20

ISDN LAN Access: Remote access security and user profile management

Reinhard Posch, Herbert Leitold, Franz Pucher
Institute for Applied Information Processing and Communications
University of Technology Graz
Klosterwiesgasse 32/I, A-8010 Graz, Austria
E-Mail: {hleitold, rposch, fpucher}@iaik.tu-graz.ac.at

Abstract

Extending local area networks (LANs) to the home is an important area of today's communication technology. Due to its global availability, making use of services offered by public telecommunication infrastructure gives a high connectivity and flexibility. There are different types of global infrastructure available to build such a remote access environment: Public switched telephone network (PSTN) using modems and wireless cellular radio systems like groupe spécial mobile (GSM) are used. However, integrated services digital network (ISDN) will replace modem lines due to its higher bandwidth and more adequate embedding. Such a heterogeneous remote access scheme needs enhanced access and traffic control. This paper demonstrates a router-based solution for enhanced ISDN call management. One of the main advantages is the separation of a strategic module which defines the behavior. However, using dial up lines to access LANs requires additional access control and user authentication. As the user profiles may vary widely, a remote access security policy is introduced, which has to deal with binding the user's access rights to the user profile. This security system is based on an information filtering scheme, which is controlled by the authenticated security servers. The authentication algorithm is interchangeable and different authentication methods can be used simultaneously. These can range from simple password-based schemes for low privileged guest profiles to cryptographic methods like zero knowledge authentication using secure ID cards for high privileged remote access profiles. Previews of future, connection oriented remote access schemes like asynchronous transfer mode- (ATM) based broadband ISDN (B-ISDN) are given.

Keywords

Remote access security, user authentication, user profile management

P. Horster (ed.), *Communications and Multimedia Security II*

1 INTRODUCTION

For data communication, commercial use of modems - operating at line rates ranging from 300 to 28.8 kb/s - has been popular for more than a decade. At a capacity of two B-channels, each with 64 kb/s, the ISDN basic rate interface (BRI) offers an enhanced alternative for many user applications. ISDN does not necessarily promise to break speed and performance records, however, it is the universal connectivity with sophisticated signaling and control mechanisms it offers, which makes ISDN the natural evolutionary path of PSTN. For digital data communication, ISDN has its main advantages in the multi media and world wide web (WWW) area due to its global availability. However, it is the popularity and high availability that increases the demand of sophisticated security systems, when using ISDN to connect into information, business or corporation networks.

This paper describes the connection of ISDN BRIs directly into LANs using an ISDN primary rate interface (PRI) with a capacity of up to 30 B-channels established simultaneously at the provider side, with a sophisticated line scheduling and authentication scheme. Therefore, a special ISDN packet driver has been developed to allow a router-based solution for the ISDN LAN access. A so-called strategic module controls the connection establishment and maintenance. In its main section this paper deals with an enhanced access control and user authentication system, which addresses the increasing demand for network security when connecting into LANs using public dial up lines like ISDN. Therefore, security modules can be attached as a part of the strategic module to allow a multitude of users (e.g. students, schools, small companies, universities, etc.) to access the institute's LAN using authentified ISDN channels within defined access sets.

The paper is structured as follows: Section 2 gives a brief overview of the network used. Section 3 introduces the ISDN packet driver CAPIPKT and describes its flexibility due to modular extending using a strategic interface. Section 4 discusses the remote access security policy, which provides profiles for a variety of different users. In section 5 a case study is given, describing the authentication procedure and the information filtering scheme controlled dynamically by security servers. Section 6 discusses security aspects of the system and gives a preview to future enhancements of the remote access solution. Finally, the paper is concluded.

2 DEPARTMENTAL LAN

Figure 1 gives a view of the configuration, which shows the present university backbone and the location of central university facilities. Although many protocols like Decnet, Novell, etc. are used simultaneously, the user datagram protocol (UDP), transmission control protocol (TCP), and internet protocol (IP) are the main targets.

