Chapter 2
Confidentiality, Integrity, and Availability Threats in PBXs

2.1 Introduction

Applied practice and specific incidents have shown that PBXs suffer from a series of problems that negatively influence the confidentiality, integrity, and availability of communications. Truth is that the academic community has not shown great interest in the PBXs' security, possibly because of their traditionally closed and proprietary nature. Luckily, with VoIP, things changed and there is a revived research interest.

Despite the increased involvement of the academic community in the security discussions, many of the traditional problems (especially the ones that are targeting devices, implementations, and services) have not been solved in VoIP, but rather new ones have emerged targeting even the protocols themselves.

Apart from technical issues, the user remains one of the weakest links in the security ecosystem. This is why this contribution mainly aims at raising user awareness. In this introductory chapter, we will briefly describe and group as many as possible of the threats in confidentiality, integrity, and availability that PBXs are facing. This way, it will be the basis for the technical discussions that will follow in the next chapters. It will also help better understand how to apply the security measures presented in the respective chapter later on.

2.2 Confidentiality

Eavesdropping is of course what comes first on mind when talking about telephony confidentiality threats. Voice communications can be intercepted in real time or recorded to be retrieved and analyzed later. Calls can be multiplexed to internal or external listening posts. They can also be rerouted to other destinations (possibly utilizing a man in the middle attack too). Apart from phone voice calls, fax calls and (given the convergence of telephony and Internet) data traffic can be intercepted and extracted.

© Springer International Publishing Switzerland 2016

I.I. Androulidakis, *VoIP and PBX Security and Forensics*, SpringerBriefs
in Electrical and Computer Engineering, DOI 10.1007/978-3-319-29721-7_2



Fig. 2.1 Serving area interface

In general, eavesdropping communications makes organizations dealing with confidential information liable. In addition to this, industries can be confronted with espionage problems. PBX hacking can lead to the interception of strategic or tactical information of the army, police, or ministries as was also proven in warlike situations [1].

Even in digital PBXs where switching is performed in a digital manner, low end phones can still be analog ones, where the audio is carried in an analog way from the PBX board to the telephone set. A simple tap connected in the cable leading to the phone (everywhere in its possible route, from the main distribution frame in the provider's premises, to the serving area interface, to the local distribution frame up to inside the telephone itself) can easily extract the audio or provide access to the line to make free calls. This is very well known as "clip-on" fraud. Figure 2.1 shows a serving area interface and Fig. 2.2 a close-up of a distribution frame. We can notice sensitive information regarding telephone numbers and routing and patching information left in small pieces of paper by the technicians. More importantly, a tool

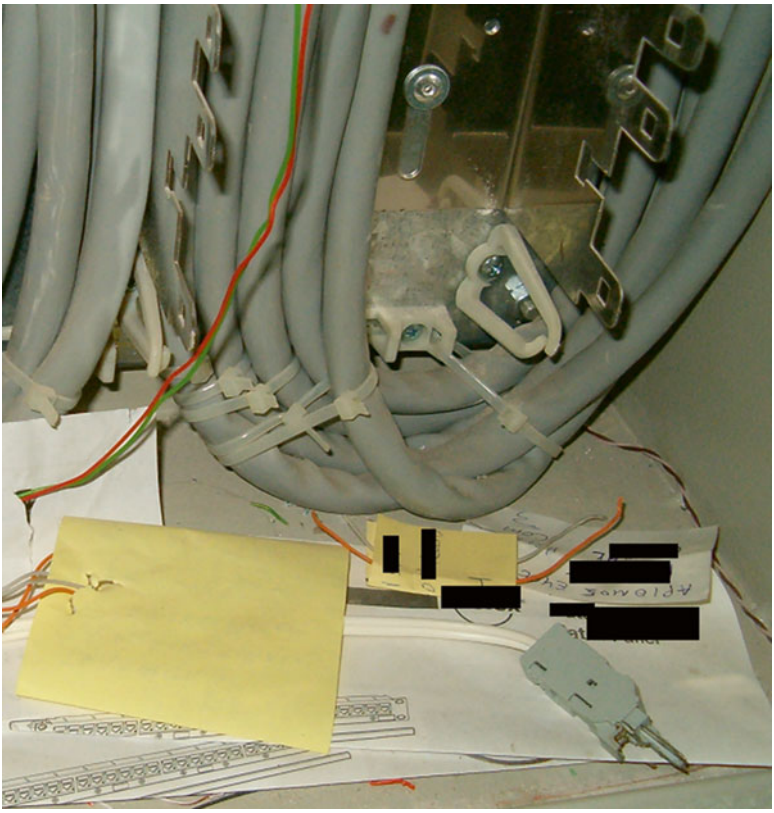


Fig. 2.2 Sensitive information left over in the distribution frame plus the tool to intercept calls

to intercept calls is seen, which when inserted in the respective connections automatically intercepts the audio without disconnecting the line at all.

