ISSN No. 0976-5697

Volume 2, No. 2, Mar-Apr 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

# PBX Design Over Integrated Services Digital Network Interface

Pardeep Kumar*
Deptt. of Computer Science & Engg. and Information Technology, Jaypee University of Information Technology, Waknaghat, H.P, India.
pardeepkumarkhokhar@gmail.com

Shiv Kumar Gupta
Deptt. of Computer Science & Engg. and Information Technology, Jaypee University of Information Technology, Waknaghat,H.P, India.
shivku2003@gmail.com

***Abstract:*** In the presents of our view we intended for use primarily by system administrators of PBX systems, but may also be useful for security evaluators. Where possible, countermeasures are described that can be applied by system administrators. In some cases vulnerabilities may be discovered that require software patches from the manufacturer. We will look at the ISDN system architecture and saw the key role played by the PBX and also will take a closer look at this device to get an idea of how it works internally. PBX design is a large and complex area, and much of the technology is proprietary

***Keywords:*** PBX, Threats, CCITT, POTS.

## I. INTRODUCTION

The Private Branch Exchange (PBX) is an essential element that supports the critical infrastructure of both government agencies and U.S. industry. A PBX is a sophisticated computer-based switch that can be thought of as essentially a small, in-house phone company for the organization that operates it [1]. Protection of the PBX is thus a high priority. Failure to secure a PBX can result in exposing the organization to toll fraud, theft of proprietary or confidential information, and loss of revenue or legal entanglements. A generic methodology for conducting an analysis of a Private Branch.

Exchange (PBX) in order to identify security vulnerabilities. These new features have opened up many new opportunities for an adversary to attempt to exploit the PBX, particularly by using the features as designed for a purpose that was never intended.

## II. PBX THREATS

The threats to PBX telephone systems are many, [3] depending on the goals of attackers.
Threats include:

A. ?*Theft of service* – i.e., toll fraud, probably the most common of motives for attackers.
B. *Disclosure of information* - data disclosed without authorization, either by deliberate action or by accident. Examples include both eavesdropping on conversations and unauthorized access to routing and address data.
C. ?*Data modification* - data altered in some meaningful way by reordering, deleting or modifying it. For example, an intruder may change billing information, or modify system tables to gain additional services.
D. *Unauthorized access* - actions that permit an unauthorized user to gain access to system resources or privileges.
E. ?*Denial of service* - actions that prevent the system from functioning in accordance with its intended purpose. A piece of equipment or entity may be rendered inoperable or forced to operate in a degraded state; operations that depend on timeliness may be delayed.
F. ?*Traffic analysis* - a form of passive attack in which an intruder observes information about calls (although not necessarily the contents of the messages) and makes inferences, e.g. from the source and destination numbers, or frequency and length of the messages. For example, an intruder observes a high volume of calls between a company's legal department and the Patent Office, and concludes that a patent is being filed. PBXs are sophisticated computer systems, and many of the threats and vulnerabilities associated with operating systems are shared by PBXs. But there are two important ways in which PBX security is different from conventional operating system security:
G. *External access/control*. Like larger telephone switches, PBXs typically require remote maintenance by the vendor. Instead of relying on local administrators to make operating system updates and patches, organizations normally have updates installed remotely by the switch manufacturer. This of course requires remote maintenance ports and access to the switch by a potentially large pool of outside parties.
H. ?*Feature richness*. The wide variety of features available on PBXs, particularly administrative features and conference functions, provide the possibility of unexpected attacks. A feature may be used by an attacker in a manner that was not intended by its designers. Features may also interact in unpredictable ways, leading to system compromise even if each component of the system conforms to its security requirements and the system is operated and administrated correctly

## III. SYSTEM ARCHITECTURE

All modern PBXs have central computer processors that are controlled from a software-driven stored program (see Figure 1). In addition, most PBXs have microprocessors dispersed throughout the switch that provide real-time signaling and supervision control as instructed from the central processor. One or more terminals and their associated port(s) provide computer operating system, database management, and maintenance access to the PBX

processor [1] [3]. Access to these functions gives the administrator or maintenance personnel total control of the PBX. Depending on the size of the PBX, these functions may be separate or combined.

