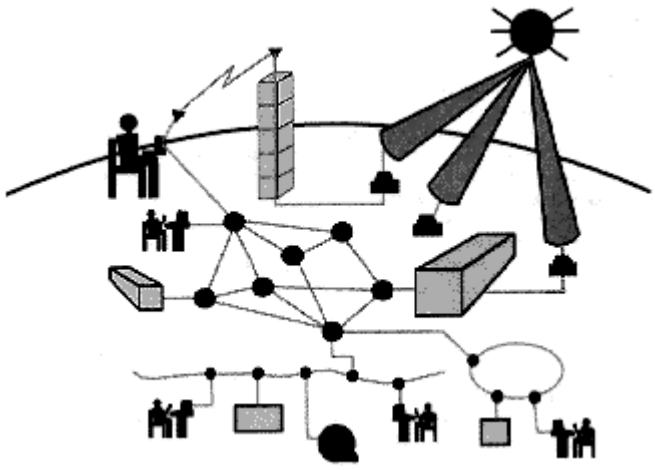
A Study of the Security Problems Associated with the Telephone Network



Santosh Rajagopalan
Department of Electrical and Computer Engineering
rajagosa@engr.orst.edu

Contents

1 Abstract

The tools available to the intruder for fraudulent use of the telephone network have evolved with the evolution of the network. DTMF tone generators were used earlier to circumvent the network's signaling mechanisms. The focus has now shifted to PBX hacking and the use of Extenders, and the use of the so-called "loops". The technology used for wiretapping has remained fairly constant, except for increased ease and increased masking from detection. The widespread introduction of cellular systems has introduced the risks of conversation monitoring and stolen airtime to a greater degree. Newer cellular systems based on TDMA and CDMA make illegal use a little more difficult as compared to the AMPS system. GSM uses a variation of the TDMA/CDMA idea, but more comprehensive security will be available only with the use of public key encryption in the proposed PACS, but this is still far in the future. In this report, methodologies for circumventing network control are studied, along with ones that do not work as much now because of remedial measures by the telephone companies.

2 "Phreaking" and Security

2.1 Introduction

The telephone network has been in existence for over a century now, however, attempts to subvert the network came sharply into focus only in the 70s. This was largely due to the introduction of the personal computer. The PC did two things: a) give birth to the hacker, whose idea of having a "good time" was to mess around systems to see how they worked, and b) introduce ubiquitous computing power, which could be easily diverted to be used on equipment that could be interfaced with the PC.

A term that came to the forefront of public discussions because of Kevin Mitnick's conviction is "phreaker". Kevin Mitnick started out his hacking career as a "phreak", using the infamous "boxes" to subvert the system until the shift to out of band signaling took away most of the ease in "phreaking".

According the "The New Hacker's Dictionary", a phreaker is " is someone who breaks into the telephone network illegally, typically to make free long-distance phone calls or to tap phone lines. The term is now sometimes used to include anyone who breaks or tries to break the security of any network."

2.2 A Short History of Phreaking

The beginning:

The first person mentioned in relation to phreaking was the so-called "Captain Crunch". He discovered how to take rides through the phone system, with the aid of a small whistle found in a cereal box. By blowing this whistle, he generated a 2600hz signal which, when used in the mouthpiece, was supposed to give him complete control over the system.

Before he was caught and jailed, he was rumored to have made about 1/4 of the calls coming out of San Francisco. After getting out, he joined Apple computer and is supposed to be still out there somewhere.
Then there was the blind man called Joe the Whistler, who was supposed to be able to whistle a perfect 2600hz tone. It was rumored phreaks used to call him to tune their boxes.

1970 to 1979

Phreaking was mainly done by college students, businessmen and anyone who knew enough about electronics [enough to make a 555 IC to generate tones] and the Phone Company. Businessmen and a few college students used the "blue box" to get free calls. The others were still there, exploring 800#'s and the new ESS systems.
ESS posed a big problem for phreaks then and even a bigger one now. ESS was not widespread, but where it was, blue boxing was next to impossible except for the most experienced phreak. Today ESS is installed in almost all major cities and "blue boxing" is getting harder and harder.

