided by an independent service provider. For this reason, in this report no distinction will be made in most cases between B channel packet services provided by the ISDN service provider and packet services provided by an independent service provider. Packet networks will generally be represented as separate parallel networks.

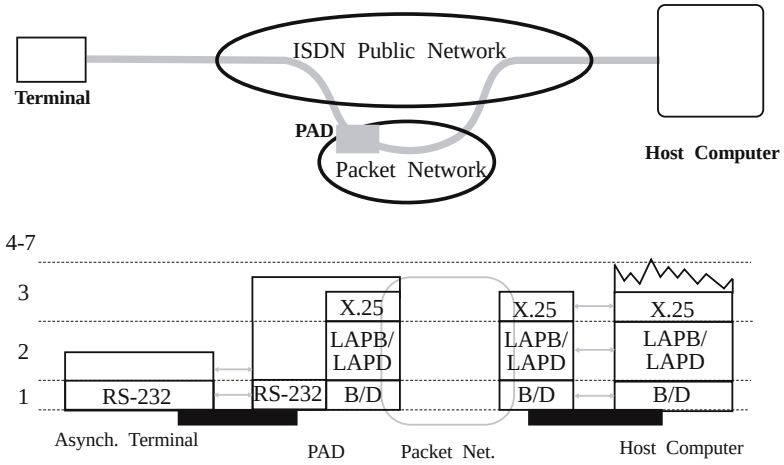
When user data is transferred over the B Channel, or through the D channel over a separate packet handler, the usual mechanism today is the X.25 *Packet Layer Protocol (PLP)*. X.25 is considered to be a layer 3 protocol, specifically a SNAcP at the bottom of layer 3, which operates over a family of related layer 2 bit oriented protocols. These protocols operate over any duplex bit synchronous binary channel, relying on a technique known as *bit stuffing* to frame packets and obtain byte alignment. The specific Data Link Layer protocol used with X.25 on the B Channel is LAPB, and on the D channel is LAPD (which is also used with Q.931 signaling packets).

X.25 is a mature protocol which considerably predates both ISDN and the ISO reference model. It is widely used with modems as well as with ISDN. X.25 is primarily an asymmetric protocol between a terminal (*Data Terminal Equipment* or *DTE*) and a packet switching network *(Data Communications Equipment* or *DCE*), not a peer-to-peer protocol, however a direct DTE to DTE mode is also defined.

Figure 9 illustrates common configurations for X.25 and ISDN, with an asynchronous terminal connected to an X.25 *Packet Assembler Disassembler (PAD)*. The PAD may be either in the user premises (fig. 9-a) or in the packet network (fig. 9-b). On the D channel only the arrangement in figure 9-a is practical, since data must be packetized to enter the D channel. The PAD is an ISDN Terminal Adapter and connects the terminal to the ISDN network and the X.25 packet network to a host computer. Although the figure shows OSI layers, note the asymmetry between the terminal and the computer, this is not conceptually a peer-to-peer, end-to-end connection, even though the terminal today is likely to in fact be a personal computer, fully capable of peer-to-peer relations, but emulating a “dumb” asynchronous terminal.



a) PAD in CPE



b) PAD in Network

Figure 9 - X.25 Terminal to Host Communications.

In combination with the Data Link layer protocol, X.25 provides for the establishment of logical connections between terminals through a packet switching network, link by link checking for transmission errors, packet sequence checking and *go back N ARQ* retransmission of lost or damaged packets. This facilitates the use of X.25 with terminals, which have no error detection and recovery capability. There are no end to end checks, however, only link by link checks, unless, in the DTE to DTE mode, one X.25 link extends from end to end.

Computer systems may not be willing to trust link by link checks without an end to end check at the Transport layer. There is a significant processing cost to each X.25 link and it is considered difficult to take advantage of channels faster than the 64 kbps B Channel with X.25. When X.25 is used in OSI networks, the processing overhead of the Transport layer is added to that of X.25.

Another service called *frame relay*, is being developed as an alternative to X.25 for use with ISDN and computer networks. Sequence checks and error recovery will not be performed, they will be deferred to higher layers. If packet errors are detected in intermediate systems the packets are discarded. This will speed packet processing in intermediate systems. There are two implicit assumptions here:

1. Errors rarely occur, therefore there is no performance advantage to recovering from them on a link by link basis.

2. There will be an end-to-end check at the Transport layer which will detect and recover from those infrequent errors which do occur.