In end to end digital systems, as well as in VoIP systems audio is traveling as digitized packets. If there is no encryption, these data packets can be translated back to audio. Specifically for PBXs there exist special hardware modules that perform the task for most brands, translating the proprietary digital signals to audible analog audio (Fig. 2.3).

Telephone sets, on the other hand, can be modified to transfer voice while on hook, with either hardware modification or software commands. Indeed, it is completely impossible to force a $10 analog phone to do something without a hardware modification, while a $200 digital phone with all these bell and whistles can (easily) be reprogrammed or commanded from the PBX to switch its microphone on, and relay the audio heard in the surrounding environment to the attacker. It transforms this way to a very efficient remotely controlled bug.

A classical way of interception is the use of special interception devices, the well-known "bugs." The topic of Technical Surveillance Counter Measures for

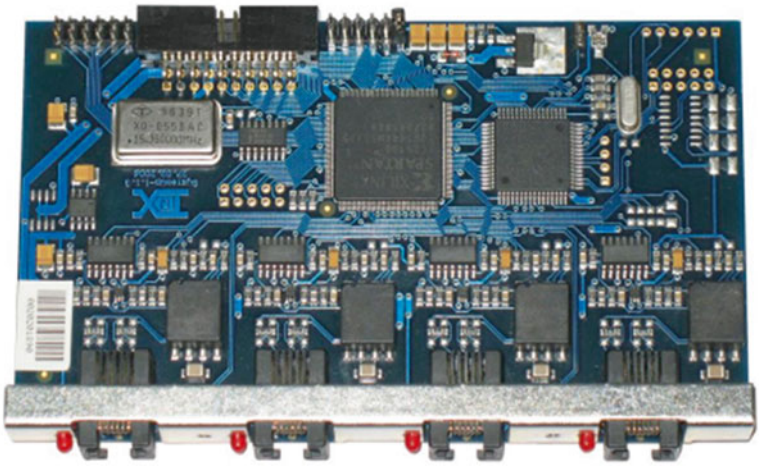


Fig. 2.3 Board translating proprietary digital audio to analog (after http://www.trx.com.pl/)

defense against electronic eavesdropping and bugging is a whole topic by itself, so we will not address it in this book. We will, however, promptly mention some information on interception devices here.

Interception devices may be placed on the telephones we use or on the cabling and the network and provider's equipment. The traditional method of clip-on, where a pair of wires (and possibly a phone) is connected in parallel with the original one, is still the most effective one! The presence of voltage on the wire itself allows the continuous and long-term operation of a transmitter bug without the need for replacing batteries such as Fig. 2.4 depicts. The latter can even be placed inside the telephone device itself. The picture of a movie spy who unscrews the handset's microphone on an old analog telephone device is very typical even though the technology used today is different. Another basic element that is worth mentioning is that of a device installed in a telephone device that can also intercept ambient conversations taking place inside the office and not solely during calls. This device can be "waken-up" and start relaying audio from the microphone of the phone, without the phone ever ringing.

Wiretaps that either record or transmit the voice are more common but it is also possible to conduct a passive interception without any kind of intervention. Signal interception from wires is possible, through induction. In Fig. 2.5 a special inductive coil is shown which intercepts telephone signals without breaking the circuit, just by picking up the electromagnetic fluctuations. The basic principle here is that according to Maxwell's equations, a varying electric field produces a magnetic field and vice versa. Physical audio in electronic devices is transformed to a varying electrical current that produces a magnetic field. So, the induction coil picks the magnetic field, transforms it back to current, and drives an amplifier to allowing overhearing the initial audio.



Fig. 2.4 Wireless transmitter for telephone conversations



Fig. 2.5 Inductive coil for intercepting telephone signals

A more elaborate technique is that of "the man in the middle." In order to intercept communications a hacker can intervene in the middle pretending (from a technical point of view) to be the other party and relaying the information to the intended party. Revealing sensitive information during a phone call is thus never a good idea unless some sort of cryptographic means is used.

Interceptions can take place in an active and/or passive way. In the active method, there is some kind of physical or technical interaction with the target phone (or network) and as such it is easier to be spotted. Active ways of interception include, e.g., connecting extra cables in the main distribution frame (clip-on) or reprogramming the PBX.