ISDN will replace the analogous PSTN lines and other existing narrowband metropolitan area networks (MANs) and wide area networks (WANs). ISDN connections can be used for remote access, LAN coupling and backup lines. Although the digital GSM network exhibits no principal difference to ISDN despite the transmission rate, digital gateways are now available and the same common application program interface (CAPI) is even offered. This situation results in a uniform application interface supporting transmission rates ranging from 9,2 kb/s to 2 Mb/s.

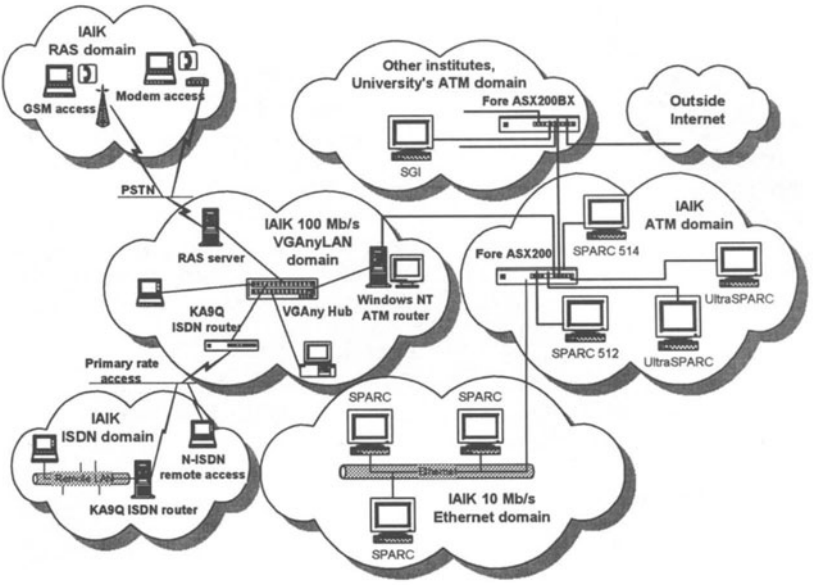

Figure 1 A schematic view of the IAIK network.

In this environment, questions of line usage, mobility of the remote stations, variability of charging, throughput, security functions, data encryption, and compression are studied. Other experiments with this network include network management, embedding security, and scheduling policies to provide access to the network for more users when channels are not readily available.

Different classes to remote access a LAN have been considered, such as serial line internet protocol (SLIP), which is used for modem lines, or GSM remote access which uses point-to-point protocol (PPP) (Simpson, 1994). The most flexible class seems to be the Ethernet class packet driver. Therefore, a special ISDN packet driver for Ethernet LAN emulation based on TCP/IP over ISDN is described in the next section 3.

3 A SPECIAL ISDN PACKET DRIVER

Packet drivers provide a simple, common programming interface that allows multiple applications to share a network interface at the data link level. Therefore, a special ISDN packet driver CAPIPKT has been developed for the following reasons:

- **Requirements:** None of the commercially available software yet meets the above stated demands, especially for a PRI.
- **Interoperability:** This is only possible if we are independent of ISDN card manufacturers.
- **Costs:** An inexpensive solution has to be provided.

- **Modularity:** With the implementation of a strategic interface, modules can be attached for different requirements. The strategic module will be described later in this section.

To connect different networks gateways, routers or bridges can be used. In our project KA9Q (Karn, 1988), a public domain, PC-based routing software is used at the institute's site to connect ISDN to the LAN (see figure 1). The CAPIPKT presented is capable of handling up to 30 connections simultaneously. In addition, the integrated IP-routing and Ethernet-bridging functions support the access of different subnets over one CAPIPKT. This allows for selective packet filtering, as the users can be assigned to several sets of access rights depending on the user profiles. This gives a coarse division of the users remote accessing the departmental LAN to several subsets of remote access profiles. A refinement of the access profiles assigning an access set to each user depending on the user's profile is discussed in section 4.