Frame relay, which provides services on an ISDN communications link roughly analogous to the Logical Link Control (LLC) services of Local Area Networks, fits better with the North American OSI protocol stack than does X.25, since X.25 provides a quasi end-to-end service which duplicates many of the error detection and recovery functions of the Transport Layer, and frame relay does not. In many large organizations LANs will be the major vehicle for communications between computers and workstations. ISDN frame relay LAN gateways will be used to connect the LANs.

Figure 10 illustrates the use of either X.25 or frame relay to connect OSI stations on different LANs through the public network. Frame relay is sometimes considered to be at the top of layer 2, while X.25 is at the bottom of layer 3. The view taken here is that their position in the OSI stack is nearly indistinguishable, and both are considered to sit atop the layer 2/3 border.

Frame relay standards and products are just emerging. For the moment, X.25 is the primary packet service available over ISDN B and D channels. In time frame relay may take the place

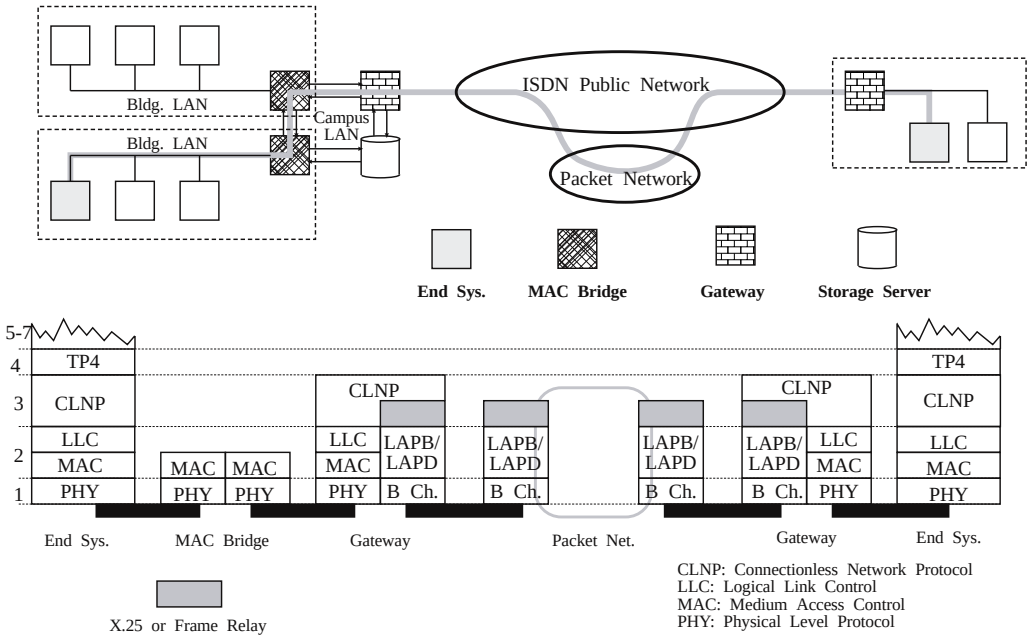


Figure 10 - Concatenated Subnetworks.

NT1: Network Termination 1

CPE: Customer Premises Equipment

TE: Terminal Equipment

NT2: Network Termination 2; typ. a PBX or multiplexor

S/U/T: ISDN Interface Points

Figure 11 - ISDN Interface Reference Points.

of X.25 in many OSI applications. Frame relay is best suited to communications between end systems, since it is not a reliable service, while X.25 attempt to guarantee reliable service and can be used with simple terminals.

A model which is often used to describe ISDN is interface oriented rather than protocol oriented. ISDN defines four interface points as illustrated in figure 11.* The *U* interface is used to connect the network transmission and switching equipment to the user premises. A *Network Termination 1 (NT1)* converts the U interface to the *T* interface. The T interface, in turn connects the NT1 to a *Network Termination 2 (NT2)*. An NT2 is a piece of customer premises switching equipment such as a Private Branch Exchange (PBX) or a multiplexor. The *S* interface, in turn connects an NT2 to a *Terminal Equipment (TE)* or to a *Terminal Adaptor (TA)*. A TE is an ISDN telephone, a computer terminal, a FAX machine and the like. A TA adapts some pre-ISDN terminal for use with ISDN, at the *R* interface point. In many cases the R interface would be the familiar RS 232 serial interface. In some cases, there is no NT2, and the S and T interfaces, which are electrically identical, collapse into an S/T interface. The S interface includes a provision for a *passive bus* to which up to eight TEs may be attached.

When the passive bus is used, all TEs share the D channel on a contention per packet basis and a D channel packet protocol with the network switch or NT2 is used to connect TEs to a specific B channel. Only one TE may use a B channel for the duration of a call. Although eight TEs may share the bus, the B channel is not a party line, and only two TEs may be active at one time. If two TEs on the same bus communicate over the B channel, they do so through the NT2 or the local office switch, and both B channels on the bus are used.

