

Spy-Ops Advisory

CELL PHONE SECURITY THREAT

Security Risk Level

Risk = 4 Elevated

1 = low – 5 = high

Statistics:

There are an estimated 2 billion cell phones world-wide.

There are an estimated 203 million cell phones in the United States.

A recent study found that Americans average 13 talking hours a month – with the 18-24 age group averaging 22 hours.

There are an estimated 400 million cell phone users in China, making them the largest single market.

In a study conducted by MIT, the cell phones was ranked as the one invention that people hate the most, but can't live without.

A Sprint survey said that 2/3 of people used their cell phone backlight to find something in the dark.



4017 Washington Road
Mail Stop #348
McMurray, PA 15317
P 888-650-0800
F 412-291-1193

Advisory

Cell phones have become a common business tool throughout the world. The devices have significantly evolved since their introduction in the mid to late 1980s to the advanced devices we have today. But with today's advanced features comes risks. Cell phones are more vulnerable than regular phones due to three dangers: eavesdroppers can listen in on your calls, thieves can bill their own calls to your account and a stolen phone contains a large amount of data about you and your contacts (your phone book, instant messages and emails).

It is difficult to rank the threat in order of severity but, hackers, mobile keyloggers, and snoopware are all competing for the top spot. Currently there are only a few thousand examples of malicious code, exploits or malware that are used to attack cell phones. However that number is going to increase dramatically according to research by Intelomics. Generally speaking, wireless service providers have invested millions to protect the network level security with little regard for handset level security. While viruses, hacks and lost or stolen phones are the security threats that most everyone thinks about there is one other threat that has emerged more recently that is the greatest threat. What if, unknown to you someone was listening to your every word in a meeting? It can and has happened and there is no technology currently available to stop it.

Cheap prepaid cell phone are commonly used to bug a room. The prepaid phones are produced in mass, can not be traced to an owner. They are inexpensive, have an unlimited range, widely available and work really well. Our security professionals have found them hidden in decorative plants, taped under tables and other places. The microphones are good at picking up voices throughout a 14 X 16 foot room. There is a variation to this threat. A similar technique is when one of the meeting participants purposely calls another phone so that the person on the other end can listen in or even record the conversation while the other meeting participants are operating under the impression of privacy.

Another cell phone security threat emerged internationally a few years ago. It is a cell phone gun. International intelligence sources believe it is being produced in Yugoslavia and Croatia and delivered around the world. These phone guns are changing the rules of engagement for law enforcement and security professionals worldwide. In the United States, the FBI, the (ATF) Bureau of Alcohol, Tobacco and Firearms, and the

Eavesdropping: Digital cell phone transmissions are scrambled for better protection, but eavesdroppers with the right equipment may be able to unscramble them.



CELL PHONE SECURITY THREAT

U.S. Customs Service have all been briefed on the phone gun. European law enforcement officials have been stunned by the discovery of these deadly decoys. One European Law Enforcement official stated, "We find it very, very alarming," To date no known phone guns have been discovered in the United States.

But that is not the new threat either! The new threat are phones with exposed keypads and touch screens. For example, a phone placed in a purse accidentally redials the last called number and all of a sudden the people on the other end can hear everything. Chances are this has happened to you. An article in the Wall Street Journal called this the new epidemic of the cell phone age which has implications far more severe than just an annoying dead air voice mail. You have either been the recipient of a call from someone who didn't mean to call you, or your phone accidentally called someone on its own. In one online pole, 70% of respondents stated they had made at least one accidental call.

Case Example #1

This occurred in a recent call made to a CEO who had just recently purchased the new iPhone. While I am sure he meant to silence the call, he unknowingly answered his phone while in a Board of Directors meeting. One was able to hear and recognize the voices of all who spoke during the call. Topics of discussion included: all the companies financials contained on the "consolidated balance sheet" as well as discussions concerning a "stock split." Clearly this falls in the category of sensitive insider information.

Case Example #2

A voice mail to a cell phone revealed a conversation a physician was having in a hospital. The doctor obviously leaned against something and accidentally called another phone. The owner of the other phone was not available and the conversation going on between the doctor, nurse and patient went into a voicemail. Conversations recorded on the voicemail contained sensitive patient medical data that clearly would fall under Health Insurance Portability and Accountability Act (HIPAA) privacy and protection compliance.

Protection

People have always been the weakest link when it comes to security. The same applies to cell phones security. When you choose a cell phone consider the issue of an unprotected keypad and accidental calling. If there is a hard protective case, you could use that as a safety mechanism. Additionally, strategically place your phone so that the keypad is not exposed to other objects or could accidentally be struck or receive pressure. But that is no guarantee either. The best protection is to set-up the password function on your cell phone. Not every phone has the ability of being password protected, but if you do have the ability to do so, you should. While the cell phone password systems used to protect phone data are fairly easy to compromise it will help to stop the accidental dialing. There is one more approach that can be used. While attending classified meetings participants are often instructed to take the battery out of their cell phones and place them on the table in front of them. It is worth the time to prevent the security risks and embarrassment of accidental dialing.

Cell Phone Gun: At first sight you would think it is a regular cell phone. It is the same size, same shape, same keypad, same overall appearance. But you may be dead wrong. Beneath the face of the cell phone lies a .22-caliber pistol. The phone gun is capable of firing four rounds in quick succession with a touch of the standard keypad.

These are illegal in most places.