1978

This year marked a change in phreaking: the Apple, now a computer that was affordable, could be programmed, and previous work could be saved on a cassette. Then just a short while later came the Apple Cat modem. With this modem, generating all blue box tones became even easier. Pretty soon programs that could imitate an operator were hitting the community. The ones that set the standard were TSPS and Cat's Meow, which were widely considered the best.

1982-1986

Line Dialing (LD) services were starting to appear in mass numbers. People now had programs to hack LD services, telephone exchanges, and even passwords. By now many phreaks were getting extremely good and Bulletin Boards (BBS) started to spring up everywhere, each having documentation on phreaking for the novice. The movie War Games was released at this time, and it made novices came out in mass numbers, trying to be phreaks. Other problems started to occur, novices guessed easy passwords on large government computers and started to play around. These kids were caught easily, and their public trials helped bring down the explosion in phreaking.

2.3 Desired Security Services in a Telephone Network

The Universal Mobile Telecommunication System (UMTS) specifications for Europe give the following security requirements:

- **Confidentiality**
  The purpose of confidentiality is to protect information from (deliberate or accidental) disclosure to an unauthorized entity. These services provide confidentiality for not only the transferred user data, but also for stored/transferred signaling and management data in the air-interface and over the wired lines. Examples of signaling related data to be protected are:

identity (user/terminal), location (user/terminal), status (user/terminal), other information (user/terminal/network operator), and charging, signaling and sensitive user data.

- **Integrity**
  The certainty that data has not been altered is called integrity. In principle, its scope covers the integrity of transferred user data, and stored/transferred signaling and management data in the air interface and over the wired lines.

- **Authentication**
  This service is used to establish the validity of a claimed identity.

- **Access Control**
  This service is used to prevent unauthorized use of a resource, including the prevention of the use of a resource in an unauthorized manner. Access control would be desirable in services, system databases, subnetworks and equipment.

- **Incontestable Charging**
  This service is used to prevent denial or not of one of the entities involved in communication which has participated in all or part of the communication. It is desirable to introduce incontestable charging between subscriber, network operator and/or service provider.

3 The Wired Telephone Network

3.1 Introduction: Where the Network Stands Now

The wired telephone network has the advantage of being around for a long time, and of being widely studied. Hence, when the first attempts at subverting the telephone network were made, fixes were proposed that solved the problem to a great extent. It is now almost uneconomical for large telephone companies to pursue all offenders, because the loss due to illegal use is very low. Hence, while the telephone companies now have the means to prosecute most offenders, they prefer to strike at a few people occasionally, so that they can make examples of them.

3.2 Phreaking methodologies

3.2.1 Boxes

Boxes are usually electronic gizmos that help the phreak to exploit the phone system. Several boxes do not work anymore, if they even worked at all when they were created. The reason boxes became so popular, is because phone systems rely on DTMF Tones for operation. The recreation of these tones, using an electronic device has shown the power that is available to the phreak.

The Blue Box:
Blue boxes use a 2600hz tone to size control of telephone switches that use in-band signaling. The caller may then access special switch functions, with the usual purpose of making free long distance phone calls, using the tones provided by the Blue Box. Blue Boxes still work in areas using in band signaling. Modern phone switches use out of band signaling. Nothing sent over the voice portion of bandwidth can control the switch. In an area served by a switch using out of band signaling, "blue boxing" is still possible by calling through an area served by older in-band equipment

Black Box:
A Black Box is a 1.8k ohm resistor placed across the phone line to cause the phone company equipment to be unable to detect that the telephone has been answered. People who call would then not be billed for the telephone call. Since most areas are now under ESS black boxes don't work anymore. Black boxes were heavily used back in the 80's.

Red Box
When a coin is inserted into a payphone, the payphone emits a set of tones to the ACTS (Automated Coin Toll System). Red boxes work by fooling ACTS into believing you have actually put money into the phone. The red box simply plays the ACTS tones into the telephone microphone. ACTS hears those tones, and allows you to place your call. Red Boxes will work on Telephone Company owned payphones, but not on COCOT's (Customer Owned Coin Operated Telephones). They can be made from modified Radio Shack tone dialers, Hallmark greeting cards, or from scratch using readily available electronic components.

