Telephone Security Group

Central Office (CO) Interfaces

November 1997

Table of Contents

The Telephone Security Group

The Telephone Security Group (TSG) is a standing committee under the Facility Protection Committee, Security Policy Board, of the U.S. Government. The TSG's membership is made up of representatives from throughout the Executive and Judicial branches of the government and the Department of Defense. The TSG's charter is to provide security policy, procedures, and countermeasures direction for telephone and telecommunications systems employed within all sensitive information processing areas. The primary instrument for doing this is the series of documents published by the TSG, known as the TSG Standards.

The TSG Standards are written for technical security personnel and the telecommunications manufacturers who supply telephone equipment for use in sensitive information processing areas. The TSG has written this Central Office (CO) Interfaces text to provide an understanding of the types of services provided by the local central office and describe how they are connected to our administrative telephone systems. It is important that managers at all levels become aware of the efforts required to provide adequate safeguards to *real* security concerns generated by today's telecommunications technology.

Introduction

The TSG prescribes protective measures for premise telephone equipment through standards aimed at isolating telephone instruments and adjuncts from inadvertent conduction of sensitive, intelligence bearing, discussions. To that end, the TSG measures contained within the TSG Standards prescribe prudent protective measures. However, telephone technology has evolved to a state where many new services and features are available from either central office systems (through the interface) or from premise telephone equipment. New services available through the interface from the central office concern the TSG, as we have not traditionally been involved with the telecommunications path beyond facility walls. The TSG recognized this shortfall, and is now engaged in educating its user population of: 1) the types of interface services, 2) the volume of communications that can be carried over the interface, and 3) the supervision performed over the interface by the CO switch. The following text will address each of the three topics listed above.

The Basics

Modern telephone interfaces have evolved from plain old telephone service (POTS) of the past into full featured wire paths with capabilities beyond those envisioned by Alexander Graham Bell[1]. In Bell's day, the wire path, known as the "twisted pair," was utilized as a means of transmitting voice from one telephone instrument to another. As technology evolved with time, the path became utilized for more functions than just transmitting voice communications. Today, the path is used to transmit voice, data, voice and data, fax, and interchannel signaling to invoke custom features, and much, much more. In some applications, the "twisted pairs" are double to create a four-wire communications path, which is capable of bearing even greater amounts of signals.

Because telecommunications services are so varied and somewhat confusing, it is worth the time it takes to learn about the basics. To begin, all telecommunications service ordered from the telephone company are delivered to the "curb" via copper wire or fiber optic cable. Therefore, the signals carried over the path are either electrical impulses or light intensity changes (however so slight).

POTS

For a moment lets focus on the electrical impulses and how they "make" the circuit work. Most POTS circuits are a pair of twisted copper wires (twisted pair) from the central office to a subscriber's location (home or office). The central office provides Direct Current (DC) on the line as a means of supervising the line, so the switch can tell if the line is working and to determine when the subscriber is asking for service. The line is also used to transmit a ring voltage to the subscriber's telephone and an audio signal (voice) when an incoming call is received. When the subscriber desires to place a call, they signal the central office of their intent by lifting the telephone handset. Electrically, the telephone will either momentarily ground one side of the wire path (called a ground start line) or loop the DC current back to the central office (called a loop start line) which signals the central office to send dial tone. Dial tone assures the customer that the central office is "alive" and signals the start of the communications phase of placing an out going call. Now, this is not to say the telephone grounds the line one time and loops the line another. The type of telephone equipment you intend to use establishes the actual signaling method and the type of line you receive from the central office. The majority of telephones in the world operate on Loop Start (LS) or Ground Start (GS) lines. Generally speaking, most telephone service is based on this primitive, yet adequate, signaling method.

These same fundamental supervisory and signaling methods are performed on fiber optic communications paths, only with the interruption or modulation of a light beam, instead of electrical current. Fiber optics and newer copper wire signaling methods are referred to as Pretty Amazing New Stuff (PANS)[2]. Pretty amazing, as it, allows for more than just a voice path.

