

# **THE TSCM JOURNAL**



*Dedicated to fostering knowledge, excellence and TSCM professionalism*

Vol. 1, No. 2

ISSN 1176-7774

## Mobile Phone Security




Special Edition

Published by the Alpha-Omega Group, S.A.  
Dunedin, New Zealand  
Copyright February 2010  
ISSN 1176-7774



*Created and Developed*  
*by*  
*Dr. Henry B. Wolfe*


This document was produced with the intent of identifying and describing mobile phone vulnerabilities not found elsewhere in a single source. It describes the resulting threats and then offers measures that will mitigate those threats. The objective is to inform users of the very real and present risk associated with mobile phone use and offer some practical advice as to how those risks can be reduced.



**Henry B. Wolfe**  
*Chairman*

*P.O. Box 6079,  
Dunedin,  
New Zealand*

*Tel/Fax: +64 3 473-7295*



**HENRY B. WOLFE**  
*PhD, FNZCS  
Associate Professor  
Computer Security & Forensics*

*Department of Information Science  
School of Business  
Corner of Clyde & Union Streets  
PO Box 56, Dunedin  
New Zealand.*

Tel 64 3 479 8141  
Fax 64 3 479 8311  
Email [hwolfe@infoscience.otago.ac.nz](mailto:hwolfe@infoscience.otago.ac.nz)  
Web [www.otago.ac.nz/business](http://www.otago.ac.nz/business)



By Dr. Henry B. Wolfe

## Introduction:

Joseph Licklider (Licklider & Taylor, 1968) 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 phones and other types of digital phones with a broad range of functions are referred to in this paper as “**mobile phones**”.

Mobile phones in recent years have become ubiquitous. Children and young adults have them. Out of a global population of 6.8 billion people, according to Scott Davis (Davis, 2008) there are 3.3 billion mobile phone users. 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. 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 consequences. An average person who uses their mobile phone many times throughout each day has what might be considered a very small prize at stake. 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. Once again even these folks do not realize that there is any real risk to them.

This paper 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 aim is to illuminate real vulnerabilities that pose real threats to all mobile phone users.

The literature review 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* by Ankit Fadia. 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 the identified vulnerabilities. However, these are only a subset of what is covered here.

## Mobile Phone Vulnerabilities:

The following is a partial list of mobile phone vulnerabilities:

### 1. **Interception of communications**

Since the 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 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) automatically turns off the encryption feature. It has been shown that this fact can be exploited using the *man in the middle attack* (Justice Department, 2005) to turn off the encryption feature between users not in the seven countries as well.



Unfortunately, the security and privacy offered by mobile phones has not kept up with the many uses that these devices have been put to. In the 1990s it was proven 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 (Biham & Dunkelman, 2000). This paper 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 in such a way that mobile phone communications can be listened to and recorded.

Wire taps are 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 this sort of tap is even done by Government agencies as a matter of course - without any warrants (the Restore Act of 2007 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 about what is to be stored there relative to the user's knowledge of potential risk and their anxiety about exploitation of that information.

## **2. Loss, Theft or Seizure**

If your mobile phone falls into the hands of another, information that you have stored on it may become available to that person. There are several ways to gain access to a mobile phone – some are cheap and some are expensive.

The *Cellebrite UFED* is one example of a generalized forensics tool and an image of its associated report is located in *Appendix A*. This device 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 the *Cellebrite* in its present form cannot extract. However, that information can be viewed and analyzed by using other forensics tools and techniques.

Passwords may be used to protect this information, 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. People use their mobile phones for storing information of a personal nature such as bank account numbers, credit card account numbers, PINs, and computer log on information. If the phone is capable of Internet interaction, then browsing history and emails will be stored there. A significant amount of identity information can be stored on an individual's mobile phone.

Availability of 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.

One method of protecting personal information on a mobile phone is to use third party encryption products. 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, 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.



### 3. Location Logging and Tracking

Mobile phones are easily tracked by service providers. 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 for the need to improve network capability.

