1. Introduction

The *Integrated Services Digital Network (ISDN)* standard will largely govern the operation of the world's public networks in the coming decades. The ISDN provides digital-circuit switched voice and data services, as well as packet-switched data services to users. In addition to end-to-end digital services, ISDN supports interworking with existing analog voice circuits and equipment. Although the provisioning of digital switching capability in the public network, which can ultimately support the ISDN, is well along, ISDN services are just beginning to become available to users in 1991. Because of the ISDN's importance in future communications, security of the ISDN applications is a significant concern. This report provides a discussion of the standards needed to implement ISDN user security.

The technical efforts leading to this Special Publication were conducted under the auspices of the Integrated OSI, ISDN and Security Program of the Computer Systems Laboratory at the National Institute of Standards and Technology.

1.1 Scope

This paper focuses primarily on security for users of the public ISDN. It considers voice and data security in the general context of communications and open systems security and provides a broad discussion of user security needs and possible solutions. It does not attempt to prescribe specific detailed solutions.

These user needs include:

- protecting information confidentiality,
- identifying the parties in communications (authentication),
- assuring the integrity of communicated information,
- controlling access to network services and customer equipment and data,
- being able to prove to a third party the fact that a communication occurred, the contents of the communication, and the identities of the parties to the communication (non-repudiation).

This report assumes that the public ISDN is largely defined and, although some additions may be possible in the interest of security, the public ISDN switching equipment already designed and installed will not be substantially changed to provide user security. Most needed user security can be provided either in user terminal equipment or by adding supplementary services accessible to users through the network.

One user security need, not treated in detail here, is availability of service. Using the technologies and methods discussed in this report users can protect themselves from most security threats except for denial of service attacks. The protection of the public network from deliberate or accidental disruption and fraud is a serious problem to users, but it is largely separable and must be addressed by the network service providers. If intruders penetrate the *Operational Support Systems (OSSs)* of the public ISDN, which manage and maintain the network, they can potentially intercept, divert or prevent user communications. With appropriate security procedures, users can prevent compromises of the confidentiality of their data, and detect impersonations, if the public ISDN OSSs are penetrated, but they cannot prevent denial of service. Attacks on the OSSs could also reveal customer service records and traffic flow information. There are now no standards for OSSs, however efforts have begun to standardize a user network management interface. The security of OSSs is an important concern of ISDN users. However, it is not clear

that the needed security provisions should be the subject of public standards and the responsibility for this rests primarily with the network service providers. It is not a subject of this report.

Some view ISDN as strictly a lower-layer communication service, without concern for the applications it carries. This is not entirely satisfying from a security perspective. On the other hand, the set of applications which may be supported by ISDN is nearly unbounded; it will be difficult to provide for the specific security needs of all applications carried over ISDN, as an integral feature of the network. For example, ISDN cannot in itself satisfy the security requirements of an application such as electronic mail (which will operate over other networks as well as ISDN), but it must provide the necessary security support which this application requires of any network.

The mechanisms needed in ISDN to support user security requirements will be defined. The appropriate location of those mechanisms within the structure of ISDN will be discussed. The relationship of ISDN security with the general concepts of security in *Open Systems* and *Open Systems Interconnection (OSI)* will be considered and this report outlines an approach to ISDN security which is consistent with developing OSI security standards. In many cases the needed services and protocols may be defined in a general manner for all networks; that is, they are not specifically ISDN problems, but more general problems, and may be addressed in a more general context than ISDN standards. It is highly desirable that the ISDN adopt security protocols and services developed for OSI wherever possible, so that information systems security as a whole can be as consistent and simple as possible. Areas where ISDN has unique requirements and where specific ISDN security standards are needed will be identified.

1.2 Need for Security in ISDN

The need for routine security in wide area telecommunications remains largely unsatisfied. Both the present pre-ISDN voice oriented network and the ISDN, which will replace it, make little provision for security. There is no systematic provision for protecting the confidentiality of user communications and, in many cases, it is comparatively easy for intruders to intercept, understand, and alter communications or originate forgeries. The network itself is vulnerable to various types of frauds. Since there is no standard, effective method for the authentication of network users, the network provides an excellent vehicle for allowing the criminal to remain anonymous while committing frauds.