As the strategic module provides for the tasks needed to control the ISDN packet driver, it is described in detail in the subsection following.

3.1 Enhanced packet driver and security functions

The strategic module provides various aspects of traffic and transport control as well as security services. This module can be seen as a managed object as well as a management program. The language used between two strategic modules or a strategic module and a special management program is simple network management protocol version two (SNMPv2) (Case, et al. 1988). The strategic module is responsible for figuring out how to control the connection where the tasks could be divided into four groups:

- **Basic packet driver extension:** CAPIPKT provides basic packet driver functions to perform a TCP/IP-based ISDN remote access. If additional functions are needed, the strategic module is invoked.
- **End-to-end signaling:** The strategic module also manages the established connections by communicating with the strategic module at the remote station, e.g. it negotiates the need for a higher bandwidth by bundling several physical connections to form one logical link.
- **Administration of connections:** The packet drivers forward received information from the ISDN telecommunication company to the strategic module for interpretation and examination, such as charging information, traffic control, and connection control services.
- **Managed object:** A management program is used, which issues management requests on behalf of the human. The strategic module is able to respond to management requests. One of the advantages of this model is that the strategic module can field requests from many different managers on many different nodes.

As shown in section 2 the router is connected to the network at the university and offers a wide range of possibilities to intruders. Therefore, security is an important topic, especially because ISDN provides a connection to the outside world. The security functions are part of the strategic module and are configured at startup time or managed from a management program. Some functions are:

1. **Callback service:** If the subscriber number is known (a profile exists for that user), the call is rejected and the user is called back, so the intruder is known if there are security attacks. Even if breaking the ISDN service provider's security mechanism is assumed to be unlikely, attacking the signaling system successfully will break the call back scheme. Thus, for high security levels the call back service can only be viewed as an extension to appropriate authentication mechanisms.
2. **Authentication service:** In addition to the previous point 1, a password authentication for a specific user has to be invoked. As the password transmitted over the network is a long term secret that is changed infrequently, an eavesdropper can pick it up and masquerade as an authenticated user. To overcome this problem, cryptographic-based authentication services like the utilization of secure ID cards (Dray, et al. 1989) have to be supported.
3. **Encryption and data compression service:** In addition to restricted traffic and access control, an eavesdropper might pick up sensitive data. Thus, secure communication between users is needed. Two such endpoints (strategic modules) can perform encryption, e.g. RSA (Rivest, et al. 1978). To increase the throughput, data compression facilities (e.g. V.42 bis standard) can be combined. For system performance reasons data compression and encryption usually calls for a separate processor at the network card anyway.
4. **Logging and auditing support:** To support the analysis of possible security attacks, the ability to log the activities and audit data passing the packet drivers must exist. Several levels of auditing are supported, they can range from evaluation of the IP address space currently used to auditing any packet transmitted.

Providing for adequate remote access security is one of the key issues of the project. Different user groups access the institute's LAN: Guest users who cannot access the university's network via Internet can make use of the university's information system service. The campus network is extended to student's homes and student hostels equipped with ISDN. An Internet access is offered to schools for educational purposes. Institute and university staff can access the institute's LAN from their homes. Obviously, the access rights of the user groups vary widely. Thus, a per-user-based access security policy has been chosen, which is described in the next section 4.

4 MANAGING USER BASED ACCESS SETS

Network security is an important topic, when using ISDN to connect LANs. In general, there are several goals, that have to be observed, when building a security system (Boozer, 1995):

- **Prohibit unauthorized dial-in access:** Only specifically authorized users should be able to gain access to the network. If an organisation wants to provide "Guest" privileges to anonymous users, it must devise a plan to shield private data from these users.
- **Provide ease of administration:** It is assumed that a security system that is difficult to set up and maintain will fail eventually.
- **Create security that is transparent to users:** If the security system is onerous or obtrusive, people will try to find ways to avoid it.
- **Centralize accounting and management:** All security systems must be monitored to ensure that they are working. This is only possible if all information is centralized.

