Are cell phones safe?

H. B. Wolfe
University of Otago, New Zealand

Abstract

We take for granted every day that we are safe from any given risk because we are protected by various standards, statutes, and laws. The cell phone has become ubiquitous and is currently being used by more than 5 billion people around the world. It is really nothing more than a small computer with a radio transmitter and receiver integrated into it. Newer phones may also record photos, videos and sound. Some have a built in Global Positioning Satellite System capability providing the ability to track the phone's physical location. Every generation of cell phone has expanded its capabilities and we are now able to communicate with the Internet in addition to normal telephone activity.

Along with these capabilities come a number of risks. Some of these are normally associated with using the Internet exposing users to malware of various kinds. However, there are other more insidious risks that are less known. This paper will discuss all of the risks associated with cell phone use including malware; loss, theft, and seizure; communications interception and loss of privacy; location logging and tracking; and bugging. Most people are not aware of these threats and believe that their service provider has put in place measures to eliminate any risks as well as protecting their privacy by the use of cryptography. While there can never be 100% safety, the accompanying discussions will cover mitigating alternatives that can be put in place to reduce the identified cell phone risks.
Keywords: data encryption, mobile phones, triggerfish, Bluetooth.

1 Introduction

In 1968 Joseph Licklidder [1], sometimes referred to as the "father of the Internet" said "In a few years, men will be able to communicate more effectively through a machine than face to face." The mobile phone is an embodiment of that forecast. Mobile phones, cell phones, personal data assistants (PDA), smart

WIT Transactions on the Built Environment, Vol 117, © 2011 WIT Press
www.witpress.com, ISSN 1743-3509 (on-line)
doi:10.2495/SAFE110061

phones and other types of digital phones with a broad range of functions are referred to in this publication as "mobile phones".

Mobile phones are ubiquitous. Children and young adults have them. Out of a global population of 6.9 billion people, according to a BBC report [2], there are 5 billion mobile phone connections worldwide. Most users of mobile phones are not aware that there is any security risk to using these devices. To put it simply, mobile phone security is far outweighed by the convenience the mobile phone provides. Many mobile phone users think that nothing untoward could ever happen to them so they are safe using their mobile phone. That may or may not be true but it really depends on the potential prize at stake. An average person who uses their mobile phone many times throughout each day has what might be considered a very small prize. For those who are famous, rich, or powerful or whose prize is important enough (for whatever reason) to devote the time and resources to make a concerted attack, there are real risks to face. The real risk is always tied to the prize at stake. Once again even these folks do not realize that there is any real risk to them.

The content of this paper documents and explores several vulnerabilities that mobile phone use brings to the user. Exploitation of the vulnerability will be explained and examined. And finally, the risk factor – the probability of a concerted attack will be considered. This is not intended to be an anti-mobile phone exposé. The writer's objective is to describe and document real vulnerabilities that pose real threats to all mobile phone users.

Searching the available literature did not provide much in the way of mobile phone security references. Most are singular in their nature, several cited in the accompanying references, focusing on only one aspect of mobile phone vulnerability. The one publication that stands out is *Hacking Mobile Phones* [3]. While there appears to be other literature scheduled for future publication, this seems to be the only current publication that brings together, in a single document, a group of identified vulnerabilities. The risks and vulnerabilities described in this paper are not meant to be all encompassing.

The following is a partial list of mobile phone vulnerabilities:

2 Interception of communications

Mobile phone communication is nothing more than radio technology, every conversation can be intercepted. There is nothing to prevent interception. What remains is the privacy of the content. If strong encryption (a definition may be found in the Glossary) were used and forced on every communication this weakness could be avoided. However, encryption is left in the hands of the service provider. They choose the algorithm and decide as a matter of course when encryption can be used and when it cannot. For example, in some systems communications between a mobile phone with another mobile phone in one of the four countries currently designated as "State Sponsors of Terrorism" by the U.S. Department of State (Syria, Cuba, Sudan, and Iran) the encryption feature is automatically turned off. It has been shown that this option can be exploited

using the man in the middle attack [4] to turn off the encryption feature between users not in the four designated countries as well.

