Enhancing Security and Robustness in ISDN Networks

Anand Nayyar
Assistant Professor
Department of Computer
Applications & IT
KCL Institute of Management
and Technology, Jalandhar

ABSTRACT

In the current time, Computer Networks are influencing the lives of Human Beings to a great extent, the evolution of public Integrated Services Digital Network (ISDN) with complete end to end digital connectivity provides a magnificent platform for networking and reliable data communications. The main objective behind this Research paper is to develop and implement methodologies in a new frame-based algorithm for successful data protection to be transmitted via ISDN which can be embedded into ISDN customer premises equipment (CPE) or at the server end of the switching equipment which will make public ISDN network look like a private network to the users and also create a secured database at the background and in turn results in the enhancement of the ISDN networks. In this paper, we present the overview of technology of ISDN, the security concerns and possible standards for ISDN security specific with most commonly used NOVELL NETWWARE ARCHITECTURE which allow data along with voice to be transmitted over the ISDN basic rate interface (BRI) line to be encrypted so that only the authenticated receiver can decrypt it.

Keywords

ISDN, Data Communications, Network Security, NOVELL NETWARE ARCHITECTURE, Data Networking

1. INTRODUCTION

ISDN stands for Integrated Services Digital Network; it is system of digital phone connections which has been available for many years. This ISDN system allows voice and data to be transmitted simultaneously across the world using end-to-end digital connectivity. The ISDN offers on-demand switched digital end-to-end connectivity over the wide area which itself is regarded as the most important feature which focuses over excessive speed data transfers of either company module or focus-data module and requires high security over its security. This enables the integration of both voice and data services over a common core network.

With ISDN, voice and data are carried by the bearer channels (B Channels) which occupy the bandwidth of 64 Kbps. Some switched limit B Channels to a bandwidth of 56 Kbps; A D Channel or Data Channel handles the signalling at a speed of 16 or 64 Kbps which all depends on the service type. The B-Channels are circuit-switched point-to-point connections and can carry pulse code modulated (PCM) encoded digital, voice or data. The D-Channel is primarily used for signalling information.

In such a care, where Network Security is not possible to be implemented on a user-to-user base which is transparent to the network, can be implemented far more quickly because modems interface in any case would enable encryption.

All Digital ISDN will give a boost to encryption of voice and data. Also, inclusion of the packet data facility for signalling on the D-Channel will make it possible for basic ISDN voice terminals to implement digital security protocols.

2. ISDN ROUTER NETWORKS

In order to properly understand the issues associated with ISDN data networks, a basic foundational understanding of routed and routing protocols is required.

In the upcoming years after the launch of ISDN in India and many other countries, companies have been demanding for more and more data transfer through ISDN based Networks, indeed increases the speed and efficiency, and further increasing the risk. According to the current statistics (2009), more than one billion channels of data transfer are being used in India for the leased data transfer through ISDN. Within this environment, ISDN may be favored for a number of roles — these include its use as a core network technology (this may involve teleworking), as a backup network to ensure connectivity in the event of failure of the primary network, for dial access to both corporate intranets and the Internet, and to supplement fixed link technologies.

ISDN as a core network technology involves making a data connection ‘ondemand’, transferring data, and clearing down the connection. This method of exchanging data is referred to as dial ondemand. Teleworking also utilizes this method of connecting, with the ISDN connection generally being made direct to a card within the portable PC itself.

But in the same duration when access to the ISDN based router modem increases the security concerns hypes itself, because more the number of nodes/disjunctions in the network, more will be chance for data loss or theft.

2.1 Dial on demand

Dial ondemand enables routers and other ISDN customer premises equipment (CPE) to exchange data over an ISDN network in an efficient way, with ISDN connections only being established when an exchange of data is required.

Dial ondemand using ISDN is ideally suited to applications requiring occasional data transfer only. At the current time, if communication for an aggregate of more than 3 to 4 hours per day is required, a fixed link technology, this may not be appropriate to a (mobile) teleworker.

2.2 Dial Backup

ISDN dial backup is used to provide resilience for a separate core networking technology, e.g. leased line. The most commonly used method of detecting a primary network failure is by using a dynamic routing protocol. The loss of a route across the primary network can then be easily and quickly detected (by loss of a routing update) and the ISDN backup link thus activated.