- **Provide firewall protection:** Firewall protection ensures that even if unauthorized users gain access to the system, they cannot see or harm valuable files.

With these preconditions, together with the environment presented in the previous sections, a security system has been implemented. Several access sets are assigned to the remote users. These access sets consist of capability lists, which describe the resources the user is allowed to consume (see (Gallagher, 1987) for a description of access sets and capability lists). An object-based approach is used to divide the resources into several classes:

- **Accessible locations:** This class of resources consists of the hosts the user is allowed or denied to access. Security servers or file servers offering software archives are instances of locations where access by low privileged users is not desired. To make the black-/whitelists describing the access sets less complex and more manageable, the use of "wildcards" is to be supported. This allows for permitting or denying access to whole networks.
- **Offered services:** To avoid misuse of the remote access offered, the access sets determine the services a user is permitted to consume. For instance, offering charged Internet services released to high-privileged users is not allowed to schools equipped with an Internet access for educational purposes.
- **Available performance:** The institute's LAN consists of several communication media. To avoid affecting the quality of services (QoS) needed by distributed applications or remote access clients assigned a high priority, low privileged users have to be sealed off from networks used for high-performance applications. The performance assigned to a specific user might be changed dynamically, as the resources available depend on the overall load of the remote access system. In addition, requests for increasing the bandwidth by channel bundling can be accepted in a way that other users are not affected.
- **Supplementary ISDN services:** This class of resources has been introduced to embed future ISDN service profiles into the user's access set. Examples of such service profiles are reverse charging, credit card calling, or multiple party services like conference calling for supporting multicast services.

Obviously, one key issue in managing the user's access sets is the need to prevent unauthorized modifications. Especially when dynamic renegotiating of the user's access sets is provided by an automated management system. Therefore, the communication between the management server and the agents has to be protected against security attacks. In (McCloghrie, et al. 1995) a per-user-based security model which performs an administratively-defined level of security for protocol interactions is described.

To implement this management scheme, a SNMPv2 module can be added to the strategic module. The standard management information base (MIB) is extended to both the access set objects, to control the access rights, and the objects needed to control the ISDN specific management tasks, such as channel bundling, call back, administration of connections, etc. (see section 3). Due to the end-to-end signaling between the strategic module and the users, transparency of the access sets exists. Thus, each user knows the access rights which are currently assigned to her/his access set.

Figure 2 gives a schematic view of the systems involved in the remote access security scheme. It consists of six main systems: (1) The user that wants to utilize the ISDN access offered. (2) The router-based remote access solution consisting of the ISDN packet driver, the

router, and the strategic module. (3) A centralized management server which controls the systems involved and performs the coordination between them. (4) An authentication server performing the authentication procedure and keeping the secrets, such as encrypted passwords. (5) A user profile server managing the access sets. (6) A log/audit server, which can log events like establishing and closing ISDN channels for accounting purposes, and log suspicious events, such as errors, failing authentication, etc. In the case of security attacks any data transmitted can be audited. Figure 2 outlines the resources the user is intended to use (access set) and denied use of (closed area). Even though the systems (3) to (6) are shown as separated physical units, these servers might be processes running on the same workstation.