Security and privacy offered by mobile phone service providers has not kept up with the many uses that these devices have been put to. In the 1990s it was proven by Wagner, Goldberg, Biryukov, Shamir and others that cryptographic methods used by various well known service providers did not in fact offer strong protection to the privacy of subscribers. For example encryption algorithms used by GSM were proven to be deliberately weakened [5]. This discussion will not delve into the reasons for weakening mobile phone security. The important point to be made is that any conversation or text message transmitted by a mobile phone can be intercepted, and the encryption provided by the service provider can be overcome.

Legal interception in the form of wire taps is usually done at the cell site, private branch exchange or at the public switched telephone network. There is nothing to stop this except local law. Laws are broken often and in the US and other countries this sort of tap is done by Government agencies as a matter of course - without any warrants. For example the US Restore Act of 2007 [6] formally authorizes this and was upheld in a Federal appeals ruling 15 January 2009. In today's world a terrorist is defined by politicians and that definition is a moving target. The decision to use a mobile phone should include consideration of what is to be stored there and the potential risk of the exploitation of that information.

3 Loss, theft or seizure

Any mobile phone that falls into the hands of a person with or without the owner's authorization and/or knowledge may be exploited. Information that has been stored on it may become available to that person. Access to a mobile phone may be gained in any of several ways – some are inexpensive and some are not.

One example (an expensive one) of a generalized mobile phone forensics tool – is the *Cellebrite UFED* [7]. This tool captures seven different types of data residing on more than 2,000 different mobile phone models. This includes the content of all text messages sent and received, video clips and images taken with the mobile phone's camera, contacts list, call logs, audio files and ring tones. It may be used as an investigative tool and forensics tool. It is possible to store further information on the mobile phone that this model of *Cellebrite* cannot extract. There are other specialized tools and techniques that enable the remaining information to be viewed and analyzed.

Mobile phones and the data stored on them may be protected by the use of passwords, however, with a little bit of ingenuity, these can often be compromised. Many phones have the capability of storing much more information than just the seven named data types. Mobile phones are often used for storing information of a personal nature such as bank account numbers, credit card account numbers, PINs, and computer logon information. If the phone is capable of Internet interaction, then browsing history and emails will be stored

there. Significant amounts of identity information can be stored on an individual's mobile phone as well.

Information found on mobile phones can be used to facilitate identity theft, privacy infringement, compromise and theft of personal information, compromise of emails, and compromise of Internet use by an unauthorized user so inclined. Identity theft is the fastest growing Internet crime. The US Postal Inspection Service [8] estimates that as many as 9.9 million Americans had their identities stolen last year. The stolen identity is used for credit card fraud, phone or utilities fraud, bank or finance fraud, official documents fraud, and other types of fraud. Recovering from identity fraud is not an easy task. According to the Identity Theft Resource Centre, the "average victim spends 607 hours and averages $1,000 just to clear their credit record".

Third party encryption products are one method of protecting personal information on a mobile phone. If the data stored becomes accessible to an unauthorized person, they would have to "break" the code. If strong encryption is used then the probability of this occurring is dramatically reduced.

Another method is to use the mobile phone only as a phone and store nothing of a personal nature on it. However, many people generally want one tool to perform all of their electronic communications, manage their life, and provide entertainment, with little consideration of the risks to their personal and business lives.

Mobile phones are being used in place of airline paper boarding passes and tickets [9]. Visa (the credit card company) is trialling the mobile phone as a credit card in Turkey [10]. Merchants can process a transaction on their mobile phones [11]. The more uses that these devices are put to, the more attractive it will be for the bad guys to discover new vulnerabilities to be exploited.