Passive interceptions, on the other hand, are very frequent in wireless systems, by just "listening" to the airwaves and decrypting the encrypted radio wave communications that flow in the air. They are focused on cryptanalysis, and can target protocols and algorithms in various parts of the network. In a typical wireless communication, the radio waves are transmitted freely in the air and they cannot be easily confined. Therefore, a potential intruder can intercept and process these signals without even coming close to the target. As a matter of fact, older, analog wireless calls could passively be intercepted using cheap gear since there was no kind of encryption at all. Digital wireless systems changed that. Up to recently, it has been traditionally difficult to intercept air waves for DECT cordless phones that are also used in PBXs. However, some open source projects during the few past years have brought this functionality to the interested user with great success [2].

Leaving aside malicious actions regarding interception of messages, there is also the lawful interception where operators are required to help law enforcement authorities. Each provider–carrier is obligated to offer mechanisms to monitor communications for the needs of authorities, following the necessary warrant. Lawful interception functionality abuse can prove to be one of the most effective spying options. Although it is a very sensitive system that should be adequately protected, successful attacks have been seen [3]. Employees with the proper authorization credentials or malicious hackers that manage to break in the system (with or without internal help) can intercept at will the calls of the targets they chose.

Administrators can also activate monitoring and debugging features that allow real-time interception. There is also software offered by 3rd party companies for the same goal. Most PBXs offer tools to silently listen to other calls, in the context of a supervisor checking the agent's performance and behavior. It is also part of the secretary–manager association, where the secretary can intrude and inform the manager about an urgent call. Both systems can be abused.

Usually, when an intrusion takes place an informatory beep in regular time intervals (e.g., every 15 s) informs the parties that the call is monitored. This is a very important point. Unfortunately, very few people realize that this tone is actually a warning about the presence of another party in the conversation. Even worse, administrators can disable this tone, or set it to a very short duration or to a non-audible tone (very high or very low frequency).

It is not always necessary to eavesdrop on the actual communication-voice call. The interception of call logs could reveal many useful connections. With call correlation and traffic analysis techniques, interesting connections can be revealed (such as the contacts of the user) and industrial espionage information gathered even without knowing the actual content of the calls, but only the identities of the parties. As an example, if the logs reveal a flow of calls between a company and the patent office, a safe assumption is that a new product is on its way to be patented. Respectively, key suppliers can be found and so on.

Among the harvested information threatening the confidentiality would be forwarded numbers in the forward tables as well as mobile phones and personal numbers present in the logs and stored in the memories of the phones and the PBX. Many users are also saving personal codes such as PINs in the memory of the phone, so these could also leak. Finally, imagine a fraudster, having the ability to intercept credit card numbers as the unsuspected client presses the keys in his phone to perform a telephone-banking transaction.

2.3 Integrity

The second major part in the taxonomy of threats deals with integrity attacks. Such attacks on a PBX vary from reprogramming it, installing backdoors for future access, altering data (e.g., erasing incriminating information), and modification of features (enable services that are banned) to economic fraud. Deleting or changing

the respective call and operation logs would cover the entry and the trails of the attackers. At the same time, it is possible to alter the communication flow, connecting lines to different destinations (possibly utilizing a man in the middle attack). Harming the integrity of data in specific files and memory locations can lead to denial of service and PBX shutdown.

As experienced administrators can attest, it is easier to find the cause of a malfunction when it manifests as a complete lack of service than it is to find out what is wrong when the system misbehaves or when the error appears sporadically. Thus, an attacker can create more damage by forcing the PBX to function incorrectly rather than launching a full denial of service attack. Changing settings is sometimes more effective than completely shutting service altogether. For example, randomly forwarding, swapping numbers, or changing caller IDs among users can cause havoc and it simultaneously takes more time to realize what is wrong.

Identification of the caller to the calling party is one of the handiest features of telephony. Of course, the ability to withhold the caller ID from being presented to the called party has been associated with an array of unpleasant acts, such as harassments, pranks, spam calls, calls from unwanted persons, and so on. Furthermore, having access to a PBX, the identity of the sender can be changed in order to make a malicious call appear legitimate or for spam purposes. This call spoofing takes place when a caller masquerades as another one. It is used to avoid paying for the service, to hide the fact that the call is an unsolicited or fraudulent one, and to avoid detection in case of attacking further nodes. Call spoofing is very important in cases of Vishing. This is a practice where fraudsters gain access to private personal and financial information by convincing their victims they are calling from their bank. Counting in the trust people have to telephone service, fraudsters are using the proper caller ID of a bank. Indeed, telephony numbers have traditionally been connected to physical locations and companies, so users tend to trust a telephone number, thinking of it as a valid form of ID.

