CHAPTER 10

Telecommunications Security

SECURITY IN PRACTICE 10.1

"Lucky" caller # 102

Kevin Poulsen was a gifted child who took to the dark side of hacking and phreaking[1] by the time he was a teenager. Given his talent, instead of being prosecuted for his initial crimes, he was employed as a consultant to test the security of the Pentagon computers. By 1988, Kevin was sought by authorities for hacking into databases detailing the federal investigation of Ferdinand Marcos and for hacking FBI computers to reveal details of wiretaps on foreign consulates, suspected mobsters, and the American Civil Liberties Union. He decided to run.

While on the run, Kevin didn't let up on his hacking activities. He burrowed deep into the giant switching networks of Pacific Bell, which allowed him access to the telecom infrastructure within Los Angeles. KIIS-FM, a local Los Angeles radio station, used to run a "Win a Porsche by Friday" contest, wherein a $50,000 Porsche was given to the 102nd caller who called the radio station after a given sequence of songs was played. On June 1, 1990, as soon as the sequence of songs was played, a slew of hopeful contestants called in a bid to be the 102nd caller. But Kevin and his friends had a different plan. They hacked into the telecom system of the radio station and seized control of the station's telephone lines. This allowed them to block out all calls but their own. He then dialed the 102nd call to "win" his Porsche 944! Besides this, he also managed to hack into various telecom systems to "win" two new Porsches, $20,000, and two vacations to Hawaii.

In 1991, an episode of *Unsolved Mysteries*, a reality crime-solving show, featured Kevin Poulsen and his exploits. Immediately after the episode aired, Kevin disabled the program's 800 number, causing all studio lines to go dead and thereby preventing callers from calling in tips. However, that wasn't enough to keep Poulsen free — shortly thereafter, employees in a supermarket recognized him from the show and tackled him in the aisle.

After the authorities nabbed him, he was charged with telecom and wire fraud and money laundering, although the more serious charges were dropped. He was sentenced retroactively to five years with a stipulation that upon his release he was not to touch a computer for three years.

He now is a legitimate computer security consultant and an editorial director and columnist for SecurityFocus.com, a well-known organization devoted to security issues.

[1] Phreaker is a hacker who goes after telecommunication systems.

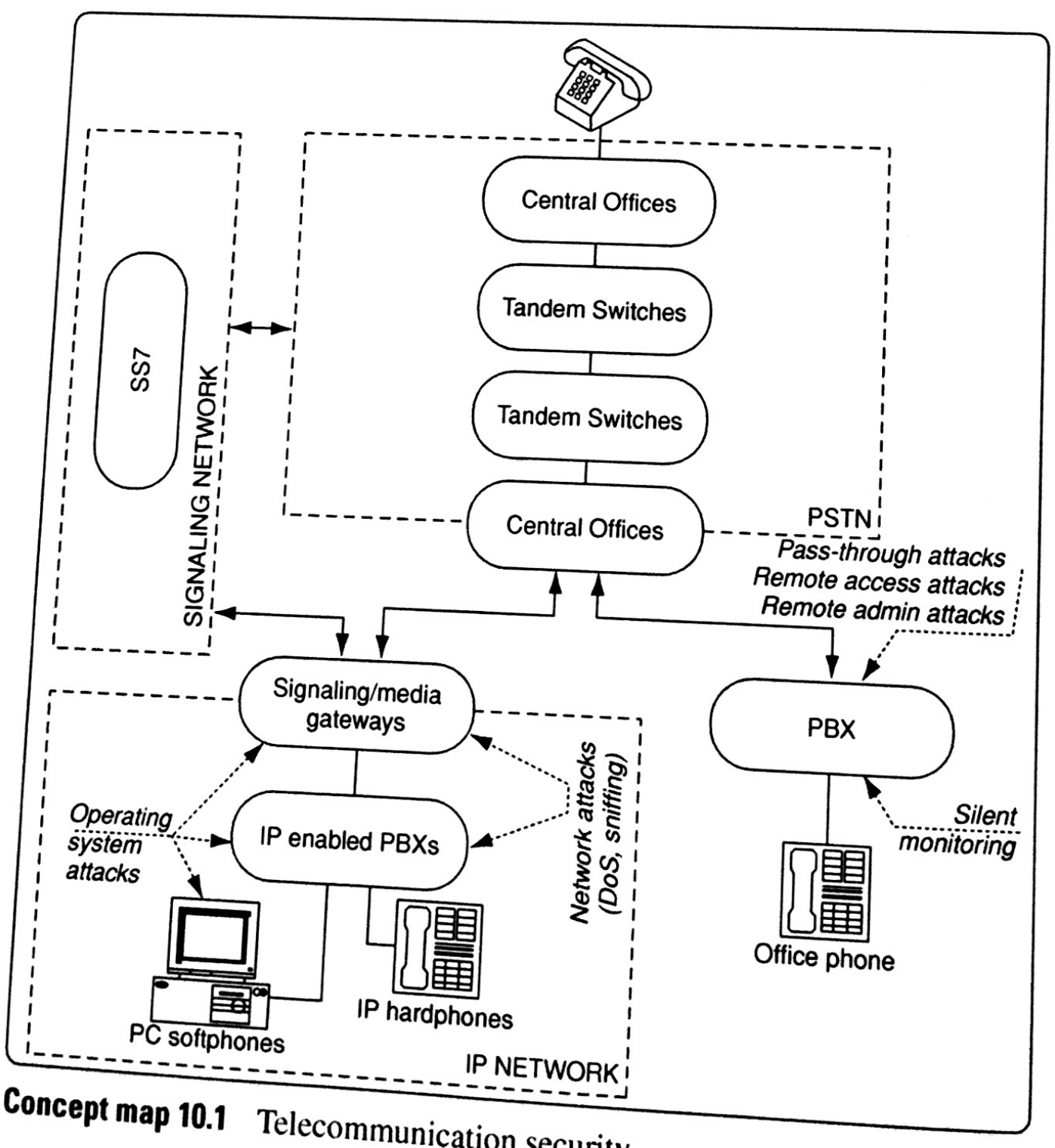
LEARNING OBJECTIVES

After reading this chapter, you should be able to

1. Understand the basic concepts and terminology for telecommunication systems, including PSTNs, PBXs, and VoIP.

2. Develop an understanding of the various risks and controls associated with key telecommunication components and services.
3. Understand the assurance considerations for assessing the security posture of a company's telecommunication systems and be able to assist in policy development for maintaining a secure system.
4. Apply security practices and principles to the telecommunication environment.

Concept map 10.1 shows the various elements of a telecommunication network, including the up-and-emerging Internet-based telecommunication. The traditional method of sending phone calls from one end to another includes the use of Public Switched Telephone Network (PSTN), which is a network encompassing various switches that connect your phone to the destination phone. A newer method of sending calls from one location to another is via voice-over-Internet protocol (VoIP) technology, which uses the IP network, which encompasses various routers that connect computers across the world. This chapter focuses on attacks on and risks associated with this environment and the controls necessary to defend against such attacks and to mitigate the risks.



Concept map 10.1 Telecommunication security

INTRODUCTION

In the previous chapters we reviewed the security of computer operating systems and of the databases and applications that reside on them. With this chapter we shift focus to security of the infrastructure that powers the communication among its users. Data has to transfer from one device to another in the same way people communicate to exchange information. We will study the security of communication infrastructures in two chapters. The first deals with voice communication and the second (Chapter 11) deals with data communications.

Before the Internet came into vogue and Web-based computing took center stage, voice communication infrastructures had long been targeted by hackers and phreakers (see Kevin Poulsen's exploits in Security in Practice 10.1). Most of these early attacks were directed toward AT&T and the Baby Bells[2] and typically aimed at obtaining free long-distance calling privileges. One famous exploit involved a plastic whistle from a Captain Crunch cereal box, which produced a perfect 2600 hertz tone. This whistle, when blown into pay phones, fooled the phone system into allowing free long-distance calls! With the growth of the Internet, attacks on computer (data) networks seem to be getting more attention in the press, but attacks on traditional (voice) networks have not diminished.

