Global Information Assurance Certification Paper

Security in Wireless Mobile Communications
Dan Reain
10/01/2004

Abstract
Mobile devices such as mobile phones, PDA's (Personal Digital Assistants, a.k.a. Palm Pilots, Pocket PC's) and laptop computers are increasingly equipped with one or more forms of wireless data and voice communication capabilities. In this paper we we'll examine the most popular wireless communications technologies employed in today's devices including infrared, Bluetooth, and WiFi, as well as the technologies behind mobile voice communications. In this survey of wireless communications technologies we'll also look at the potential security risks introduced in each and provide risk mitigation strategies.

Mobile devices such as laptops, mobile phones, and PDA's have become ubiquitous in modern society. These tools are becoming less expensive and more feature-packed with each new generation of the technologies. The advent and subsequent maturation of mobile communications technologies have enabled mobile device users to have access to voice and data services from virtually anywhere, and without being tethered by wires. Unfortunately this convenience comes at a price- when communications go out over the air there is an introduction of additional security risk. Let's take a look at some of the common ways in which mobile communications are implemented and how security risk can be mitigated.

Infrared

One of the earliest implemented and most common wireless communications technologies employed by modern mobile devices is infrared, using the IrDA-Data specification. IrDA uses light in the infrared range for communications between mobile devices and is a point-to-point, ad-hoc data transmission standard. A common application for IrDA is for sharing information between PDA devices- often referred to as "beaming". It's common to have two PDA users "beam" their contact information (often referred to as an electronic business card) to each other instead of manually writing down the information or physically exchanging business cards. IrDA can also be used between a mobile phone and a PDA to synchronize phonebook information, to allow the PDA to use the phone as a modem to obtain internet connectivity, or between a PC and a PDA for sharing of personal information or "syncing". It should be noted that there are myriad applications for IrDA, but these are just some of the most common applications among mobile devices.

Because IrDA uses light, IrDA communications do not pass through walls or objects. It is a "line of sight" technology that that relies on its short transmission range for security. IrDA is also not omnidirectional- the IrDA spec calls for the width of the infrared beam to not exceed 30 degrees. The communication range

for IrDA is approximately one meter and the data transfer speed for most implementations is up to 4 Mbps[1].

Because of the short communication range, there are virtually no security measures built in to the IrDA specifications, and any security is left to the application layer to implement. An example of application layer IrDA security would be a scenario in which two PDA users "beam" contact information to each other. Before the transmitted data is accepted by the receiving PDA, the user is prompted by the device OS whether to accept that data or not[2].

Due to the lack of link-level security, it is possible to eavesdrop on an IrDA data exchange by detecting reflected light and filtering out noise created by ambient light.

IrDA signals can bounce off of walls, mirrors, and other objects and can travel through windows[3]. It is important not to underestimate the ability of an IR signal to bounce in a closed environment. Consider the following example cited in Infosec News:

On a recent flight to San Jose, CA thirty one laptop computers being used by passengers were identified as having an active IrDA port. In twenty six cases the IrDA port allowed unrestricted access to all files on the respective laptops. This vulnerability allowed roughly 5000 pages of documents to be downloaded from the computer during a one minute period. Since up to 8 sessions may be active at any time this would allow over 600 pages per minute to be downloaded in parallel from eight computers all at the same time[4].

This example underscores the importance of securing the oft-ignored IR port on laptop computers as well as other mobile devices. In addition to the possibility of theft of data, there is at least one instance of an IrDA-related operating system vulnerability that could be used to create a denial of service condition: Microsoft

---

[1] Birk, Andreas, Dr., "Infrared". http://www.faculty.iu-bremen.de/birk/lectures/PC101-2003/17bluetooth/bluetooth/irda.html

[2] "What is infrared and where is it used?". http://www.irda.org/displaycommon.cfm?an=1&subarticlenbr=14

[3] "IrDA versus Bluetooth: A Complementary Comparison" http://www.dpi.net.ir/pc/MobileComputing/articles/IrDA%20versus%20Bluetooth%20A%20Complementary%20Comparison.htm

[4] James M. Atkinson, http://www.landfield.com/isn/mail-archive/2000/Aug/0143.html

security bulletin ms01-046[5] describes a Windows 2000 vulnerability (fixed in service pack 3) in which a specially crafted IrDA packet is transmitted to a vulnerable system, causing that system to bluescreen and restart. These examples also illustrate how the implementation, not the specification, of a technology can create weaknesses in its use.