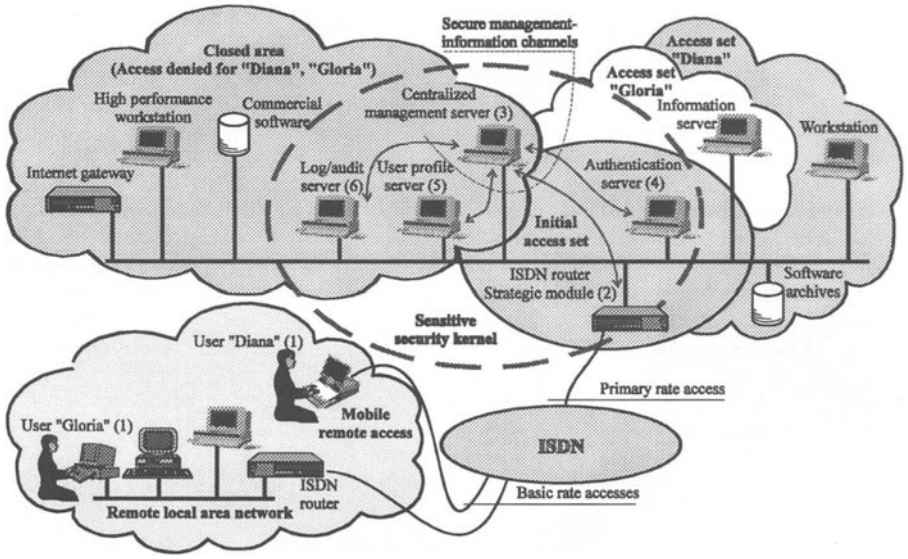

Figure 2 The security management system.

User authentication is the central aspect of the security policy introduced. The strategic module makes it possible to control both the ISDN channels on the one hand, and the data transmitted on the other hand. Thus, the security modules have to carry out the functions related to the access sets, that are applied at the entry point of the remote access - the ISDN B-channel. To perform the access restrictions defined by the user's access set, an information filtering system, which is controlled by the authenticated management server, has been added to the strategic module. The information filtering can range from a packet filtering scheme at the data link layer packet level protecting the security servers from unauthorized access, to a service filtering scheme operating at the application layers and restricting the services offered to a specific user. The authentication and information filtering aspects are discussed in the following section 5.

5 USER AUTHENTICATION AND INFORMATION FILTERING

As the variety of users remote accessing the institute's LAN using different platforms - e.g. different operating systems are used - makes supporting existing authentication procedures necessary (in (Lin, et al. 1996) a short overview to solutions available is given), the authentication procedure must be interchangeable and support different solutions simultaneously. As a first step, the terminal access controller access system (TACACS) (Finseth, 1993), a password-based authentication scheme, has been implemented. The advantage of a TACACS implementation is, that the router-based LAN can be linked to Cisco routers, because Cisco routers support TACACS and are very common. As TACACS transmits passwords in plain-text format, it is used for very low privileged accesses only. An improvement on this weakness of TACACS is provided by TACACS+, an authentication protocol based on message digest 5 (MD5) (Rivest, et. al 1992) password encryption.

To reach higher security levels, the channel handshake authentication protocol (CHAP) (Lloyd, et al. 1992), a three-way handshake protocol based on MD5 one-way hash functions, is to be supported. CHAP is used by PPP implementations like remote access service (RAS). Due to the support of existing commercial and non-commercial authentication solutions, a flexible remote access scheme is provided, as the users are not limited to a specific platform. Only the authentication servers have to be installed and adapted to exchange management information with the management server. However, the system aims to implement and experiment higher security levels supported by cryptographic algorithms like zero-knowledge authentication (Feigenbaum, 1992) applied to secure ID cards and token cards (Dray, et al. 1989).

To allow for using different authentication protocols, the authentication procedure is performed between the user and an authentication server. The strategic module performs information filtering and shields sensitive areas. The module is informed about successful authentication by the management server. The actions which have to be performed when a user establishes a link to the departmental LAN are described as follows:

- **Authentication:** Initially, the user is assigned to an access set, which provides for communication with the authentication server only. Thus, the access set assigned to the user is limited to the authentication service. After performing an authentication procedure initiated by the user, the authentication server transfers the result to the centralized management server. The further steps are: If the authentication fails, a log/audit server is informed about a possible security attack and requested to log the event. In addition, the strategic module is requested to close the physical ISDN channel. If the user authentication is successful, the management server fetches the user's access set from the user profile server.
- **Access set assignment:** The access set assigned to the user is transferred to the strategic module. For this transmission, a secure channel is used and the resources assigned are made available. As several access rights can change dynamically, such as the bandwidth offered, the management server can change the access sets on demand.
- **Re-Authentication:** Periodical verification of the identity of the peer user is provided. Thus, the authentication server can be requested to repeat the authentication procedure after a certain period of time. As re-authentication is useful only in the case of an established physical link, the centralized management server is informed about the current state of the physical links.

