FIGHTING INSIDE A VEHICLE | DENTAL EMERGENCIES | AMBIDEXTROUS SHOOTING SKILLS

TACTICS AND PREPAREDNESS

SKILLS AND SURVIVAL FOR ALL SITUATIONS

APRIL 2015 ISSUE 18 - TACTICSANDPREPAREDNESS.COM

IANL @ FREERANGESTOCK.COM

PROTECT YOURSELF FROM NETWORK SPIES

BY: BRANDEN WILLIAMS

When you look through history, you can find certain points in time when one technology overcame the ubiquitous nature of another.

Some examples are: the use of the internal combustion engine over steam engines, telephones over telegraph and email over fax. Somewhere in the late 1990s, mobile phones started to take over from land lines. Probably the clearest point in which you can see this eclipse occurring is when pay phones were abandoned in favor of cell phones; the use of pay phones dropped dramatically as the use of mobile phones grew.

Cell phones of the 1990s were fun for all thanks to their analog signals. I can remember driving out to a rural town to fix a computer and the folks there used their scanners to eavesdrop cell phone conversations just as a means to pass the time. The hour I spent listening to those calls was more entertaining than any single hour of television I've ever seen. Soon, staticy analog signals were exchanged for garbled digital ones where we routinely asked, "Can you hear me now?" Snooping on cell phone conversations went by the wayside. Some providers even added encryption to their transmissions for additional protection (remember Nextel?).

Today, technology continues to get better, faster and smaller. The amount of computing power we carry around in our pockets in a mobile phone rivals rooms of computers in the 1960s. For the most part, we still don't understand the technology—we just tap and swipe. Mobile phones are not perfect devices and have two main forms of continued on next page

CONTENTS

01 PROTECT YOURSELF FROM NETWORK SPIES
BY BRANDEN WILLIAMS

05 BOOK REVIEW: SOME THOUGHTS ON SCOUTS AND SPIES, WRITTEN BY GERRY BARKER
REVIEWED BY KEN JAVES

07 WHY YOU NEED AMBIDEXTROUS SHOOTING SKILLS
BY GREG LAPIN

10 FIGHTING INSIDE A VEHICLE
BY ANDREW CURTISS

13 DENTAL EMERGENCIES IN AUSTERE ENVIRONMENTS
BY CHRIS CASSELL

15 GEAR REVIEW: TROY INDUSTRIES AK-47 RAIL

16 USE TRACKING SKILLS TO PROTECT YOUR PROPERTY
BY FREDDY OSUNA

19 ON LEADERSHIP: ACTION, REACTION, COUNTERACTION
BY COLONEL S. RANDY WATT

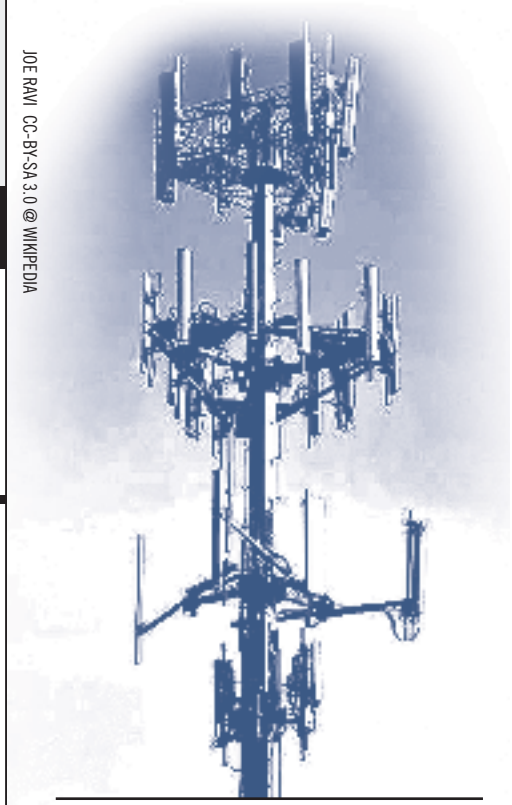
STAFF

DAVID MORRIS and **"OX"** — Publishers
CHRIS GRAHAM — Editor
www.chrisgrahamauthor.com
JOHN HIGGS — Copy Editor
BETTY SHONTS — Graphic Designer

compromise: first with the device itself and second with the network.

We tend to forget that the mobile device is just another computer. It can be vulnerable to all of the same kinds of hacks that could compromise your laptop and it's always connected to a network. Android users must be especially vigilant as the upgrade path for the operating system is sometimes complicated due to the handset manufacturer and users routinely fall victim to fake apps that are really malware designed to control your device.