Although any wireless communication method has its vulnerabilities, those inherent in IR can be mitigated by taking a few steps:

- If you don't use IR on your mobile device, disable it. If you do use IR, enable IR functionality only when needed.
- Be aware of your surroundings when using IR. IR signals can bounce off of walls and travel through windows.
- Don't transmit sensitive data if other IR-enabled mobile devices are readily visible.
- Be aware of whether your laptop will serve or accept files via the IR port to unauthenticated users, and disable that functionality.
- Ensure that IR-enabled devices are not kept where the IR port could easily be accessed through a window, open doorway, etc.
- If you are prevented from locking down your IR port in your device OS or don't know how, physically cover it with opaque material such as electrical tape.

Bluetooth

Bluetooth is a wireless cable replacement technology implemented on an increasing number of mobile devices. PDA's, mobile phones, laptop computers, and other mobile devices use Bluetooth rather than the less convenient and bulkier cables to share information with each other and provide network services wirelessly. A traditional example is using Bluetooth between a PDA and a laptop or cellular phone. The devices can share information such as calendar entries, to-do lists, address book entries, email, and can also share files. PDA's or laptops can use Bluetooth to communicate with a mobile phone for the purposes of using the phone as a modem to connect to the Internet or to dial in to a private network. The number and type of Bluetooth enabled devices is rapidly increasing, and more innovative applications for this popular technology are becoming available all the time.

With Bluetooth communications, as with other wireless technologies, we lose the security inherent in hardwired connections and therefore we need to be aware of

---

[5] "Microsoft Security Bulletin MS01-046"
http://www.microsoft.com.technet/security/bulletin/ms01-046.mspx

the security implications of transmitting data between mobile devices over the air. Users of Bluetooth, or any wireless technology, should be aware of the attack vectors that can be used to compromise over-the-air communications. Can data be read from your Bluetooth device by unauthorized parties while the device is in your pocket or briefcase? When using your Bluetooth device can someone capture the data you are transmitting? First we need to know a little about how Bluetooth works and then we can move on to how it can be exploited.

The process employed by Bluetooth to set up authorized communications between devices is called pairing. In Bluetooth pairing, a special key called a link key is established between two previously unknown devices[6]. A second type of key, called the initialization key, is created using the Bluetooth addresses of the two devices, a random number, and a shared secret, or PIN. The initialization key is only used during pairing and therefore used only once. A third key, the PIN number, is usually entered in to each device by hand and is not transmitted in the clear between devices. Once devices are paired, authentication must take place before communications can begin. Bluetooth authentication is performed with a challenge response scheme. The receiver sends a 128 bit challenge to the initiator who applies the E1 cipher to it, its Bluetooth address, and the link key. The initiator then returns the 32 most significant bits of the result. The receiver confirms the response, and the authentication is then complete[7].

Bluetooth radios, depending on the class of radio in use, can transmit data up to 100 meters. Most PDA and mobile phone devices however are class 3 devices which can transmit data up to 10 meters. This means that generally, an attacker must be within relatively close physical proximity of the target.

Eavesdropping, or the monitoring a Bluetooth communications session by a third party, is made difficult in an authenticated session. The Bluetooth authentication mechanism does not transmit the complete challenge/response pair, and the E1 cipher used is not easily invertable, so even if an attacker recorded the complete authentication challenge/response session, they could not easily ascertain the link key. However, if an attacker can determine the PIN (which must happen via direct observation or guessing) and the attacker has recorded the pairing session, deriving the link key is much more simplified. Once the link key is known, encrypted communications can be decrypted, opening up the possibilities of eavesdropping, impersonation, and man-in-the-middle attacks.

---

[6] Xydis, Thomas G. and Blake-Wilson, Simon, "Security Comparison: Bluetooth Communications vs. 802.11." 1 February 2001. http://ccss.isi.edu/papers/xydis_bluetooth.pdf

[7] Vainio, Juha T., "Bluetooth Security". 25 May 2000. http://www.niksula.cs.hut.fi/~jiitv/bluesec.html

Bluetooth devices can also introduce the risk of revealing location information[8]. Imagine an organization with a network of strategically placed Bluetooth access points. As a user carrying a Bluetooth device in discoverable mode moves about the building, the access points constantly attempt discovery of all devices within its range. By correlating the information from multiple access points one can derive the movement patterns of the owner of the Bluetooth device, how much time was spent in a particular area, if a particular area has been entered, and how much time certain Bluetooth devices spent in proximity of each other.

