International Journal of Creative Research Thoughts
Volume 1, Issue.4, April 2013
ISSN:-2320-2882

ORIGINAL ARTICLE

GSM BUG

NEHA S.THAKARE
P.I.E.T,NAGPUR
mail_neha2010@rediffmail.com

SNEHAL S. CHICHATE
P.I.E.T, NAGPUR
snehal_chichate023@rediffmail.com

ABSTRACT

Most, if not all, cell phones rely on some form of GSM network for communication with the cell phone network, as well as connection to other cell phones and land-lines. Internationally, GSM is the favored form of communication for cell phones, and providers that are based on it abound in areas like Europe and Asia.

BACKGROUND

GSM stands for Global System for Mobile communications. Because all voice and data on a GSM protocol are digital, GSM is considered a "2G" type of network. GSM got its start in 1982 when the European Conference of Postal and Telecommunications Administrations attempted to create a cellular network standard for European use.

Network structure

A GSM network consists of three components: the Base Station Subsystem (BSS), the Network and Switching Subsystem (NSS) and the GPRS Core Network. The BSS routes traffic from cell phones into the NSS. The NSS itself is the modern-day equivalent of a switchboard. It takes calls and data routed from the NSS, and sends it off to their destinations. The last component, The GPRS core network, is optional, but its task is to take any non-voice data (primarily Internet access) and route it to websites and other places where the data should go.

Frequencies

GSM operates on four different frequencies: 850 MHz, 900 MHz, 1800 MHz and 1900 MHz. The frequencies most commonly used are the 900 MHz and 1800 MHz bands, and are standard GSM frequencies in Europe. However, in North America, the frequencies commonly used are 850 MHz and 1900 MHz, since the previous bands were already being used in the Americas.

SIM Cards

The most apparent characteristic of a GSM network-based cell phone is known as a Subscriber Identity Module card, or SIM card for short. A SIM card is a small object that fits into the slot of a GSM-based cell phone. The SIM card stores all of the account information about that particular cell phone's user, and also stores information about the person's contacts as well.

TYPES OF BUGGING DEVICES

There are many types of audio bugs (hard wire, radio frequency, optical and acoustic). Sometimes combinations of these are used to form a hybrid bug. 'Acoustic' bugging is the direct listening without any Rf or hardwire transmission system, such as, stethoscopes, wall contact microphones or even a glass on the wall, shotgun microphone or parabolic reflector.

Optical devices

These normally convert audio signals into transmitted light pulses and this is converted back to audio signals when received. The main use for this system is the laser bounce principal, which relies on the propagation of sound waves, causing vibrations on objects such as windows. The laser beam is projected onto these, and is modulated by the small vibrations which, when received, can be converted back to audio signals by a similar principal to a CD player. These systems are very expensive, awkward to use and easily detected.

Radio Frequency Transmitters

Probably the most commonly and widely used of all the devices is the RF transmitter bug. At the lower end of the scale you will find the free oscillating VHF transmitter, transmitting on the commercial FM band 88-108 MHZ or the VHF air band 108-140MHZ. These devices are inexpensive easy to use and require no specialized receiving equipment. Due to their low cost, there is very little incentive to recover these once planted. This is the type of bug most often used by private investigators and individuals, and the chance of finding the person who plants it, is low.

UHF Transmitters

Again these transmitters are crystal locked to a particular frequency, usually between 350 MHZ - 1GHZ and require a dedicated receiver, but offer greater penetrating power and privacy over the VHF types; these transmitters are very expensive and are often confined to professional use.

GSM Bugs

Perhaps the most recent and powerful addition to the spies arsenal is the GSM bug or sometimes known as the infinity bug. These devices use the GSM mobile telephone system to transmit the conversation from the target area to any telephone in the world. These devices can be built into a wide variety of everyday items. Yet another variation of this is the spy phone when software is loaded onto a target phone turning it into a bugging device.