2.3 Dial top up

Dial topup can provide an efficient means of providing additional bandwidth ondemand in certain scenarios, i.e. a simple leased line connection may be supplemented by an ISDN connection during peak periods to cope with the additional traffic demands made at that time. The network designer should aim to distribute these traffic demands equally between the two links.

I. SECURITY

Security is increasingly a key concern for any business connecting to a public network, and the explosive growth of the Internet has highlighted this. Security is necessary to safeguard sensitive data and protect against fraudulent use of corporate resources; Authenticating users on the system and limiting authorization rights are keys to good security. Although perfect security does not exist, there are a number of techniques available which offer varying degrees of protection. It is common for a number of techniques to be collectively employed for increased protection. These are implemented in some form by all organizations to protect company sensitive information. Network access lacks any good personal authentication standard. But that should be looked at more as a screening device than strong access control, the report adds. Effective access control requires effective authentication. One such method might be biometric recognitions that contain personal ID information, information about their access privileges and a private access key designed not is read directly. Provision could be made to bind all the user's privileges into one card. Security techniques available for Security during the access of ISDN in data networking include the following:

• *Authentication*
All ISDN connections use the point-to-point protocol (PPP). It is usually recommended for the use of CHAP wherever possible, which involves the called station (i.e. router) sending a challenge to the remote station, i.e. another router, which replies with a value produced by applying a one way Hash function to the 'challenge string' and other specifics, as required, (i.e. the 'password' is not transmitted across the link). If this reply matches the station's own hash calculation, authentication is acknowledged.

• *Filters*
These may be applied to particular interfaces within a router, and may be used to filter users based on a layer 3 network addresses and protocol type (e.g. IP, IPX). A firewall is a comprehensive filter with additional, powerful facilities to detect faked packets. Both the source and destination addresses can be used for this purpose, and may, for example, prevent access to a particular server for any dial in user.

• *Dial back*
On connection, the call is immediately cleared (usually following authentication) and the user is called back on a preconfigured number; It is possible to negotiate this within PPP. This represents a much higher degree of security, and has the added advantage that connection costs will be accumulated at a central site (typically the company host site).

Dialback is not recommended where short transfer of one or two packets is to take place, for example, with an SNMP poll to obtain basic router information.

• *Authentication server*
An authentication server is a more recent development. It is a dedicated server for remote access login, and provides authentication, authorization and accounting (AA A) functionality. They are accessed by the called router when the initial ISDN connection is made. Users are authorized against details held within the server, which may, for example, be configured for dial back, restrictions on command usage, restrictions on access time (e.g. daytime only) and connection period, all on an individual or group basis.

• *Encryption*
The aforementioned techniques aim to restrict access to a central dial in site. However, thus far there is no protection for data while it is carried via the public network; this could potentially be illegally monitored or intercepted by a third party. Encryption is employed in order to ensure data cannot be understood by a third party as it requires a unique key, held only by the originator and receiver, in order to decrypt the information. There are various levels of encryption, the level of security offered being derived from the algorithm used, the key size and the frequency with which keys are changed.

II. INCREASING THE ROBUSTNESS IN NOVELLNETWARE ARCHITECHTURE

The basic issue of discussion is about the Novell Netware Architecture which is being used and whose implementation is more than 90% when counted on the global scale in ISDN based networks because of its simplicity as it is a client based Operating system, which provides a great flexibility for the client to access because it is a true client server based operating system. Tying NetWare together is a directory service called NDS (Novell Directory Services). Everything in the network is tied into and managed by NDS. NDS can even manage non Novell systems such as NT domains and Win2K Active Directory information. So, in order to secure the entire architecture a specific algorithm is designed and implemented, and this algorithm is restricted to only the Novell Architecture for application.

• ***Embedding/Transmission Algorithm:***

Step 1: Modulate the Analog code from the workstation A to a Normal Digital Signal and Bind a Process Log file with it.