The other kind of compromise occurs in the network itself. Cell phones are divided into two main groups when it comes to communication: Global System for Mobile Communications (GSM) and Code Division Multiple Access (CDMA). The adoption of GSM far outpaces CDMA throughout the world, largely thanks to European mandates to use that technology for interoperability and independence. GSM is based on a consortium while CDMA comes from Qualcomm. Here in the US, if you have an AT&T or T-Mobile phone, you are using GSM. If you are on Sprint, Verizon or U.S. Cellular, you have a CDMA phone. This is why you will see devices branded only with certain carriers—the radio hardware is physically different. Both technologies are good for communications, but are simultaneously quite hackable.



JOE RAVI CC-BY-SA 3.0 @ WIKIPEDIA

above: A genuine cell phone tower. For less than $200, you can set up your own fake base station that mobile phones will associate with and be able to text and talk through.

Every year in August, hackers and security specialists descend upon Las Vegas for two prominent security conferences and every year, the attacks experienced have gotten more creative. Over the last five years or so, security researchers have focused on mobile technology to understand how to take advantage of its vulnerabilities. The U.S. government has done this for years at significant cost, but given that computers continue to get better, faster and smaller, it is now well within the reach of hobbyists. For less than $200, you can set up your own fake base station that mobile phones will associate with and (provided you do things properly on the backend) they will be able to text and talk through your base station. Not only can you see the traffic clearly going through your base station (unless it is encrypted like a TLS transmission or an iMessage chat), but you will be able to identify the device by ID and location.

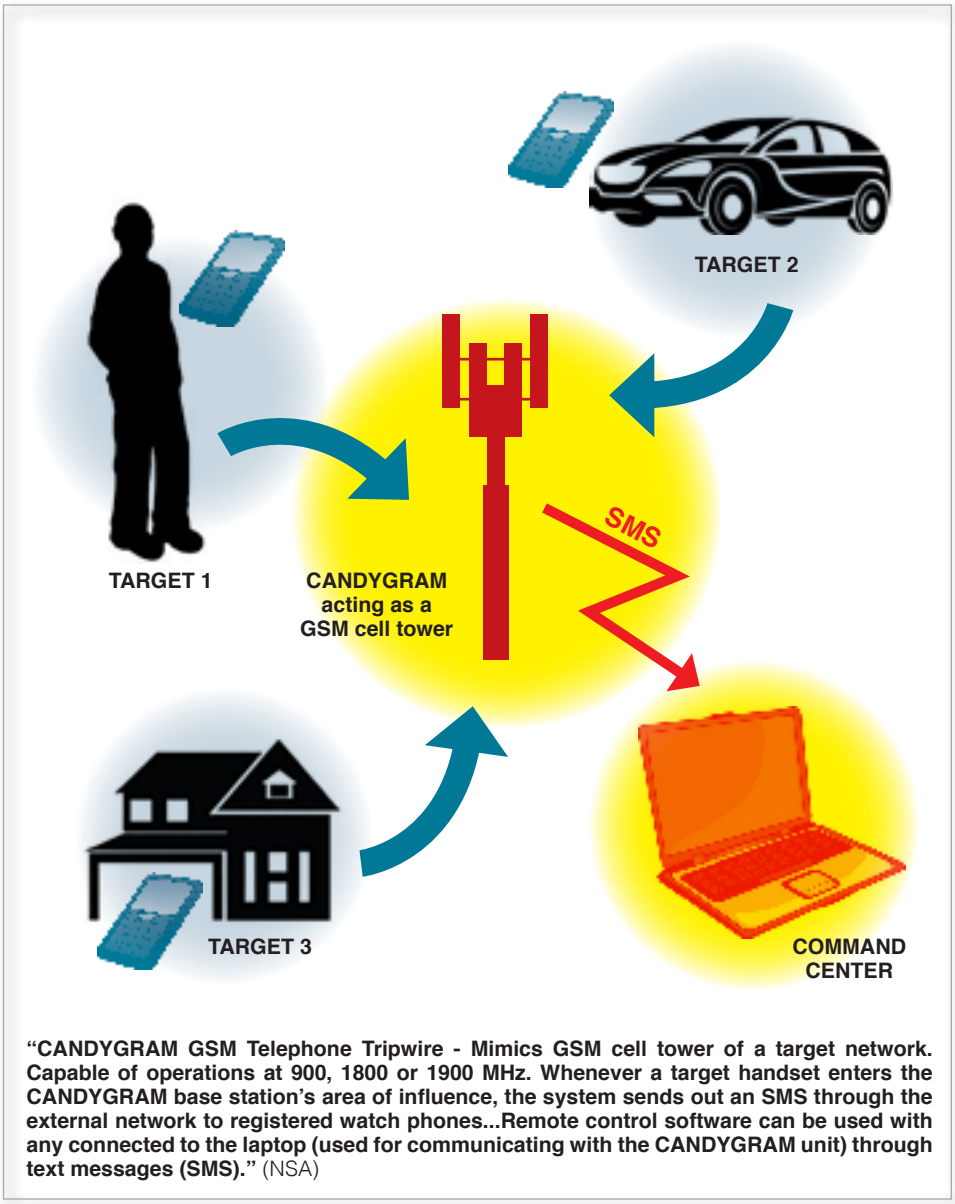
Current security research on cellular hacking comes in the form of cheap, disposable GSM phones that can be connected to a laptop via USB or via femtocells—those devices that you can get from your cell provider to boost coverage in your home. It will talk to the cell phones in range of the box and then send the calls over your broadband connection. Researchers have broken into these devices, taken control of them and looked inside the traffic going back to the provider. The devices come with a maintenance port, which allows the device to be compromised by an attacker and then inspect the data as it passes through the femtocell. Essentially, with a little bit of eBay browsing, anyone can obtain the required equipment for a fake cell phone tower.