Beige Box
This is one of the most used boxes, and is known by several names. The [Acrylic] [Beige] [Bud] [Aquamarine] [Razz] [Beagan] [Lego] [Peell] Boxes are all the same thing: a home-made lineman's handset, usually a one-piece "flip phone" unit, with the modular plug removed and replaced with a pair of alligator clips. The idea is to attach the alligator clips to any exposed outdoor or indoor phone connection terminals, to make calls that will be billed to whoever owns the line. Generally, the lineman's handset is one of the easiest ways to phreak, one of the few that works everywhere universally even today, and is considered quite lame because no real skill is involved. It's literally just theft of service, and not from the phone company but from their customers. The easiest targets are supposed to be homes because most houses have grey terminal boxes somewhere on the exterior, unprotected.

3.2.2 War Dialers/Scanners

Scanning is a way to dial every number in a certain exchange. Example dial every number from 555-000 to 555-9999, while only dialing each number once, and recording what is found. To do this, one would use what is called a war-dialer. The objective is to look for strange tones and/or telephone company test numbers. This technique is used to find loops, ANIs and CNA numbers.

3.2.3 Loops

Using a war dialer, if a constant tone (either a high or a low tone) is found, it could indicate the presence of a loop. Loops are a pair of phone numbers, usually consecutive, like 836-9998 and 836-9999 which the Phone Company uses for testing. Loops are used by phreakers to make free phone calls in the following way: Each loop has two ends, a 'high' end, and a 'low' end. One end gives a (usually) constant, loud tone when it is called. The other end is silent. Loops don't usually ring either. When BOTH ends are called, the people that called each end can talk through the loop. Some loops are voice filtered and won't pass anything but a constant tone; these aren't much use to the phreaker.
To make a call: First, call the end that gives the loud tone. Then if someone calls the other end, the tone will go quiet. If you now act like the phone just rang and was answered by you, the person calling will think that he/she just called you. The phone bill goes to the loop, i.e. the Phone Company. Loops are supposed most useful when you want to talk to someone to whom you don't want to give your phone number.

3.2.4 ANI/ANAC numbers

An ANAC (Automatic Number Announcement Circuit) number is a telephone number that plays back the number of the telephone that called it. ANAC numbers are used to find the telephone number of a pair of wires. Phreakers use it when they are using beige boxes to know the number of the wires the box is connected to.

3.2.5 CNA numbers

CNA stands for Customer Name and Address. The CNA number is a phone number for telephone company personnel to call and get the name and address for a phone number. If a telephone lineman finds a phone line he does not recognize, he can use the ANI number to find its phone number and then call the CNA operator to see who owns it and where they live. Normal CNA numbers are available only to telephone company personnel. Private citizens may legally get CNA information from private companies. Two such companies are: Unidirectory (900) 933-3330 Telename (900) 884-1212. Note that these are 900 numbers, and a call to them costs approximately one dollar per minute. This number is used by phreakers if they only have a person's number and they want a name to go with it, maybe for getting information using what is called "social engineering".

3.2.6 Extenders

Extenders are set up by the telephone companies as a courtesy to its subscribers. An extender serves the same purpose as a calling card. It would be impractical for a person who travels a lot or who is off at a school to drop 10 quarters into a payphone every time he wants to make a long distance call. So to make things easier for their customers, long distance companies have set up extenders for their customers. To dial a number using an

extender, the customer has to dial the 1-800 number given by the Phone Company, then [2] the authorization code, and the [3] number they wish to call. [2] and [3] may be in any order, depending on the phone company.
Phreakers crack extenders in the following way: they call 1-800-xxx-xxxx, trying different numbers here using a war dialer. This is not normally done from the their home phone, because 1-800 numbers are usually monitored for unusual activity, and ANI enables the calling number to be recorded at the phone company. The kind of tone on the line identifies the presence of an extender. Then, the phreaker tries to find out whether the security code is expected first or the destination number is expected first. Next, he tries to guess the correct authorization code using a "Code Hacker", or by hand. The most practical way to hack codes is supposed to be with a code hacker for the computer. A good code hacker supports random touch tone spacing, random time between attempts, templateable codes, variable time between code and destination number, has at least 500 random destination numbers, etc. This is done to avoid being caught by the tracking software available with most 1-800 numbers at the exchange.

