Abstract—In the following work we present an easy to read essay about the array of threats that modern telephony systems face, that will prove, hopefully, useful for both administrators and simple users. We have taxonomized these threats and we have further provided some useful tips for safeguarding these systems in order to keep enjoying one of the most valuable goods: That of communication.

Index Terms—Telephony Threats, Telephony Fraud Communication Systems Security

“It is not a matter of if, it is a matter of when”. Most of us have come across that saying, regarding a computer or network incident. Many articles have been written to alert users and help administrators deal with the problems and much work has been carried out to safeguard the computing and network infrastructure. But what about our plain old telephone? Can you recall any information regarding the classical telephony threats?

There are many issues concerning the threats telephony faces. We tried to address with a comical spirit, some of the basic problems that exist and threaten the telephones’ security. We taxonomized them in an easy to read essay that will prove, hopefully, useful for both administrators and simple users. Our analysis is mainly focused on Private Branch Exchanges (PBXs). A PBX is a telephone exchange serving an individual organization or company with connections to the PSTN (Public Switched Telephone Network) [9]. It is actually a private switch or router that connects a group of telephones and provides a wealth of features.

As telephony security is usually lacking compared to IT security, the opportunities for crime are numerous. The first thing that comes into mind is of course unauthorized access of our telephones and the relevant results. Losses due to computer incidents are usually estimated and it is indeed a very complex procedure yielding wrong results many times. Economical losses due to a telephony incident on the other hand are immediately obvious. Imagine a telephony fraud taking place unnoticed for a substantial period. A month later you can see the poor accountant looking at the phone bills, or the damage reports which usually come in a box rather than in an envelope. Apart from the apparent cost of the bill, lost revenues and additional expenses can skyrocket the total loss to astronomical amounts.

Who is actually engaging into such actions? Telecom fraudsters fall into three basic groups: those who do it for fun, those who do it to save money and those who do it for profit [2]. At the lower end of the impact scale are skilled individuals, usually teenagers trying to break in just for the challenge. The most common threat to a network is the malicious hacker who is usually trying to earn personal benefits by employing his skills in network management and programming to deploy various illegal activities such as call sell operations using stolen codes and accesses. He could also intercept phone calls and logs providing valuable information, especially in cases of industrial spying.

Typical methods of abuse by malicious hackers involve the misuse of common PBX functions such as DISA (Direct Inwards System Access), call forwarding, voicemail and auto attendant features. DISA is designed to allow remote users to access a PBX to place log distance calls as if
they were at the same site as the PBX. Fraudsters unfortunately are another category of remote users. Voicemail use poses two possible threats. One is that if wrongly configured, they can give access to dial tone in order to place a call. The second one is the inherent dangers of stealing the information contained in them or even taking them over [10].

Wireless calls can passively be intercepted using the proper gear. A classical way of interception is the use of special devices, the well known “bugs”. A more elaborate technique is that of “the man in the middle”. In order to intercept a wireless communication a hacker can sit in the middle pretending to be the other party and relaying the information to the intended party. That is why revealing sensitive information during a phone call is not a good idea unless some sort of cryptographic means is used.

At the other end of the spectrum is the organized crime. A common use of a compromised telephone network is to use it as a screen for covering-up illegal activities such as ring operations, drug selling, money laundry etc. The call begins usually from payphones because they can offer anonymity and they are easy to find and accessible from almost everywhere. Then the call is routed through many private telephone branch exchanges (PBXs) to make it extremely difficult to trace. This “looping” is a very effective way to mislead authorities from tracing them. The technique however, is on the decline with the advent of convenient prepaid mobile phones [3].

Organized crime has its own customer base that demands cheap international calls and will break into PBXs to serve this base. Knowing that the window of opportunity will close eventually they try to maximize their revenue by exploiting quickly and aggressively the compromised PBX [2]. Selling calls to high cost international destinations is the most usual fraud taking place. The unsuspected administrator who has not properly secured his PBX will face a very unpleasant surprise.

Another sensitive point in a company’s telephone network consists of the internal phones placed in publicly accessed areas (i.e. in the lobby or in the elevator). As a matter of fact there is also a whole category in relevant articles in underground electronic magazines regarding what is called “elevator phreaking”. Such phones are easy to access and as an internal part of the network can easily be misused to expose vulnerabilities. Furthermore they are a great access point for all those who mean to cause harm to the network and its infrastructure. A person can easily slip a “bug” or use them just to place a free call. So they have to be both protected and confined in places that not everyone has access to them. In case they are really needed any necessary steps must be taken in order to secure them and make sure that they cannot cause problems. A special case of an internal phone is the operator’s console. If not properly administered, it may have the ability to change setup features and operational data. It could for example unblock barred destinations or leverage call abilities on certain phones.

Most administrators use firewalls and check their computer network’s health regularly. Unfortunately the telephone network can help breach the firewall protection. All it takes is an unauthorized modem hooked up in an internal line and presto! Access to Internet is now possible and viruses and trojan horses lurking can now find their way in through an unguarded entry point.

To make things worse, a dialup line connecting the telephone exchange’s CPU to the maintainer’s modem in order to remotely administer the switch can be misused causing not only telephone problems but also providing a way to enter the computer network. The Maintenance Port [10] as it is called, is usually protected with a simple to guess or default password making it easy to defeat. Having access to the switch, the hacker can reprogram it, turn on functions such as DISA and shut down other functions such as call logging. There is a well known technique, called “war dialing” which consists of calling every single number a company owns in order to discover modems and electronic services to abuse. According to a recent survey [11] regarding information security controls, “testing and review procedures including a “war dial” of inbound phone lines to identify active modems” ranked last in a list of 80 controls. In other words, the identification and tracking of modem connections was incomplete, of low quality and not rationalized causing a significant risk that shouldn’t be neglected.