Now let's take a look at some of the currently known attack types for Bluetooth devices.

Bluesnarfing[9] is one of the methods of surreptitiously downloading data from a Bluetooth enabled device. In a Bluesnarfing attack, the attacker connects to the target device in such a way that the target is not notified of an incoming connection attempt. Data that can be accessed includes the entire phonebook, calendar, and IMEI number. The IMEI number, or International Mobile Equipment Identity, is the code that is used to identify the phone to the mobile carrier and is used in illegal phone cloning operations.

In the Backdoor attack, the attacker establishes a trust relationship, or "pairing" with the target device in such a way that the pairing does not appear on the target's list of paired devices. The attacker can then freely access all available information and services that the device makes available via Bluetooth, including Internet access.

In a Bluebug attack, the attacker connects to the serial connection profile of a Bluetooth device making it possible to initiate phone calls, manage contact information, send and receive SMS messages, obtain internet connectivity, and even monitor conversations in the vicinity of the phone!

Bluejacking is an attack that has become somewhat of a social phenomenon. It takes advantage of the way that Bluetooth implements the sharing of services available on a particular device. With some services, like dial up networking (DUN), a device must have paired with the device offering the service before that service can be used. On most devices, however, the sharing of PIM (Personal Information Management) data generally does not require pairing- the receiving device will accept any request. In the Bluetooth transmission of PIM data to a device (which must be in discoverable mode), the name field of a contact entry is transmitted to the target before any authentication or acceptance of the

---

[8] Wetzel, Suzanne and Jakobsson, Markus. "Security Weaknesses in Bluetooth". 2001. http://www.informatics.indiana.edu/markus/papers/bluetooth.pdf

[9] "Serious flaws in bluetooth security lead to disclosure of personal data" http://www.thebunker.net/release-bluestumbler.htm

connection takes place. Using this method, a bluejacker creates a contact entry with his message in the name field. When he instructs his device to transmit the entry, the device will discover any Bluetooth devices in discoverable mode that are within range. The bluejacker then picks a device from the list, and the name field is transmitted and then displayed on the target device. The user of the target device is then prompted to either accept or reject the entry. Imagine a target sitting in a coffee shop or other public place, Bluetooth-enabled phone sitting on the table. The phone chimes and the user looks down to see the message "Nice shoes!" appearing on the phone's screen. The target has just been bluejacked. This may seem fairly harmless and while that may be true today, this practice has some serious implications down the road. The "bluejacked" name field message is accepted automatically and with no authentication. What if the OS of a particular device contained a vulnerability whereby a specially crafted message would cause a pairing to take place? The attacker would then have unfettered access to all the data and services available to the device.

Worms that propagate via Bluetooth have now been observed in the wild. The Cabir[10] worm spreads via Bluetooth and infects some phones using the Symbian operating system. This worm has no payload other than rapidly draining the batteries of an infected device due to its constant searching for other devices to infect, but this can be viewed as a proof-of-concept of the potential for attacks on Bluetooth-enabled devices.

Mitigation strategies

- Put your device in "invisible" or "nondiscoverable" mode. In this mode Bluetooth is still enabled but the device will not show up in a scan initiated by another device. This will make it much more difficult for an attacker to identify your device as a target.
- Perform a factory reset of your device. This will erase all personal data input into the device, but it will also remove any traces of past pairings and help protect against Backdoor attacks from those previously paired devices.
- If you receive an unsolicited pairing request, make sure to answer "no" so that the request is not accepted.
- When pairing Bluetooth devices, do so in a private place and use random, longer PIN numbers.

WiFi

WiFi, or 802.11x networking, like Bluetooth, is a wireless communication technology that has become very common in mobile devices. More and more

[10] "SymbOS.Cabir" 6 July 2004. http://securityresponse.symantec.com/avcenter/venc/data/epoc.cabir.html

PDAs and laptops are coming standard with some form of WiFi built in. This section will give an overview of the security issues surrounding WiFi and how mobile device users can mitigate some of the risk that WiFi introduces.

WiFi is the commonly used name for Ethernet over wireless networks. It stands for Wireless Fidelity and is used to refer to any type of 802.11 network whether it be 802.11b, 802.11a, 802.11g, etc.