- **Clearing:** Clearing is initiated by a log-out sequence, a time-out system, the detection of a security attack or the fact that a physical ISDN connection is down, or a logical IP connection timed out. In such cases, the strategic module is requested to return to the initial state and close the physical links.

Figure 3 shows as a case study the authentication procedure for the password-based TACACS solution. Solid arrows represent the user data to be transferred, dashed arrows depict the additional management information transmitted. Note that attempts to transmit packets other than authentication requests are discarded by the strategic module until the user's access set is loaded. This is because the strategic module usually does not evaluate the data transmitted. The whole situation is controlled by the management server. If the user's remote access computer is equipped with a strategic module, the user can request her/his access set using the strategic module's end-to-end signaling functions. Thus, the access set assigned is transparent to the user.

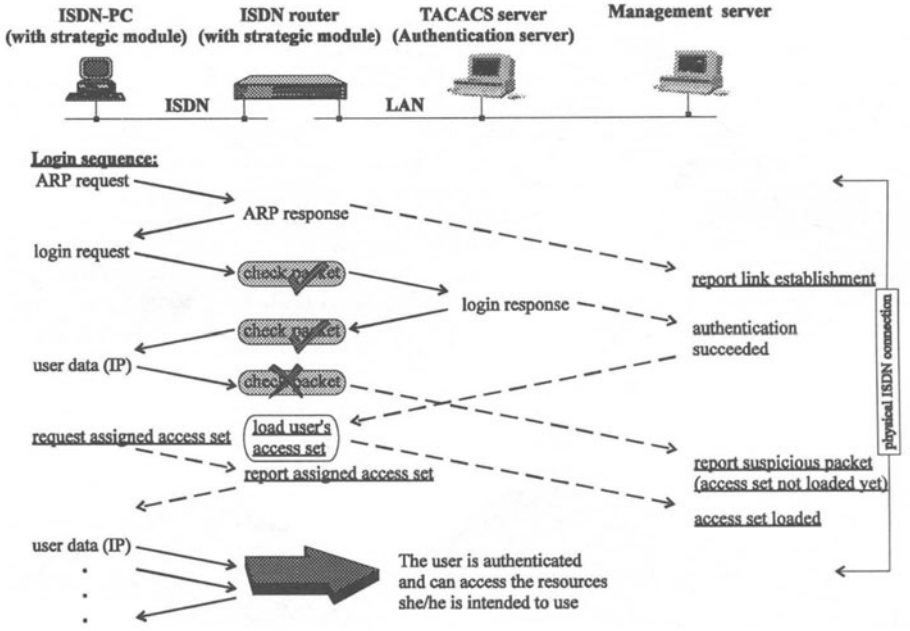

Figure 3 The authentication procedure.

The strategic module performs specific information filtering. Information which is out of the user's access set is discarded. The filtering functions operate at different layers, according to the resource classes assigned to the access sets, as described in section 4:

1. **Accessible locations:** At the network layer, IP addresses are evaluated. Thus, a packet filtering scheme is used (Chapman, 1992) and the packet driver acts as a packet filtering

firewall (Cheswick, et. al. 1994) controlled by the management server. The packet filtering mechanism divides hosts into accessible and non-accessible ones. An efficient way to deny access to groups of hosts exists, if the domain names according to the logical IP connections currently used are evaluated. Thus, wildcards can be used to deny/permit access to specific groups, e.g. denying **.com* will shield a specific user from the multitude of commercial sites. Therefore, the domain name service (DNS) has to be used, which operates at the TCP/IP application layer. By performing an inverse DNS query, the strategic module can decide, whether a domain name belongs to a location, that the user is permitted/denied use of.