PANS

Newer telephone service is built on the basics of copper wire or fiber cables and provides better methods to supervise the line, and new ways to send/receive signals between the central office switch and the subscriber. An example of this is a Custom Local Area Signaling Service (CLASS). CLASS is normally provided over a LS line, which permits a subscriber to send additional signals to the switch during an in-progress call (known as channel interoffice signaling). An example of this is Call Waiting, where the subscriber can suspend one call and receive another call on the same line. They do this by "flashing" the hook switch which signals the central office to place the first call on hold and release the audio from the second call. The subscriber can toggle between calls by repeated hook switch flashes. CLASS doesn't work with GS circuits because the hook switch flash would ground the line and sever the call. One will admit that CLASS is pretty amazing, but how is it at all possible? Most of the amazing new stuff is attributed to the computerization of the CO switch where the switch performs the supervision, switching, and completion of calls.

PANS include other new services such as Asynchronous Transfer Mode (ATM), Time Division Multiplexing (TDM) services known as T-Spans, Frame Relay, and Integrated Services Digital Network (ISDN). Each of these communicating methods enhance the phone company's ability to send greater amounts of service to their subscribers without having to install more copper wires. This is possible by digitizing the subscriber's communications and bundling them together with other digitized signals and placing them on the same wire path. (Naturally, the process has to be reversed before it reaches the single line telephone customer.) From this ability to manipulate bulk call processing between its central offices, the phone company is able to offer bulk services to its larger customers who operate their own Private Branch Exchange (PBX) telephone switches. Hence, many PBXs operate using bulk services such as T-Spans and ISDN trunks, as well as GS and LS lines. PBXs also operate on lines such as Direct Inward Dial (DID) and Wink Start (WS) trunks, which permit the public switch to communicate with the private switch in channel interoffice signaling protocols.

CENTREX

CENTREX is a business offering whereby subscribers may receive custom subscriber services like that of LS CLASS (listed above) to a group of telephones within a small office. CENTREX utilizes the power of the central office switch to provide features like Caller ID, Call forwarding, Speed Dialing, Voice Mail, etc., much like the features provided by a PBX. The marketing scheme behind CENTREX is to provide custom PBX features to small subscribers who can't afford to purchase a PBX (or don't have the need for a PBX, yet desire the features).

The one attribute of CENTREX that is inconsistent with TSG recommendations is Hands-free intercom. Hands-free intercom permits one telephone in an office group to call another telephone within the office, and complete the call without the called party having to physically touch the telephone. With a PBX this task is accomplished within the system itself and usually doesn't leave the office environment. However, with CENTREX the hands-free intercom requires a CO line, which means the audio travels across the PSTN where it can be intercepted and eavesdropped upon.

On a more positive note though, custom-calling features (e.g., Speed Dialing, Redial) provided by CENTREX can be considerably more secure than the identical PBX feature. The reason behind this claim is the CENTREX provider is the "telephone company" who typically employ skilled technicians to administer their switches and provide security monitoring. This skilled staff is dedicated to ensuring the switch functions without interruption or phreaker[3] intrusions. Unfortunately, PBX owners can rarely afford to employ a skilled staff to provide the same security monitoring.

In summary, the size of the copper [or fiber] path into the office hasn't actually increased in size since the early days of POTS. Rather, the copper path has been more efficiently "optimized" to appear much large than before (when compared to the shear volume of information it once handled to what it can now bear). Likewise, the growth of the interface path has raised the necessity for the local CO switch to supervise the interface, such that it is in almost constant communications with the subscribers premise equipment. Many telephone subscribers are unaware of the signaling and supervision that occur between their phone and the phone company. A lack of understanding the interface does not necessarily mean that we should be concerned with things we know little of, but rather those things which are known to cause harm (vulnerabilities).

Billing Services

The telephone companies offer a few other custom interfaces which are better categorized as billing services. These interfaces are called Wide Area Telecommunications Services (WATS) and Federal Telephone Services (FTS), which are built upon the basic interfaces mentioned above (i.e., LS, ISDN, and T-Spans). The significant difference is WATS and FTS are reduced toll services, which mean the subscriber has been offered a cost reduction on long distance calls because they use so much of it.