Although traditionally voice and data communication channels have been separate, with the advent of technologies like Voice-over-IP, BlueTooth, wireless networking, and Internet Telephony, the two are fast merging. Essentially, your phone is turning into a PC, and your PC is turning into a phone. This is what is referred to as convergence in industry parlance. Although several new, exciting, and cool features and functionalities are being offered as part of this convergence, this has increased exposure to attacks. Given the convergence, there is now a strong and renewed interest, both from intruders and security professionals, in the technology and the security of these infrastructures.

This chapter provides an overview of traditional telecommunications infrastructure and introduces the readers to the merger between it and data networks. The chapter follows the same model as previous chapters in that it covers risks to telecommunications environment and provides controls to mitigate them.

TELECOMMUNICATIONS PRIMER

The telephone was invented in March 1875 by Alexander Graham Bell. Bell had been researching for a way to let people through a wire using electricity. He had his device rigged up in his laboratory with the other end in an adjacent room, where his assistant, Thomas Watson, was waiting. One day he accidentally spilled acid on his clothes and called for his assistant, "Watson, come here, I want you." Watson came running exclaiming that he had heard Bell through the device. And thus the telephone was born.

Ever wonder how calls travel from your home phone to your friend's phone across continents? Conceptually, telephone networks are similar to computer networks. That is, in your company's computer network, your computer sends data to a company router, which talks to an Internet-hosted router, which talks to more Internet routers, until it reaches the

[2] "Baby Bells"

destination computer. Similarly, in a telephone network, your phone sends your voice to a company phone switch,[3] which sends the call to an external phone switch (AT&T, Sprint, etc.), which may communicate with more switches, until it reaches the destination phone. This telephone network is called the **public switched telephone network** (PSTN).

Public Switched Telephone Network (PSTN)

The PSTN is the world's collection of interconnected voice-oriented telephone networks and equipment, both commercial and government owned. Conceptually speaking, PSTN is the Internet of the telecommunications world. Rather, one could call the Internet the PSTN of the computer-networking world because PSTN preceded the Internet by several decades. In fact, many Internet messages are sent over the PSTN network infrastructure. What exactly makes up the PSTN? We will describe the key components of a PSTN here and follow it up with their interactions with each other in the subsequent section.

- **End nodes:** We are all very familiar with the end nodes such as home phones, office phones, cell phones, modems, fax machines, and pagers. These are the devices that either initiate a call or receive a call.
- **Switches:** In the early part of the 20th century, human operators acted as intermediaries to connect callers to receivers. The operator would receive the call, ask the caller who he wanted to talk to, and patch the caller's phone line to receiver's phone line. Over the years, electronic switches automatically connected caller to the receiver, thereby eliminating the need for human intervention.
- **Private branch exchanges:** A **private branch exchange (PBX)** is a company-owned private phone switch that allows for significant cost savings. It connects employees of a company with each other. So, when an employee in the company calls a fellow employee in the same location, the PBX can route calls internally without using any of the external telephone company's billable resources.
- **Central offices:** A **central office (CO)** is a telecommunications office centralized in a specific locality to handle the telephone service for a given region. It is the location where the local telephone company houses its telephone equipment and backbone. Telephone lines connect each house to a CO; this connection is called the **local loop**. The CO houses phone switches that decide if a call has to be routed within the same locality (local calls) or if it needs to be passed onto other (tandem) switches for routing (long-distance calls).
- **Tandem offices:** These are locations that host heavy-duty intermediary phone switches that receive calls from CO switches and pass them on to either other tandem switches or to destination CO switches. **Tandem switches** typically never receive calls directly from end customers, and most of the traffic they handle is long-distance calls.
- **Transmission:** The most common type of transmission media for phone calls is a simple pair of copper wires running from people's homes to the local phone switch.

[3] A phone switch is not to be confused with networking switches. Although the nomenclature is the same, the functionality and the design of a phone switch is completely different from that of a network switch.

These pass the caller's and receiver's voice in an **analog**[4] format and send them to a phone switch. Within offices, the transmission media typically carry **digital** signals for intracompany calls. A variety of transmission media, including fiber optical cables and satellite transmissions connect phone switches. Almost all transmission between phone switches is digital to ensure better transmission quality.

- **Signaling systems:** In addition to the above mentioned components, the PSTN includes a **signaling** system, which is used for call control. It provides functions like connecting and disconnecting callers, determining best route for calls, and providing features such as call forwarding, caller ID, and three-way calling. The most common signaling standard used is called Common Channel Signaling System (also called SS7 or C7).

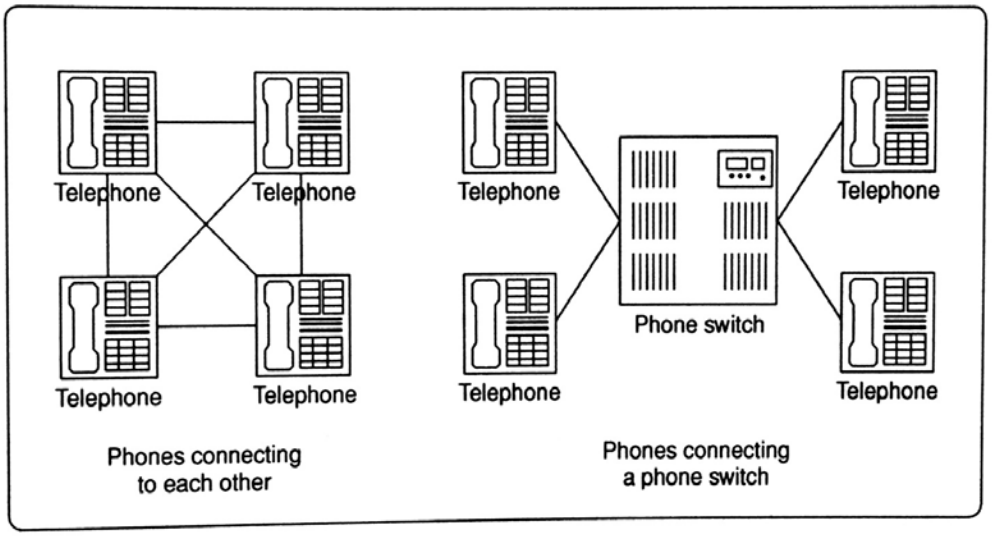


Figure 10.1 Need for phone switches

A Closer Look at PSTN

Now that we have described the key components of the PSTN, let us review the PSTN in more detail. If there were only two phones in the world, you would need only one wire connecting the two. If you have only four phones in the world, you need six wires connecting each phone to each other, as shown in Figure 10.1. If you had 100 phones, you would need 4,950 wires, and if you had 10,000 phones, you would need 49,995,000 wires. Obviously a telephone can't have a direct connection to every other telephone.

Phone switches solve this problem by acting as an intermediary broker for all phone conversations. As shown in Figure 10.1, only one connection per phone is required under the phone switch model. A phone connects to the phone switch and asks for an open circuit, a connection pathway, and is connected to the destination phone. The capacity of the phone switch or the number of circuits available for the callers is calculated by using statistical

[4] An analog signal uses continuously variable electrical impulses representing the voice over the media, whereas a digital signal converts the voice into discrete electrical impulses, 1s and 0s, for transmitting information.