Microwave & VLF Specialized Transmitter

All the transmitters listed so far can be detected reasonably easily with basic equipment and an understanding of basic principles. Once you enter the realm of microwaves and VLF transmitters you can range from as low as 5KHZ to over 1000 GHZ and a specialized knowledge of radio and surveillance techniques are required to use or detect these devices. Other types of devices which can be

equally difficult to find are the type that superimpose the transmission on the top of a legitimate transmission, such as commercial radio station, other variations of rf transmitters may use frequency inversion circuits. The detection of such devices is possible, but most only by specialized counter surveillance companies and certainly not by many private investigation companies, claiming to be specialists in this field.

Hardwire Bugs

Often referred to as a wire tap, this form of surveillance is the most reliable and gives high quality results. The wiretap can be installed onto existing wiring i.e.: telephone or alarm systems. The hardwire bug in its simplest form is a microphone.A pair of thin wires or a track of conductive paint leading back to a listening post and connected to a high gain amplifier or recording device. The only drawback to this system is the concealment of the wires and the fact that if they are discovered they can be tracked back to the listening post. Often hardwire bugs are used from outside the premises, either by placing a miniature microphone into an air vent, or any other opening or by just locating the microphone near an opening, as often all the conversation in the room can be overheard if you use a quality audio booster, such as the one we supply.

WHAT IS GSM BUG?

A GSM bug is a listening device which uses the mobile phone networks. The bug is battery powered and waits in standby mode (just like a mobile phone) until a call is made to it. It then answers the call, without making a noise, allowing the caller to listen in around it. Also like a mobile, the GSM bug listening device has a SIM card in it, this is the number you call to listen in to your bug and spy. These GSM bugs had several major advantages over the old transmitting bugs:

- Legal transmission
- Longer battery life

- Only the person with the phone number of the SIM in the GSM Bug could listen.

The battery life would be about two weeks of standby, which was shortened with average calling in times to a useful life of about a week. On this model, where the batteries are outside of the case, a 3 x AA battery holder is attached. A larger 3 x D size battery holder could be added, giving a battery life of 2 months plus! In addition, the GSM Bug could be hardwired into a car using a special 12 volt adapter lead. The microphone on this model was at the end of 1 metre of mic cable, so that the bug could be hidden well away, just the tip of the mic needed to point into the room or car cabin. Other variants of this model had the battery pack and mic built in, so the GSM Bug was just a compact black box.

More recently, GSM Bugs have become available from far shores which are smaller, rechargeable and with extra features such as the ability to call you when conversation is detected. Such a GSM listening device is our Mini GSM Spy Bug which is our currently standard spy bug suitable for most applications.

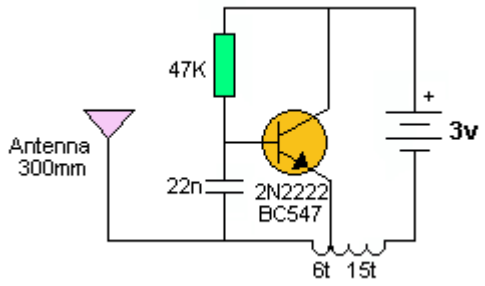
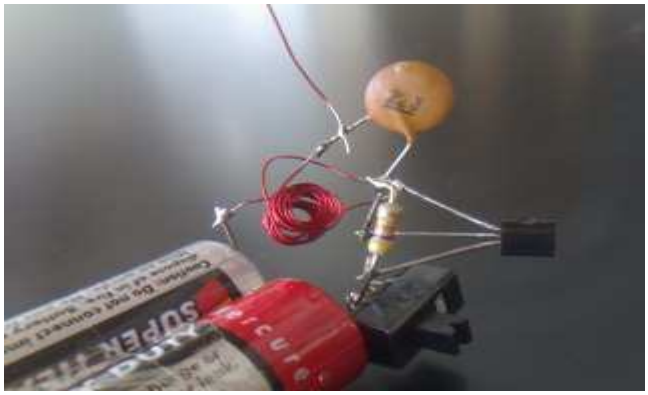


Fig. shows the circuit diagram of GSM Bug.