WiFi functionality in mobile devices can be used in two modes: infrastructure and ad-hoc. In Ad-Hoc mode two mobile devices establish network connectivity directly with each other, much like connecting the network ports of two PC's together with a crossover cable. In infrastructure mode, the device becomes a node on a larger Ethernet network and can communicate with any other node connected to the internetwork. An example of an infrastructure mode connection would be using a laptop or PDA to connect to the WiFi access point in a coffee shop for purposes of Internet connectivity or in a home network for file and print services sharing. Since infrastructure mode is the mode used for access to the Internet, we'll concentrate on infrastructure mode scenarios.

The majority of WiFi access points can operate in either "open" mode, which does not encrypt packets sent out over the air, or WEP (Wired Equivalency Privacy) mode, where packets are encrypted based on an encryption strength chosen by the administrator of the access point. Most access points today offer the use of both 64-bit and 128-bit encryption key lengths. The general idea is that the longer the encryption key, the harder it is to discover that key and decrypt the encrypted packet. However, due to the way WEP is implemented, WEP keys are not considered to be the primary weakness of WEP[11]. The main weakness of WEP lies in the implementation of key management. WEP relies on a 24-bit Initialization Vector (IV) that gets appended to the WEP key whether the key is 64 or 128 bits in length[12]. Because the IV is only 24 bits in length, there are a limited number of possible IVs. This means that eventually IV's will be reused. Because the IV is transmitted in the clear with each encrypted packet, if an attacker can capture enough packets they will find packets that use the same IV. The attacker can then use this information to more easily crack the WEP key. These types of attacks are well known and tools to exploit these weaknesses are widely available on the Internet. WEP with a 128-bit key length will do fine to protect against casual monitoring, such as a neighbor or fellow coffee-shop patron sniffing WiFi packets, but if someone really wants to compromise your WEP-enabled network, they will eventually be able to.

---

[11] "What's Wrong With WEP?" 09 September 2002. http://www.nwfusion.com/research/2002/wepprimer.html

[12] "Practical Wi-Fi Security: The realities of wireless security" http://www.hp.com/sbso/productivity/howto/it_wifisecurity/realities.html

WPA, or WiFi Protected Access, is a newer security standard that consumer WiFi equipment makers are increasingly including in their products. WPA attempts to improve upon the weaknesses of WEP by introducing better key management. WPA uses the same RC4 encryption as WEP, but introduces 48-bit Initialization Vectors, which significantly reduces the problem of Initialization Vector reuse. WPA also improves upon WEP's use of the Integrity Check Value (ICV). With WEP, the way the ICV is implemented makes it trivial to forge packets. WPA's implementation of this functionality, an 8-bit value called the MIC (Message Integrity Code, also called Michael), is included in the encrypted packet just before the ICV[13].

Another security feature often found on consumer WiFi equipment is MAC address filtering, where the access point can be configured to only allow only known network cards access to the wireless network. This level of protection will provide a moderate level of added security to a home network and will help in keeping the casual user from being able to associate with your access point. Some pay-for-access access points, such as those in hotels and internet cafés, use this method to prevent unpaid access, but isn't a viable method for keeping a dedicated hacker out of your wireless network. MAC addresses are quite easily spoofed.

In using public WiFi access points, such as those available in hotels and internet cafés, security is left up to the end user since these access points generally operate in "open", or unencrypted mode. This is to make it easier for patrons to connect to the wireless network, increase operation speed and minimize the need for supporting technical issues involved with gaining WiFi access. Since the data a mobile device transmits is being sent in the clear to the access point, one should consider the security of his or her connection to be even less so than using a wired connection to connect directly to the internet. Because the data is being sent over the air in cleartext, it is subject to being easily monitored by anyone within WiFi range of the access point. In using a public access point, also consider that your device is on hostile network, and appropriate security options, such as up-to-date security patches for your device's OS and a software firewall product, should be implemented. Even though a public access point may be a firewall/wifi device, keep in mind that the firewall protects the wifi network from attacks from the internet- it does not protect the nodes on the wifi network from each other!

Using public access points to access corporate data or access sensitive data should also be done with extreme care. Most corporate environments require the use of some type of VPN to access the corporate network via the internet. VPNs are an effective way to mitigate risk in wireless network use, and VPN clients are becoming increasingly available for PDA devices as well. To better secure sensitive information such as financial data when communicating with websites

[13] . http://www.wi-fiplanet.com/tutorials/article.php/2148721

via any type of access point, look for SSL-enabled sites so that these types of transactions are not sent over the air, or over the internet, via cleartext.