4 Location logging and tracking

Service providers track mobile phones. As a service provider, it makes sense to do this in order to manage their service. Network analysis requires this activity in order to recognize any specific cell station overload. Information captured for this purpose may provide an indicator to service providers for the need to improve network capability.

The fact that your mobile phone is being continuously tracked may be of interest to other people. It violates your privacy only if this tracking information becomes available to persons outside the network provider for uses other than network analysis. It may, in some jurisdictions, be illegal for a network service provider to disclose this information without a warrant or subpoena. Although, anecdotally a few dollars in the right pocket can often produce the desired results. GPS technology is not required to enable tracking. GPS is becoming a normal function of the newer smart phones. That information can be extracted through other means on mobile phones with the GPS capability.

An effective way to stop your physical movement being tracked using your mobile phone location data or internal GPS is to turn your mobile phone off and remove the battery as well. On a few phones, turning it off merely puts it into

"sleep" mode that can be reactivated externally. However, on some phones removing the battery is either impossible or so difficult as to make it impossible. In those cases, products [12] are available that will insulate the phone (like a Faraday cage) so that no signal will escape from the user's phone nor be received by the user's phone.

Law enforcement has developed technology that enables the tracking of a targeted mobile phone, interception of its communications, and enables the mobile phone to become a listening device – a bug. This is known as Triggerfish [4] is type of surveillance is done as a matter of routine in America without the requirement of having to present evidence of probable cause to a judge who, if convinced, would issue a warrant that specifies who, what, when, where, and for how long the specified target may be placed under surveillance.

The principals of Triggerfish technology are freely available to anyone who has the resources and determination to accomplish the same functionality. One method is to build or buy an IMSI (International Mobile Subscriber Identity) catcher [13]. This is used for capturing GSM mobile traffic in limited circumstances. Then the decision becomes whether the target is worth pursuing. (Like many surveillance devices this may be illegal in some jurisdictions.)

5 Bugging

All mobile phones do not have identical capabilities. It is possible on some mobile phone brands to call and answer the phone without causing it to ring or react in any overt way. This presents a challenging risk. If you were in confidential or important high level negotiations, and a mobile phone were able to be silently activated, whoever modified the mobile phone could activate that phone from outside the room and listen in at will. The opportunity to discuss the progress of negotiations could be clandestinely listened to by the opposition. This "feature" could be used in many ways to disadvantage a person or parties. The matter of legality will not stop someone who is determined to find out information to raise their advantage. It is strongly recommended that you protect private conversations where mobile phones are present.

One method of protecting private meetings is signal blocking where mobile phones may be present. These devices are illegal in some jurisdictions. However, if they are not illegal in the jurisdiction where you are working, they can be used to secure a room or location where sensitive meetings take place. One version even has a remote control to turn it on and off and is ideal for use in sensitive areas. Signal blockers or jammers broadcast a strong jamming signal on various signal bands that interferes with the phones ability to connect to the mobile phone network.

The "roving bug" is used by law enforcement to intercept normal conversations [14]. This technology enables the person performing the surveillance to remotely activate the microphone on the targeted mobile phone. This allows the mobile phone to be used as a listening device to hear what is going on in the immediate vicinity of the activated phone. This capability is a part of Triggerfish technology [4]. The best protection from this sort of

surveillance is to remove the battery from the mobile phone or insert it into a protective pouch when it is not needed.

6 Targeted data acquisition

Mobile phones are frequently used to access the Internet. As mentioned, they also store personal information such as passwords, encryption keys, bank account numbers, credit card numbers, PIN numbers, and computer logon details. Most new phones come with Bluetooth functionality. This allows the user to communicate wirelessly with their computer or other devices. This feature provides a convenient way to back up your contact lists and other information. The attack is called Bluetooth Slurping.