3.2.7 PBX cracking

A PBX is a Private Branch Exchange, a small telephone switch owned by a company or organization so that calls made by employees outside can be multiplexed onto a fewer number of phone lines. The reason that PBXs can be used by phreakers to make phone calls is that some of theme are set up so that if you dial the PBX, followed by an authorization code, you can then dial out to any long distance phone, without incurring a phone charge. This arrangement is made so that an employee working on a company assignment can make a call without being charged for it. A PBX is usually preferred by a phreaker because, unlike 1-800 numbers, a PBX has a limited tracking ability. PBXs are found and cracked using exactly the same method used for extenders.

3.2.8 VMB Stealing

A VMB is a Voice MailBox. A VMB is a computer that acts as an answering machine for hundreds or thousands of users. Each user has their own Voice Mail Box on the system. Each mail box has a box number and a pass code. Without a pass code, it is only possible to leave messages to users on the VMB system. With a pass code, one can read messages and administer a mailbox. Often, mailboxes will exist that were created by default or are no longer used. These mailboxes may be taken over by guessing their pass code. Often the pass code will be the mailbox number or a common number such as 1234. This is a somewhat benign form of phreaking, since there is no illegal charging of phone calls: the phreaker only uses the VMB to receive his/her own messages.

3.3 Wiretapping

There are many different types of taps: transmitters, wired taps and induction taps to name a few. Wired and wireless transmitters must be physically connected to the line to work.

Wireless Taps

Once a wireless tap is connected to the line, it can transmit all conversations over a limited range. The phones in the house can also be modified to pick up conversations in the room and transmit them. These taps are usually powered off the phone line, but can have an external power source. There is even one type of wireless tap that looks like a normal

telephone mike. All that has to be done is replace the original mike with this and it transmits all conversations.

Wired Taps

Wired taps, on the other hand, need no power source, but a wire must be run from the line to the listener or to a transmitter. There are obvious advantages of wireless taps over wired ones. There is also an exotic type of wired tap known as the 'infinity transmitter' or 'Harmonica bug'. In order to hook up one of these, the linetapper needs access to the target telephone. It has a tone decoder and switch inside. When it is installed, someone calls the tapped phone and before it rings, it blows a whistle over the line. The transmitter receives the tone and picks up the phone via a relay. The mike on the phone is activated so the caller can hear all conversations in the room. There is a sweep tone test which can be used to detect one of these taps. If one of these is on the tested line, then when the test # sends the correct tone, a click is heard.

Induction taps

Induction taps have are preferred over taps that must be physically wired to the phone, because they don't have to be touching the phone in order to pick up the conversation. They work on the same principle as the suction-cup tape recorder mikes available at radio shack. Induction mikes can be hooked up to a transmitter or be wired.

The Easiest Way

The quickest method wiretappers use is simply to cut into someone's phone line, preferably where the owner can't detect it (near the garage or behind the pole, for example) and wire in their own head-set. The mouthpiece is then removed, so the person being tapped can't detect the wiretapper's breathing or other noise. If the wiretapper can't stick around, he uses a high-impedance coupling transformer and feeds the wire into a tape recorder. To save tape, most tappers use a recorder that records automatically when it hears a voice. Another procedure is to find the right "pair" (the two wires that go into the house of the victim and that of others in your building or apartment). The boxes that contain pair terminals are called terminal boxes and can usually be found in basements of apartments or office buildings, or occasionally on the outside wall of a building. A wiretapper typically will have an accomplice call the number being tapped. That puts about 90 volts on the line. The tapper takes two fingers and run them down the row terminal. When the right phone pair is hit, a jolt is felt. Once the right lines have been found, a listening device is then attached.