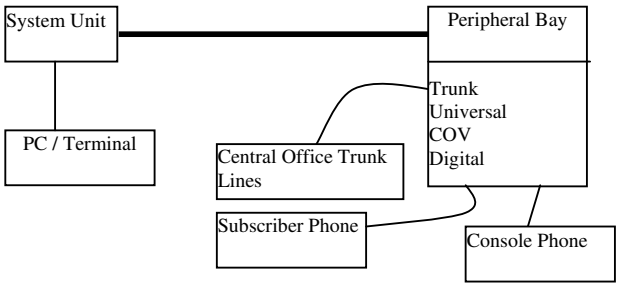



Figure: 1 PBX Block Diagram

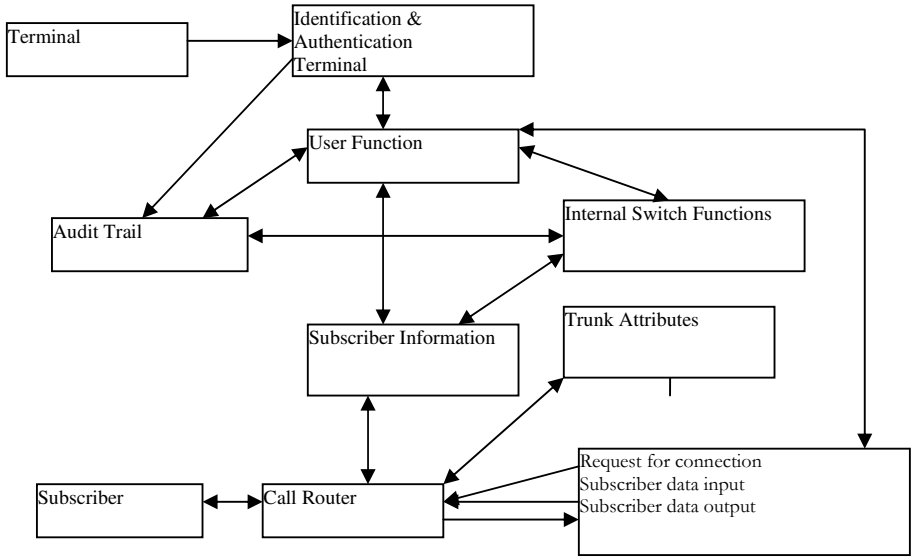



Figure 2: PBX Functional Architecture

## V. TECHNICAL ISSUE

Remember that the goal of ISDN is to present the user with a digital bit pipe at either the T or S reference point. Before we look closely at this interface, it is worth noting that the term interface has a different meaning in the ISDN world than it has in the OSI world in figure. 3(a) we see the by now familiar OSI picture, in which the term "interface" refers to the boundary between two layers on the same machine [4]. The horizontal lines are the protocols. The CCITT view of the world is different. CCITT is primarily concerned with the interface between the carrier's equipment and the customer's equipment, so they have defined "interface" to mean the peer protocols in the lower layer, as shown in figure 3(b). When discussing ISDN, we will use interface in the CCITT sense

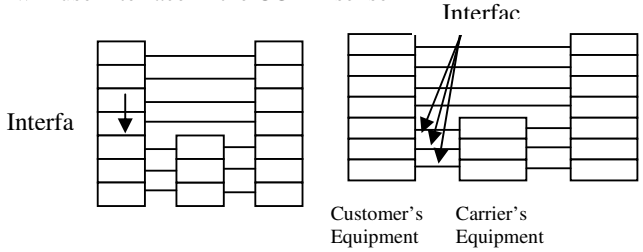



Figure. 3(a) Interface in the OSI model. Figure. 3(b) Interface in the ISDN model.

## IV. FUNCTION ALLOCATION

Although most PBX functions are software driven, the PBX under study should be examined to determine how specific features are implemented so that potential vulnerabilities can be explored [2]. For example, conferencing can be implemented in hardware or software. Knowing the design implementation will aid in determining if an adversary may be able to exploit the function. Figure 2 shows a typical PBX functional architecture.