Recently, a technology company discovered a series of fake cell phone towers in and around the Washington D.C. metro area[1]. While criminals and foreign intelligence services are possible suspects, it may be likely that U.S. government agencies are the responsible parties for these towers. There are a number of obvious uses for such towers from a surveillance perspective.

There are a number of government agencies, private corporations and individuals that could benefit from information captured from a fake cell tower. Any voice call that was not encrypted could be saved to a digital file and replayed or distributed easily. Text messages not protected by encryption are easily captured. This type of surveillance technique goes along with some of the more subtle methods of security. It's akin to a camera placed in a smoke detector near a door instead of something more overt and obvious. Companies may choose to include their own methods of using fake cell towers at their corporate campuses. Maybe it's to gather competitive information or maybe it's just used to track employee movement. Given the low cost of these technologies, it is reasonable to assume that they are widely employed.

Policing agencies around the world use these methods to track the presence and movement of devices. Are you attending a large rally? Chances are that your IMEI (or the unique device identifier for your cell phone) will be captured to note that your device was present at the rally. There is much debate possible about the propriety of governmental collection of this information, but let's consider that it would be done for legitimate forensic purposes. The goal could be that if a crime happened at the rally, devices that are not present could be more easily excluded from further investigation than those that were present.

Of course, the part we can control is what we as individuals choose to trust and why we choose to trust it. There is little reason to implicitly trust any wireless (or wired for that matter) communication method. This includes cell phones, Wi-Fi, satellite, packet radio, FRS/GRMS, and long-haul microwave communication. If you can get near or in-between the two parties, it is possible to capture the traffic. This means that if you want to keep things private, you need some kind of encryption. This can be accomplished a number of ways, but typically is based on the communication method and some additional application installed on the device. Given the number of surveillance programs currently known to the public, it's best to never trust the transport method used to get the message from point A to point B. If you are unfamiliar with the kinds of programs you can use to protect your information in transit, you can poke around on the internet for some good clues. Voice is probably the more challenging mode to do well for an average citizen, but it is possible. Text-based transmissions are trivial to encrypt, but don't forget that the provider of your products and services may be coerced or incentivized to cooperate with unwanted snoopers or even be purchased by them.

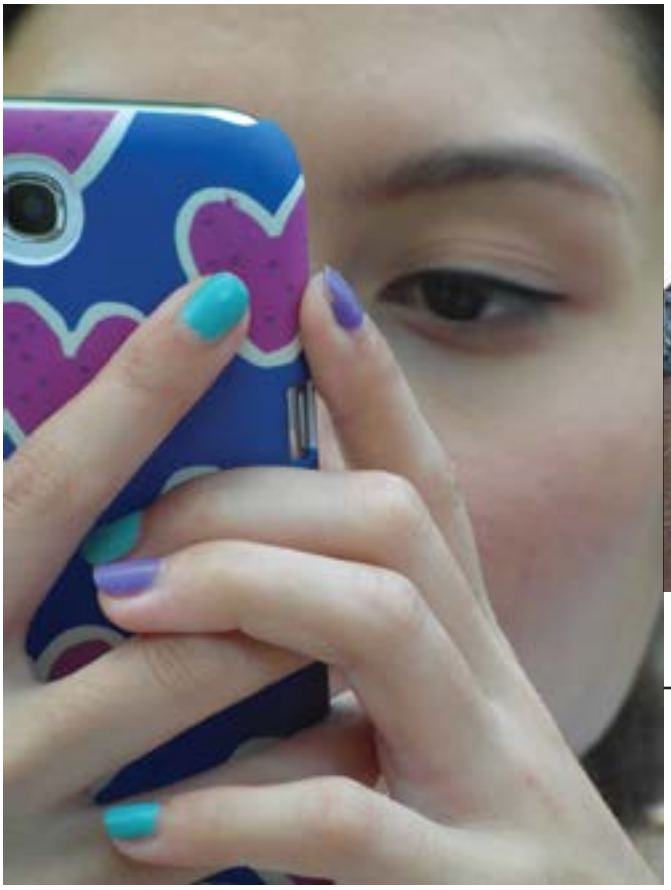


"CANDYGRAM GSM Telephone Tripwire - Mimics GSM cell tower of a target network. Capable of operations at 900, 1800 or 1900 MHz. Whenever a target handset enters the CANDYGRAM base station's area of influence, the system sends out an SMS through the external network to registered watch phones...Remote control software can be used with any connected to the laptop (used for communicating with the CANDYGRAM unit) through text messages (SMS)." (NSA)