However, 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 or disclosure results. *GPS technology is not required to enable tracking.*

The only way to avoid the tracking of your physical movement being tracked using your mobile phone location data is to turn your mobile phone off and remove the battery as well. On a few phones, turning it off merely puts into “sleep” mode that can be reactivated externally.

An overarching 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.

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

This is a 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 (Justice Department, 2005). This 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.

While *Triggerfish* may refer to law enforcement’s technical capability, the principals of this 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 (Strobel, 2007). 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 your jurisdiction.





#### 4. Bugging

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, the opposition may leave the room (leaving a mobile phone there) and activate their phone from outside the room. 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 consideration that it might be illegal will not stop someone who is determined to find out information to raise their advantage. It is strongly recommended you protect private conversations where mobile phones are present.

Signal blocking is one method of protecting private meetings where mobile phones may be present. *Appendix B* contains an example of a mobile phone blocker. 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. The version in *Appendix B* has a remote control to turn it on and off and is ideal for use in sensitive areas. These devices broadcast a strong jamming signal on various signal bands to interfere with the phones ability to connect to the mobile phone network, therefore, making the phone think there is no service coverage.

Law enforcement makes use of what has been termed a “roving bug” (McCullahgh, 2000). 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 targeted phone. This capability is a part of Triggerfish technology (Justice Department, 2005). The best protection from this sort of surveillance is to remove the battery from the mobile phone when it is not needed.

#### 5. Targeted Data Acquisition

**Bluetooth slurping:** 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 phones. This feature provides a convenient way to back up your contact lists and other information.

The risk lies where Bluetooth is enabled as the default or left active after the download and backup procedures. At this point anyone with the appropriate gear such as the BlueSniper Rifle (see *Appendix C*) for example (Cheung, 2005) can detect enabled Bluetooth, connect to the mobile phone, and download the entire contents for their own use from a distance (up to a mile and potentially beyond). In many jurisdictions it is illegal to do this; however, that may or may not be a deterrent. So for the general mobile phone user it is time to understand this feature MUST be turned off when not in use.

#### 6. Spam, Viruses, Malware, etc.

Current mobile phone technology is 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 many mobile phones. This is an area that will develop in the future – particularly since there is such a fruitful and unaware target audience.



## 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 and/or not storing personal data, the risk of being exploited by an unauthorized person who has gained access to information on your phone can be reduced.

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 or just paranoid, then you might want to take precautions and protect your mobile phone usage with the suggested procedures and security measures discussed in this paper.

In summary the suggested measures includes:

- **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 when you do not want your movements tracked.**
- **Remove the mobile phone battery to protect against being bugged by "roving bug" technology.**
- **Protect your personal data using a third party strong encryption product.**
- **Disable Bluetooth to protect against the compromise of data on your phone.**
- **Use an anti-malware product to protect yourself from Internet attackers.**

## Summary:

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.

## 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.

**Strong encryption** refers to using an encryption/decryption algorithm that cannot be broken by any means within a timeframe that would enable the breaker to take advantage of the information that is within the encrypted file.

## References:

- 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.
- 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:  
Part 1 -- <http://www.smallnetbuilder.com/content/view/24256/98/>  
Part 2 -- <http://www.smallnetbuilder.com/content/view/24228/98/>
- Davis, Scott, *Mastering Grails: Grails and the Mobile Web*, 17 June 2008, From the Internet:  
<http://ibm.com/developerworks/java/library/j-grails06178/>
- Fadia, Ankit, *Hacking Mobile Phones*, Thomson Course Technology PTR, Boston, Massachusetts, 2006, ISBN: 1-59863-106-3.
- 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>
- Licklider, J.C.R. and Taylor, Robert S., "the Computer as a Communications Device", *Science and Technology*, No. 76, April 1968, pp 21-31.
- McCullagh, Declan, *FBI taps cell phone mic as eavsdropping tool*, ZDNet News, 1 December 2006, from the Internet: [http://news.zdnet.com/2100-1035\\_22-150467.html](http://news.zdnet.com/2100-1035_22-150467.html).
- Strobel, Daehyun, *IMSI Catcher*, Chair for Communications Security, Ruhr-Universität Bochum, 13 July 2007.
- Universal Declaration of Human Rights*, adopted and proclaimed on December 10, 1948 by the General Assembly of the United Nations. *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>