Another billing service exists which is called "toll free" calling. Toll free calling involves numbers with the prefix of 1-800 or 1-888 in which the number dialed is re-routed to an existing service interface, and the called party pays for the call, not the calling party. Toll free interfaces can be established within the Local Access and Transport Area (LATA[4]), within several LATAs or nationwide.

Lastly, a billing service exists which involves the prefix of 1-900, 976 and "look-a-likes"[5], which charge exorbitant fees for calls placed to them. These billing services have been the focus of the Federal Communications Commission (FCC) as unsuspecting callers are complaining about being billed outrageous toll fees for nebulous services. The roots of 1-900 can be traced back to *directory information services*[6] where a telephone subscriber derives payment by billing a per-minute service charge for assisting customers over the telephone. One such legitimate service in the Washington metro area was "Dial-a-Nerd" where callers were charged $5.00 per minute for computer advice/assistance they received during the call.

The TSG Standards and What They do for you

The TSG standards prescribe protective measures to prevent the loss of audio, through the employment of administrative [unsecured] telephones, from within sensitive discussion areas. The recommendations contained within the TSG Standards are primarily directed at telephone instruments and PBXs through "trusted" design or prudent system configuration. Either method is equally suitable, yet the Standards lack an explanation or appreciation for the type of service being provided on the CO interface.

Properly configured, the interface and telephone equipment work in unison to provide reliable communications. However, if improperly configured the system may provide marginal service and may be a source of security concerns. A third possibility exists; proper configuration yet poor performance. This could be caused by a number of interface problems, which can be categorized in two broad topics: 1) administrative, and 2) technical.

Administrative

Some administrative concerns arise from too few telephone lines and too many telephone lines. This could result in callers being blocked from service until a line is available or a situation where you're over billed for lines that may never be used. To few could impact job performance while too many could deplete your telecommunications budget. PBX based systems require administrative system measurements to ensure that the CO interfaces (trunks) are alive and performing as desired. It has been our experience that most PBX trunk outages are found by system administrators after customers complained about an overall lack of performance. This means that the PBX owner should establish an active system measurement protocol, and one should not wait for the CO to identify interface (trunk) problems.

Another administrative concern arises from an industry practice where long distance providers compete for subscribers. The practice is called "slamming" which involves illegally switching subscribers from one long distance company to another without their written consent. This practice rarely disrupts service, but usually results in higher long distance toll charges for long distance calls. The FCC cracked down on this practice, but the best defense is to establish a direct liaison between your system administrator and your telephone company sales representative. The liaison should also clearly define that any and all changes to the telephone service profile should be at the individual direction of your system administrator, and they [CO] are not to effect any changes without your system administrator's permission.

Technical

Some of the technical concerns over interfaces include; clip-on-fraud, secondary dial tone seizures, remote maintenance, and others. Clip-on-fraud involves the theft of dial tone by an outside intruder who literally clips onto the interface and uses the line as if they were the legitimate user. This results in service charges incurred by other users. Unfortunately, clip-on-fraud is nearly impossible to prevent and extremely difficult to detect. Monitoring your system for usage and reviewing your telephone bill are the best countermeasures to clip-on-fraud. If you suspect clip-on-fraud, report it to your telephone service provider and local law enforcement officials.

Secondary dial tone seizure is a technical problem stemming from a PBX system maintenance parameter known as disconnect timing. Disconnect timing determines the time required before the local PBX will recognize that the serving switch or distant PBX has disconnected from a call. Secondary dial tone seizures occur when a caller lingers on the line after placing a call. They wait for the called party to hang-up, then immediately touch tone the distant PBX during the disconnect timing interval such that the PBX is spoofed into providing dial tone. Once dial tone is received, the caller places an out going call at the expense of the PBX owner. The best countermeasure for secondary dial tone seizures are twofold; 1) reduces the disconnect timer interval to the shortest possible interval[7], and/or 2) stay on the line and wait for the caller to disconnect from the call.