Among the spying capabilities of intelligence services and even criminals around the world are the ability to mimic cell towers to eavesdrop on cellphone communications. The "Candygram" GSM telephone tripwire and other classified NSA network spy device documents are available on Wikipedia. Search "NSA ANT catalog."

On the issue of device tracking, if you are trying to avoid this, the best way is to just leave your cell phone at home if you are going to a place where you don't want to be tracked. If you need communication, disposable cell phones may be your only option. Just be sure to only turn it on when you need it and destroy it when you are done. Be wary of who you communicate with as broadcasting your burner number to multiple people defeats the purpose of keeping your location information private. Of course, watching a cell phone establish a pattern of movement and uncharacteristically stop, break pattern or parallel another device can be alerting too.

Ultimately, the most important lesson here is that technology is hackable, traceable and copyable. There are things you can do to make yourself safer while using these devices, but it requires consistent vigilance. It may be foolish not to assume that you are being listened to and your traffic is monitored, so take the appropriate counter measures to



GIRL WITH PHONE IANL @ FREERANGESTOCK.COM. BUILDING GEOFF TRIM @ WIKIPEDIA

above: Cell towers and cell phones are everywhere. How can you keep your communcations secure? left: If you connect to free WiFi, assume people are eavesdropping.

keep the content private. How many people do you think will go through their entire lives without being eavesdropped or spied upon at some point?

WHAT CAN YOU DO?

Cellular technology is pervasive, but there are still things you can do to improve your privacy. If you prefer not to be tracked by the signal in your cell phone, you can always buy physical burner phones and forward your number to those devices. Or better yet, just leave your device at home. If tracking of your location is not as important as the confidentiality of your communications using the phone, there are several options to assist:

Refrain from using SMS (basic text messaging that comes with all mobile phones) to send sensitive information. Instead, use something like Apple's iMessage, CyberDust or Wickr. All of these programs will do different things, but your goal is to first keep the message safe from eavesdroppers and then secondly cause messages to destroy themselves after a period of time. You can look in your phone's App store to find the one that looks best for you.

If you need a temporary number, for example to contact a buyer for an item you want to sell on Craigslist, consider using a burner app on your phone. Burner and Hushed are two that I have used with great success. Each will assign a temporary number to your phone and direct both text and voice traffic through it. These are not free, but they are very reasonably priced. When you are done, just burn the number and go.

If you connect to free WiFi, you must assume people are eavesdropping. Some apps on your mobile device will automatically encrypt their communication on the back end (as to not trust the network), but it may not be obvious to you which ones do this. If you have communications you need to keep private, then be sure you are not trusting that coffee shop network. Using the above methods will help in this situation.

Be wary of Android apps (or Cydia apps for iOS) that are not in official App stores. You may unintentionally install malware on your device that can do very bad things to your phone and your privacy.

Be sure you have two step authentication turned on for your favorite services such as Google, Facebook, LinkedIn, Twitter, and Apple iCloud. This will reduce the risk of having someone steal your credentials. In addition, use a password manager to generate random passwords for all of these services. Never use the same username/password combo twice.

Any computer you use can be compromised. The smart phone in your pocket is a computer that communicates nearly continuously with other devices and stations. Criminals, competitors, foreign intelligence services and self-serving commercial entities have already targeted you. Even unscrupulous government personnel who prefer to circumvent the 4th Amendment to The U.S. Constitution rather than go to the trouble of obtaining judicial warrants and conducting legitimate investigations into specific criminal activity (or who wish to collect your data for other reasons) have demonstrated the ability and intent to steal your data as a means of achieving their preferred end. The "rogue" cell stations discovered around Washington, D.C. serve as a warning to the prudent. Regardless of who is trying to breach your security, it is up to you to minimize your vulnerabilities to them. ✔

[1] See http://brando.ws/celltowerdc. "Tech company finds mysterious fake cell towers in DC area

BIO

Branden R. Williams (www.brandenwilliams.com) DBA, CISSP, CISM is a seasoned security executive, ISSA Distinguished Fellow, and technology consultant. Learn more about how CDMA spying works (http://brando.ws/Defcon18CellPhone), IMSI Catching (http://brando.ws/IMSI-Catching) and IMSI Privacy (http://brando.ws/IMSIPrivacy).