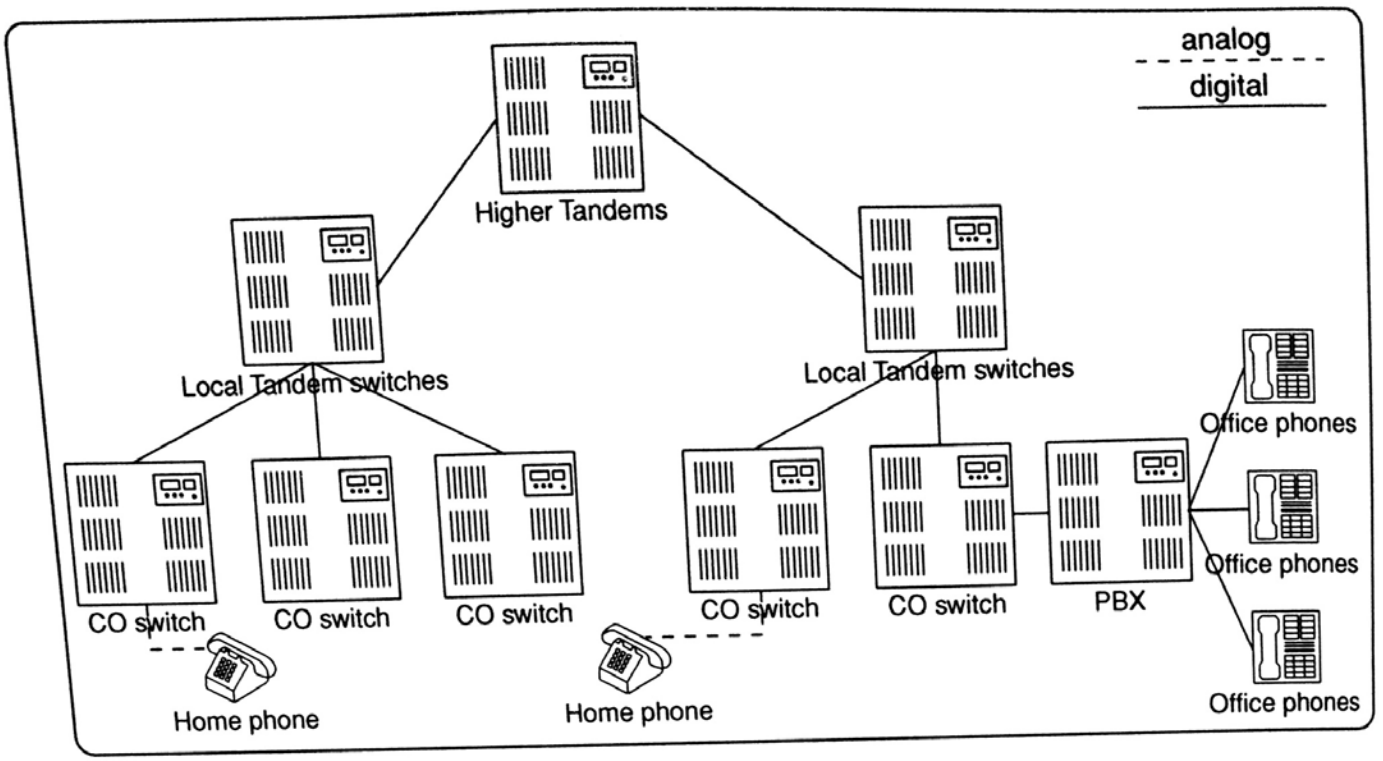


Figure 10.2 Hierarchy of phone switches

Erlang formulas,[5] which account for factors like number of simultaneous phone calls and average duration of communication over the phone.

As mentioned earlier, central office switches connect directly with the end users' phones. Because there are thousands of CO phone switches in the world, they can't connect to every other CO phone switch. So instead, they connect to bigger **tandem switches**. The CO switches calls between telephones, and a tandem switch exchanges calls between phone switches. Soon there is a hierarchy of phone switches, as depicted in Figure 10.2. The COs and tandems are typically owned by governments or private telecommunication companies. For individual companies, it may make business sense to own its own switch (called **private branch exchanges**) so that they don't have to pay COs for the intracompany calls between its employees.

When you call your friend across the world from your home telephone, the call goes to the CO switch, and then to local tandem switches, which send the call to higher tandem switches, which carry it internationally. When the call reaches the local tandem switch in the destination country, it is delivered to the local CO for delivery to your friend's home phone.

Now that you know the path a call takes, let us review the techniques used to transmit voice from your telephone to your international friend's phone. Most home phones are connected via a single pair or via two pairs of copper wires to a central office. Again, this physical cabling between your home and the CO is called the **local loop**. The cabling between various switches, called **trunks**, can be made of copper wires, coaxial cables, microwave links, or fiber media.

[5] These formulas are named after Agner Krarup Erlang, a Danish mathematician in early 19th century. These formulas are amazingly useful and accurate even today.

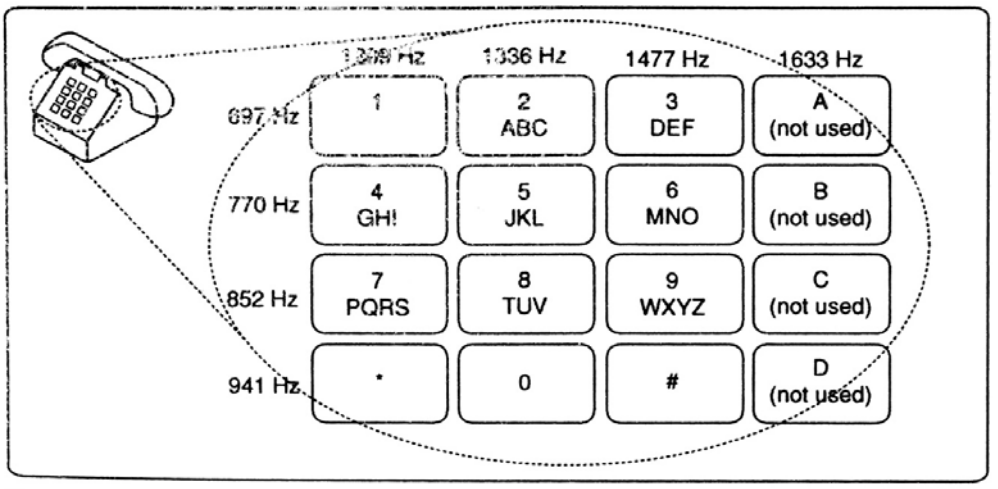


Figure 10.3 Dual-Tone Multiple Frequency (DTMF)

The goal of the transmission medium is to allow electrical impulses, which represent voice, to pass back and forth. These signals are passed from your phone to the CO (user-to-network) and from the CO to other switches (network-to-network).

User-to-network communication transmission from your home phone to the CO is typically done in an **analog format**, wherein continuously variable electrical impulses are sent over the media. Analog transmissions use a signaling method called **dual-tone multiple frequency** (DTMF). Under DTMF, each key on your phone keypad is represented by two frequency tones, which are sent to the CO to indicate the key you pressed. For example, as shown in Figure 10.3, pressing the "4" key on a keypad would send two tones: one of frequency 770 Hz and the other of 1209 Hz. The CO reads these frequencies and understands that a "4" was pressed. Once the CO receives the digits, indicating a call request, it sends a signal down the PSTN network, asking for a connection path to be established. This process of establishing a connection path, or opening a circuit for communication across the PSTN, is called **switching**.

Network-to-network communication occurs between switches. Because analog signals can't travel very far without distortions (**noise**) being introduced in them, they are converted into digital signals at the CO, and these digital signals are sent to other switches in the PSTN. The digital format of transmission eliminates the pitfalls of analog signaling by converting the analog signals into 1s and 0s and sending these 1s and 0s as electrical signals over the media.

The conversion of analog signals into digital (modulation) is done at the CO via methods such as **pulse code modulation** (PCM). Under PCM, an analog voice signal is read 8,000 times a second, and each reading is stored in a 8-bit format (a bit is either 1 or a 0). Thus a digital snapshot of one second's worth of the analog voice conversation is stored in 64,000 bits. Hence the PCM transmission speed for a single voice conversation is 64,000 bits per second, or 64 kbps. That is, each voice conversation requires a digital transmission capacity of 64 kbps.[6]

[6] With the more advanced adaptive differential pulse code modulation (ADPCM), voice can be sent at speeds as low as 16 kbps without significantly affecting quality.