Risk mitigation strategies for using WiFi with mobile devices:

- Use software-based firewalls on mobile devices. There are now firewall implementations in software available for a variety of mobile device platforms.
- When communicating sensitive data to a web application, use the SSL version of the site
- Use VPNs to secure communications traversing public networks
- Configure 128-bit WEP or (preferably) WPA on access points

Mobile phone security

In order to properly relate the security risks and possible risk mitigation strategies in mobile phone usage, it's important to understand a bit about how mobile phones operate and the evolution of the technology. In this section we'll look at the differences between analog and digital networks and the possible attack vectors in each.

Analog, or 1G service was introduced in the early 1980s and used FDMA (Frequency Division Multiple Access) technology. FDMA was defined by AMPS, the Analog Mobile Phone System standard. This type of service suffered problems with capacity and security. A casual user equipped with an off the shelf radio frequency scanner could monitor cellular phone transmissions. It was trivial to continue monitoring even when a mobile user would move between the transmission range of one tower and into another tower's range by simply adjusting the frequency of the channel being monitored.

AMPS was later upgraded to D-AMPS, or Digital AMPS, and used digital FDMA, a 2G technology. Still using the 800 MHz band, it solved some of the capacity issues of AMPS since communications could then be digitally compressed to take up less bandwidth. Radio frequency scanners alone could no longer be used to listen in on phone conversations, and the FCC halted the sale of scanners that could monitor those frequencies. TDMA is a widely used 2G technology.

The latest development in mobile phone technology is the packet-switched, or 3G network, providing access to both voice and data services. CDMA and GSM are considered 3G voice services and GPRS and EDGE are the services for data.

Although mobile phone networks today in the U.S. are digital, and the FCC prevents the sale of frequency scanners able to scan the mobile phone communication bands, it is not impossible to intercept mobile phone conversations. Older, pre-FCC ban frequency scanners are still obtainable and

some of the current scanners are modifiable so that these frequencies can be monitored. Easily monitored analog networks are still in use today, and digital network subscribers roaming into an analog service area become vulnerable to eavesdropping. Eavesdropping on digital network calls is much more difficult, but again not impossible[14]. Digital network test equipment is obtainable, albeit for a hefty price (around the $50,000 range), and can be used to monitor calls. Although casual frequency scanners will not be able to listen in on digital mobile phone conversations, there are varying degrees of difficulty in eavesdropping with different digital network type.

CDMA and TDMA networks encode calls but do not encrypt them. With CDMA calls are not transmitted on a single frequency, but spread out as a coded signal across the frequency spectrum. Each call is modulated with a unique code that is used to both encode and decode the signal. Monitoring is made difficult because calls are spread across a range of frequencies. With TDMA, calls are transmitted on a single frequency but multiplexed by time. Each call is assigned a frequency and a time slot within that frequency. Because multiple calls are effectively intermingled, monitoring is made difficult. However, because a single frequency is used it is a simpler matter to pick out a single call with the right equipment. GSM was designed with security in mind- GSM transmissions are encrypted and are very difficult, if not currently impossible, to monitor. That is not to say that GSM is completely impervious to eavesdropping however. Law enforcement agencies (and of course service providers) do possess the very expensive equipment necessary to monitor calls no matter what type of network is being used[15].

In addition to being subject to monitoring, mobile phones can also be used to monitor the physical whereabouts of the user. The location of user can be triangulated by monitoring the phones signal strength with multiple communications towers. Also, the FCC has mandated that by 2005 cellular phones have a feature called E-911 that provides location information about 911 callers to within 100 feet of the device so that emergency response services can find callers.

Another risk in cellular phone use is cloning[16]. Cloning is the illegal practice of providing false credentials to a cellular provider with the intent to defraud. Besides the risk of incurring unauthorized phone charges, there is the risk of the

---

[14] "Israeli Scientists Hack GSM Technology" http://www.cellular.co.za/news_2003/091103-Israeli-GSM-hack.htm

[15] "Wireless Communications: Voice and Data Privacy". August 2004. http://www.privacyrights.org/fs/fs2-wire.htm#3

[16] "Cellular Phones". http://rf-web.tamu.edu/security/secguide/V2comint/Cellular.htm

possibility of impersonation of the authorized user of the phone. Using the same equipment as an eavesdropper, a third party can gain enough information about a phone over the air to recreate that phone's configuration on another phone. With GSM phones, a potential cloner needs physical access to the phone long enough to obtain enough information, usually only a few minutes. Additionally, GSM phones store the provider and subscriber information necessary to use the phone on a special data card called a SIM, so if someone can simply steal the SIM they can install it in another phone. SIM cards can also contain information such as contacts, calendar, task lists, etc. that could be compromised if the SIM is stolen.