3.4 A Note on Legal Wiretapping

Legal wiretaps are the most common way for the Phone Company to check a person's calling activity. Under court order, the Phone Company may attach a "Pen Register" to a person's phone wires at the central office. The device gives a printout of all calls, local and long distance, going out of the phone including time of day, duration of call, and, of course, the recipient's number. It's used mostly by law enforcement agencies to check who the person's calling in the hope that the other party will shed some light on the person's alleged wrongdoing. Law enforcement agencies often prefer the Pen Register to an out-and-out wiretap. It takes less work, less manpower (the Pen Register is automatic; the policemen just

come by the phone company and pick up the printout), and less hassle to obtain a court order for its installation, because it's less of an invasion of privacy than a wiretap.

3.5 Note on Cordless Phones

A cordless phone is the least secure means of communications, since a conversation can be picked up using any commercially available scanner. The cellular band is in the 869.010 to 894.000 MHz range, in 30 kHz steps. That makes a total of 835 possible frequencies to scan, which isn't much for teenagers hanging around on a Sunday afternoon with nothing to do.

4 Subverting the Cellular System

4.1 Additional Issues

There are three security levels that can be achieved in wireless networks:

Level 0:

No Privacy

Level 1:

Equivalent to wireline, for routine conversations. Here, a significant level of effort is required to crack a conversation.

Level 2:

Commercially secure, for "proprietary" conversations, containing sensitive data for corporations. Assumed to take 10-25 years to crack.

Level 3:

Government/ Military secure.

The security requirements for wireless networks

Privacy Requirements

a) Privacy of call set up information.
b) Privacy of speech.
c) Privacy of data.
d) Privacy of user location.
e) Privacy of user identification.

f) Privacy of calling patterns.

Theft Resistance Requirements

a) The system must have a clone resistant design, i.e. it should not be possible to construct a phone identical to an authorized phone, through which calls can be made.
b) Fraud when the service is being installed or being repaired must be eliminated.
c) The user of the system must be uniquely identified to the system.
d) The mobile phone must have unique information contained in it that reduces or eliminates the potential for stolen phones to be reregistered with a new user.

Radio System Requirements

If a cryptographic system is designed, it must function in a hostile environment characterized by bit errors caused by:

a) Multipath fading and thermal noise
b) Interference
c) Jamming
d) Ans should also have support for handoffs.

System Lifetime Requirements

The algorithm must consider the best cracking algorithms available today and must have provisions for being updated in the field.

Law Enforcement Requirement

A somewhat controversial requirement is that law enforcement agencies must be able to wiretap the phone, when a valid court order is received.

4.2 Security in AMPS

The original AMPS system used a 10 digit Mobile Identification Number (MIN) and a 32 bit Electronic Subscriber Number (ESN). All data is sent unencrypted. Data is shared between systems on bad MINs, ESNs, and MSN/ESN pairs. When a mobile telephone roams into a system, first the bad list is checked (to see if it's a stolen/defaulting phone) and then a message is sent to the home system to validate the MIN/ESN pair. The Intersystem communications are sent via SS& using a protocol called IS-41.

How well this works

Though in theory, all calls in AMPS can be validated in real time to check if it is being made from a stolen phone, in reality, networks have not been standardized completely yet, and many systems do not perform authentication of the phone.

MIN/ESN with no voice privacy is supposed to be now woefully inadequate for use in a wireless system. Cellular scanners, which can be used to monitor conversations and/or pick up MIN/ESN pairs (which could then be later used to clone phones), were banned by the FCC, but are still plentifully available in the used market. Equipment exists to decode the cellular data stream and control a scanner for tracking and monitoring cellular phone calls, and many cellular phones can be reprogrammed via hardware or software. Thus there is absolutely no security in North American analog cellular systems.

4.3 An Improvement: Security in TDMA/CDMA cellular protocols

The TDMA and CDMA cellular protocols use a Shared Secret (Key) Data (SSD) stored in the network and the cellular telephone. At the time the telephone unit is placed in service, a 64-bit A-key is entered into the unit and into the network in a database called the Home Location Register (HLR). From the A-key, SSD-A and SSD-B are derived and used to authenticate the telephone and establish a voice privacy key.