---

* A standardized U interface was not a part of the original conception of ISDN. In the United States, however, there will be a single standard U interface between the network and customer premises.

For users the major purpose of OSI is a number of Application layer services. Among them are the *File Transfer, Access and Management* (*FTAM*) protocol, *Directory Services* protocol and the *Message Handling System (MHS)* electronic mail protocol. Some of these applications, particularly the last two, are intended as much specialized teleservices which run directly on ISDN with X.25 as they are OSI applications. Therefore the application itself can provide whatever end to end services may be needed in the application, including security services, and does not depend entirely upon OSI end to end services. Moreover these applications involve functions beyond the scope of data transmission, in particular data storage, with its own distinct security requirements.

In addition to the Directory Services and MHS, which are intended to run directly on ISDN as well as the OSI stack, there are several other specialized services or teleservices defined for operation over ISDN, and more may be expected. The existing services are primarily derived from services defined for the analog telephone network. They include, Facsimile, Teletex, Videotex and Telex. We may soon expect standards for motion video over the B channel and video conferencing. Some of these services use the ISDN B channel as an end to end pipe, and the functionality is embodied in the TEs. Some however, for example mail or directory services, may rely on a service provider attached to the network. Many other specialized information services, although not necessarily fully defined by standards, may be attached to the network.

The OSI Reference model and the various International Standards which specify the layers of the model are insufficient to guarantee interoperation of conforming equipment. There are too many options. To enhance interoperability, the *Government Open Systems Implementation Profile (GOSIP)* [FIPS 146] governs the specific selection of OSI protocols suites used in the Federal Government. Both ISDN and the SP4 Transport layer security protocol are expected to be included in future versions of GOSIP. Their relationship to the other protocols included in GOSIP is shown in figure 12.

3.2 ISDN Standards Status

The *International Telecommunications Union (ITU)* is an international organization which promotes cooperation and development in telecommunications, particularly in the provision of worldwide service capabilities. Only national governments may be members of the ITU. One of the organizations in the ITU is the *International Telegraph and Telephone Consultative Committee (CCITT)*, which is the organization which develops the international ISDN standards. These international ISDN standards are called *Recommendations*, and the ISDN Recommendations are produced on a four year cycle and adopted at a four year plenary meeting. The most recent ISDN Recommendations were adopted at the Ninth Plenary Assembly in 1988 and are informally called the *Blue Book*. The previous recommendations, adopted at the Eight Plenary Assembly were called the *Red Book*. The individual subcommittees of the CCITT are called *Study Groups*, and Study Group XVIII is the primary ISDN committee. A faster process for adopting Recommendations was accepted at the 1988 Assembly, and it is possible that the process will be faster in the future.

Since the ITU is an organization of governments, the State Department of the United States is the official member of the CCITT. However, the national positions are primarily developed by the U. S. industry, largely through the vehicle of the *Exchange Carriers Standards Association (ECSA)*. Within the ECSA, *Standards Committee T1 - Communications* serves as the U. S. technical equivalent of the CCITT. T1 is accredited by the *American National Standards Institute (ANSI)* and standards developed by T1 become ANSI standards. T1 develops the U. S. technical positions for the CCITT and produces ANSI standards which generally follow the outline of the CCITT recommendations, but interpret them in the context of the United States.