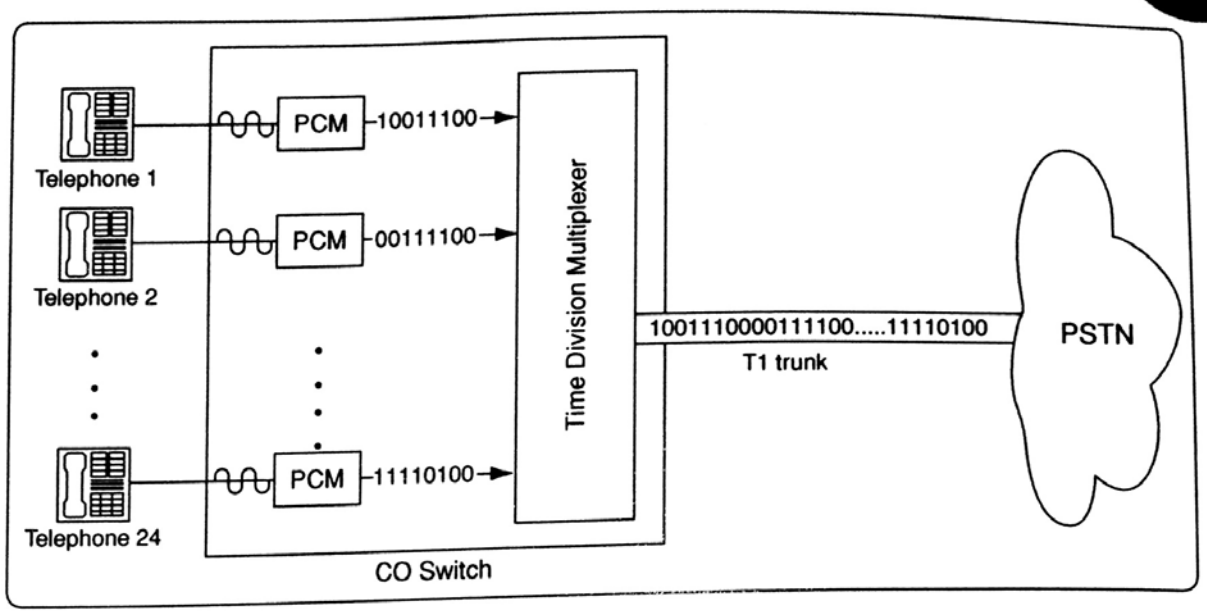


Figure 10.4 Modulation and multiplexing

After conversion of analog voice into digital signals takes place, these signals are combined in a special way so that different conversations can be sent over the same network without them mixing with each other. This process of combining several signals into one specially time-delimited signal is called **time division multiplexing (TDM)**. Figure 10.4 shows how different signals are converted (modulated) and combined (multiplexed) for transmission over the PSTN network.

A bundle of 24 such voice conversations is called a T1 carrier, which has the capacity to transmit 1.544 Mbps (24 x 64 kbps). Switches can have higher bandwidth trunks ranging from T1 to T3 carriers (45 Mbps) or even optical OC-48 networks (2.488 Gbps).

After voice signals are converted and combined, a connection[7] path, or a circuit, is set up for their transmission over the PSTN. The PSTN is called a **circuit switched network** in that, once a connection circuit is established between the sender and receiver, no one else can use the same circuit until the original conversation is completed. The bandwidth provided to you over the circuit is yours and yours only, even when you pause or stop talking during the conversation.

So, how exactly is a circuit set up? To be able to open and close circuits, messages (signals) are passed back and forth, such as "I want to talk," "Open a circuit," "Are you busy?," "Can you take a call?," "I am done talking," and "Close the circuit." This signaling is accomplished via an out-of-band network called **common channel signal** (CCS) network. This network talks to every switch on the PSTN and passes it various signals for call setup and teardowns. It is called an out-of-band network because the circuits that are available and used for voice communication are *not* used for signaling. A completely separate network is used for signaling.[8] The current system used for implementing a CCS network is **Signaling**

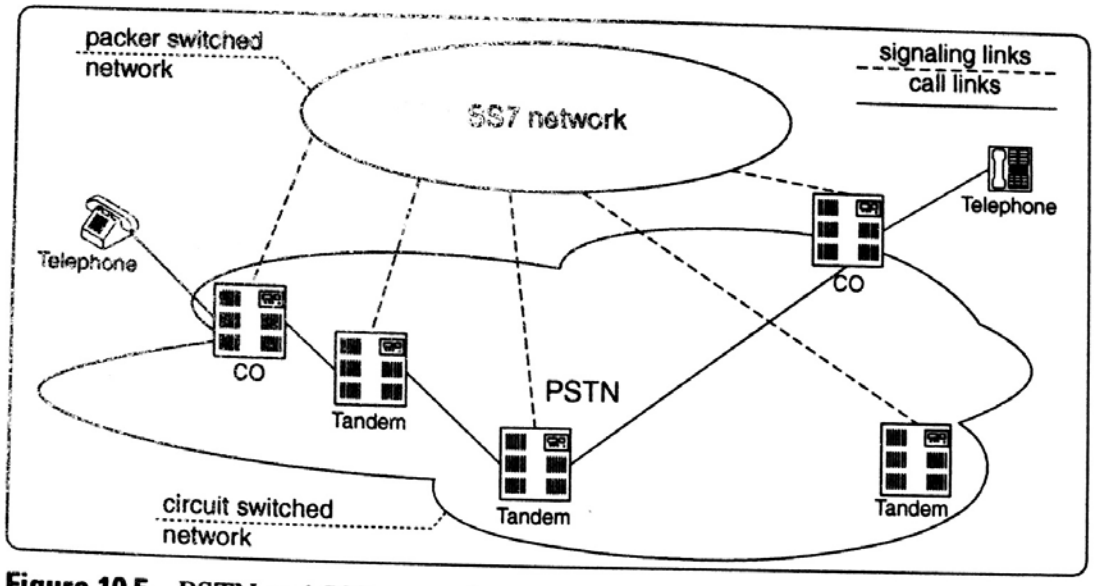


Figure 10.5 PSTN and SS7 networks

System 7 (SS7). Figure 10.5 illustrates the concept of an out-of-band signaling system. Note that the SS7 network is not a circuit switched network, even though it supports the circuit switched PSTN. Rather, it is a **packet switched network**. We will cover packet switching in detail in the next section.

Voice Over IP Networks

Until recently, you would pick up your phone attached to the PSTN, and talk with someone. Then you would go to your computer attached to the Internet and instant message someone, send e-mails, and surf the Web. The two networks, the PSTN and the Internet were used for different purposes: one to send voice, the other to send data. With the growth of **Voice over IP (VoIP)** technologies, however, the two networks are merging. Put simply, VoIP allows users to send *voice* packets over the Internet—the same way the data packets from your e-mail are sent over the Internet. With VoIP, your computer becomes your phone because it allows you to make phone calls via your PC. Or you can use VoIP-enabled phones which look and feel just like your regular PSTN phones, except that they have an Ethernet connection to a local area network.

How exactly does VoIP work? It works the same way a computer communicates over the network.[9] The technology used in a computer to send an e-mail across the Internet is the technology behind VoIP networks. This technology is called **packet switching** and is the basis of the Internet. Under a packet switching network, voice is split into smaller data packets before it is sent on the network. Each packet is then labeled and transmitted individually on the network. These packets travel individually and likely take different routes to their destination. Once all the packets arrive at the destination, they are recompiled into the original voice. The details of a packet switching network, such as IP addresses, subnets, routers, and TCP/IP protocol stack, are covered in detail in Chapter 11 and hence will not be presented here.

[9] J. Davidson, J. Peters, and B. Gracely, *Voice Over IP Fundamentals*, Indianapolis, IN: Cisco Press, 2000.