2. **Offered services:** To provide for a service-based access set assignment at the transport layer, UDP and TCP ports are filtered. By binding the ports to the IP addresses, the strategic module acts as a socket filtering firewall.
3. **Available performance:** To shield low privileged users from networks needed for high performance applications, packet filtering mechanisms are used as described in point 1. In addition, the strategic module filters attempts to establish an additional B-channel by rejecting the call, if the bandwidth is needed for high privileged users. This is similar to filtering of supplementary ISDN services as described in the next point 4.
4. **Supplementary ISDN services:** These objects are related closely to ISDN and cannot be described as a filtering mechanism according to a specific TCP/IP layer. However, due to the object-based description of the resources, the signaling functions indicating a supplementary service can be viewed as a piece of information transmitted to the strategic module, which decides between accepting (i.e. delivery) or rejecting (i.e. filter) the supplementary service. Thus, these services can be controlled by the management station by assigning an information filter to the access sets.

The sections 4 and 5 have presented a SNMPv2-based management and user-based security scheme. Flexibility is given by interchangeable authentication protocols. The following section 6 will discuss security aspects and enhancements for a future ATM WAN.

6 SECURITY CONSIDERATIONS AND FUTURE ENHANCEMENTS

Due to both the multitude of user groups accessing the institute's LAN ranging from low privileged guest users to high privileged users, and the different authentication schemes that can be used, there are additional considerations. For instance, consider a high privileged user accessing the departmental LAN from her/his home equipped with a secure ID card reader. Allowing a mobile access using an insecure authentication protocol like TACACS and binding the access set to the high privileged user only, offers an easy way to break into the system by wiretapping. Thus, access sets have to depend on the level of security that the user authentication offers.

The security kernel consisting of the strategic module and the servers involved in the authentication procedure (see figure 2) has to be protected in such a manner that intruding into these servers is unlikely. In addition, any communication between these servers has to be authenticated to protect against attacks, such as IP spoofing: An intruder allowed to access the institute's LAN might masquerade as a host, so that he/she is allowed to access a server

belonging to the sensitive security kernel. In (CERT, 1995) and (Bellovin, 1989) similar attacks are described, where an intruder might use a low privileged account to access the LAN and accesses hosts out of her/his access set using TCP/IP services. Thus, the system presented does not protect against attacks - known or unknown - that are due to the insecurity of TCP/IP or the operating system used. However, an upper bound of the level of security is given with the level of security the authentication protocol offers. Thus, insecure protocols like TACACS, which transmits plain-text passwords, have to be replaced by appropriate authentication schemes as soon as these schemes are available for the platforms used by the remote users.

As described in section 4 and section 5, the authentication procedure is carried out between the user and an authentication server. The information filtering functions located at the strategic module restrict the remote access to the authentication server until the user is authenticated and her/his access set is transferred to the strategic module. One advantage of distributing the tasks needed to perform user authentication and access set control is that different communication infrastructures can be equipped with the remote security system. Therefore, a SNMPv2-based strategic module controlling both the physical entry point of the remote access and the data passing this entry point is needed. Thus, the system can be extended to a future B-ISDN WAN, by developing a service module equivalent to the strategic module. This is currently being studied and implemented at the IAIK for the ATM LAN/MAN infrastructure shown in figure 1.

7 CONCLUSION

The growing popularity of ISDN has resulted in a multitude of systems to remote access LANs. This was driven by the fact, that ISDN offers - compared to modems - a more adequate bandwidth, shorter set-up times, and an increased reliability. Using the connection oriented, circuit switched 64 kb/s B-channel is not secure. Therefore, security functions providing for user authentication are needed.