In the past, the public analog telephone network used *in-band signaling* for network control. The tones used by switches to signal other switches could be introduced by users through their telephone instruments. This was widely exploited to defraud network service providers. The public network has now been substantially converted to *out-of-band* signaling between switches, eliminating this opportunity for fraud. The ISDN extends the out-of-band signaling to the local loop and user terminal, through a separate 16 kbps digital *D channel* used for signaling between the terminal and the network.

This itself does not make ISDN public networks secure from fraud. It remains to be seen how vulnerable the ISDN terminal-to-network signaling protocols will prove to be to fraud, when ISDN is widely available to the public. There are no access control, authentication or confidentiality provisions in the ISDN terminal to network signaling protocol. Moreover, users will also be able to obtain X.25 packet services through the D channel. The operational, maintenance and administrative systems of the public network typically use X.25 packet services. If it is possible to penetrate these systems from any D channel via X.25, then the security exposure may be grave.

The need for strong security in telecommunications is becoming urgent as electronic documents replace paper in commercial transactions. Many of the traditional safeguards and practices which applied to paper have not been adequately extended to cover electronic documents. Forgery or alteration of unprotected electronic documents is simple compared to forging or altering paper documents. It is often easier to tap a communications line and intercept all the traffic on that line, than to intercept and read paper mail.

As the public network is converted to the ISDN standards, ISDN will become pervasive and will broadly affect citizens, businesses and government. Ordinary analog voice telephones are now routinely used to check account status, place orders, transfer funds and pay bills. Protection for these transactions is provided only by rudimentary authentication checks such as Personal Identification Numbers or credit card expiration dates. The ISDN will facilitate a great expansion of personal and business transactions over the public network. The potential for electronic fraud and gross intrusions on privacy and confidentiality through the public network will expand correspondingly, unless suitable standards are adopted and pervasively used.

1.3 The Opportunity

The combination of digital communication via ISDN and evolving security technology provide an opportunity for significant improvements in public network security. When ISDN makes ubiquitous digital communication of voice and data a reality, the digital signals can readily be encrypted to maintain confidentiality and integrity of voice, data and image traffic. The inclusion of a packet data facility for signaling will allow fairly basic ISDN voice terminals to implement digital security protocols. Public key cryptography makes key management practical on a large scale, allows electronic signatures that cannot be forged, and provides a means for reliable authentication without shared secret keys.

A foundation of common security standards for ISDN, particularly for authentication, confidentiality and integrity can provide the needed platform upon which the specific security needed by various ISDN applications can be built. Because of its digital nature, ISDN can accommodate this foundation. The needed security technology exists; it remains only to adopt it to ISDN and incorporate it in standards.

Security is not free, but if implemented on a wide scale with suitable standards, the benefits are significant and the cost need not be excessive. If the market is sufficient, then the cost of developing integrated circuit security devices is justified. It remains only to develop and implement the needed standards and to incorporate them in ordinary practice. The availability of pervasive security in the ISDN network would provide a strong incentive for users to convert from analog service to digital service.

1.4 Security Policies and Domains

For effective communications security an explicit and well-defined *security policy* must be enforced. A security policy is, "The set of laws, rules and practices that regulate how an organization manages, protects and distributes sensitive information."[DOD 5200]. A security program includes the set of measures used to implement the policy. Measures to protect data include physical security (*e. g*., locks, guards and perimeter alarms), procedural security (*e. g.,* separation of duties and authority, review and release procedures, etc.) and cryptography. A *security domain* is a set of users who share the same security policy.

Although it is not normally formalized, each individual or family may be considered a separate security domain having its own security policy. How an individual locks his doors, how he lists his telephone number (is it unlisted? does the listing reveal his sex?), how he answers his door

and telephone, how he responds to requests for information and what he considers private are just a few aspects of the informal security policy that each of us individually has.