On the Control channel, the radio system transmits a random number, RAND that is received by all cellular phones. When a PS accesses the system, it calculates an encrypted version of the random number using SSD-A and transmits to the network the desired message with its authentication. The network does the same calculation and verifies the user. All communications between the phone and the Base station are encrypted to prevent decoding of the data and using the data to clone other phones. Furthermore, each time a user places or received a call, a call counter is incremented. The counter is used for clone detection, since clones will not have a call history identical to the legitimate phone. AMPS plans to support the SSD in the future. The PCS versions of CDMA, PACS, CDMA/TDMA, TDMA, and W-CDMA all support SSD. The Intersystem communications are sent via SS& using IS-41.

How well this works

This system has a reasonable privacy/security, but it requires the system to exchange keys of visiting mobile stations, so the question of trust between systems comes in. The only place at which wiretapping can be done is at the switch, since the airlink is encrypted. The security of this system therefore depends on the security at the switch.

4.4 GSM: Security, the European Way

GSM uses its own unique algorithm and does not share secrets between cellular or PCS systems. It uses a token based authentication scheme. When a mobile telephone roams into a system, a message is sent to the home system asking for sets (3-5 typically) of triplets consisting of: (unique challenge, response to the challenge, and a voice privacy key derived from the challenge). Each call that is placed or received uses one triplet. After all the triplets are used up, the visited system must send a new message to get a new set of triplets. The Intersystem communications use SS7 and a different protocol than IS-41.

How well this works

The security of this system is similar to that of the SSD systems, however the positive aspect is that it does not require the system to exchange keys when the user moves around. The algorithms and keys used by the Mobile and its home system need not be known by the visited system. There are some potential problems here if the tokens are reused because of the latency to obtain new triplets. Since the token based system doesn't support a call history count, it has a lower resistance to cloning than SSD or public key systems.

4.5 The Future?

PACS will optionally support public key encryption. The key length is not yet defined. The complete system operation is also not yet defined. Public key systems do not need communications to the home system to validate the mobile telephone. The intersystem communications are still needed to validate the account and to get user information. These Intersystem communications have not yet been defined.

How well this [will?] work[s]

The privacy and security is strongest here, since the Mobile User and the Network never reveal their private keys, even to one another. This system, is, however still pretty much in the design phase, and has associated with it the problems of the complexity of encryption operations.

5 Conclusion

A study of the security problems associated with the telephone network reveals a few vulnerabilities that are essentially the same as that in computer systems. For example, we find backdoors left by programmers that are later found by curious people (loops, for example), circumvention of security by going to a lower layer (tapping), inadequate password protection (extenders, PBX, mailbox cracking) etc. The ideas used for enforcing security in a computer system would probably be effective in the telephone network too, with some fine-tuning for its unique problems. When fixes are made, we will probably find that just as in a computer system, the subversives follow close on the heels of the security enforcers.

6 References

1) A. Barba, E. Cruselles and J. L. Melus. *The Customer Premises Networks in the Universal Mobile Telecommunication System: Security Aspects*, Wireless and Mobile Communications, Kluwer Academic Publishers, 1994.
2) Vijay K. Garg, Joseph E.Wilkes. *Security and Privacy in Wireless Systems*. Wireless and Personal Communication Systems, Prentice Hall International, 1996.
3) Randy H. Katz. *Security and Privacy in Wireless Systems*. CS division, University of California, Berkeley.
4) William Stallings. *Cryptography and Network Security*, Prentice Hall International, 2nd ed., 1999.
5) Eric S. Raymond. "The New Hacker's Dictionary", MIT Press
6) "The Jammer" and "Jack the Ripper". The Official Phreaker's Manual. http://listen.to/att
7) "Forest Ranger". *Wiretapping, Bugs on Lines and Listening in*. http://www.textfiles.com/phreak/WIRETAPPING/mism37.hac
8) *Management Information Systems*, University of Illinois http://www.uic.edu/cba/cba-depts/ids/definitionMIS.htm