ISDN is layered in a way similar to the OSI model, although the correspondence is far exact and many of the ISDN protocols are unrelated to the OSI protocols found in the same layer. Like its OSI counterpart, the ISDN physical interface. To start with, ISDN uses a new kind of connector, completely unrelated to the 25-, 37-, and 9-pin D connectors used for RS-232-C and RS-449. The ISDN connector has eight contacts. Two are used for transmit and transmit ground. The remaining four are used to allow NT1 or NT2 to power the terminal or vice versa. By using this balanced transmission scheme, like RS-422-A, the ISDN cable can be 1 km long with good noise immunity.

As mentioned earlier, the ISDN bit pipe supports multiple channels interleaved by time division multiplexing. Several channel types have been standardized:

A - 4 kHz analog telephone channel
B – 64 kbps digital PCM channel for voice or data
C – 8 or 16 kbps digital channel
D – 16 or 64 kbps digital channel for out-of-band signaling
E – 64 kbps digital channel for internal ISDN signaling
H – 384, 1536, or 1920 kbps digital channel

It is not CCITT's intention to allow an arbitrary combination of channels on the digital bit pipe. Three combinations have been standardized so far:

A. Basic rate: 2B + 1D

B. Primary rate: 23B +1D (U.S. and Japan) or 30B + 1D (Europe)
C. Hybrid: 1A + 1C

The basic rate and primary rate channel are given in figure 4.

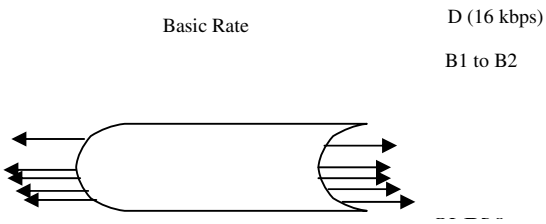



Figure 4. Basic Rate and Primary rate digital pipe.

The basic rate should be viewed as a replacement for POTS (Plain Old Telephone Service) for home and small business use, and for individual employees in a large company. Each of the 64-kbps B channels can handle a single PCM voice channel with 8-bit sample made 8000 times a second (note that 64-kbps means 64,000 here, not 65,536). Signaling is on a separate D channel, so the full 64 kbps are available to the user (as in the CCITT 2.048 Mbps system and unlike the U.S. and Japanese T1 system).

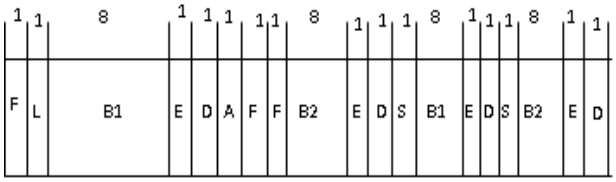
The idea of giving the user two channels instead of one is primarily marketing reasons. Customers are encouraged to perceive the two ISDN channels as an improvement over the one channel POTS system. Without some visible improvement the carrier might have a hard time convincing customers that ISDN is a good idea, since it is more expensive and many customers are not really all that interested in whether the signaling is analog or digital. A typical use for two channels might be for two people to talk on the telephone while looking at a document on the second channel. For data transmission, the B channels may be sub multiplexed into 32 kbps, or lower rates, but of course all the sub channels must begin and end at the same terminals [5][6]. The basic rate D channel is 16 kbps. Calls are requested by sending messages on it. A typical call-setup message would specify which of the B channel to use, the ISDN telephone number to call, and various other options (e.g., collect calls).

The D channel is divided into three logical sub channels:
The s sub channel for signaling (e.g., call setup),
The t sub channel for telemeter (e.g., smoke detectors) and
The p sub channel for low bandwidth packet data.

The primary rate interface is intended for use at the T reference point for businesses with a PBX. It has 23 B channels and 1 D channel at 64 kbps in the U.S. and Japan and 30 B channels and 1 D channel at 64 kbps in Europe. The 23B + 1D choice was made to allow an ISDN frame fit nicely on AT&T's T1 system. The 30B + 1D choice was made to allow an ISDN frame fit nicely in CCITT of 2.048 Mbps system.

The thirty-second time slot n the CCITT system is used for framing and general network maintenance. Note that the amount of D channel per B channel in the primary rate is much less than in the basic rate, so it is not expected that there will be much telemetry or low bandwidth packet data there[8] [9].The hybrid configuration is intended to allow ordinary analog telephones to be combined with a C channel to produce something vaguely reminiscent of the basic rate. It is not very close and everyone knows it, but it is better than nothing.