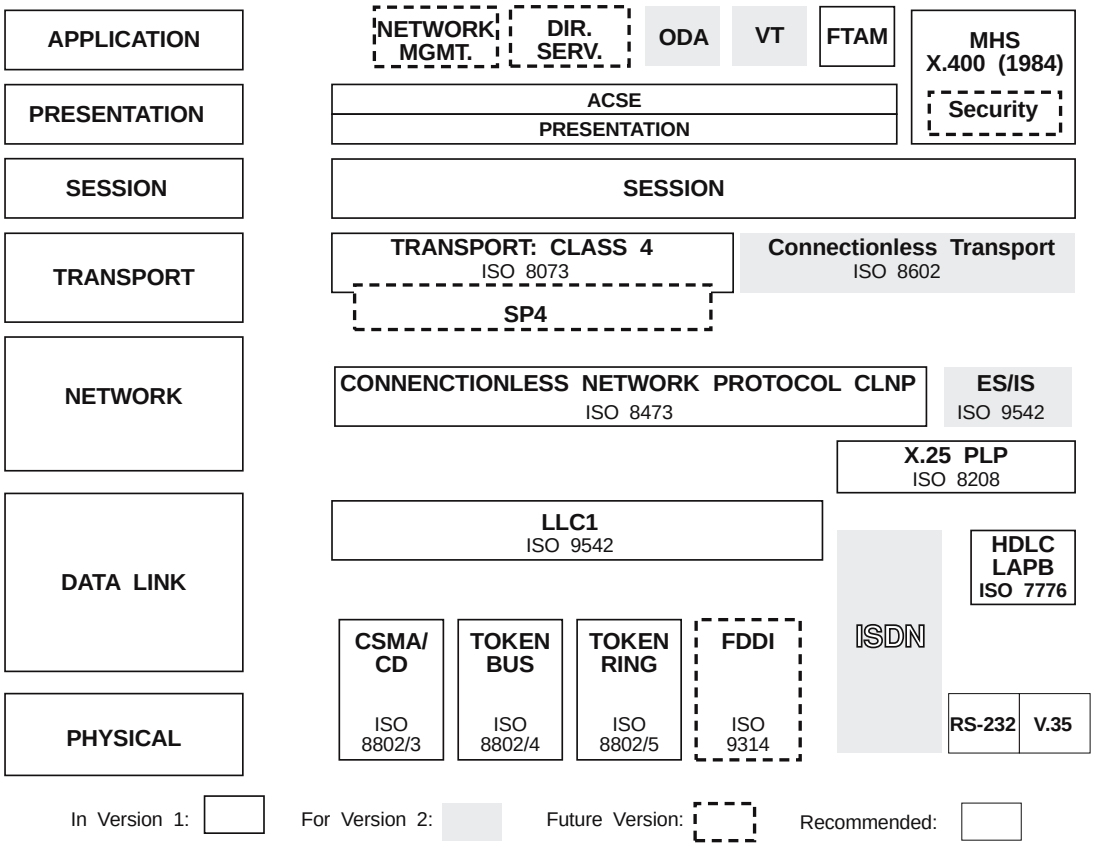


Figure 12 - U. S. GOSIP Profile.

The ANSI standards may select from the options or alternatives in the CCITT recommendations and add features or options not included in the recommendations. Within T1, ISDN is dealt with by *Technical Subcommittee T1S1: Integrated Services Digital Networks*. T1S1 is effectively the U. S. counterpart to CCITT Study Group XVIII.

Before the divestiture of AT&T into the present AT&T, which manufactures switching equipment, computers and terminals, and is the nations largest interexchange (long distance) carrier, and seven independent *Regional Bell Operating Companies (RBOCs)*, the Bell System Technical Standards provided the detailed specifications which allowed the national telephone network to operate together. This function has been largely assumed by *Bell Communications Research (Bellcore)*, which produces *Technical Requirements (TR)* documents which are used by the RBOCS as equipment procurement documents, and further define the ISDN standards and services as implemented by the RBOCs.

The RBOCs serve about 100 million subscriber lines, about half of those in the United States. Other carriers may choose to follow the TRs in many cases. Bellcore does not coordinate the business decisions of the RBOCs, which individually choose which services to offer and their deployment schedule. Moreover, granting the Bellcore TRs the status of recognized national standards is inherently objectionable to independent operating companies and long distance carriers who are not owners of Bellcore and have no say in its decisions. On the one hand the

Bellcore TRs will surely exert a powerful force for practical standardization, because of the market they represent, but on the other hand they probably cannot be considered standards, nor be referenced as standards in federal procurements, because of Bellcore's restricted ownership.

To further promote ISDN compatibility and define specific services, a *North American ISDN User's (NIU) Forum* has been created with the sponsorship of the National Institute of Standards and Technology. The forum has three principal objectives:

- Provide a forum for users to influence the developing ISDN to reflect their needs.
- Identify ISDN applications and develop implementation requirements for those applications to facilitate timely and interoperable multi-vendor implementations.
- Solicit user and product provider participation in this process.

The NIU forum consists of two workshops, the *ISDN User's Workshop (IUW)* and the *ISDN Implementor's Workshop (IIW)*. In the NIU process, the IUW produces Applications requirements, which describe potential applications of ISDN and their requirements. The IIW then develops Applications Profiles, Implementation Agreements and Conformance Criteria which allow interoperable implementations of solutions to the Applications Requirements. The IIW includes Applications Profile Teams and expert groups. There is an Expert Group on ISDN Security. In general, the Application Profiles are to be based upon approved standards. Since there are now few approved ANSI, ISO or CCITT standards for security, the ISDN Security Expert Group in the IIW has a challenging task. The NIU Security Expert Group has developed a list of security services for ISDN which includes the five OSI services (Confidentiality, Access Control, Authentication, Non-repudiation and Data Integrity) and adds to them Availability and a Notary Service.