## Appendix A:

The Cellebrite in use – capturing the contents of a Blackberry<sup>1</sup>



<sup>1</sup> <http://www.cellebrite.com/The-Cellebrite-UFED-Universal-Forensics-Extraction-Device.html>



**Example Cellebrite Report**

The screenshot shows the UFED Report Manager interface. The title bar reads 'UFED Report Manager - (Untitled content pack\*)'. The menu bar includes 'File', 'UFED', 'Tools', and 'Help'. The toolbar contains icons for 'New', 'Open', 'Save', 'Settings', and 'Read UFED'. On the left is a sidebar with icons for 'Optional Information', 'Report', 'Contacts (194)', 'SMS (1151)', 'Calls log (740)', 'Images (92)', 'Videos (1)', 'Audio (59)', and 'Ringtones (0)'. The main content area is divided into three sections:

### Examination Report Details (manually entered)

Case / File Number (Manually entered):	0001
Examiner's Name (Manually entered):	[Redacted]
Department (Manually entered):	Information Science
Location (Manually entered):	Dunedin
Notes (Manually entered):	Blackberry

### Phone Examination Report Properties

Selected Manufacture:	Blackberry
Selected Model:	Blackberry 8900 Curve
Detected Model:	8900
Revision:	4.6.1.133
IMEI:	[Redacted]
Manufacturer Code:	262616D9
Extraction start date/time:	21/09/07 11:41:20 AM
Extraction end date/time:	21/09/07 12:09:08 PM
Connection Type:	USB Cable
UFED Version:	Software: 1.1.1.7 UFED , Full Image: 1.0.2.2 , Tiny Image: 1.0.2.1

### Phone Examination Report Index

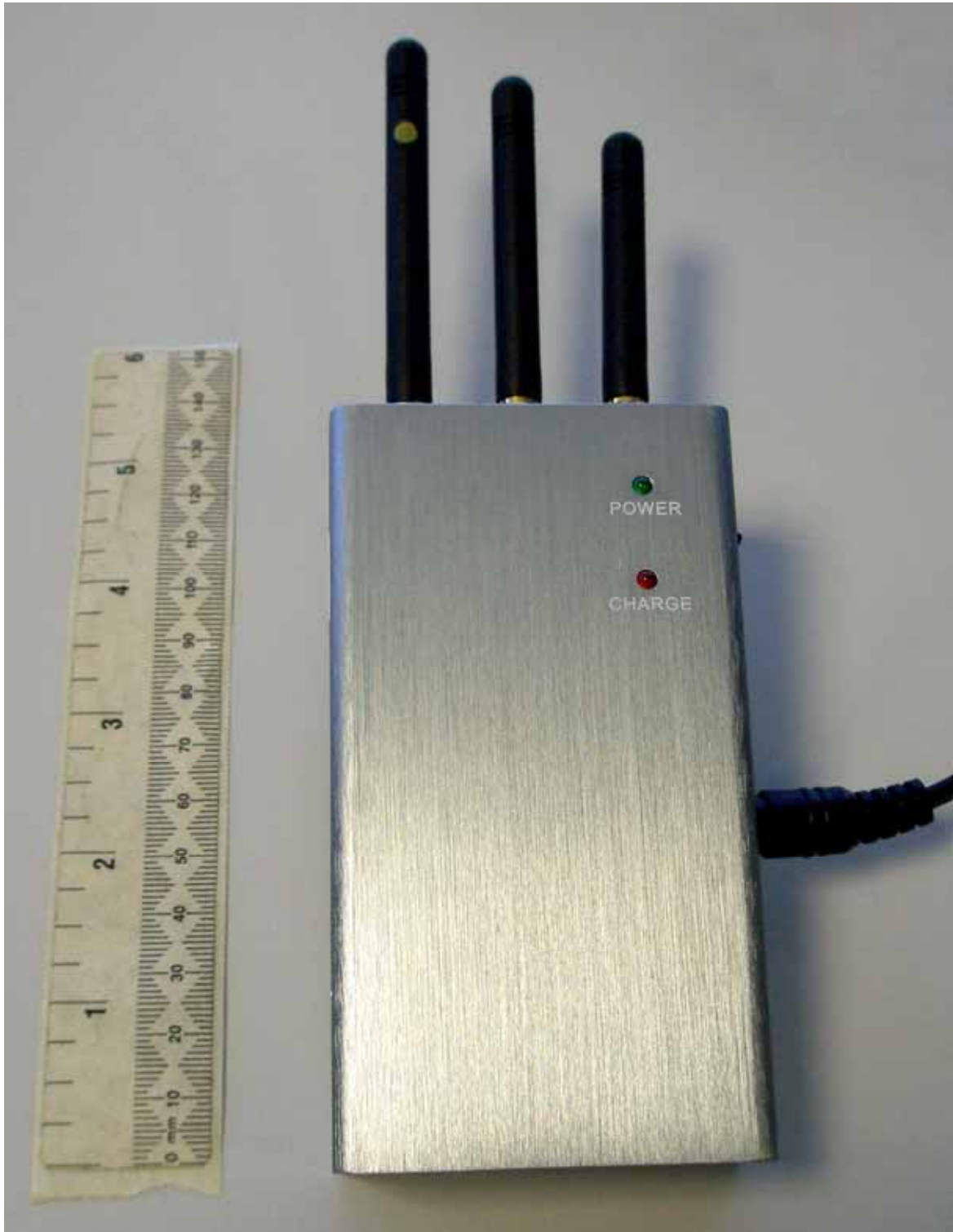
<a href="#">Contacts</a>	Selected
<a href="#">SMS - Text Messages</a>	Selected
<a href="#">Call Logs</a>	Selected

There are seven different categories of data captured by the *Cellebrite* in logical mode. Each can be of use in different circumstances. For example all images photographed by the phone's camera are clearly visible. All text messages are in the clear and each may be read easily. This provides an important investigative capability.



## Appendix B:

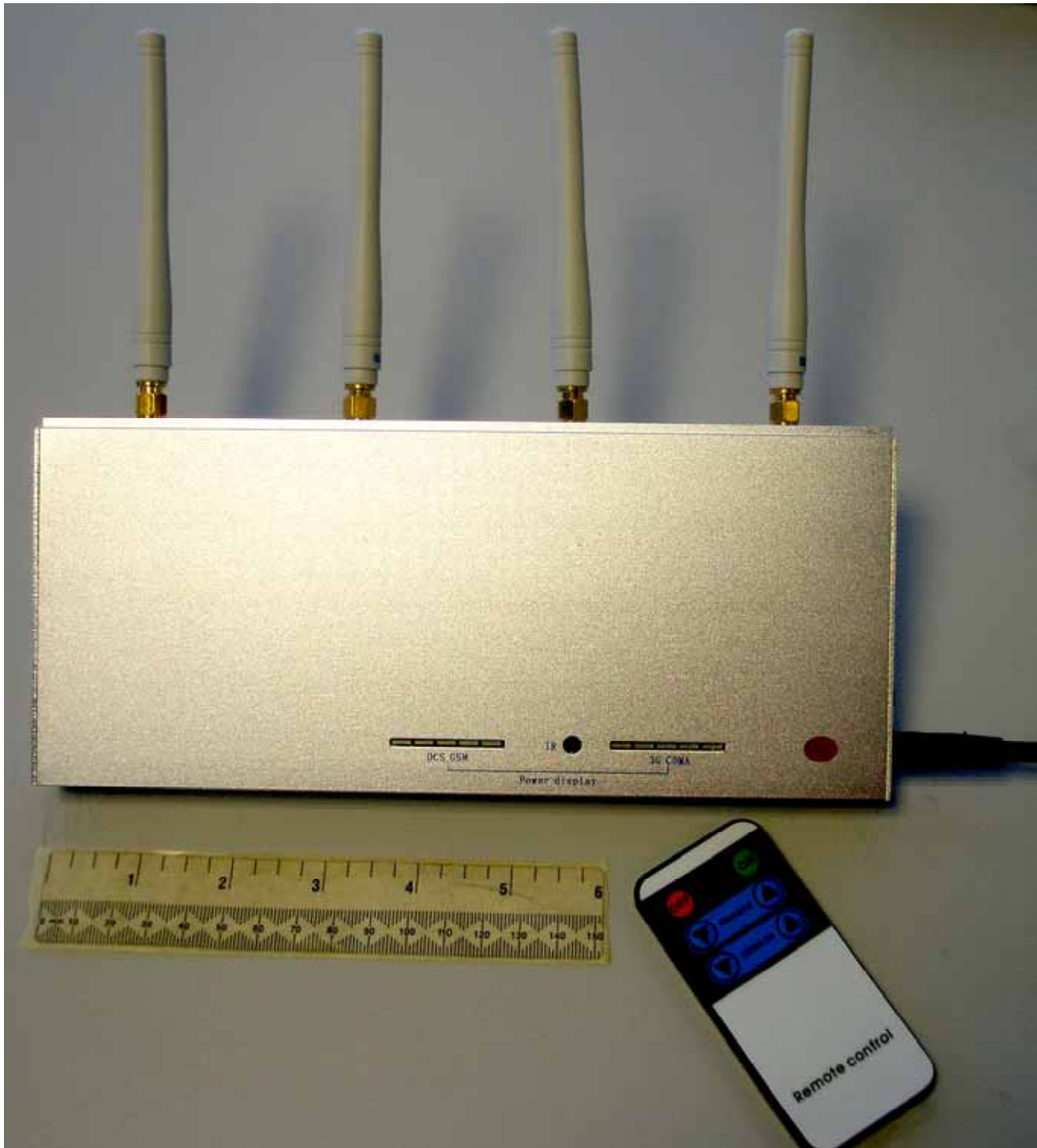
Cell Phone Blocker/Jammer –20 meter range<sup>2</sup>. Blocks 3G, GSM, CDMA, & DCS.



<sup>2</sup> <http://www.spymodex.com/jammer002.htm>



**Cell Phone Blocker/Jammer<sup>3</sup> –30 meter range with remote control. This is used for permanent installations like a Board Room for example. Blocks 3G, GSM, CDMA, & DCS.**



<sup>3</sup> <http://www.spymodex.com/jammer009.htm>



Cell Phone Blocker/Jammer – actual use example<sup>4</sup>.



<sup>4</sup> <http://www.spymodex.com/jammer001b.htm>





## Appendix C:

*How To: Building a BlueSniper Rifle - Part 1*, by Humphrey Cheung, March 08, 2005



John Hering – the builder

*How To: Building a BlueSniper Rifle - Part 2* by Humphrey Cheung, August 12, 2005



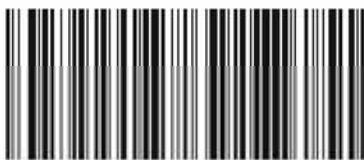
## Biography



Dr. Wolfe has been an active computer professional for more than 50 years. In 1979 Dr. Wolfe took up an academic post at the University of Otago and for the past twenty or so years has specialized in computer security. During that period he has earned an international reputation in the field of electronic forensics, encryption, surveillance, privacy and computer virus defenses.

Dr. Wolfe writes about a wide range of security and privacy issues for *Computers & Security*, *Digital Investigation* (where he is also an Editorial Board Member), *Network Security*, the Cato Institute, *Cryptologia*, and the *Telecommunications Reports*. He is a Fellow of the New Zealand Computer Society. He is also a member of Standards New Zealand SC/603 committee on Security, a member of the New Zealand Law Society's Electronic Commerce Committee, and was on the Board of Directors of the *International Association of Cryptologic Research* finishing up in January 2003.





ISSN 1176-7774