Staying with the integrity analysis we will also examine two nontechnical effects of integrity attacks in PBXs, psyops and fraud. Psyops is short for psychological operations, which can be defined as “Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals” [4]. Examples of such incidents would be to play propaganda messages to all internal users (they would listen to them as soon as lifting the handset). It could also connect callers and incoming lines to recorded messages. Messages could be played by PAs (public address system–loudspeakers) connected to the PBX. Furthermore, constantly ringing phones or phones ringing in the middle of the night could cause severe discomfort, annoyance, or even fear.

Apart from Psyops, as telephony security is usually lacking compared to IT security, the opportunities for crime are numerous. Unauthorized access of telephone service with the relevant economic losses due to bills is a major concern. Losses due to computer incidents are usually given only as an estimate and it is indeed a very complex procedure yielding wrong results many times. Economic losses due to a telephony incident on the other hand are immediately obvious. As was seen in the

```
<CHFLME:?

Change follow me relation

CHFLME: <FM-TYPE>,<ORIG-DNR>sr[,<DEST-NUMBER>];

If DEST-NUMBER is omitted the follow me relation of ORIG-DNR will be erased.

<CHFLME:0,101,102;
EXECUTED
<CHFLME:0,101;
EXECUTED
<CHFLME:0,201,0[redacted];
EXECUTED
```

Fig. 2.6 Setting up a call forward to an external number in a command line interface

introduction, the costs attributed to telecom fraud, and specifically PBXs are not easily appreciated reaching $72 to $80 billion [5]. Imagine a telephony fraud taking place unnoticed for a substantial period. Apart from the apparent cost of the bill, lost revenues and additional expenses can skyrocket the total loss to astronomical amounts. Money laundering through PBXs is also effective, while consequences after a multimillion fraud in calls starting from a company's PBX would lead to financial and business disaster. Even terrorist organizations are thought to be embracing telecom fraud to generate funds [6, 7].

Fraudsters abuse telecom services (using stolen codes and access and charging third party users), allowing use of the infrastructure by non-authorized persons, making free calls or selling these calls via a call-selling operation, making a profit. Call-selling operations to high cost international destinations can prove to be very profitable when promoted to certain groups of people who have increased communication needs, such as students, refuges, foreigners, military personnel, and imprisoned ones. In case the company owns a free calling, 800 number, then it is even more alluring for the attacker since even the initial call (from a payphone usually) is free. Moreover, a simple forwarding of a seldom-used extension to an overseas number can be easily commanded, as shown in Fig. 2.6.

Fraudsters can actually steal expensive boards of the PBX (e.g., the CPU board) and parts of the infrastructure that can be later sold in the black market. Luckily, in some brands, expensive boards such as the CPU board are protected by means of cryptographic hashes. A side effect of this would be the resulting denial of service as will be discussed later on. In a lighter tone, an attacker can control a whole PBX in order to win in a contest where players are calling in a Radio or TV station. This was achieved by Kevin Poulsen; hacking the KIIS-FM 102 station's PBX he managed to be the 102nd caller as required by the competition, wining this way a Porsche 944 [8].

Compromised PBXs calling premium rate services (that can explicitly be set just for the purposes of receiving calls from these infiltrated PBXs) or high cost destinations such as overseas or satellite networks can lead to extensive bills. Consider 100 compromised PBXs in a country, each calling such services or destinations 1,000 times per day. Assuming a cost of $10 per call yields a total of $1million per day in

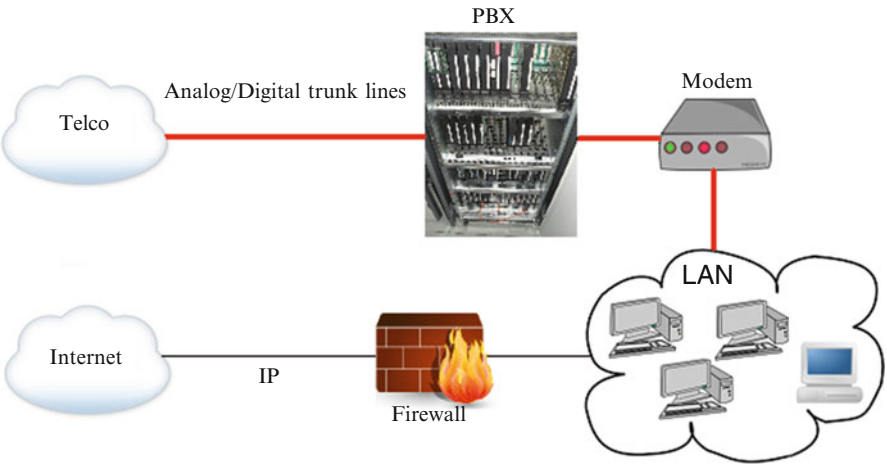


Fig. 2.7 Firewall bypass due to a non-authorized modem

bills! The attacker could even be aiming at calls that are terminated in another country. This way, local operators would owe the foreign ones a substantial amount due to call termination rates leading to significant economic losses for the country. A side effect would be the international circuits blocking as described in the denial of service section.