One of the major goals of ISDN is terminal portability. Current ISDN standards and products do not meet this goal. In general, present TE equipment must be designed and tested to work with specific switch products. Indeed, some switch vendors maintain two models of terminals to work with different generations of their switches. TE vendors find that TE firmware must be updated whenever switch software is updated, and a TE which used to operate properly with a switch may fail to do so when the software of the switch moves to a new release.

A part of the reason for terminal nonportability is the many options and features allowed by the ISDN standards. Different switch vendors select different sets of features. Switch vendors also implement many proprietary features which are not defined in ISDN. Many of these proprietary features are motivated by a desire to allow public telephone service providers to offer Centrex services comparable to the advanced features of private branch exchanges.

At the present time ISDN implementations are confined to small islands, typically only a single switch or a few similar switches. This is a far cry from the vision of a vast global ISDN. Bellcore is attempting to address these problems with a series of TR's called Phase 1. They include ISDN Foundation TRs and End User Feature TRs. If all goes well, some degree of practical terminal portability should be a reality by the end of 1991, with more complete service portability in Phase 2 by 1993. This applies to the areas serviced by the RBOCs, and it is to be hoped that Bellcore's work will be adopted more broadly. The operation across international boundaries of any services beyond basic voice and 64 kbps circuit switched data services is very uncertain.

The ISDN was also broadly conceived as a universal service for all network users. It was once thought that, at some point in time, all subscribers in the network would be converted over to

ISDN lines. For all practical purposes this goal has been abandoned; it is recognized by network service providers that there is no advantage to ISDN for many subscribers and a forced conversion would be an untenable political and business proposition.

Indeed there are several disadvantages to ISDN for residential and small business subscribers, who may have little use for the 64 kbps digital service. They have a large investment in their present terminal equipment and wiring. For example, although ISDN supports up to 8 terminals on the same passive bus, two or three parties cannot simply pick up extensions on the same line and participate in the conversation as they do now. Another disadvantage to ISDN service for some purposes is that the TE is not powered by the network as are analog telephones. With ISDN a backup power supply is needed for TEs, or a power failure causes a telephone failure.

Instead of pressing for universal ISDN service, service providers are installing the ISDN infrastructure in their networks, but unbundling the ISDN features and making them available to analog subscribers. Call waiting, call forwarding and calling line ID features are now widely available to analog subscribers. They are supported by ISDN capable switches and SS7. Although estimates vary somewhat, it is more or less generally agreed that, while only a small fraction of subscriber lines in the United States will be ISDN lines in 1995, the majority of subscriber lines will be serviced by switches which support SS7.

Eventually, the ISDN standards will provide the infrastructure for worldwide telephony. ISDN services will be available anywhere in the developed world. Full portability of ISDN terminals and switches may never be a reality, but the basic services will be transportable across national boundaries between TEs. An all-ISDN world wide telephone network, however, seems improbable. Many users will continue to use analog terminals for the foreseeable future.

Finally, another development not originally anticipated by ISDN is mobile cellular telephony. The 1980s was a period of explosive growth for cellular telephone systems. The present system uses digital control but analog voice channels. Work has recently begun on standards for an advanced digital cellular mobile telephone system. The data rate for this service will probably be 8 kbps, and it will require the development of inexpensive voice coders at this rate. With a number of 8 kbps channels assigned to one higher rate carrier on a time division multiplexing basis, broadcast spectrum utilization will be enhanced. There also has been some speculation about using cellular radio to deliver voice services to residences, perhaps as a competitive alternative to traditional wire line carriers, or as a less expensive alternative to copper where densities are low.

There are many implications for ISDN security. The first is, that for the near term, ISDN security services should require little more from the ISDN than the ability to set-up and terminate 64 kbps B channels. Broad, consistent near term availability of any other services is uncertain. Longer term security may be able to use D channel packet services; certainly this would be highly desirable. A second is that any supposition of an all ISDN network is unrealistic for the foreseeable future. Security functions developed for ISDN may have to interoperate with pre-ISDN terminal equipment. It should also be designed to interoperate with new digital cellular telephone services, not originally anticipated by ISDN.

3.3 Threats

The ISDN security threats include:

- Denial of service
- Intrusion into network customer data

- Use of ISDN network to penetrate a customer system
- Use of the network for fraud
- Intrusion on the confidentiality of ISDN communications.
- Modification of communications

Denial of service attacks include physical damage to CPE, network links and switches. Even if no actual attack is involved, accidents and disasters can cause loss of service. Switches can also be attacked by penetrating the switch software to either disable the entire switch or to affect a particular subscriber in some way, perhaps by diverting his calls or disabling his line.