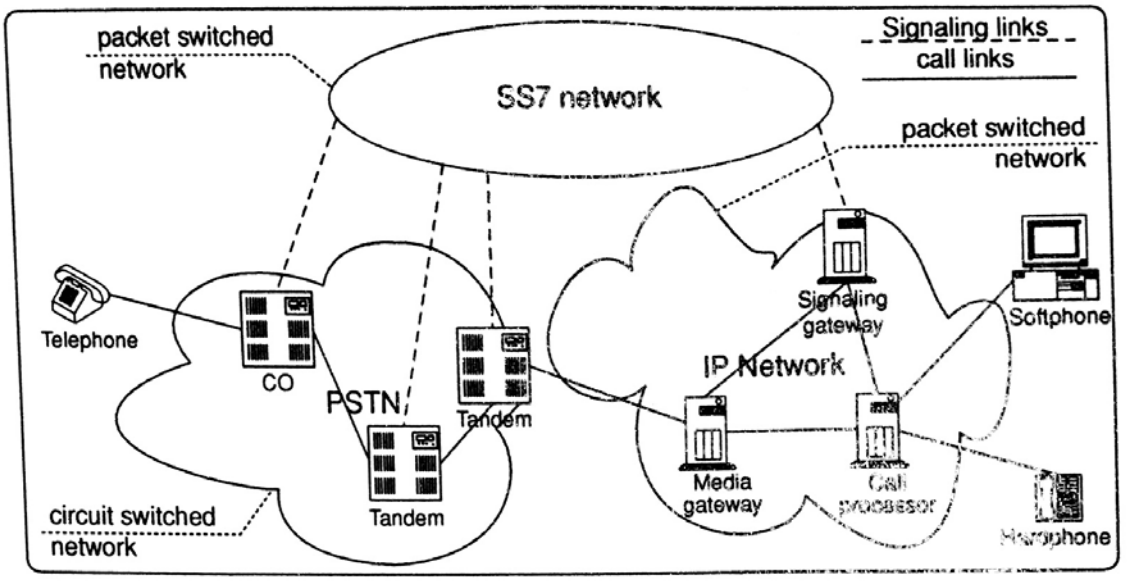


Figure 10.6 VoIP and PSTN networks

For VoIP to work, the following components need to be in place as shown in Figure 10.6.

- **IP network**: Traditional phones use the PSTN to send calls from one end to another. VoIP phones require an IP network to send digitized voice data, or packets, from one end to another. The IP network needs to be fast enough to ensure that there are no jitters and latency in passing voice packets; otherwise the call quality will suffer. If the IP network is to carry voice, it has to be able to prioritize voice packets over any other packets.
- **Protocols**: These are the rules followed for transmission over VoIP networks. Some of the key VoIP protocols include (1) real-time protocol (RTP) that provides for reliable transfer of voice over the packet switch network and (2) H.323 and *session initiation protocol* (SIP), which provide for signaling over data networks for call setups and call control.
- **Call processors**: Call processors have several names (call manager, call agents, call controller) but the most apt name for it is **softswitch**. Call processors essentially act as a software-based phone switch, or the equivalent of a PSTN switch. They set up and monitor calls, translate phone numbers into IP addresses, authorize users, coordinate call signaling, and may control the bandwidth utilization on each link. The amount of functionality provided by a call processor depends on the particular VoIP vendor.
- **Media gateways**: Almost no one has a pure IP network; PSTN is present everywhere. Hence there is a need to broker transmission between the data network and the voice network. Media gateways perform this function as intermediaries between the IP network and the PSTN. They convert packets from IP network to PCM encoded voice on the PSTN side, and vice versa.
- **Signaling gateways:** These mediate the signaling functions between the IP network and PSTN. For example, they provide correlation between the H.323 signaling on the packet network side and the SS7 signaling on the PSTN side.
- **End nodes**: These can be personal computers with software running on them that mimic phones (**softphones**) or IP hard phones. IP hard phones look and feel like

regular phones, except they have a connection to the local area network instead of a connection to the PSTN phone switch.

The Promise of VoIP Networks

VoIP offers many advantages over PSTN networks. Because voice and data travel over the same network, businesses now don't have to manage and maintain two separate networks. **Converged networks** allow for significant cost savings, especially because PSTN setups are typically more expensive to manage. Data, video, and voice cannot converge on PSTN as it is today, but a VoIP-enabled network can easily do so. Because most users already have a broadband connection at home that can handle data and video, adding voice is fairly easy, compared to adding data and video to analog phones.

VoIP also offers enhanced features and applications. Although phones have provided a few additional features over the years such as caller ID, *69, and call forwarding, these can't compare with the explosive growth of features on the data side. PSTN doesn't allow for features like obtaining stock quotes on the phone, playing back voice mail on PC, having e-mails read to you on your phone, filtering phone calls based on caller and time of day, or ringing three different phones in different locations simultaneously. A VoIP network can easily provide these features.

With PSTN networks, the cost of sending a voice depends on time and distance. Calls during evenings and nights are cheaper than during daytime. In addition, international calls cost more than long-distance calls, and long-distance calls are more expensive than local calls. However, the same is not true for you sending e-mails. The cost of sending an e-mail to your classmate is the same as the cost of sending e-mail to your pen pal across the world. Because VoIP uses the same IP technology, distance and time become irrelevant under VoIP networks. Most of the costs incurred by the network can be expected to be fixed (capacity) costs.

With PSTN, calls were delivered by the PBX to a static location: your home. You couldn't visit your grandparents in a different state and have calls follow you. VoIP offers location independence, because calls can be delivered wherever the user is located. Because VoIP routing isn't tied to the copper wires terminating into your home, you can essentially move around anywhere and receive your calls.

In addition, maintaining PSTN phones in a company is expensive. Every time an employee changes locations, offices, or job assignments, someone has to physically connect, modify, and/or disconnect phone stations. With VoIP, all this can be done remotely.

Finally, VoIP offers increased efficiency. In a circuit switched network, silence consumes the same bandwidth as someone speaking. Under packet switching network, only the bandwidth that is required is used. If there are no packets to send (silence), then no bandwidth is used.

Management Concerns

Telecommunication systems are at the heart of all communications within a company and between a company and its customers and partners. Without telecommunication infrastructure, a company would not be able to conduct day-to-day business, and its survival will be at risk. Communication failures lead to loss of market share, financial losses, legal

liabilities, and regulatory sanctions. Hence, the availability of telecommunications is a key management concern.

Businesses provide customer service using telecommunication infrastructure; they establish call centers with automatic call distribution (ACD) to receive customer calls and intelligently route them to appropriate customer service representatives or departments. Failures in communication systems have detrimental effects on customer satisfaction—an obvious concern for companies. In addition, these failures impact day-to-day employees' communications within a company.

Communication systems are often a vital strategic asset for companies that allow them a competitive advantage to survive and grow. For example, transportation companies have the majority of their workforce in the field (yards, tracks, etc.) with minimal or no access to computers. Hence, phones and radios are the only way to manage that workforce. Some companies, like the Home Shopping Network or QVC, rely almost exclusively on phone systems to collect orders and generate revenue. A loss of a communication system would significantly affect operational efficiency and revenue of such companies.

The security and integrity of phone communication and voice mails is also a key concern. Companies often discuss strategic plans, financial information, and legal strategies over phones. An unscrupulous competitor with access to this information can cause disaster for a company. On the other hand, unauthorized monitoring of employee communications can cause privacy-related legal liabilities for companies. Consequently, management expects that these systems are fairly well secured and tamper proof against unauthorized users.

▶ COMMON RISKS AND CONTROLS

The previous sections provided an overview of telecommunication infrastructure and its components. Now let us review the associated risks and controls. Note that with the emergence of VoIP, the distinction between telecommunication security and computer security is increasingly blurred. In the next few years, PSTN security issues will take a back seat to VoIP risk exposures.

Direct Inward System Access

Phone switches (PBXs) allow a remote-access feature where employees on the road can call a toll-free number and make long-distance calls that are billed to the company that owns the switch.[10] This feature, **direct inward system access (DISA)**, also known as **remote access**, essentially permits callers from the public network to access a customer premises PBX system to use its features and services. This way, remote employees don't have to carry calling cards or cash to make business-related phone calls when they are on the road.