Remote maintenance is not necessarily an interface attribute, rather it is a privilege extended to a caller or group of callers who are authorized to enter into and perform maintenance on a customer's premise equipment. Since remote maintenance is a privilege, it needs to be closely protected and monitored. It has been the TSG's experience that most often remote access is established and left in the hands of the external user. Unfortunately, an external user does not always exercise the necessary diligence to maintain sound security. Often times remote access is mimicked by other users (phreakers and hackers) who seek to break into customer premise equipment to conduct fraud. The TSG prescribes direct measures for the protection of remote maintenance ports such that the port cannot be used to reconfigure the system.

Remote access to premise telecommunications systems is another daunting problem seen by many TSG member agencies. Remote access is a means to extend premise telecommunications services to employees who are on travel or otherwise out of the office, yet require system access. Like remote maintenance, remote access is a privilege, which should be closely guarded and monitored to ensure the interface, is not being utilized as a gateway for fraud.

CENTREX *Hands-free intercom* is inconsistent with TSG recommendations. CENTREX subscribers should consider deleting this feature if they employ it within sensitive discussion areas.

NOTE: As denoted in the above two examples, CO interfaces can be utilized for many services beyond just telephone communications. The interface can be used for any number of privileged services, which provide access to fax, data, LANS, and other media services. The interface is not at risk of exploitation itself necessarily; rather it becomes the vehicle for information exploitation. All users should be aware of the number of facility services, which are assigned outside access and closely monitor their use. If exploitation is suspected immediately change passwords/privilege permissions and notify the appropriate security personnel.

Summary

This TSG Information Series is dedicated to the process of informing telecommunications managers of the types of central office interfaces available from the local telephone company. We feel it is important to understand the type of services available, the relative capacity of each link, and the supervision conducted over the link by the central office switch. We hope each reader can identify the difference between the available interfaces such that they can understand what communications are possible, what signaling is used, and what supervision is used across the interface. From that understanding, the TSG hopes to involve each reader in the process of reviewing and evaluating the type of CO interfaces they employ, and to provide them with corrective security measures when vulnerabilities are identified.

Appendix A

The following list contains commonly used terms which describe the type of services offered by most local telephone companies[8]. These services are used in both homes and offices, with single line telephones, multi-line telephones, key telephone systems, electronic key systems, and private branch exchanges (PBXs). Occasionally, the type of service ordered from the telephone company needs to be tailored to the subscriber's customer premise equipment (CPE).

ATM - Asynchronous Transfer Mode (ATM) is a high bandwidth, low-delay, packet-like switching and multiplexing technique used on SONET. (See also SONET below.) Usable capacity is segmented into fixed-size cells, consisting of header and informational fields, allocated to services on demand.

CENTREX - CENTREX is a business telephone service offered by a telephone company from a local central office. Centrex is basically single line telephone service delivered to an individual's desk (the same as you get in your home) with features, i.e., "bells and whistles," added. Those "bells and whistles" include intercom, call forwarding, call transfer, toll restrict, least call routing and call hold (on single line phones).

CLASS - Customer Local Area Signaling Services (CLASS) is based on the availability of channel interoffice signaling. Class consists of number translation services, such as call-forwarding and caller identification, available within a local exchange of a Local Access and Transport Area (LATA). CLASS is a service mark of Bellcore. Some of the phone services which Bellcore promotes for CLASS are Automatic Callback, Automatic Recall, Calling Number Delivery, Customer Oriented Trace, Distinctive Ringing/Call Waiting, Selective Call Forwarding and Selective Call Rejection, etc. CLASS is also referred to as LS CLASS, which stands for Loop Start Custom Local Area Signaling Services (CLASS on a LS line). CLASS is also a descriptor for a Facsimile group in accordance with the EIA/TIA (Electronics Industry Association and the Telecommunications Industry Association). CLASS is also a descriptor for the type of end office associated with the Public Switched Telephone Network. There is generally five categories of Central offices Class1= regional toll telephone switching office, Class 2= a second level toll switch, Class 3= third level toll switch, Class 4 = the fourth level toll office where customer assistance in placing/receiving calls is provided through live operators, Class 5= an end office whereby most residential and office telephone service is administered.

CPE - Customer Premise Equipment (CPE) is telephone equipment that is owned, not leased, by the telephone service subscriber. CPE can consist of single or multiple line telephones, key telephone units, electronic key systems, or PBXs.

Dial Tone - The sound you hear when you pick-up a telephone. Dial tone is a signal (350 + 440 hz) from your local telephone company that it is alive and ready to receive the number you dial. The PBX, not the central office, generates dial tone from a PBX.

DID - Direct Inward Dialing (DID) is a method to dial directly behind a PBX to an internal subscriber. DID is a type of trunk service provided over a standard central office subscriber line, normally Wink-start in nature. DID service usually only passes the last four digits to the PBX, as the prefix is assumed.

DISA - Direct Inward System Access (DISA) is a PBX service, which permits callers to access PBX calling features. Normally, DISA is provided with a barrier code restriction, which prompts callers to identify themselves with an access code to prevent toll fraud.

Dry Line - (aka Dry circuit) a circuit over which voice signals are transmitted and which carries no direct current.

FDDI - Fiber Distributed Data Interface (FDDI) is a 100 Mbps fiber optic LAN. Frame Relay - Frame Relay switching is a form of packet switching, but uses smaller packets and requires less error checking than traditional forms of packet switching. Frame Relay does not support voice.

FTS - Federal Telecommunications System (FTS) is a private telephone network, shared by all federal government agencies. (Same as WATS, but sold predominately to the USG.)

Ground Start - A central office service where one side of the wire trunk (typically requires that it be the "ring" side) is momentarily grounded to initiate service from the CO switch. The resistance is nominally 550 ohms.

Glare - Glare occurs when different users seize both ends of a telephone line or trunk at the same time for different purposes.

Glare Resolution - Ability of a system to ensure that, if both ends seize a trunk simultaneously, one caller is given priority and the other is switched to another circuit.

ISDN - Integrated Services Digital Network (ISDN) is a totally new concept of what telephone service is becoming. ISDN is merging voice and data services into one uniform standard to be transported and interpreted worldwide. ISDN adopts "out-of-band-signaling" rather than "in-band" channel signaling. ISDN is available in several US (North American) service offerings:

- BRI - Basic Rate Interface is 144 kbs of band width to the curb over two wires which is commonly known as 2B + D. 2B+D is a designator for 2 Bearer channels and 1 Delta channel. The Bearer channels are used to bear data (digitized data or voice) while the Delta channel is used to provision the Bearer channels.

- PRI - Primary Rate Interface is 1.544 mbs of bandwidth delivered to the curb over four wires, which is commonly known as 23B+D. 23B+D is a designator for 23 Bearer channels and 1 Delta channel. The Bearer channels are user to bear data (digitized data or voice), while the Delta channel is used to provision the Bearer channels. When all Bearer channels have been provisioned, the Delta channels itself can be utilized as a communications bearer.

- 0B+D - Zero B plus D is a modified ISDN offering[9] where the customer receives no Bearer channels per se, but rather they receive a 16 kbs Delta channel to send and receive data (digitized data or voice).

Loop Start - A central office telephone service which requires the tip and ring wires be bridged through a resistor to initiate service from the CO switch.

PANS - Pretty Amazing New Stuff (PANS) is a coined phrase to describe the ISDN service intended to replace POTS.

POTS - Plain Old Telephone Service (POTS) is the basic service provided to most telephone subscribers. It's nothing fancy, with no added features. POTS are usually associated with rotary dial or touch tone service without the bells or whistles. POTS are normally LS or GS circuits.

Ringdown - The tie line connecting phones in which picking up one phone automatically rings the other phone. In a ringdown circuit, a ring current (AC) is sent down the line that current may light a lamp, set off a bell, or buzz a buzzer; the idea is to alert the person at the other end to the incoming call. Ringdowns are dedicated point-to-point circuits and cannot be used for placing dialed number calls.