If Bluetooth is enabled as the default or left active after the download and backup procedures it is possible to access it. At this point anyone with the appropriate gear such as the *BlueSniper Rifle* [15] can detect enabled Bluetooth, connect to the mobile phone, and download the entire contents of the targeted mobile phone for their own use from a distance (up to a mile and potentially beyond – without the owner's knowledge). In many jurisdictions it is illegal to do this; however, that may or may not be a deterrent. Mobile phone users should understand that this feature MUST be turned off when not in use.

7 Spam, viruses, malware, etc.

Most mobile phones are now Internet compatible. This opens the device to all types of malware found on the Internet. Anti-malware applications specifically for mobile phone use are available in the marketplace and should be used as a matter of course. However, this software is not standard and not compatible with many mobile phones. This is an area that will develop in the future – particularly since there is such a fruitful and unaware target audience. About 20% of all cell phone apps contain malicious code [16]. It cannot be detected by anti-malware software. In one case, "Jackeey Wallpaper, collects your phone number, subscriber identification, and other things and reports this information back to www.imnet.us. That site is evidently owned by someone in Shenzhen, China." [17]. If you decide to download an app just remember that once it is installed it may be reporting your details to its master. Do you want that? When it asks you for access to your personal details just say no.

Using Twitter and other social networking sites can make stalking possible [18]. This can be done where geotags are active on tweets and photos. Tools are available (Reaper and Stalker for example) that can extract longitude, latitude and time from data streams. That information tells the tools' user where the targeted mobile phone is (within about 15 feet) and when. That information could make it possible to easily stalk someone. Images posted to the various social networking sites may provide incite for someone with criminal intent to know what assets of interest are located where. Instructions [19] for disabling the photo geotag function on iPhone, Blackberry, Android and Palm devices can be found on http://icanstalku.com.

Some mobile phones, in an attempt to prevent viruses and Trojans, wall off various mobile phone features. A program called Soundminder [20] is capable of listening to the mobile phone's microphone for credit card numbers. It "parses the audio file, interprets the numbers, and sends them to another app that passes them on to a remote server". Mobile phones are not secure…..

8 How can users better protect themselves

This paper has discussed various vulnerabilities and potential threats. These threats originate from different sources. Risk is the probability that any one or more of the vulnerabilities discussed is exploited against you, the user.

There are certainly random risks. Most of these are from the Internet. Therefore, the user should install mobile phone specific anti-malware software to protect from some threats. Using the mobile phone wisely can also reduce risk. By making use of third party encryption products the risk of your communications being exploited by someone who is eavesdropping on your calls and texts can be mitigated. If you insist on storing sensitive personal information on your mobile phone, then the use of a third part encryption product can prevent an unauthorized person who has gained access to that information from being able to make any use of it.

When considering targeted risk, the important issue is to think about the prize available to a potential attacker. Are you a controversial person? Are you famous or rich? Are you engaged in illegal activities? Are any of your close friends engaged in illegal activity? Do you have any obsessive enemies? In each case, the prize will vary in its attractiveness to a potential attacker.

On the other hand, if you are careful about your privacy, then you might want to take precautions and protect your mobile phone usage with the suggested procedures and security measures discussed in this paper.

9 Summary

In summary, the suggested measures include:

- Protect your communications by using a third party strong encryption product.
- Be mindful of your phone's location to minimize the opportunity of it being stolen or lost.
- Remove the mobile phone battery or place it inside a purpose protective envelope (Faraday cage) when you do not want your movements tracked.

- Remove the mobile phone battery or place it inside a purpose protective envelope (Faraday cage) to protect against being bugged by "roving bug" technology.

- Protect your personal data by using a third party strong encryption product.

- Disable Bluetooth to protect against the compromise or copying of data on your phone.

- Use an anti-malware product to protect yourself from Internet attackers.

- Remember, an analysis of 300,000 free apps showed that 23% of iPhones and 47% Android apps use third party code that may be interacting with user information – don't download them or say no when you are queried for personal information at installation time [16].