Mitigating cellular phone risk

- When selecting a cellular phone service, be aware of the technology that the service uses. For a higher level of security, choose a GSM or CDMA service.
- Be aware of your provider's policies on data retention and privacy.
- Find out if your provider keeps location information about your phone. Avoid services that store this data.
- Don't communicate private information such as credit card numbers and sensitive corporate data via cellular phone.
- If your phone is stolen or lost, contact your service provider immediately.
- Use your phone's lock feature when you are not using the phone.
- Don't carry a cellular phone into a classified area or place where sensitive conversations are held.
- Find out if your cellular provider provides PIN services. PIN services require the input of a PIN for every call made, but they can be effective in preventing phone cloning.
- Do not keep your phone in an unattended car.
- Do not give your phone to anyone you do not trust implicitly.

Additional risk is introduced any time a mobile device transmits information over the air. Whether you are beaming contact information to an associate via IR, using wireless networking with a PDA or laptop, or just talking on a mobile phone, you should be aware of the different ways in which your information could become compromised and how you can protect yourself against these threats. Fortunately, a lot of this risk can be effectively mitigated by understanding the technology in use and taking some simple steps to protect yourself.

References

Birk, Andreas, Dr., “Infrared”. http://www.faculty.iu-bremen.de/birk/lectures/PC101-2003/17bluetooth/bluetooth/irda.html

“What is infrared and where is it used?”. http://www.irda.org/displaycommon.cfm?an=1&subarticlenbr=14

“IrDA versus Bluetooth: A Complementary Comparison” http://www.dpi.net.ir/pc/MobileComputing/articles/IrDA%20versus%20Bluetooth%20A%20Complementary%20Comparison.htm

James M. Atkinson, http://www.landfield.com/isn/mail-archive/2000/Aug/0143.html

“Microsoft Security Bulletin MS01-046“ http://www.microsoft.com.technet/security/bulletin/ms01-046.mspx

“Serious flaws in bluetooth security lead to disclosure of personal data” http://www.thebunker.net/release-bluestumbler.htm

Vainio, Juha T., “Bluetooth Security”. 25 May 2000. http://www.niksula.cs.hut.fi/~jiitv/bluesec.html

Potter, Bruce and Caswell, Brian, “Bluesniff- the Next Wardriving Frontier”. http://www.shmoo.com/~gdead/dc-11-brucepotter.ppt

Xydis, Thomas G. and Blake-Wilson, Simon, “Security Comparison: Bluetooth Communications vs. 802.11.” 1 February 2001. http://ccss.isi.edu/papers/xydis_bluetooth.pdf

Wetzel, Suzanne and Jakobsson, Markus. “Security Weaknesses in Bluetooth”. 2001. http://www.informatics.indiana.edu/markus/papers/bluetooth.pdf

“SymbOS.Cabir” 6 July 2004. http://securityresponse.symantec.com/avcenter/venc/data/epoc.cabir.html

“Wireless Communications: Voice and Data Privacy”. August 2004. http://www.privacyrights.org/fs/fs2-wire.htm#3

“Cellular Phones”. http://rf-web.tamu.edu/security/secguide/V2comint/Cellular.htm

Vanderploeg, Alan. “ Wireless CommunicationsSecurity” http://www.wirelessgalaxy.com/cellularrelatedarticles/wirelesssecurity_art.html

"Israeli Scientists Hack GSM Technology"
http://www.cellular.co.za/news_2003/091103-Israeli-GSM-hack.htm

"Practical Wi-Fi Security: The realities of wireless security"
http://www.hp.com/sbso/productivity/howto/it_wifisecurity/realities.html

Geier, Jim. "WPA Security Enhancements" 20 March 2003. http://www.wi-fiplanet.com/tutorials/article.php/2148721

"What's Wrong With WEP?" 09 September 2002.
http://www.nwfusion.com/research/2002/wepprimer.html

Last Updated: July 24th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor