6. Placement of ISDN Security Services

Figure 27 illustrates the possible ISDN security interactions. In this illustration a user may be either an Application layer computer process or an actual human user. The TE or terminal is the initial point of connection to the ISDN network. Users may be associated with a particular TE, or they may be mobile. The TE may be connected directly to the public ISDN network, or through an NT2 (typically a PBX). The TE and NT2 are collectively *Customer Premises Equipment (CPE)*. *Specialized Security Applications (SSA)* are connected to the users through the public network.

6.1 User-to-CPE

The primary user-to-CPE security interaction is authentication and access control. If privileges are to be bound to specific lines and terminals, then access to the terminals must be controlled. In some cases this may be by physical control of access to the terminal, but in most cases it will require that authentication and access control be built into the terminal or the PBX, or both.

A significant advantage of authentication and access control at this layer is that broad standards are not necessarily required. Access control could be built into a terminal by requiring a personal token and perhaps a password to activate the terminal. This could be done as a proprietary feature of the terminal.

A weakness in access control which is confined to a terminal is that an intruder might physically remove the protected terminal and substitute his own terminal. Therefore for strong access control it should extend to the next layer of the network hierarchy, either to the PBX or to the public network. The terminal should be required to authenticate to the PBX or public network. Where terminal or user authentication is implemented in a PBX, standards are not strictly necessary, however without standards secure terminals will not be portable with different PBXs. At the

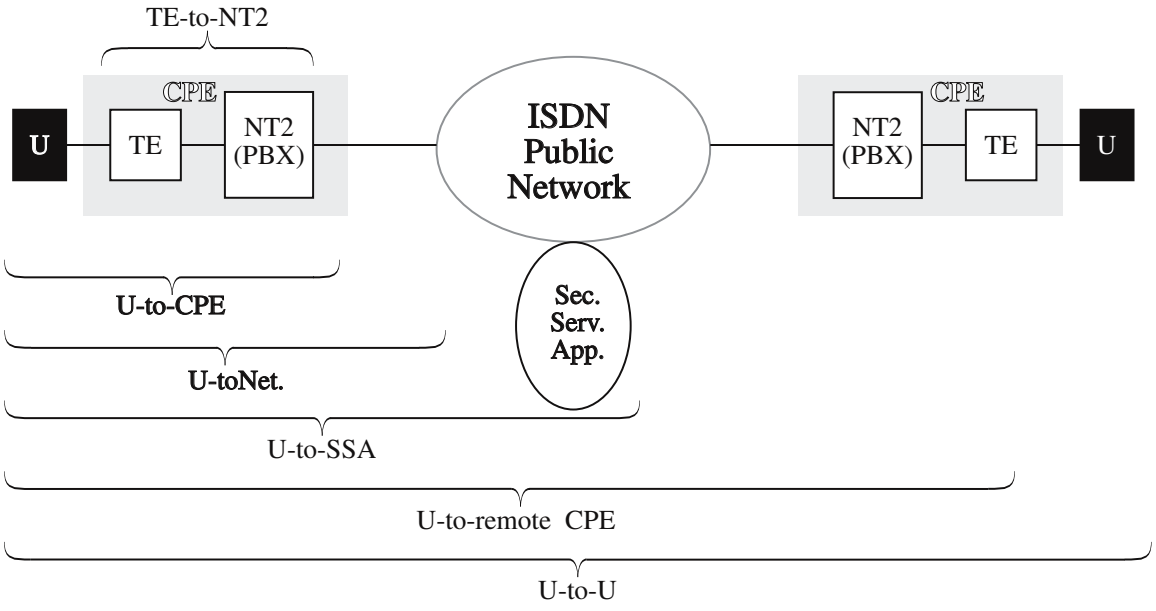

Figure 27 - Diagram of ISDN Security Interactions.

present time, ISDN PBXs typically implement many proprietary features, and terminal portability is more a pious sentiment, than a reality, in the PBX environment.

Security audit information could also be collected in CPE. If users authenticate before using a terminal, then a record of the user who placed each call would be appropriate security audit information in a highly secure environment.

6.2 User-to-Network

For the purpose of this discussion, and subsequent sections it is not necessary to distinguish between the user and the CPE. To the extent required, the user is assumed to authenticate himself to the CPE, to have passed whatever access controls are required by the CPE. For security purposes the user and CPE are bound together.

The primary user-to-network security functions, if implemented, would be authentication and access control. In this case standards would clearly be required. Significant enhancements would be needed in public network switches to implement user authentication. In the context of the public network, the primary access control consideration would be user access to network services, such as 900 or long distance. Such access control services might be offered to subscribers to prevent unauthorized use of business phones or to prevent children from making inappropriate use of home telephones.

Unless forced to do so by regulatory agencies or legislation (for example to prevent children from calling sexually oriented telephone services), the implementation of access control features is a business issue for service providers. Would a business oriented centrex authentication and access control feature generate significant additional revenues for public network service providers? It might eventually be necessary for public networks to offer such centrex services to compete with similar services offered by PBX vendors, even if the direct extra revenues for these services did not pay for their provisioning.

Public network service providers may also be motivated to provide improved authentication for the use of telephone calling cards to reduce fraud. This, again, is a business issue, and may be resolved only in the broader context of personal identification for all credit and financial transactions. Also, to the extent that public networks allow dial up access to sensitive resources and databases, and to operational and maintenance facilities, improved authentication standards could make a significant reduction to network vulnerability to fraud and denial of service attacks.

It is reasonable to expect that carriers will eventually encrypt most trunks, and may reasonably be expected to offer secure routing to major users who require it. User to network local office (ISP1 or ISP0 layer) services are more problematic, and will depend upon the development of suitable switch line cards and software to manage them. Encryption at this layer provides a degree of traffic flow confidentiality which is difficult to achieve otherwise, but it is not likely that there will be a large market for this service, and it may not be commercially viable.

The principal presently defined user-to-network service, which will be used for security, is the Calling Line ID. In the absence of better authentication, it will be used for this purpose and for inward access control. There is a danger that this relatively weak feature will be too heavily relied upon, because it is what is available.

In general, ISDN standards will be required to support user-to-network security, or any other user-to-network service.

6.3 User-to-SSA

A large variety of User-to-Security Service Application (SSA) interactions may eventually result. The major ones will probably be for key distribution, authentication, and access control, where the SSA will be a trusted third party which supplies PACS or verifies security attributes. Others may offer notarization services, secure conversion services (*i. e.*, conversion of secure analog to secure ISDN digital voice), or secure mail services.

Standards will be necessary to make most user to SSA functions practical. Since the SSA usually provides a trusted functionality, authentication standards will be necessary for most SSA applications.

6.4 User-to-User

A great many ISDN security services will be implemented primarily on a user-to-user basis, perhaps with the assistance of an SSA for authentication or access control. There are three principal reasons for this:

- The public ISDN network is ponderous and evolves slowly. The provisioning of security functions in the network may not offer service providers a strong return on the investment required. Although ISDN services are only just beginning to become available from the nation's public networks, there is already a huge investment in ISDN compatible switching equipment which does not incorporate security. While some security features might be incorporated as software changes to the switches, such changes require years to design, code, test and deploy. Hardware changes are even more difficult. At this point user investment in ISDN is minor, but current service provider investment is significant.
- User-to-user security is transparent to the network, and can be implemented by users where and as needed, much more quickly than features or services can be added to the network.
- Many security concerns are essentially end-to-end concerns and it is desirable that only the end entities need participate in the security and be trusted. Several networks and service providers may be involved in a secure communication and it would be difficult to be assured of consistent security and trust except on a user-to-user basis.

Authentication, access control and confidentiality are all likely to be addressed primarily on a user-to-user basis, with assistance in some cases from an SSA or the network. For example, if traffic flow confidentiality is required, then user-to-network services are required.

In a strict sense, standards are not absolutely required for user-to-user services. For some applications, there could be proprietary secure terminals. This would be quite undesirable, and standards will be needed to develop a large commodity market for secure terminals, and allow users to communicate securely with all users with secure terminals, rather than with just those with the same brand or model. However, except for certain specific ISDN related functions, such as circuit switched services, the standards do not necessarily have to be specifically ISDN standards. Broader, OSI oriented security standards will suffice for many data applications which use ISDN for some or all of the low layer data transport.