10 Conclusions

An overarching philosophical concept can be characterized by the phrase "if you don't have anything to hide, then you won't have anything to worry about". This is an invalid argument by those with an agenda of stealing your privacy and/or identity. This is why:

- **It is a faulty assumption that privacy is about hiding "bad" things.**

- **The argument's premise is about "hiding a wrong".**

- **It is a faulty assumption about privacy and its value – that privacy has no value.**

- **Collection of random information about individuals is referred to as surveillance.**

- **Constant surveillance has a chilling effect on public discourse, freedom of thought, freedom of association, and freedom of action.**

- **It wrongly assumes that everyone is guilty of something.**

On December 10, 1948 the General Assembly of the United Nations adopted and proclaimed the *Universal Declaration of Human Rights* [21]. Article 12 enshrines every person's right to privacy. Why would anyone want their movements tracked and recorded? This is simply not about having anything to hide. This is purely about the individual's human right to privacy.

Mobile phones are not secure. They can be attacked and used in many ways not normally considered by users. This paper has explored some vulnerabilities, explained how they may be exploited, and described what the real risk is to the mobile phone user. Finally, it offers preventative measures to mitigate the real and suggested risk to any given mobile phone user.

11 Glossary

A vulnerability is a flaw or weakness in the design or implementation of hardware, software, networks, or computer-based systems, including security procedures and controls associated with the systems. Vulnerabilities can be intentionally or unintentionally exploited to adversely affect an organization's operations (including missions, functions, and public confidence), assets, or personnel.

A threat is any circumstance or event with the potential to intentionally or unintentionally exploit one or more vulnerabilities in a system, resulting in a loss of confidentiality, integrity, or availability. Threats are implemented by threat agents. Examples of threat agents are malicious hackers, organized crime, insiders (including system administrators and developers), terrorists, and nation states.

A risk is a combination of the likelihood that a particular vulnerability in an organization's systems will be either intentionally or unintentionally exploited by a particular threat agent and the magnitude of the potential harm to the organization's operations, assets, or personnel that could result from the loss of confidentiality, integrity, or availability.

Man in the middle attack is a form of eavesdropping where the attacker is able to make independent connections to the victims and relay messages between them. The attacker may inject or delete messages at will. The two victims believe that they are talking directly to each other over a private connection, however, the attacker actually controls their communication.

A **geotag** consists of the geographic coordinates of where a mobile phone with a GPS capability is at any given time. These tags (longitude – geo:lon and latitude – geo:lat) are attached to photos (JPEG files) at the time the photo is taken, SMS messages, and other files.

Strong Encryption is an encryption method that has been vetted by the cryptographic community and found to be without any flaws that could be exploited. Once this attribute is proven, then the size of the keys define the key space and how long it would take to derive the keys for any given message by the use of a brute force attack. A brute force attack tests each key for that entire key space – one at a time. The size of the key space can make encryption strong if the time necessary to carry out a brute force attack will not produce a result in a useful timeframe. For example: the International Data Encryption Algorithm (IDEA) has been in the public arena for twenty years having been repeatedly analyzed and tested. It is considered to be a strong encryption algorithm and it has a key space of 2128 – that equates to the number 340 with 36 zeros after it – or more than all of the atoms in the known universe. No computer in existence

today or considered possible in the foreseeable future could step through that number of keys in anything less than millions of years.

References

[1] Licklider, J.C.R. and Taylor, Robert S., *The Computer as a Communications Device, Science and Technology*, No. 76, April 1968, pp 21-31.

[2] BBC, *Over 5 billion mobile phone connections worldwide*, 9 July 2010, http://www.bbc.co.uk/news/10569081

[3] Fadia, Ankit, *Hacking Mobile Phones*, Thomson Course Technology PTR, Boston, Massachusetts, 2006, ISBN: 1-59863-106-3.