The paper described a remote access security solution that allows for authentication of any user who accesses the institute's LAN via the ISDN PRI capable of handling 30 B-channels simultaneously. A special ISDN packet driver is used, which supports modular extensions over an open strategic interface. Due to an object-based description of the resources an authenticated user is allowed to access, the access sets assigned to the user can be controlled by the SNMPv2 management protocol and, thus, be changed dynamically by a centralized management server.

The main advantage of the solution presented is the ability to use different authentication protocols simultaneously. With this scheme, almost any authentication protocol can be applied to the system. Even the access set assigned to a particular user can vary, depending on the level of security the authentication protocol offers.

8 ACKNOWLEDGEMENTS

This work was sponsored by the Austrian National Bank, jubilee funds project number 4849 and 5639.

9 REFERENCES

Bellovin, S. M. (1989) Security Problems in the TCP/IP Protocol Suite. *Computer Communications Review*, v.19 no.2, pp. 32-48.

Boozer, C (1995) Remote Access Security, Whitepaper. *Funk Software, Inc.*

CERT (1995) IP Spoofing Attacks and Hijacked Terminal Connection. *CERT Coordination Center*, Carnegie Mellon University, Advisory CA-95:01.

Case, J., Fedor, M., Schoffstall, M., Davin, J. (1988) A Simple Network Management Protocol (SNMP). *RFC 1157*, SNMP Research.

Chapman, D. B. (1992) Network (In)security through IP Packet Filtering. *Proceedings of the 3rd USENIX UNIX Security Workshop*, pp. 63-76.

Cheswick, W. R., Bellovin, S. M. (1994) *Firewalls and Internet Security*. Addison Wesley.

Dray, J., F., Smid, M. E., Warnar, R. B. J. (1989) Implementing a Access Control System with Smart Token Technology. *NIST Draft*, National Institute of Standards and Technology.

Feigenbaum, J. (1992) Overview of Interactive Proof Systems and Zero-Knowledge. *Contemporary Cryptology: The Science of Information Integrity*, IEEE Press, pp. 423-439.

Finseth, C. (1993) An Access Control Protocol, Sometimes Called TACAC., *RFC 1492*, University of Minnesota.

Gallagher, P. R. (1987) A Guide to Understanding Discretionary Access Control in Trusted Systems. *National Computer Security Center*, NCSC-TG-003-87 Lib. No. S-228,576.

Karn, P. (1988) Amateur Packet Radio and TCP/IP. *ConneXions*, v.2 no.9, pp. 8-15.

Lin Ping, Lin Lin. (1996) Security in Enterprise Networking: A Quick Tour. *IEEE Communications Magazine*, v.34 no.1, pp. 56-61.

Lloyd, B., Simpson, W. (1992) PPP Authentication Protocols. *RFC 1334*, Lloyd & Associates.

McCloghrie, K., Rose, M., Waters, G. (1995) User-based Security Model for SNMPv2. *Internet Draft,* User Configuration MIB for SNMPv2 Agents.

Rivest, R. L., Shamir, A., Adelmann, L. (1978) Obtaining Digital Signatures and Public Key Cryptosystems. *Communications of the ACM,* v.21 no.2, pp. 120-126.

Rivest, R. L., Dusse, S. (1992) The MD5 Message-Digest Algorithm. *RFC 1321*, MIT Laboratory for Computer Science and RSA Data Security, Inc.

Simpson, W. 1994 Point-to-Point Protocol (PPP), STD 51, *RFC 1661*, Daydreamer, July 1992.

10 BIOGRAPHY

Reinhard Posch received his PhD in Informatics and Telecommunication at the Graz University of Technology. Since 1984 he is full Professor and head of the Institute for Applied Information Processing and Communications Technology since 1986. Herbert Leitold is student assistant at the Institute for Applied Information Processing and Communications Technology since 1995. Franz Pucher is assistant professor at the Institute for Applied Information Processing and Communications Technology. He received his PhD in 1993 at Graz University of Technology.