A security policy covers more than communications security. Data is stored, processed and accessed as well as transported. Communications, however, often involves crossing boundaries between security domains. Each independent company or organization, or each subunit of the same organization may have its own security policy, suited to its needs and capabilities. Any confidential communication between these organizations crosses security domain boundaries. Business and commerce are international. Laws regulating security and privacy vary from state to state and country to country. In some countries the law may forbid sending encrypted data across borders. Security policies must comply with different national laws, subdividing security domains within international business organizations. To meet commercial needs, ISDN security must cross not only security domains but also international borders.

Although the basic cryptographic technology to support secure communications is well known, interworking between separate security domains remains a difficult problem. ISDN security must support a range of policies suitable for different communities and applications, as well as interworking among them.

Many significant social policy concerns can be viewed as security domain interworking problems. Consider, for example, credit records. They are compiled by one party but are properly confidential to the subject of those records. In most circumstances they should be released only to parties specifically authorized by the subject. Those parties must also maintain the confidentiality of the records. The addition of data from unreliable sources to credit records and particularly the deliberate addition of false credit reports must be prevented.

Similar issues attend many financial, medical and criminal justice records. The confidentiality and use of records are now the subject of legislation and will receive more legislative attention.

Today individuals are increasingly mobile, often moving to pursue their careers. The use of cash for large transactions, or simply to rent a car or buy an airline ticket, is considered unusual at best and possibly a sign of criminal activity. On the basis of the possession of plastic credit cards merchants broadly extend credit to complete strangers with no authentication of personal identity. A large catalog industry now takes orders primarily over the telephone, shipping merchandise, often within 24 hours, on the basis of a credit card number given over the telephone. A good credit rating and possession of credit cards are necessities of modern everyday life.

The public network is the main carrier by which these sensitive records are gathered and accessed. It must support users with a great variety of security policies. The problem is compounded by the successive chain of domains which is involved. By itself, ISDN cannot solve the crossdomain interworking, a problem which is general to all communications systems, but it must support some of the basic mechanisms required to provide secure interworking between domains. The problem is central to the fabric of modern society, and is as much a social policy issue as a security issue.

1.5 Federal Role in ISDN Security

In the United States, the *National Security Agency (NSA)* is charged by law with protecting classified data. The security resources and expertise of NSA are unrivaled. The *National Institute of Standards and Technology (NIST*) has responsibilities for the security of unclassified information. Under PL 100-235, The Computer Security Act of 1987, NIST is assigned the, "responsibility for developing standards and guidelines needed to assure the cost-effective secu-

rity and privacy of sensitive information in federal computer systems drawing on the technical advice and assistance of the National Security Agency,"...

NIST participates in voluntary security standards efforts. The Federal Information Processing Standards (FIPS) and Guidelines developed by NIST are used by federal agencies, by state and local governments and by private industry to protect sensitive information. The best known of the security FIPS is FIPS PUB 46-1 *Data Encryption Standard (DES)*. The DES defines a symmetric-key encryption algorithm that is widely implemented in commercially available products. In addition to its use by Federal agencies, the DES is widely used by business, particularly in banking and other financial applications.

NIST works with industry to develop security standards that are broadly acceptable and meet the needs of both industry and government. In doing this, NIST draws upon the expertise of NSA and attempts to bridge the gap between the world of classified security, where many of the algorithms and security devices are classified and must be themselves protected, and the world of commercial security and standards, where the algorithms are typically known and often published in standards.

If security is to be broadly implemented across independent domains throughout the world, with widely available, inexpensive equipment, then it must use algorithms and protocols known to all. The only secrets will be the sensitive data and a limited number of security parameters (e. g., keys, passwords, etc). The security hardware itself must be sensitive only to the extent that it stores secret security parameters.

Both classified and sensitive but unclassified communications can use the same basic protocols with appropriate specific algorithms for encryption, authentication, access control and the like. This will facilitate the use of commercial networks and communications equipment for national security purposes, providing additional alternatives for classified communications, saving users money and providing additional revenues for commercial carriers and equipment vendors. NSA and NIST are working cooperatively toward this goal. The protocols for ISDN security must therefore support both the open algorithms for commercial security and the more restricted algorithms needed for classified information.