The physical layer frame format for basic rate traffic from NT1 or NT2 to TE1 is shown on figure 5.the frame is 48 bits, of which 36 are data. It is sent in 250 $\mu$ sec, giving a data rate of 144 kbps, but occupying 192 kbps of bandwidth including the overhead. The F bits contain a well defined pattern to help keep both sides in synchronization. The L bits are there to adjust the average bit values. The E bits are used for contention resolution when several terminals on a passive bus are contending for a channel. The A bit is used for activating devices. The S bits have not yet been assigned. Finally, the B1, B2, and D bits for the user data




48 bits in 250 microsecond=gross data rate of kbps
36 data bits (16B1 , 16B2, 4D)in 250 microsecond =net data rate of 144 kbps
F=Framing bit L=DC load balancing E=Echo of previous D bit
D=D channel (4 bits X 4000 frames/sec=16 kbps) A=Activation bit
S= Spare bit

Figure 5. Physical layer frame format for basic rate NT to TE traffic at the S or T reference points.

It is important to realize that figure 2.31 is the physical layer frame format. The user data is just a raw bit stream [10] [7]. There is no error checking, no checksum, no redundancy, no acknowledgement, and no retransmission. If error occur, they must be handled by higher layers in the OSI model. All ISDN does is provide the user with raw physical bit streams using the B channels (and to a lesser extent, the D channel).

The ISDN bit stream can be used to support either circuit switching or packet switching, depending on how bursty the traffic is. In the circuit switching scenario, the ISDN customer calls up the destination and uses a 64-kbps channel as a physical layer connection for transmission digitized voice, data or anything else. The entire 64-kbps is dedicated to the call throughout its duration. The change will typically be proportional to both the duration of the call and the distance, but not to the volume of data sent.

In the packet-switching scenario, the ISDN customer calls up a nearby IMP. This connection is used to transmit packets from the customer's equipment to the IMP, which transmits them to the final destination via a traditional packet-switching network. The advantage of this scheme is that the call to the IMP will generally be a local call, so the change for the service will be the cost of a local call plus a certain amount per packet. If the volume of traffic is low, for example, an interactive terminal, this method of usage may be cheaper.

## VI. REMARK

When used to access a packet-switching network, the ISDN line is analogous a host-IMP link in the ARPANET. In effect, ISDN gives home users high bandwidth access to a packet-switching network as well as the possibility of dialing direct calls where that is more appropriate.

## VII. REFERENCES


[1] Dalvit, L., Alfonsi, R., Mini, B., Murray, S., & Terzoli, A. (2006). "The localisation of iLanga, a next generation PBX". Poster presented at the Southern African Telecommunication Networks and Applications Conference (SATNAC), 3 - 6 September 2006, Cape Town.

[2] Datapro Information Services, PBX Systems: Technology Overview, Rich Costello,1999.

[3] E. A. Butakov, Methods for the Synthesis of Switching Devices from Treshold Elements (in Russian), Energiya:Moscow. 1970.

[4] J. DeTreville and W. D. Sincoskie, "A distributed experimental communication system," IEEE Journal on Selected Areas in Communication, Vol SAC-1, No 6, Dec 1983, pp. 1070-1075 [5]. "Integrated Services Digital Network (ISDN); Diversion supplementary services; Digital Subscriber Signalling System No. 7 One (DSS1); Part 1: Protocol specification." ETSI EN 300 207-1, 2001.

[6] "Digium Wildcard TE110P Single T1/E1 PCI card VoIP SIPIAX Asterisk PBX." [Online]. Available: http://www.voipsupply.com/

[7] A. Shneyderman and A. Casati, "Fixed Mobile Convergence." McGraw-Hill Osborne Media, 2008.

[8] http://ws.afnog.org/afnog2004/t2/930-telephony/telephony.ppt

[9] Susbielle, J.F. (1998) Internet Telephony, Ed. By Eyrolles, Vol. 1, pp. 191-239

[10] Tanenbaum, A.S., and Van Steen, M.: Distributed Systems: Principles and Paradigms, Upper Saddle River, NJ: Prentice Hall, 2002