[10] R. Kuhn, *PBX Vulnerability Analysis*, [illegible] pubs/800-24/

Risks

The obvious risk for DISA ports is toll fraud. Intruders often sift through phone books and company literature and engage in war-dialing to identify DISA ports and then attempt to exploit them to make long-distance calls. Even if the DISA ports have authorization/barrier codes installed, they can be cracked. Once an intruder knows the right codes, the combinations are sold to the public. The company with the switch is then left paying toll charges for the calls.

Controls

- Evaluate the necessity for remote access—if it is not required, disable DISA ports. If it is required, consider issuing off-site long-distance calling cards.
- If DISA has to be enabled, make sure it is protected with strong authentication and/or barrier codes.
- Use an unpublished telephone number for this feature. Intruders often scan telephone directories for local numbers and 800 numbers used for remote access. Keeping the remote access number out of the phone book helps prevent it from getting into the wrong hands.
- Limit the area codes and countries that can be called via the DISA ports to only the ones required for business reasons.
- If possible, offer no dial tone on DISA ports. This will often prevent the automated war-dialers used by intruders from identifying the DISA ports.

Maintenance Ports

Phone switches (PBXs) also provide access to its internals via **maintenance ports** wherein support personnel can dial in via a phone to perform administrative tasks. This feature is also called the **remote administration** feature of the PBX for obvious reasons. Unlike remote access ports, remote administration ports typically don't allow placement of phone calls; rather, they allow for the administration of the PBX. However, with remote administrative capabilities, an intruder can create new phone extensions or mailboxes, change company announcements, or remove calling restrictions. Hence, compromise of a remote administration (maintenance port) can have far greater security ramifications than remote access (DISA) ports.

Risks

Intruders engage in war-dialing to identify maintenance ports and then attempt to crack user IDs and passwords to get access to the phone switch. If they get access to the PBX, they pretty much control the PBX and can commit toll fraud, silently monitor conversations, reroute calls, and cause denial of services.

Controls

- Ensure all logins for maintenance and administration ports have strong quality, nondefault passwords.
- Enable intruder lockouts wherein the account is locked out after a fixed number of invalid login attempts.

- Log successful and unsuccessful login attempts and, importantly, review the logs periodically.
- Consider deploying "lock-and-key" devices where the dialing modem has to perform an encrypted challenge-response handshake before the receiving modem will allow a connection to the PBX.

Silent Monitoring

A **silent monitoring** feature is often available in phone switches that allows for a user, given special access to this feature, the ability to monitor calls of other personnel. This feature is often employed in a call-center type of environment because supervisors listen in on customer calls to customer service representatives to ensure quality of responses. Although phone switches often can be configured to provide an audible notification when calls are being monitored, companies often don't do this so that they can better gauge customer–employee interaction. The American Telemarketing Association considers undetected monitoring as the most effective method of protecting the business and consumer public from misrepresentation, harassment, and generally poor-quality communications.

Risks

The legal ramifications of silent monitoring have to be carefully considered by companies. In general, federal laws do allow for unannounced monitoring of *business-related* calls, and state laws require a beep tone or a recorded message informing callers that their call may be recorded and/or monitored. However, the laws vary from state to state and have different viewpoints on calls from within state versus calls from outside the state. A company can expose itself to legal and privacy-related liabilities if the laws aren't carefully considered. In addition, if silent monitoring isn't properly configured, unauthorized personnel listening to conversations could compromise confidentiality of voice conversations.

Controls

Silent monitoring should not be enabled without a legal review. Even though companies can monitor business-related calls without any notification, it makes good business sense to notify employees of company policy on monitoring and obtain a consent form. Also, companies should ensure that the callers hear a "your-call-may-be-monitored-and-recorded" message when they call in. In addition, a periodic review of the silent monitoring configuration should be performed by trained audit professionals to ensure that it is configured per business requirements and that unauthorized silent monitoring is not enabled.

Telecom Scams

Historically, the telecom industry has been beset with various telecom scams, many of which are still prevalent.[11] The scams cost individual users and companies huge sums of money because of toll fraud. Some of these scams are discussed next.

[11] Avaya Corporation, http://support.avaya.com/

Risks

Intruders often engage in **shoulder-surfing**, a technique in which they employ a video camera in public places like airports and train stations. Supposedly, they are taking pictures of their families. In reality, they are actually recording people using their calling cards. An intruder can essentially record the finger movements of people on the phone keypad to capture calling card/DISA numbers and later sell them for a price.

Most people are familiar with 1-900 and 1-976 numbers used to access a variety of services, such as sports scores, betting services, psychic hotlines, and weather forecasts. It is not common knowledge, however, that Local Exchange Carriers ran out of 976 numbers and issued other prefixes that work the same as 1-900 or 1-976 numbers. The fees charged for calls to these prefixes are the responsibility of the caller and can range as high as $250 per call or per minute. A common scam is the **pager/beeper scam**, where unsuspecting callers get paged with a 976 or 976 look-alike number and are lured into dialing those numbers to return the pages, thereby getting stuck with huge toll fees.

Many variations of **pager/beeper** scams exist where voice mails, e-mails, or faxes are sent, typically with an urgent family emergency or win big money type of message, all in an attempt to get the receiver of the message to make calls to toll numbers. Some companies offer fax-back services, where if you provide your fax number, they fax you back a catalog of their services or products. These companies can become a victim of a similar fraud, where the unscrupulous owner of the 976-type toll numbers requests hundreds of catalogs at their toll number, leaving the company stuck with a huge bill.

Intruders would often employ **social engineering** (discussed in Chapter 13) in a con game also known as **operator deceit** to take advantage of the gullibility of company employees or operators. For example, an intruder makes a call to an internal employee and then claims to have gotten the wrong number and asks to be transferred to the operator. When the employee transfers the call, the operator sees the call as a call from an internal number. The intruder then asks for an outside line. Because the operator trusts the internal number, he connects the caller (intruder) to an outside line, leaving the company to bear the charges for the call through the outside line.

Unfortunately, fraud can occur from unscrupulous internal employees, too. For example, companies often provide 1-800 numbers with "if-you-know-your-party's-extension-please-dial-it-now" type of options. Internal employees can misuse this feature by **call forwarding** their extension to their home number—and then advertising the 800 numbers to their families and friends as a way to reach them at home (at the cost of the company, who pays for 800-number costs for personal calls).

Controls

Employee education aids in preventing scams from succeeding. Companies should periodically caution their users against social engineering and other aforementioned scams. In addition to employee education, technical controls can limit the amount of toll fraud. These include restricting your telephone network from dialing toll numbers and limiting call forwarding to only those with business need.

Finally, audit controls, in terms of ensuring logs of phone calls are maintained and periodically reviewing them for suspicious calling patterns, can identify toll fraud within a company network. This should include a review of (1) calls made to nonbusiness locations,

(2) calls originating with the same calling card numbers from different physical locations, and (3) calls made from the most frequent calling card users.

Voice Mail and Conferencing Systems

Most businesses have voice mail and conferencing systems as part of their telecom infrastructure. These systems are a great way for businesses to exchange messages and conduct conferences with their business partners, customers, and employees. If these systems are not properly managed and secured, companies can be hit with several thousand dollars worth of damages or disclosure of sensitive information to their competitors.

For example, in 2003, several individuals and small businesses with voice mail systems were victimized by the "Yes–Yes" attack and subsequently held accountable by AT&T for bills worth thousands of dollars. Under this scam, phreakers broke into voice mail systems using default passwords like "1234" and changed the outgoing voice mail recording to say "Yes"—pause—"I will accept the charges," or in some cases say "Yes"—pause—"Yes"—pause—"Yes" over and over again. Phone numbers leading to these mailboxes were then used for third-party billings. The phreakers would place a long-distance phone call and ask the operator or typically automated system to forward the charges. The operator/automated system then called the hacked phone number, which responded "Yes," tricking the phone company into believing that the line's owner agreed to accept the charges for the call. These charges racked up as high as $20,000, and AT&T held voice mail owners accountable.[12]

Another attack occurred in March of 2002. In the midst of shareholder voting for a merger between Hewlett Packard and Compaq, someone leaked a voice mail message from former chairwoman and CEO Carly Fiorina to CFO Robert Wayman regarding her concerns with respect to the votes. This message was later used in a lawsuit against the merger.