ISDN networks will maintain subscriber data, particularly the records of calls made. This information is properly confidential to the subscriber and may be quite sensitive. If the network systems are penetrated, then an intruder may obtain this information. Both the operational network, which collects the data and the administrative system are possible points of attack.

Since the telephone network is the principal means of providing remote access to computer systems and networks of all sorts, it is an obvious and widely used vehicle for intrusion into these systems. Almost every outside penetration of a computer system begins with a telephone call. The purpose of the intrusion may be fraud or theft, sabotage, to obtain confidential information, or simply for the fun of doing it. The ISDN network cannot prevent such attacks, but it can make available confidentiality and authentication means which the end systems can use to detect and thwart the attacks.

The telephone network is one of the principal instruments of fraud in modern society. Much of the fraud is petty, some is major, and the total cost is undoubtedly substantial. Electronic fraud sometimes involves substantial funds transfers, and may not always be detected or reported. Some telephone fraud involves obtaining confidential information, including credit records, law enforcement records, telephone numbers, and the like. The network itself is often defrauded. Since the telephone network is a pervasive communications medium, this will continue; it is impossible to entirely eliminate fraud via telephone. The inherent anonymity of callers in the present network is the great advantage of the telephone as an instrument of fraud.

It is illegal to tap ISDN phone lines without a court wiretap order. It is, however, not difficult to do so. The law is not likely to significantly deter wiretapping in espionage cases, and may not do so in other cases. Cellular and wireless telephones are particularly vulnerable. It is also possible to modify data sent over the network for fraudulent or malicious purposes. Although this requires more sophistication than a simple wiretap, it would not be extremely difficult.

ISDN security is however, more than simply responses to specific deliberate threats. Much damage may be done by error, noise, accident, confusion, misunderstanding and inadvertence as well as by intent. The same signature, integrity, notarization and authentication services may also apply in these cases as in cases of deliberate fraud. A digitally signed and notarized electronic document may settle a dispute caused simply by an error. The value of good security practices is not limited to preventing deliberate attacks, and much security would still be good business practice in a world free from deliberate fraud, theft and intrusion.

3.4 The ISDN Security Environment

Figure 13 illustrates the broad environment into which ISDN security must fit. ISDN security must begin with the user. For the purposes of ISDN security a user may be a person, some organizational entity (e. g., the dispatcher), or a computer process acting for either the person or

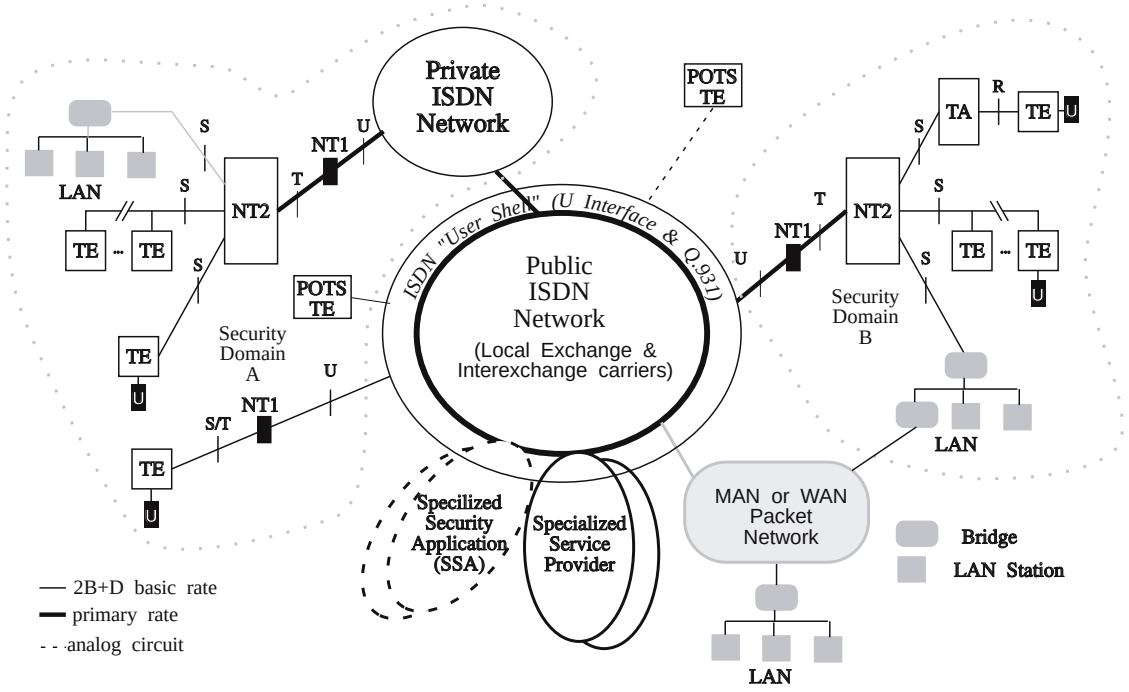


Figure 13 - ISDN Security Environment.