In addition to NSA and NIST, many Federal agencies have a strong interest and role in the general subject of communications security policy. Many agencies maintain large electronic databases of sensitive information that are accessed, collected or distributed electronically. Obvious examples include the Internal Revenue Service and the Social Security Administration. The confidentiality of various official economic estimates must be maintained until they are released. The data upon which they are based may be reported electronically. The integrity of the electronic communications of the Treasury and the Federal Banks are vital. An intrusion into the Air Traffic Control communications system could cause disaster.

Among the most directly affected agencies are law enforcement agencies. They maintain databases of sensitive information, disseminate that information where needed and yet must protect that information from misuse. A great part of law enforcement consists of compiling databases of information and correlating that information to reveal a pattern which indicates an illegal activity. Computers and electronic communications greatly facilitate this, but at the same time raise the specter of infringement of the privacy of the public. Widespread dissemination of security technology may also frustrate law enforcement data gathering. Law enforcement agencies, the Congress and the courts will all deal with the implications of communications security standards and policy.

At least one security relevant feature of ISDN, *Calling Line ID*, (often referred to as *Automatic Number Identification* or *ANI*) is under attack as an invasion of privacy. This issue is discussed in Section 1.6 below. It is likely that Federal action may be required if this feature is to be generally available or differing state restrictions may make it impossible to provide a consistent nationwide network service.

1.6 Privacy and Confidentiality versus Accountability

While the terms *confidentiality* and *privacy* share a common context of secrecy, privacy is used to describe the desire or right to be left alone and not be disturbed. Confidence implies trust and belief, that is, the sharing of secrets. A secret, not shared with another, is private, but not a confidence. In the context of ISDN security, the term confidentiality is used to describe the transmission of information between two or more parties without divulging that information to any unintended parties or intruders. Privacy in ISDN refers to the capture, accumulation and release of information about subscribers, particularly where that information may enable intrusion upon the seclusion of the subscribers, or the use of the network for unwanted intrusion on network subscribers.

Balanced against the legitimate desire of subscribers for confidentiality and privacy is the need to hold them accountable for their use of the ISDN. When subscribers misuse the network, they should be held accountable. If commercial transactions are conducted over the network, rather than with paper, then the parties must be able to hold each other accountable. Achieving accountability, however, is to some extent in conflict with broad constructions of confidentiality and privacy.

Confidentiality involves both the contents of communications and *traffic flow confidentiality* (*i. e.,* protecting the identities of the parties, amount of traffic, length of transmission, *etc*). Confidentiality can be compromised in a number of ways. An intruder may be deliberately intercepting information. Deliberate intrusion may be easy in the case of cellular radio telephony or wireless telephones and local area networks (LANs), but signals can be intercepted by intruders on copper wires, fiber optic cables, and along either terrestrial or satellite microwave links. Confidentiality can also be compromised by crosstalk in the network, although all-digital transmission significantly reduces the likelihood of this.

Intrusions may or may not be illegal, depending upon the circumstances. Federal laws forbid wiretaps on domestic private electronic communications by private parties and by law enforcement or other government agencies, except under limited circumstances as specifically defined by law. Nevertheless, illegal or not, it is usually easy to tap local communications loops.

While confidentiality may be achieved by physically protecting the communications links and, to some degree, by legislation forbidding the interception of communications, the most general and convenient means of ensuring confidentiality are cryptographic techniques. As more and more business transactions take place electronically over ISDN, the use of cryptography to protect the communications of private businesses and individuals will grow.

There are several ISDN privacy concerns. The first involves the Calling Line ID supplementary service. Unlisted subscribers pay to keep their numbers secret to deny others the ability to intrude on their privacy by calling the unlisted number. If every time someone is called from an unlisted number, this number is revealed to the called party, the caller's privacy is allegedly infringed.