Risks

The most obvious risk associated with voice mail is the use of trivial easy-to-guess passwords. Although users typically change passwords on their computers frequently, almost no one changes passwords on their voice mail. (When was the last time you changed the passcode on the your answering machine? Office voice mail? Be honest.) Poorly secured voice mail accounts can lead to fraud, corporate espionage, and privacy concerns.

In addition to recording and retrieving messages, voice mail systems can offer the **zero-out option**. After pressing zero, or some other configured numbers, the caller can connect to the operator. Phreakers break into voice mail systems with poor passwords, use the zero-out option to get to the operator, and ask him to place a toll call. The operator sees this as an internal call, trusts the caller, and places the call.

Similarly, conference calls often have default or reused passcodes for users to join the meetings. This is especially true for recurring conference calls where the same passcode is used week after week. If the competition gets hold of the passcodes to conference calls, they can listen in on sensitive business conversations.

[12] Eventually AT&T agreed to drop the charges after two

▶ SECURITY IN PRACTICE 10.2

Security of converged devices

With VoIP technology, data and voice networks converge. In addition to transmission media converging, one is also seeing the end user devices converging. Personal digital assistants (PDAs) and other handheld devices are increasingly offering telephone services in addition to computing features. On the other hand, smart phones are increasingly providing computing features such as e-mail and related applications in addition to basic telephony. Technologies such as J2ME, WML, SIP, and Bluetooth networking are essentially blurring the lines between the telephone and computing worlds. Your PC is becoming your phone and your phone is becoming your PC.

With this convergence and bundling of features, security of end-user devices is even more critical. Also, vulnerability of these devices increases because the number of avenues for communication and software on the devices becomes more complex and more functional. Over recent years, attacks on these converged devices have slowly but surely risen.

As early as September 2000, a virus known as Phage was released to affect Palm OS–based PDAs. It was capable of spreading from one application to another within the same PDA. Recently, in June 2004, the first mobile phone virus was reported. This virus, known as Cabir, was more or less a proof of concept virus and didn't do anything malicious. It did have worming capabilities, in that it could "hop" from one device to another. Every time a mobile phone turned on, Cabir would launch itself and scan neighboring devices within 30 meters (the range of Bluetooth networking) and try to replicate itself by infecting vulnerable devices in the proximity. Cabir easily spread within 20 countries and could very well have been carrying a malicious payload. In July 2004, a trojan program called Brador was identified that opened back doors in PocketPC devices. In addition to viruses and worms for these converged devices, attacks like Bluejacking (spamming devices with unsolicited messages) and Bluesnarfing (stealing contact information from end-user devices) are growing.

Security experts are divided on the rate of growth of these attacks but agree that malicious attacks are imminent. They recommend that users practice safe synchs, don't beam with unknown PDAs, and don't download promiscuously.

Controls

- Companies should ensure that all voice mails have strong and difficult-to-guess passwords. No voice mail should have passwords like 1234 or 1111. This requires user education and voice mail system configurations that force quality passwords and periodic password changes.
- Zero-out options should be avoided as much as possible. If they are required, the operators should be trained to verify caller identity before placing the call.
- Businesses should work with their COs to block third-party billing to company phone numbers. This will preclude the "Yes–Yes" scam.
- Unused voice mail boxes should be deleted or disabled to prevent unauthorized usage.
- Similarly, all conference calls should have quality passcodes to join the meetings. Periodic meetings should have different passcodes.

VoIP Security

In most environments, VoIP shares the same converged network. Although this adds more functionality for users and reduces costs for businesses, it exposes voice communications to the same network risks[13] that plague data communications (Chapter 11 covers network-related risks in detail). Security in Practice 10.2 discusses attacks on converged

[13] D. R. Kuhn, T. J. Walsh, and S. Fries, *Security Considerations for Voice Over IP Systems*, January 2005. http://

devices. With convergence, you are essentially putting more eggs in the same basket. Some risks to VoIP networks include the following.

Risks

Under PSTN networks, voice was circuit switched. It was sent over communication paths that were *dedicated* to the conversation. As long as the conversation was going on, no one else could use the same path. On the other hand, VoIP networks are packet switched, so the communication paths are *shared* and easily accessible by multiple users. This makes VoIP networks more susceptible to **sniffing** attacks, wherein an unauthorized program on the shared communication path can listen ("sniff") to the VoIP packets and eavesdrop on a conversation. All the tools required for sniffing, including those VoIP enabled, are readily and freely available to the public on the Internet. Therefore, administrators shouldn't assume that expensive specialized equipment is needed to intercept VoIP.

Because calls are sent over a data network shared by others, it is possible for attackers to conduct a man-in-the-middle attack, or **call hijacking**. Under this attack, an attacker would logically sit between the caller and the receiver, intercept the voice data, modify it, and forward it to the receiver without the receiver knowing anything about it. In a variation, the attacker may just intercept the call and impersonate the receiver.

Under a **denial of service (DoS) attack**, malicious users flood communication pathways with unnecessary data, causing a traffic jam–type of situation on the network. This prevents any data from moving on the network. Under the PSTN for voice and Internet for data model, a business can still communicate via voice if the data network is taken down by a DoS attack. For instance, you could still use the phone to call the IT help desk if your computer was down. With the convergence of voice and data on the networks for VoIP, a DoS attack can take out both the phone and the computer.

Under traditional voice networks, PSTN equipment is highly specialized and proprietary and hence difficult for intruders to hack into. Devices like telephones perform only one specialized task: receive and make calls. In addition, the phone switches are fairly unique to the manufacturer, and the specifications of them are not easily available. With VoIP, your PC is the phone and does many other things, besides making phone calls, while being connected to the Internet. It makes phone calls, displays stock tickers, and presents Web pages on the display console. VoIP gateways and servers increasingly use nonproprietary open standards and well-known Internet technologies for communication. Because of these reasons, VoIP networks are more susceptible to attacks than traditional phone networks. Typically, attacks on operating systems of PCs and servers can also affect VoIP communications. For example, you can get a virus via an e-mail that can also hijack your phone connection. You could also be VoIP spammed—if you think telemarketing calls are a pain, imagine wading through dozens of prerecorded voice messages for porn and Viagra in your voice mail![14]

Controls

Encrypt all VoIP traffic so that if someone sniffs your network, all they capture is encrypted data, and they can't easily listen in on conversations. Most VoIP vendors offer some

[14] On the flip side, VoIP "spamming" can have its benefits, too. For example, government agencies are already evaluating using VoIP technology to broadcast emergency notifications.

out-of-the-box encryption; ensure that the encryption routines are strong. Also, remember data that is encrypted has to be decrypted at the receiving end. This can affect network throughput and can contribute to latency and jitters in conversation. As a result, ensure that the network used for VoIP is fast enough to overcome the encryption overhead, or else your voice quality will deteriorate.

Although VoIP environments share the same physical network, it is still possible to logically segregate the two. In essence, using technologies like **virtual local area network (VLAN)**, it is possible to segregate data traffic from voice traffic even though they share the same travel medium. Users and applications on one VLAN can't talk to users and applications on other VLANs. This effectively precludes the exposures of data networks from spreading to voice networks. Segregating traffic also allows prioritization of the different traffic. Voice traffic can be assigned a higher routing priority, **quality of service (QoS)**, to ensure better voice quality. You won't mind if an e-mail arrives a second or two late, but you sure would notice if there were pauses in your voice conversations.

If possible, use VoIP hardware phones instead of VoIP softphones. IP hard phones are VoIP-enabled devices that look and feel like typical phones with handset and dial pads but are connected to the data network instead of PSTN. VoIP softphones are software that adds the phone functionality to the PC so that you can make and receive calls via your computer's microphone and speakers. Softphones are more vulnerable to attacks compared to hardware phones. The PCs that host softphone software reside on the data side of the VLAN and are more vulnerable to all sorts of attacks already prevalent in data networks. In addition, PCs can be vulnerable targets because of operating system weaknesses, applications and services, and configuration. A compromise of the PC can provide entry points into the voice side of the VLAN.