Secondary Dial Tone - Secondary dial tone is dial tone received by a PBX user when they've dialed a trunk access code to place a public switched telephone network (PSTN) call. PBX users first receive PBX derived dial tone when going off-hook to place an outbound call. However, to obtain secondary dial tone, the PBX user must dial a trunk access call (typically numbers 7, 8, or 9). Secondary dial tone is dial tone that can be derived from a PBX when the called party disconnects from the call, yet before the PBX disconnects from the line. Secondary dial tone, if captured, can permit out-dialing from the PBX whereby the PBX owner pays for the call[10].

SONET - Synchronous Optical NETwork (SONET) is a family of fiber-optic transmission rates from 51.84 mbps to 13.22 gbps, created to provide the flexibility needed to transport many digital signals with different capacities, and to provide a standard for manufactures to design from. SONET is an optical interface standard that allows inter-working of transmission products from multiple vendors (i.e. mid span meets). It defines a physical interface, optical line rates known as Optical Carriers (OC). OC-1 = 52 mbps, OC-3 = 155 mbps, OC-9 = 466 mbps, etc.

SS7 - Signaling System 7 (SS7) is a system supervision protocol designed by Bell Labs and offered to the CCITT in 1987. SS7 signals have three basic functions; Supervising - monitoring the status of the line or circuit to see if it is busy, idle or requesting service, Alerting - indicates the arrival of an incoming call, and Addressing, transmitting, routing and destination signals over the network.

T-SPAN – Refer to the T-1 description below.

T-1 - Also known as a T1 or T-Span. This service is a digital transmission link with a capacity of 1.544 Mbps. The T-1 uses two pairs (four wires) of normal twisted wires to communicate 24 channels of voice communications. However, voice is digitized in a PCM coding scheme for transmission over a T-1 path. T-1 and ISDN PRI have the same total channel capacity, but are provisioned and networked in a totally different manner. T-1 uses in-band signaling, where PRI uses out-of-band signaling.

(NOTE: T1, T-1, T=Span, DS1, and the like, all describe a digital telecommunications link of 24 channels each 64 kbps. E-1 and others describe the European equivalent, but is 2.048 kbs divided into 30 channels.)

Trunk - A communications line between two switching systems. The term switching systems typically includes equipment in a central office (the telephone company) and PBXs. A Tie trunk connects PBXs. Central office trunks connect a PBX to the switching system at the central office.

Tie Trunk - See Trunk above.

WATS - Wide Area Telecommunications Service (WATS) is basically a discounted toll service provided by long distance and local phone companies. AT&T started WATS but forgot to trademark the name so it's now used as a generic term for reduced toll service.

Wet Line - (aka Wet circuit) A circuit carrying direct current. Current usually derived from the central office battery.

Wink Start - A signal sent between two telecommunications devices as part of a handshaking protocol. On a digital connection such as a T-1 circuit, a wink is signaled by a brief change in the A and B signaling bits. On an analog line, a wink is signaled by a change in polarity (electrical + and -) on the line.

NOTE: The telephone service provided by the host central office (CO) is usually in the form of Loop Start or Ground start lines. They work in fundamentally different ways, yet achieve the same results...signaling the CO switch that you have a demand for service. Most PBXs work better on Ground start lines, while most single line instruments and key systems function better on loop start service. Ensure that you order the proper service for the premise equipment you desire to use.

---

1. Alexander Graham Bell invented the telephone and received a patent on it in 1876.
2. POTS vs. PANS is a telephone company satire about their service to the public.
3. Phreaker is a slang term for a **ph**one b**reaker** (aka hacker of telephone systems).
4. LATA is normally used as IntraLATA to describe a service within the same switching area or InterLATA used to describe several service areas.
5. Look-a-likes are a myriad of telephone numbers that sprang up which function just like 976 numbers. Because of FCC rulings, most of these fee-for-services have either closed down or moved offshore.
6. *Directory information services* are not to be confused with information directory services (411) of the telephone company (a.k.a. operator/directory assistance).
7. An interval that is too short may result in premature disconnect.
8. Most definitions were derived from Newton's Telecom Dictionary (Fifth Edition) Harry Newton.
9. 0B+D is a service offering of *Bell Atlantic* and may not be available in other service areas.
10. Secondary dial tone derived from a disconnected call routed through a PBX is a toll fraud concern.