Step 2: Pass this Digital Code to the 1Way Complex maker and check if the output received is in a symmetric or asymmetric form.

i) If found in a symmetric form, decrypt the code in DES* and extract the 56 bit key.
ii) If found in an asymmetric form, decrypt the code in RSA** and extract the public and private key.

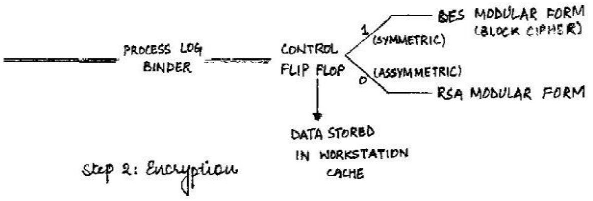


Fig. 1: Encryption Algorithm for the scale.

Now, we have the decrypted keys, save the process in the process log, and now bind this process log to the achieved keys.

Step 3: Pass this Digital Encrypted Code (DEC) to the Server through Data Transfer Lines (DTL).

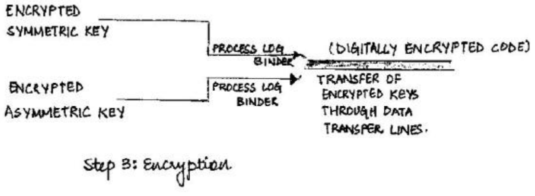


Fig. 2: Encryption Algorithm for the same.

The Data is Successfully Transmitted to the Server.

• ***Extraction/Decryption Algorithm***

Step 1: The Server will now check the process log, and decrypt the code according to the associated encryption algorithm.

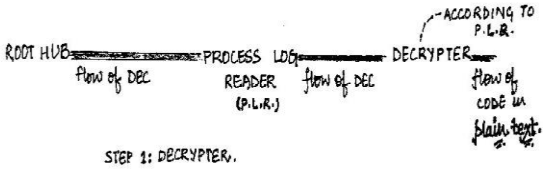


Fig. 3: Decryption Processing

Step 2: The Same Digital Code will be passed on through a Modem for decryption of the digital code back to the analog code for it's decipher.

Step 3: Now from the extracted code fragment the NOS, will process the commands for execution like printing and will store the process log in the memory in the same bit base format, with a biometric lock over it which will further increase the robustness to the attack and securely execute the command and will also store the access key and execute the same effectively and securely even in NOS.

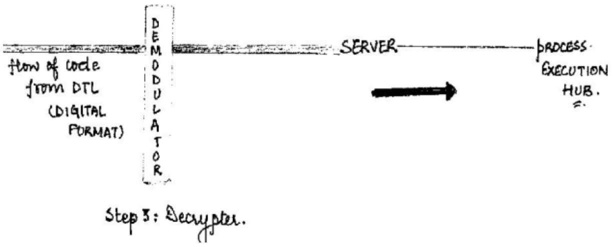
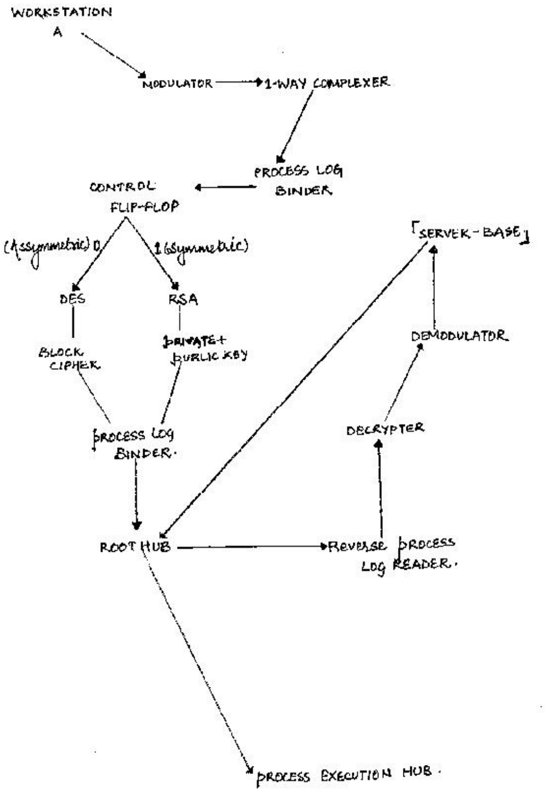


Fig.4: Demodulating the sub code



Experimental Attacks

2.4 Sniffing Attack

Sending a packet sniffer onto this algorithm, Netware Device, where a packet sniffer is an application that captures data packets, which can be used to capture passwords and other data in transit over the network

Now, the modulator cannot differentiate between the digital and analog signals to the device mechanism and hence rejected the application modification significance as a sniffer is restricted to application on plain leased lines, if this sniffer is placed on the same, it will receive the encrypted/staggered code which is of no use.