Secure the operating systems of the VoIP equipment, such as VoIP gateways, call servers, routers, switches, workstations, and phones. Chapter 7 covered operating system security in detail, but in general, remember to (1) enforce strong authentication methods, (2) implement restrictive access controls lists, (3) disable all unnecessary services and ports, (4) periodically review configurations, and (5) keep up with security patches and upgrades.

Deploy **firewalls** and **intrusion detection systems (IDS)**, covered in detail in Chapter 11, to protect VoIP equipment from network-based attacks. Firewalls act as a perimeter sentry to prevent unauthorized traffic from entering or exiting. IDS systems review the traffic coming in and out to identify malicious traffic and alert administrators.

ASSURANCE CONSIDERATIONS

Telecommunication security was often limited to review of phone switch configurations to mitigate the risk of toll fraud and unauthorized monitoring. However, with the growth of VoIP, the line between telecommunication security and computer security is increasingly blurred. The following factors need to be considered when reviewing the security of telecommunications infrastructure.

Often companies will spend huge sums of money building a data center to physically host and secure various computer servers and devices. However, they often overlook the **physical security** of telecommunication closets. These closets host equipment for all the phones for the floor connection and various routing devices for sending calls through to the switch. Often these closets are left open or have minimal security.

One of the favorite methods for phreakers to make calls at company expense is to exploit various pass-through features to connect to the PBX and get a dial tone. These include various systems like voice mails, which provide zero-outs, conference lines that connect to operators, and automated attendants that may have hidden options to dial out. Such pass-through to PBX features must be carefully weighed and disabled as far as possible.

The telecommunications industry has been replete with various scams, and often company users get hit. These include shoulder surfing, "Yes–Yes" attacks, operator deceits, and pager exploits. New scams emerge every day. Businesses should invest in user education so that the users are aware of these attacks and understand their responsibilities in protecting company resources.

Phone switches do provide remote access (DISA) and remote administration (maintenance ports) features that allow users to access the switch and its features remotely. These features need to be disabled as far as possible. At a minimum, they need to be secured and periodically audited. In addition, with the growth of VoIP-enabled PBXs and softswitches, remote administration takes on a new dimension as it becomes Web enabled. This opens more doors for intruders to exploit.

Information systems auditors should work with key telecommunications personnel to review the system configurations to ensure telecommunications security. The review should include configurations for silent monitoring, remote administration, voice mail and conferencing system configuration, and various other switch features.

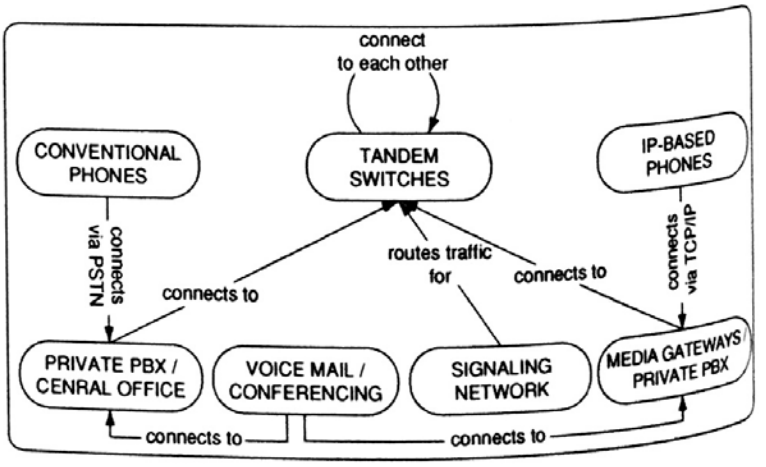
With the growth of VoIP, the telecommunications landscape is fast changing. With VoIP, the phone switches and adjunct systems like voice mail servers are built on standard platforms like Windows or Unix and utilize standard Internet technologies. This necessitates that the review of telecommunications goes beyond just PSTN review and includes a review of security practices for operating systems (services, applications, patches, authentication, authorization) and for network security (encryption, ports, modem access, firewalls, IDS).

▶ SUMMARY

Telecommunication systems are mission critical for businesses to ensure they can communicate with their suppliers, customers, and employees. Failure to protect these systems can affect all facets of a business, including communication, customer satisfaction, revenue generation, operations, and privacy.

Similar to the Internet of the computer world, the public switched telephone network (PSTN) is a global network that connects various telephone systems across the world. As shown in summary Concept map 10.2, the PSTN is composed of various end nodes: the telephones, the local phone switch (central offices), and higher-order switches called tandem switches. Businesses often deploy their own switch, called the private branch exchange (PBX), so that they can route intracompany calls without having to talk to (and pay) the COs. Transmission from home phones to COs is typically in an analog format. However, transmission between PBXs, COs, and tandem switches is almost always in digital format.

The PSTN uses circuit-switching technology, wherein a *dedicated* circuit is established between caller and receiver



Concept map 10.2 Summary concept map

for the duration of the call. The same path is used throughout the conversation. This can be expensive compared to packet switching network because the dedicated circuit is always in use during the conversation, even if the two parties are silent. Voice over IP (VoIP) technology uses a packet switching network to send voice over data networks. A packet switching network breaks down the voice into data packets and sends them over a *shared* path. Upon reaching the destination, these packets are reassembled back into voice. In addition, packets may take different paths to reach the destination. With VoIP technology, businesses enhance functionality, blur the distinction between phones and computers, and obtain convergence of voice and data networks. Both PSTN and VoIP networks have risks associated with them that need to be controlled to ensure security, integrity, and availability.

Companies need to secure the direct inward system access (DISA) ports, which are used to provide long-distance calling to remote users. Failure to secure DISA ports can lead to significant toll charges. In addition, maintenance ports, which are used for remote administration of phone switches, are common targets for intruders. Phone switches also offer silent monitoring capabilities, which if not properly configured and controlled can lead to eavesdropping. Telecommunication environments are rife with various scams that can lead to loss, toll fraud, and disclosure of sensitive information. Some common scams include shoulder-surfing, operator deceit, luring a pager/beeper to call toll numbers, and exploiting fax-back services. Further, individuals and businesses need to secure their voice mail and conferencing systems to avoid toll fraud and prevent disclosure of sensitive messages and conversations.

Voice over IP networks add a great deal of functionality and have significant potential to save on expenses for businesses. However, VoIP networks inherit all the security problems associated with data networks typically not present on PSTN networks. This includes exposures such as sniffing attacks, denial-of-service attacks, call hijacking, and attacks on VoIP equipment. To protect against these attacks, VoIP implementations need to use all the security precautions associated with network security and operating system security.

▶ KEY WORDS

Analog/digital transmissions
Call forwarding
Call hijacking
Central office
Circuit switched network
Converged networks
Denial of service (DoS) attack
Direct inward system access (DISA)
Dual-tone multiple frequency (DTMF)
Erlang formulas
End nodes
Firewalls
Intrusion detection systems (IDS)
Local loop
Maintenance ports
Noise
Network-to-network communication
Operator deceit
Packet switched network
Pager/beeper scam
Physical security
Private branch exchange (PBX)
Public switched telephone networks (PSTN)
Pulse code modulation (PCM)
Quality of service (QoS)
Remote access
Remote administration
Shoulder-surfing
Signaling
Signaling System 7 (SS7)
Silent monitoring
Sniffing
Social engineering
Softphone
Softswitch
Switches
Switching
Tandem switches
Time division multiplexing (TDM)
Trunks
User-to-network communication
Virtual local area networks (VLAN)
Voice over IP (VoIP)
Zero-out option

▶ MULTIPLE-CHOICE QUESTIONS

1. DISA ports are used by companies to:
a. provide remote administration.
b. enable calling cards for employees.
c. provide remote access.
d. All of the above

c. DISA/remote access
d. Each of these is a possible exposure.

3. Which areas of expertise are needed to secure newer telecommunications systems?
a. Understanding of PSTN networks
b. Security of computer operating systems