Although oxymoron, it seems that low end and cheaper PBXs are less vulnerable than the larger PBXs with richer functionality. The configuration of a small PBX is practically impossible to be attacked (in order to intercept or change the integrity of data) from outside since such PBXs do not offer any remote access to the administration at all! As a matter of fact, their programming usually takes place by dialing special codes issuing the respective commands, using a phone already connected in the PBX. Even with the absence of remote administration, however, they are still subject to denial of service attacks, internal fraud, and/or hardware modifications.

Closing the integrity section, it must be noted again that the PBX can be the weak link to target the IT platform that is interconnected with it (either for administrative only or for full service reasons such as the case with VoIP). When a PBX is linked to an organization's IT network, malicious hackers can find an easier point of entry (in case the PBX maintenance port is not adequately secured) into the critical assets, customer databases, and business applications of the target.

There is also another great risk in regard to PBX and IT interconnection: Some users are connecting unauthorized modems in their phone lines in order to bypass enforced Internet access policies. They do that by connecting their PCs to the telephone network via the PBX (instead of using VPNs and corporate secured and tested solutions). As shown in Fig. 2.7, the upper part of the connection bypasses the firewall, providing access to the corporate network via a modem. Employees are even using remote access programs to work from home. An attacker could find these modems using war dialing (as will be explained in the next chapter), enter

their PCs, and jump to the IT network, bypassing firewall security and further penetrating the network as an internal user. There are many cases where a perfectly well-designed computer network is brought down due to errors and omissions in the telephone network. It is rather oxymoron to invest into computer security but to forget to invest into telephone security. This is why total security can only be achieved with combined efforts and supplies between IT and telecom world.

2.4 Availability

Integrity implies there is availability in the first place. There is no point discussing about integrity when a system does not work at all! Given telephony's omnipresence, its availability has been considered a given fact. Truth is, however, that it is relatively easy to block PBX communications. A lack of effective telephone communication can cause annoyance for its users [9]. More importantly, the service of hospitals can be damaged by phones which are not working [10]. It is frightening to imagine not being able to call a hospital in an emergency. Furthermore, national economy could suffer great losses if a targeted attack was to render useless industry's telecommunication lines. In any case, it is apparent that in the modern demanding business environment a company or organization cannot survive without telephone service.

The fact that telephony network outages can have serious consequences became clear by the 9/11 terrorist attacks on the World Trade Center. The telephony network for first responders was lost rapidly, and due to failing backups the problems with the network continued. This led to more difficulty with arranging rescue and recovery [11]. At the same time, the inability to reach beloved ones can cause stress for many people, which opens a possibility for deliberately bringing down networks to perform psyops of the same nature during warlike or in harassment situations.

A new form of denial of service is connected to credit card fraud. Fraudsters are blocking the phone lines of victims as to inhibit the bank from informing them about abnormal behavior concerning their credit card. This is arguably more a problem for household lines rather than PBXs. Both, however, might be using wireless phones (practically DECT sets, since analog wireless phones have long ago ceased to exist). As with every other wireless technology, DECT handsets can be victims of jamming attacks that mask and overcome in power the legitimate signals rendering phones unusable.

Proceeding, an attacker can affect the availability of the system for both management and communication itself, affecting administrators and the internal and external users. He could cut off administrator's access by changing passwords, disabling remote access, and shutting connectivity to IP and serial port communications. Incoming and outgoing lines could be administratively set out of service, effectively isolating the PBX from the outside world. More aggressively, deleting the database which contains the setup of the PBX or files from the operating system could completely halt the switch. Interestingly, at least one manufacturer has specific login accounts with the sole purpose of halting the PBX or deleting and reinstalling the settings database, effectively wiping the existing setup. With the same logic, it is pos-

sible to overwrite the firmware of the boards of the PBX using its firmware update tools. Finally, a simple shutdown command could be ordered. Placed in a UNIX-like cron file, this keeps the PBX shutting down at predetermined time intervals.