the entity. The user may or may not be bound to a specific line or terminal, indeed the user may be highly mobile and may carry his security attributes with him wherever he goes. Since humans use any available simple telephone instrument for a wide range of transactions, the reliable authentications of human users of ordinary ISDN telephones is a serious concern.

The user interacts with ISDN *Terminal Equipment (TE)*. TEs include voice phones, answering machines, integrated voice/data terminals facsimile machines, specialized terminals such as automated teller machines and the like. In many cases, the TE will be a computer connected to the ISDN network thorough some sort of ISDN interface device or card. When the TE is a computer, the user is a computer process acting as the agent for either a person or an organizational entity.

The TE may either be directly connected to the ISDN network, or it may be connected to a *Private Branch Exchange (PBX)*, which is in turn connected to the ISDN public network. In the ISDN jargon, a PBX is a *Network Termination 2* or *NT2*. Collectively, the TEs and the NT2 equipment are called *Customer Premises Equipment (CPE)*.

The public ISDN is an amalgam of numerous interconnected service providers. In the United States they are either considered local exchange carriers (local telephone companies) or interexchange carriers (long distance telephone companies). In general, the local exchange carriers have a monopoly over residences and small businesses in their operating areas. Local exchange carriers are regulated by both the Federal Communications Commission (FCC) and state Public Utility Commissions (PUCs). There is constant tension over the respective authority of the FCC and the PUCs. There are three main interexchange carriers. The local exchange carriers include seven large former AT&T Regional Operating Companies (RBOCs), which serve about half the

telephone lines in the country, one large "independent" local exchange carrier (of size comparable to the RBOCs), and numerous smaller local exchange carriers.

The public network must be able to protect itself from fraud and threats to service availability. This is a business necessity for the service providers. Service providers must also preserve the confidentiality of customer service records. The public network is too diverse to be expected to provide strong assurances of user to user security, particularly confidentiality and authentication. There is no one authority capable of imposing and managing a security program which could ensure this.

Application layer services, called *specialized services* or *teleservices* may be provided to users through the ISDN. Specialized services include (X.500), packet Message Handling Service (X.400) and a variety of other value added application services. The *network service providers* themselves may be *specialized service providers* or the services may be provided by other service providers with access to the network switches.* Some general teleservices, such as X.400, will incorporate security into the more general application. The specialized service providers may also offer security applications, such as key management. In this report, such a security oriented application will be called a *Specialized Security Application (SSA)*.

In addition to the specialized services which may be attached to the network, packet handlers may be incorporated in network switches to provide packet services as a part of the public network. Independent packet networks may also be connected to the local exchange switches. A variety of packet network services, including "secure" networks may ultimately become accessible through the local switches.

Users in many different security domains will communicate with each other over the ISDN network. In addition to the public ISDN network, there will be private ISDN networks, and a variety of data networks, including Local Area Networks (LANs), Metropolitan Area Networks (MANs), and Wide area Networks (WANs), which may be connected to the public ISDN network through gateways. Analog *Plain Old Telephone Service (POTS)* will continue to be supported by the public network and may consist of a majority of local lines for the next few decades.

The burden of user-to-user security over ISDN will fall of necessity on the CPE. The security solutions chosen in the CPE, should allow not just for ISDN, but for the alternative communications available.

3.5 The Human Component of ISDN Security

ISDN is both a telephone network and a data network. People interact with people, relatively "stupid" machines, and computer systems over the ISDN network. Computers will also interact with computers. The previous communications standards work of OSI and ECMA have dealt largely with the interactions of computer systems. In ISDN security we must also consider security in the context of human interaction, often largely unaided by a computer, or consider if there are means whereby computer based security functionality can be extended to all telephone users.

---

* The rights of local exchange carriers, particularly the RBOCs, to provide value added services, the conditions under which they may do so, and the nature of the access which they must provide to independent supplementary service providers is currently a matter of regulatory, political and legal dispute.