[4] US Justice Department, *Electronic Surveillance Manual*, June 2005, Triggerfish – technology that poses as a cell tower – also known as cell-site simulator it also uses a digital analyzer. This technology tricks mobile phones into sending their serial numbers, phone numbers and other information to the person using such technology. See the US Department of Justice's at: http://www.justice.gov/criminal/foia/docs/elec−sur−manual.pdf

[5] Biham, Eli & Dunkelman Orr, *Cryptanalysis of the A5/1 GSM Stream Cipher*, Progress in Cryptology – INDOCRYPT 2000, Bimel Roy & Eiji Okamoto – editors, Springer, India, December 2000, ISBN: 3540414525.

[6] US Restore ACT – HR-3773, aka: *Responsible Electronic Surveillance That is Overseen*, US Government Printing Office, 2007.

[7] Cellebrite *Universal Forensics Extraction Device* system real time mobile forensics, extracts information from 95% of all cellular phones, http://www.cellebrite.com/forensic-products/ufed-standard-kit.html

[8] US Postal Inspection Service, *Identity Theft is America's fastest-growing crime*, http://postalinspectors.uspis.gov/investigations/MailFraud

[9] Milward, David, *Paper boarding pass set to disappear*, 15 July 2010, From the Internet: http://www.telegraph.co.uk/travel/travelnews/7892577/Paper-boarding-pass-set-to-disappear.html

[10] Economic Times, *Your mobile phone can also be a credit card*, 27 August 2010, From the Internet: http://economictimes.indiatimes.com

[11] Sweezey, Timothy, *About Mobile Phone Credit Card Processing*, 7 January 2010, From the Internet: http://ezinearticles.com/?About-Mobile-Phone-Credit-Card-Processing&id=3538398

[12] Identity Stronghold, markets the *Cell Phone Stronghold Bag*, among other things, for mobile phones that do not allow battery removal. http://www.idstronghold.com/Cell-Phone-Stronghold-Bag

[13] Strobel, Daehyun, *IMSI Catcher*, Chair for Communications Security, Ruhr-Universität Bochum, 13 July 2007, From the Internet: http://www.crypto.rub.de/imperia/md/content/seminare/itsss07/imsi_catcher.pdf

[14] McCullagh, Declan, *FBI taps cell phone mic as eavesdropping tool*, ZDNet News, 1 December 2006, from the Internet: http://news.zdnet.com/2100−1035_22-150467.html

[15] Cheung, Humphrey, March 08, 2005, *Bluesniper* – a device designed to target and capture data from Bluetooth enabled mobile phones from a distance of a mile or more. Plans in two parts available from the internet - Parts 1 and 2: http://www.smallnetbuilder.com/content/view/24228/98/
[16] Weinschenk, Carl, *Apps, App Stores and Security*, the IT Business Edge, 28 July 2010, see: http://www.itbusinessedge.com/cm/blogs/weinschenk/
[17] Takahashi, Dean, *Updated: Android wallpaper app that takes your data was downloaded by millions*, 28 July 2010, From the Internet: http://venturebeat.com/2010/07/28/android-wallpaper-app-that-steals-your-data-was-downloaded-by-millions/
[18] Greenberg, Andy, *Researchers Show How Twitter*, Twitpic Make Stalking Simple, 19 July 2010, http://blogs.forbes.com/firewall/2010/07/19/researchers-show-how-twitter-twitpic-make-stalking-simple/
[19] Whisper, *Warning issued about camera phone pictures and GEOTags*, 5 September 2010, http://www.shoutingquietly.com/index.php/2010/09/05/geotags/
[20] Greenberg, Andy, *Researchers' Android Trojan Can "Hear" Credit Card Numbers*, 19 January 2011, http://blogs.forbes.com/andygreenberg/2011/01/19/researchers-android-trojan-can-hear-credit-card-numbers/
[21] United Nations General Assembly adopted and proclaimed the *Universal Declaration of Human Rights* on December 10, 1948. Article 12 says: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." http://www.un.org/Overview/rights.html