Another effective denial of service technique can target the software and hardware protection of PBXs. Modern PBXs employ protection against unauthorized copying and black market selling utilizing some form of hardware key, usually with a field programmable gate array (FPGA) integrated circuit. The FPGA holds a specific hash that is coupled to the hardware present in the PBX. If somebody tampers with this protection mechanism, the PBX will enter a limited functionality mode and eventually will shut down, protecting the vendor's profits and the PBX from illegal interventions and black market operations. Specifically for PBXs exported to third countries, the hardware key can only be shipped from the manufacturing country since local dealers do not have access to it, further extending the time needed to restore its functionality.

It is not always needed to have physical access in a PBX in order to harm its availability. A remote denial of service in the communication abilities can be achieved by another PBX (or an array of PBXs) attacking the target with hundreds of calls per minute. This attack could be used against the better-protected PBX where the attacker could not obtain access. It effectively blocks the incoming and outgoing lines and the legitimate users cannot utilize them anymore since they are constantly busy. As an example, a typical E1 PRI European ISDN line offers 30 voice channels (23 with T1 lines used in USA). Assuming short calls of 10 s, including the setup time, a rate of 180 calls per minute can be achieved against the target. A medium size PBX with three E1 lines can launch 540 calls per minute against a given target. This would easily overwhelm most small PBXs. In a full ISDN environment with call setup times of less than 1 s, the whole duration of the call could be as little as 2 s, yielding a 2,700 calls per minute rate from the same three E1 setup. But, even if the target has enough capacity in lines, it could be well possible that the shear rate of calls causes a bottleneck in another part of the system, e.g., the automated attendant (press 1 for sales, 2 for accounting, etc.) or the Interactive Voice response platform (say sales to get to sales, accounting for accounts, etc.). This blocking of lines scenario closely resembles the denial of service and the distributed denial of service attacks of the computer networks, where instead of packets, calls are now flooding it. In any case, a classical computer denial of service could target the administrative computer platform. Along the same line, a possibly more annoying way of attacking the availability of a given phone is to place consecutive calls to it, effectively making it ring nonstop. The user is then forced to unplug it.

At this point, another interesting effect of the repeated calls attack could be the overloading of international circuits. Indeed, the international circuits' capacity is usually limited. With an array of PBXs calling random destinations abroad, the links could be saturated and the country cut off from the international network. In order for the attack to fully succeed, it should be launched against PBXs that are being served from all possible international connectivity providers–carriers. Since communication circuits are two-way, the attack would have the same effect using compromised PBXs in the target country only, performing outgoing calls, or compromised PBX in other countries performing incoming calls towards the target country.

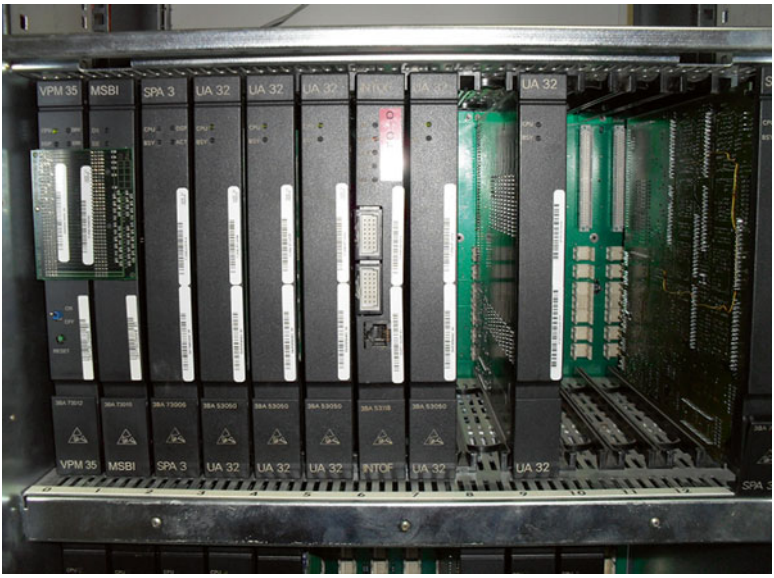


Fig. 2.8 Close-up of boards

Returning to hardware, a non-confirmed and as far as the author knows not researched, yet somehow plausible, attack on PBXs is the following. By intervening in the firmware of the PBX, it could be possible to force the PBX to perform functions that could lead to physical failure of its electronic components. Especially for analog lines that employ relays, an attack could force the relays into a constant rapid on–off loop that would ultimately burn them or it could force the ringing signal to permanently be applied in a phone, possibly burning its ringer circuit. Looped reboots or file access could also wear the hard disc of the PBX. The consequences of such attacks are far less severe compared to damages caused to an industrial system by similar means (such as Stuxnet caused). None the less, these attacks can still be implemented to bring down a PBX.

Another factor that often slips our attention is the probability of theft of (parts of the) PBX. Modern telephone exchanges use expensive and easily removed and carried equipment (e.g., exchange cards—boards, Fig. 2.8), so a couple of minutes would be enough for an incident to take place causing apart from the economic damage also an outage. At the same time, this board can host a memory chip or a hard disc storing valuable information (in an unencrypted way most usually). As a matter of fact, the theft can be only temporary, lasting for a few minutes. It is only that long it takes for a malicious person to install software or tamper with the electronic circuits.

Finally, let us not forget that interruptions in the service are not always caused by attackers. More than often, technical glitches, bugs, or environmental disasters cause extended scale and duration service interruption incidents. This is why protection against environmental elements and disasters is essential.

2.5 Other Threats

Apart from the confidentiality, integrity, and availability issues, PBXs face other threats too that combine all the previous. A common use of a compromised telephone network is to use it as a screen for covering-up criminals' illegal activities such as ring operations, drug selling, money laundering, etc. A covert call usually originates from payphones because they can offer anonymity and they are easy to find and accessible from almost everywhere. Further anonymity is granted while the call is routed through many PBXs to make it extremely difficult to trace. This "looping" is a very effective way to mislead authorities from tracing them. The technique was on the decline with the advent of convenient prepaid mobile phones but is expected to catch up again, since new legislation requires prepaid mobile phones to be register with valid IDs before being used. This anonymity can be exploited to attack other targets, making the compromised PBX an intermediate point and its owner possibly held liable for the attack.

At the same time, the compromised PBXs (and especially voice mail systems) can be a repository of illegal information to be exchanged by the fraudsters. Encrypted messages could be stored by criminals and retrieved by their peers (e.g., for drugs dealing) while multiparty calls can take place, organizing actions.

A side effect (or a deliberate one) is the adverse publicity and the damage to the reputation of a company that has been hit by such an incident. Indeed, customers could be denied telephone service, or a disgruntled ex-employee can forward company's incoming lines to sex lines. Even worse, clients could be connected to an adversary's line. A fitting example here comes from the early days of telephony. Almon Strowger invented an automatic telephone exchange because he was convinced that the wife of a competitor being an operator at a manual telephone exchange was sending calls to her husband instead of him whenever someone asked for the service they both offered.

Speaking of adverse publicity, an ever growing percentage of emails in the Internet are spam. The same can eventually happen with voice calls. Spam could be defined as unsolicited commercial messages from unknown originators. It is well possible that a compromised PBX can take place in such an act, by relaying audio messages to randomly chosen telephone numbers. The user gets a call and at the other end of the line, the prerecorded message starts playing passing political propaganda or trying to convince him to visit a website to hopefully make a transaction buying a good or service.

So far we have examined technical threats. However, it is not always necessary to be technically savvy to abuse a telephone network. A very common technique for accessing it is the use of social engineering; people who pretend to be someone else use their persuasion to extract valuable information for the network itself or information that can be helpful for infiltrating it. There are two good examples here, one is the use of social engineering by a person that impersonates a trusted one (e.g., an employee) via the phone and extracts information from a secretary, a username and a password to login to the network, and the other is a person who gives false information and impersonates a network technician in order to extract information about

the whereabouts of the PBX. Gaining this way the guard's approval to access the PBX he has full access to the network. Further examples of social engineering can be found in [12].

2.6 Specifically for VoIP

As already stated, most threats already discussed affect VoIP the same way they affect classical TDM PBXs. Voice over IP Security Alliance (VoIPSA) [13] has nonetheless provided a specific security threat taxonomy. It includes social threats, eavesdropping, interception, and modification threats, service abuse, intentional interruption of service (including denial of service), and other interruptions of service.

Social threats exploit vulnerabilities of VoIP in regard to caller ID and the lack of a "physical" bond of a given number to an actual address. Eavesdropping counts on unencrypted traffic that can be "sniffed" all the way along the network, much easier than actually clipping-on cables in an underground cable. Indeed, there are dozens of tools for decoding video and audio streams. Interception and rerouting of calls are possible by targeting specific vulnerabilities in the protocols and the signaling during call setup. Denial of service can be achieved not only by direct attacks to VoIP protocols and implementations but also by attacking the supporting computer network infrastructure (traffic flooding, attacks in the DNS servers, etc.).

In any case, VoIP is implemented using a range of components and protocols that all have potential vulnerabilities, bugs, and exploits as presented in [14].

- VoIP Elements
  - Call control elements (call agents)

    Appliance or server-based call control—Internet protocol private branch exchange (IPPBX)
    Soft switches
    Session border controllers (SBCs)
    Proxies
  - Gateways and gatekeepers

    Dial peers
  - Multi-conference units (MCUs) and specialized conference bridges
  - Hardware endpoints

    Phones
    Video codecs
    Other devices and specialized endpoints
  - Soft clients and software endpoints

    IP phones
    Unified messaging (UM) integrated chat and voice clients

Desktop video clients
IP-based smartphone clients

– Contact center components

Automated call distribution (ACD) and interactive voice response (IVR) systems
Call center integrations and outbound dialers
Call recording systems
Call center workflow solutions

– Voicemail systems

- Protocols
  - H.248 (Megaco)
  - Media gateway control protocol (MGCP)
  - Session initiation protocol (SIP)
  - H.323
  - Skinny call control protocol (SCCP) and other proprietary protocols
  - Session description protocol (SDP), real-time protocol (RTP), real-time control protocol (RTCP), and real-time streaming protocol (RTSP)
  - Secure real-time transport protocol (SRTP)
  - Inter-Asterisk eXchange protocols (IAX and IAX2)
  - T.38 and T.125
  - Integrated services digital network (ISDN)
  - Signaling system number seven (SS7) and SIGTRAN
  - Short message service (SMS)

The point to be made is that despite the trends and the changes in technology from TDM PBX to VoIP PBX, threats are still the same, the methods are more or less the same, and only technical details in specific attacks change. We will shed some more light on the technical details in the next chapter.

2.7 Conclusion

It is more than clear that PBXs face an increased array of threats that affect their availability, confidentiality, and integrity. Apart from voice communication, enhanced capabilities and services including phone banking transactions raise even stronger security issues.

Although modern technology security area is a constant battleground, telephony security levels are not high enough. This presents a vast opportunity for telecom carriers and service providers too. They can play a proactive and strategic role in protecting their subscribers, both through education and through the security software they should deploy across their networks.

Manufacturers on the other hand should proceed to better-designed interfaces and systems generally, richer in security features. Special software could help users mitigate some of the security risks offering embedded encryption options as well as automated backup features and options to detect fraud.

To combat the threats, before rushing to technological solutions the first step could be the awareness and better education of users. Following this introduction, we will continue with a more technical chapter before presenting security solutions.

References

1. Akhvlediani M (2009) The fatal flaw: the media and the Russian invasion of Georgia. Small Wars Insurgencies 20(2):363–390
2. deDECTed. https://dedected.org/trac
3. Prevelakis V (2007) The Athens affair. IEEE Spectrum, July 2007
4. The Free Dictionary (2012) Psychological operations. http://www.thefreedictionary.com/psychological+operations
5. CFCA, Communications Fraud Control Association (2009) Worldwide Telecom Fraud Survey
6. CFCA, Communications Fraud Control Association (2003) Worldwide Telecom Fraud Survey
7. Ars Tsechnica (2011) How Filipino phreakers turned PBX systems into cash machines for terrorists. http://arstechnica.com/tech-policy/news/2011/11/how-filipino-phreakers-turned-pbx--systems-into-cash-machines-for-terrorists.ars
8. Brisbane (2006) http://www.bris2600.com/hall_of_fame/poulsen.php
9. BBC News (2011) Exeter hospital phones 'cannot understand Devon accent'. http://www.bbc.co.uk/news/uk-england-devon-14649238
10. St. Cloud Times Minnesota (2011) BRIEF: fire causes problem for hospital phones. St. Cloud, Minnesota. http://www.newsorganizer.com/article/brief-fire-causes-problem-for--ac0a083204b6cc060f0c2d0edede85fa/
11. Luiijf E, Klaver M (2011) Insufficient situational awareness about critical infrastructures by emergency management. TNO Defence, Security and Safety
12. Mitnick KD, Simon WL (2002) The art of deception: controlling the human element of security. Wiley, Indianapolis
13. VOIPSA (2005) VoIP security and privacy threat taxonomy public release 1.0, 24 October 2005. http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf
14. Rhodes-Ousley M (2013) Information security: the complete reference, 2nd edn. McGraw-Hill Education, New York



http://www.springer.com/978-3-319-29720-0

VoIP and PBX Security and Forensics
A Practical Approach
Androulidakis, I.I.
2016, XI, 103 p. 59 illus., 35 illus. in color., Softcover
ISBN: 978-3-319-29720-0