2.5 Trojan Bombarding

Releasing a Trojan horse which is a program which seems to be doing one thing, but is actually doing another; A Trojan horse can be used to set up a back door in a computer network system such that the intruder can gain access later. Even if we release a Trojan in this network, it will return the hacker back with the DEC which is again of no use as the compiler code, encryption mechanism would be unknown, because the only thing flowing in the entire network is DEC KEYS and the not the data itself.

2.6 Data Stealing

We tried to steal the data using a hardware keylogger, which is a tool designed to record ('log') every keystroke on an affected machine for later retrieval. Its purpose is usually to allow the user of this tool to gain access to confidential information typed on the affected machine, such as a user's password or other private data. But the data commands are always being given in an analog form but NOS is designed for DIGITAL CODE BASE, so keyloggers are ineffective and also NOS does not support such files

3. CONCLUSION

ISDN holds a unique position within the data networking world. It offers scalable ondemand digital connectivity over the wide area, and supports a wide range of networking applications. Currently, ISDN is primarily used as a backup mechanism for connectivity in the unlikely event of core network failure, but there is a significant trend towards greater use of ISDN as a primary network. There has been considerable effort in recent years to enhance the functionality available within routers to support transport of the most prevalent protocols across the ISDN. The generic aims of this development remain to maximize bandwidth utilization and minimize connection times. However, issues such as security are becoming increasingly important and there have been significant developments in recent times. So, for this a new algorithm/work flow/data transfer mechanism is being created which can increase the robustness to attacks in the same. On an experimental base, the robustness to the basic architecture is increased by 2530% in a common scale when this algorithm is implemented.

Further developments will occur as the ISDN evolves, in particular with functionality implemented in ISDN attached routers. Its unique role within the data networking world will ensure that the current rise in demand for ISDN continues into the foreseeable future.

4. REFERENCES

[1] King T J: 'An overview of advanced data networks', BT Technol J, 16, No 1, pp 9—15 (January 1998).

[2] 'I.421 Standard', BTNR 190, Vol 3 (1984).

[3] Day J D and Zimmermann H: 'The OSI Reference Model', Proc of IEEE, 71, pp 1334—1340 (December 1983).

[4] Simpson W: 'The Point-to-Point Protocol (PPP)', RFC 1661 (July 1994).

[5] Lloyd B and Simpson W: 'PPP Authentication Protocols', RFC 1334 (October 1992).

[6] Sklower K, Lloyd B, McGregor G, Carr D and Coradetti T: 'The PPP Multilink Protocol (MP)', RFC 1990 (August 1996).

[7] Postel J: 'Internet Protocol', RFC 791 (September 1981).

[8] Hedrick C L: 'Routing Information Protocol', RFC1058 (June 1988).

[9] Malkin G: 'Routing Information Protocol Version 2 — Carrying Additional Information': RFC 1723 (November 1994).

[10] 'IPX Router Specification', Version 1.10 (November 1992).

[11] Moy J: 'Open Shortest Path First (OSPF) version 2', RFC 1583 (March 1994).

[12] Forrester S E et al: 'Security in data networks', BT TechnolJ, 16, No 1, pp 52—75 (January 1998).

[13] Case J D, Fedor M, Schoffstall M L and Davin C: 'Simple Network Management Protocol (SNMP)', RFC 1157 (May 1990).

[14] BT Technol J Vol 16 No 1 January 1998.

[15] Fernandez, I.B. Subbarao, W.V.: 'Encryption based security for ISDN communication: technique and application'(Apr1994.