When a PBX is linked to an organization’s IT network, a poorly protected maintenance port can offer an open and undefended “back door” into such critical assets as customer databases and business applications [1]. Imagine a fraudster, having the ability to intercept credit card numbers as the unsuspected client presses the keys in his phone [3]. 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. Total security can only be achieved with combined efforts and supplies between IT and telecom world.

Apart from fraud and interception, another hit in our infrastructure can come from what is called “denial of service” which is caused either intentionally or unintentionally and severely harms the integrity of our network especially if we don’t have alternative routes or backup lines for our connections. In simple words, we cannot use our telephone to place or receive calls since it is no more operating. A company short on ethics could hire somebody to sabotage the telephone exchange of their
competitor making it impossible to do business and causing huge losses. Finally a disgruntled former employer with a disordered sense of amusement could render such a telephone exchange useless in order to take revenge.

Is might seem so far that we are left unable to defend ourselves against the evil. This is not the case. There are many simple steps a savvy administrator can take to shield the PBX [7,12], starting from proper education of the users and himself in order to increase the awareness of the system’s security features and vulnerabilities. Properly communicated security policies should follow. Technical measures such as frequent system passwords changing, barring of premium rate calls, careful assignment of station privileges etc. can only be effective as soon as the users are educated. Manuals, directories and other internal documents should be treated as confidential. Call logging should always be enabled and checked for unusual activity and strange call patterns. Furthermore, call forwarding to external destinations should not be allowed. Especially regarding maintenance port, every serial port connection should be traced to its destination. The modem should be switched on only when the maintainer needs to perform some action and with a well defined time schedule. Dangerous features such as DISA and voicemail deserve also special attention. It is better to be disabled or even removed if they are of no use. Otherwise, in collaboration of the manufacturer, every suggested measure, patch and upgrade should be applied.

The physical infrastructure and especially the expensive one should be protected with proper security measures, be kept in a controlled environment not easily accessible to everyone, and be well hidden from people that don’t need to know where it is. In many companies, everyone is invited to have a look at their expensive PBX (Private Branch Exchange), which is waiting behind an open door. Just follow the signs that lead to the place. As a matter of fact many companies tend to advertise their “treasures” by signs and labels making it easier for the determined one to find. Modern telephone exchanges use expensive and easily removed and carried equipment (i.e. exchange cards) so a couple of minutes would be enough for an incident to take place causing apart from the economical damage also an outage. Furthermore protection from unauthorized access is a must because access to the premises means complete access to our network. A “bug” or other intercept device could be planted there, at the heart of our network.

Another usually forgotten aspect is the protection against environmental elements and disasters. A fire could burn our infrastructure endangering also human lives. A flood could prove extremely harmful for the sensitive and expensive equipment while a water pipe leak can cause a severe damage and a complete collapse of the network which will not be easy to deal with. It is of great importance to take all the appropriate measures to guard against such incidents. In case of a natural disaster, such as an earthquake, there should always be provision for disaster recovery procedures.

Besides technical means, common sense and tidiness can help a lot. Equipment, patching and connections should be well documented not only to help technicians in their job to easily expand and service the network but also to make it possible to easily identify and remove any “external” elements, such as “bugs”. Moreover, in case of a disaster as stated in the previous paragraph, proper labeling and documentation could speed up the repair time.

Protecting our equipment is not enough. As we will see, our trash needs also protection and proper ways of disposal. Hackers or other persons trying to get access to our network often use the so called “dumpster diving” technique which can give them valuable information about our security protocols, anti hacking measures, the topology of our network and possible soft spots in security or in the infrastructure, or even worse give them access codes and usernames which can lead them directly into our network. The technique is carried out by just inspecting our trash hoping to find valuable data. It is thus of great importance to destroy all sensitive data before disposal and not just leave them in the dumpster as an easy prey for anyone to find.

So far we 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 false ID 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 that gives false information and impersonates a network technician in order to extract information about the whereabouts of the PBX and take the secretaries approval to access it, and from there to have full access to the network. Further examples can be found in [4]. Education and properly enforced security procedures and policies can help mitigate the danger.

Closing our analysis we will move from threats coming from outside to threats that originate form the inside. Insiders can prove to be a very difficult enemy hard to deal with. They can prove a valuable ally for a hacker, providing him with passwords and information about the infrastructure. They could also simply give him permission to enter a company and poke around the equipment. Finally insiders could act by themselves exploiting our assets, planting “bugs” etc. For example, an employee, contractor or even a cleaner could forward a seldom-used extension to an overseas number and make international calls by calling a
local rate number in the office. Needless to say who is actually paying for the call.

With the advent of new telecommunication technologies which are based around open communications via the Internet Protocol (VoIP) the situation will get even more complicated. The introduction of these technologies means that IT and telecoms managers need now to become even more alerted to prevent new and existing threats that are typically associated with data networks, now impacting voice networks. Conventional PBXs typically use proprietary protocols and specialized software and have fewer points of access than VoIP systems. With VoIP, opportunities for eavesdroppers are multiplied [8]. Without diligent attention, telecoms systems are in grave danger of becoming the weak link in the network and utterly defenseless against targeted attacks.

PBX fraud has been allowed to flourish due to ignorance and naivety. Telephony security has remained a poor second place to IT security [3]. Hopefully this simple taxonomy with the comical perspective of things and the headlines that come with the illustration will help to better understand the dangers and the problems and will always be a good quick reference guide for the administrators. After all, it is not a matter of if… it is a matter of when!

REFERENCES