SOME TYPES OF GSM BUG ARE

1. GSM spy bug

This device is designed to help you listen in on a conversation. Simply insert a SIM card, place device strategically and when you are ready to listen in on a conversation, dial the SIM card. The device is perfect for eaves dropping, device auto answers and you can listen to conversations without being noticed

Example of when to use: An important meeting in your office has been scheduled to take place in the boardroom. You are not invited for the meeting but you want to know what is being discussed and who is talking about you. Buy this listening device - Insert a SIM card (GLO/MTN/etc) into the device - Place the device in a secret location in the boardroom - When the meeting is scheduled, simply call the number of SIM card placed into device -You will now be able to hear what is being discussed and get important information.

APPLICATIONS

1. GSM car bug

This product has been specifically designed to be hidden and hard-wired inside a vehicle (car/van). The purpose of the unit is to provide the ability to listen to what is happening inside the vehicle from anywhere in the world. This is achieved because the device uses mobile phone technology within. This superb GSM bug unit delivers excellent audio quality and has an external microphone (approximately 1.5 meters in length) and internal lithium ion rechargeable battery pack. This means that even if the car battery is disconnected, the bug will still remain switched on ready for use. The rechargeable battery pack is continually topped up by trickle charge from the 12V Car/Van battery, so once installed the unit can be just left in place to be available for listening in on demand. To use the bug function, it is a matter of simply calling the SIM card that you have put in the device. The unit will automatically answer the call and without giving any

indication open up the microphone so that you can listen to the surrounding environment (the inside of the vehicle). When you have finished listening, then it is a matter of ending the call at your end.

Calculator bug device is a voice activated and dials in GSM audio bug with shock sensors with a built in rechargeable 5200Mah Li-Ion battery giving it an amazing battery life. The voice activation can be activated and deactivated by SMS commands and the sensitivity of the voice activation can be changed by sending an SMS command to the device. The GSM band modules are 900/1800/1900. The standby time for this unit is around 35 days.

DISADVANTAGES:

GSM technology, which stands for Global Standard for Mobile Communications, is the mobile phone technology standard used in the United States by T-Mobile and AT&T. However, there are some problems with the technology, some of which can be solved by switching to the more modern CDMA standard . According to Cellular News, call quality problems, including dropped calls and missed calls are common problems with GSM technology. These problems result directly from the technology in use. GSM technology cannot accommodate as many callers on a single cell tower as the more modern CDMA technology. This means that callers in areas where there are not a preponderance of cell towers may find that the call problems on GSM will be more common technology (only the older 2G technology though) that is commonly used by people all over the world.

CONCLUSION

The GSM bugging devices have been cleverly adapted to use mobile phone technology and networks to listen into and relay live audio. GSM based bugs are small, simple to deploy, require very little power and are accessible from anywhere in the world, making them one of the most common threats to privacy and security.

The latest generations of GSM bugs are getting ever more sophisticated. They can use motion and vibration detection to sense when a room under surveillance becomes occupied. Eavesdroppers can also use multi-switchable microphone inputs to listen in to conversations being held in different locations. And if undiscovered, GSM bugging devices can be more or less left on permanently to capture vast amounts of information over very long periods of time.

Detecting illicit or unauthorised mobile phone use and the presence of GSM bugs is difficult as their signals are easily lost among the background hum of legitimate GSM and mobile communications.

The good news is that counter surveillance technology is developing rapidly too. Systems are now available to detect, identify and locate even the most sophisticated GSM transmitters

REFERENCES

1.www.google.com
2.Wireless Communication By T.S.Rappaport
3.Google scholar.com
4.www.alfavitaelectronics.com