Absent legislation forbidding this, Calling Line ID can be used to build the network equivalent of mailing lists, which undoubtedly intrudes upon the privacy of subscribers. The use of police tip lines, whistle blower lines, suicide counseling lines and similar valuable services may be curtailed as the public fears that their anonymity is compromised by Calling Line ID. It is argued that there is an established right to anonymity over the telephone. The reporting of Calling Line ID has been limited in some states by public utility commissions and in other states has been held by courts to be illegal. Some operating companies now offer blocking services which block the Calling Line ID service on selected outgoing calls, while at least one state requires that Calling Line ID be blocked on all calls from unlisted numbers.

While Calling Line ID has legitimate uses, it is objectionable in that it may be automatic. It is dangerous in that it is at best a weak form of authentication. A standard form of strong personal authentication via ISDN terminals might be possible via D-channel user-to-user signaling. A caller could be requested to authenticate by the called party. Such a standard form of voluntary strong authentication, which is discussed further in section 6.4, would solve many security problems and the privacy concerns of Calling Line ID.

By tradition there is also an expectation that telephone conversations are private conversations between two parties, as if those parties were conversing face to face in some isolated location. This makes these conversations private and deniable, in that what was said is the word of one party against another. Recording telephone conversations without advising the other party may violate laws and generally violates normal conventions of privacy.

Another major privacy concern is the observation and accumulation of data about subscribers. Privacy implies freedom from systematic observation, and the systematic recording of personal data. Although each event recorded might be innocuous in itself, and not essentially private, the systematic accumulation and analysis of these events may be regarded in the aggregate as infringing individual privacy. Thus the call detail records legitimately kept by service providers may be held to be confidential between the subscriber and the service provider. Unauthorized release of these records to a third party, even (or perhaps particularly) a law enforcement or security agency, may be considered an intrusion upon privacy.

Detection and recovery from security violations requires the maintenance of security audit information. Without appropriate safeguards such records may be misused, and there is the potential that systematic records of electronic communications kept to detect fraud, intrusion or for other security purposes will be considered to violate the legitimate privacy of innocent users.

As electronic transactions continue to replace paper transactions and, as the power of networks and computers to recognize, store and analyze data increases, these privacy concerns will grow. Any attempt to monitor the public ISDN and collect data to detect fraud, illegal activity or security violations must be conducted with due concern for privacy. When such databases are created, access to them must be strictly controlled, and their use limited to a narrowly defined legitimate purpose.

Both privacy and confidentiality rights must be balanced against the need for accountability and legitimate social, law enforcement and security needs. If Calling Line ID discourages reporting of crimes, it may also discourage harassing calls and false alarms. If it can allow the building of intrusive phone lists, it can also facilitate better customer service. It may even enhance privacy by facilitating the screening of incoming calls. If every state has a different law and policy on this feature, it may become impractical for ISDN service providers to provide it in the cases where it is legal and would be useful.

As it becomes pervasive, cryptographic technology will not only be used to protect legitimate communications, but those of criminals as well. By its very nature large scale organized crime involves extensive communication. The interception of communications by law enforcement agencies is a powerful tool against such criminal organizations. Widely available cryptographic products may render useless approved interception of communications for law enforcement.

When does the systematic monitoring of calls and the recording of the Calling Line ID to detect the penetration attempts of hackers, or other frauds, become an infringement of the privacy rights of all users? What safeguards are required to ensure that it does not? What are private communications and what, if any, private communications should not be lawfully encrypted? Can an individual be compelled to reveal a cryptographic key protecting an encrypted communication that may be incriminating? Do the special privacy privileges of telephone conversations extend to text or facsimile messages delivered over the public ISDN network or to voice mail?

These issues are much broader than just ISDN security; they involve all electronic communications and records and encompass fundamental notions of the privacy and confidentiality rights of citizens. However, the problem is particularly acute with ISDN, because of its roots in the public telephone network and the consequent pervasive involvement in everyday life. These and many other such questions must be answered in the coming years to provide ISDN security which properly balances privacy, confidentiality and accountability concerns.