The fundamentals of human to human interaction over ISDN remain nearly the same as they have been in the analog telephone era, except that the called party may have a fairly reliable indication of the caller's number, until some general human authentication system is adopted for ISDN. The essential question is, "to whom am I speaking?"

Where parties are known to each other, they may recognize each other's voice. Traditional challenge and reply password authentication can be applied over the telephone. However only rudimentary protocols are practical with untrained humans. For the general public, memorizing and using a 4 digit personal identity number (PIN) is probably about the practical limit. An individual can only be expected to memorize at most two or three such PINs. If more are needed, the individual can be expected to write them down and carry them, compromising security. Thorough training and discipline are required to maintain security on normal telephone calls.

Humans are capable of exercising judgement. They may detect an attempted telephone fraud or penetration by exercising judgement. In some emergencies good judgement may dictate abandoning normal procedures, but this is also a weakness for the impostor to exploit. Telephone impostors practice "social engineering," making posing as someone else a fine art.

A reliable and socially acceptable means of strong personal authentication through normal ISDN telephones is badly needed. If available, it would make a great contribution to security. Telephone access to confidential information should be based upon reliable authentication, business transactions should be authenticated or signed, and access to information resources should require authentication.

When humans deal with intelligent machines through a telephone a basic mismatch in capabilities exists. The telephone keypad provides a very limited interface to computer systems. Only rather simple protocols are practical. In many cases the human will be untrained, further limiting the interface. Applications to date include dial-up account inquiry services and automated teller banking machines. Remote voice mail capabilities are now being offered by local operating companies.

Much more elaborate services are potentially possible using personal computers. The computer provides a much more elaborate interface to support the application and can implement security protocols. Banking services, shopping services, reservation services and the like are now offered.

It is likely that inexpensive home and office computer systems will soon include a powerful computer, page display, scanner, page image printer, ISDN port or modem, voice telephone, and voice answering machine with storage equivalent to a filing cabinet or more, all integrated into a compact desktop package, with appropriate integrated software. Such an integrated voice, data and image system will provide a single integrated personal solution to document preparation, storage and communications.

By extrapolation from the past decade, such systems should be widely available by 1995 and ubiquitous by the end of the century. Already hardware to support all the functions described above can be added to standard personal computers for comparatively modest prices. All that remains is to integrate the hardware, and, what will be more difficult, the software. It is reasonable to expect that nearly all offices will use such systems by the end of the century and most professionals will have home systems.

These will be very powerful general computers, perhaps supported by graphics or digital signal processors. They will have at least the computational power of present mainframe computers (just as today's PCs easily match the power of 1980 vintage mainframes). They will be capable of encrypting digital voice in real time, using fairly strong algorithms, without dedicated cryptographic circuits.

Increasingly, computers are portable. The portable computer may simply be a module which detaches from the standard desktop integrated computer. The portable unit may include most of the functions described above, except perhaps the printer and scanner. A portable computer system may become a basic tool for every business traveler. Every person who now carries a briefcase home may soon put a portable computer in it. If this occurs, however, it will reflect a communications failure, because the ISDN network should provide the needed communications between home and office.

A security mismatch may occur when computer systems are connected to "dumb" equipment, such as existing FAX machines, particularly when they are not attended by an operator. Compatibility with existing equipment will be necessary, but this equipment cannot accommodate complex protocols as the computer can. The security problem is likely to be most acute with equipment such as facsimile machines intended for unattended operation. This should only be a transitional problem, however, as older equipment passes on to oblivion. The dumb FAX machine may shortly become as irrelevant as the black and white television.

Computer mail and directory services will become available. Mail services will include security to limit access and protect confidentiality. Directory services will provide key management and might provide Privlege Attribute Certificate services.

While powerful security functions can be built into these computers, a formidable educational process is required on the part of the humans who operate them. Even assuming "user friendly" security software, there will be much to learn. Teaching users good security practices and getting them to use it will not be easy.

Indeed, access to such computers and the skills to operate them may be a divisive force in society. As user friendly as software may become, mastering it will be a barrier for those long out of school and the educationally disadvantaged. Computer access and literacy may become key to full participation in society and as fundamental as reading, writing and arithmetic. The introduction of widespread communications security and the integration of it into ordinary life and business will be as much a social and educational problem as a technical problem.

Voice only telephones will remain. We may hope, however, that they will increasingly provide a port to attach a computer, or perhaps a simple authentication device. It will be desirable to provide at least some sort of authentication for voice telephone users. While existing terminals such as FAX machines will complicate the transition, in the end security need support only voice terminals and end computer systems. The greatest security problem will be education.