Global Information Assurance Certification Paper

Technological Advances and the Effect on Physical Security

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b

Valdo Araiza
3/30/2004

Abstract

The strides in technology each year have surpassed the previous year by leaps and bounds and will probably continue to do so in the future. Information technology continues to advance in ways that greatly benefit society on many levels but as the increasing benefits develop so do the security vulnerabilities associated with information technology. Hardware and software is being released to the general public that can help people be more productive but this same technology can be used to infiltrate or impede practiced physical security measures whether that effort is intentional or not. In this paper we will explore both sides of this technology. We will look at the side of technology that is designed to benefit physical security defenses and solutions along with the side that can be used as a physical security threat.

The Technology

Computers and the hardware associated with them are processing faster, taking up less physical space, storing massive amounts of data and becoming much easier to use. Software and the code or language used to develop programs has also improved to where these applications are smaller, faster, and again much easier to use or write.

We start by looking at the personal computer or workstation itself. Only a few years ago the personal computer was a large rectangular box that required the use of two hands if anyone planned to relocate it not to mention having to move the monitor. Today the idea of "smaller is better" remains in the foreground of computer design. There are a number of big name manufacturers as well as some small companies that are building computers that perform as well if not better than many large computers, yet they take-up less space than that of a cigar box[i]. Computer monitors have also progressed from the large square box that resembled a television and took over a majority of your desk to very thin liquid crystal displays, or gas-plasma displays and even to "spy-movie" levels with eyewear models available[ii].

Now let us explore the advances in mobile computing. The laptop computer has evolved in processing power as well as decreasing in weight and size. The laptop of today can keep pace with most of its desktop workstation counterparts as far as processing power is concerned. Due to the improvements to the physical aspects of today's laptop, the days of seeing a large bag that would hang over someone's shoulder and barely qualify as carry-on luggage are all but gone. The recent development of both hardware and software technologies have helped the development of what may be considered a small laptop, which would be the Tablet PC. The Tablet PC can be described as a cross between a laptop and a notepad. Most tablets are designed so that you can open it and use the keyboard

in the same manner as a laptop, or you can simply keep it in what may be described as a closed position and use a stylus to tap, select, and write directly on the LCD screen. The increasingly popular PDA (i.e. Pocket PC and Palm) is advancing right along with PC and Laptop technologies. These hand-held devices are built with the processing power and memory equivalent to PCs of just a few years ago yet they are small enough to keep in your shirt or pant pocket. Some of the other devices that are making amazing advances in technology are the cellular or mobile phone, digital camera, multimedia devices and removable portable data storage devices. So how do these devices or electronic gadgets affect physical security?

Physical security is often thought of as the fences, gates, doors, and locks but it does go much further than that. The extent of physical security will depend on the value and confidentiality of the items contained within your facility, whether that is tangible goods, monetary items, classified or sensitive documentation, computer data, or even personnel. Often we become complaisant with current security measures in place and forget to look at how fast technology is growing. The various ways these items can become susceptible to a physical security breach continues to increase each day. Let us look at physical security from the very outside and make our way in to see where some of the threats and defenses lie.

From the Outside

When you look at outside physical security threats the technology improvements in the past several years have changed that whole landscape of physical security. Whether you want to refer to it as WI-FI, 802.11x, or simply wireless technology, the advances in the field of wireless networking have caused the popularity to increase at an astonishing rate. Public wireless access is increasing to where you can walk into many coffee shops, fast food chains, and airports and are able to obtain a wireless connection to access the internet or possibly your office. The improvements to the technology, along with the reduction of cost in wireless networking, has made it very alluring to both the employee that may be looking for easier or increased production as well as the individual that may be attempting to maliciously intercept any wireless transmitted data that may be of benefit to them.

Manufacturers are now making laptops, Tablet PCs, and PDAs with wireless technology built right into the device so there is no need to purchase and install additional hardware. Many facilities are beginning to implement wireless networks due to cost and convenience. The cost to run network cabling to each computer in a facility can get costly when you compare the cost of setting up a wireless network infrastructure. Since many computers come with or can be easily modified to support wireless connectivity the option for wireless networking becomes very appealing. The problem with wireless technologies is that you do not have any control over where the information is being sent. Wireless transmissions move through the air and generally have no specific direction or

endpoint, unlike a cabled network that has a beginning (or source) and an end (being the destination).

The onset of wireless networking has brought upon a practice known as **War driving.**[iii] *(War driving is when a person drives around businesses and neighborhoods attempting to locate a wireless access point (AP) by using a portable device running a utility that sniffs out and catalogs wireless APs.)* The act of war driving has become a kind of cult hobby or sport and often may not have malicious intent, but there exists the treat of those individuals that are out to gather what may be deemed confidential or sensitive data.

Once a WI-FI signal is located someone can then lock onto that signal and begin to collect the information that is being transmitted, which is referred to as **sniffing**[iv]. *(Sniffing – Capturing raw network traffic and filtering it to look for specific information)* The thing that makes this practice so appealing to the thief is that he or she can gather data without ever needing to enter the facility. Today's technology allows sniffing to be conducted by someone with an antenna attached to his or her equipment while in a nearby office or building, a parked vehicle, sitting on a park bench or even simply walking around several hundred feet from the source of the wireless transmission. If an employee within the facility has a laptop, Tablet PC, or PDA that is capable of wireless networking and he or she has not had the device configured correctly it can become an "open-door" to wireless sniffing and the data on the device or even data residing on the LAN (Local Area Network) that the device may be a member of can be easily compromised.

Another more recent use for the WI-FI technology is wireless cameras. These cameras can be placed in positions to monitor and record visitors, personnel, and delivery times all without ever being detected. Many of these cameras are small enough to be unseen and can be powered by a small battery for hours. So how can you protect your facility from the seemingly invisible wireless attack?

The first step in any organization is to implement a clearly defined policy on wireless technology use. If wireless devices are permitted in the workplace then who is allowed to use them; where will they be allowed to be used; and what network resources will they be allowed to have access to via wireless connection? If unauthorized use is discovered what will be the action taken? Have a policy for visitors and vendors as well and make sure that they review this policy so that they understand what action may be taken. Once this policy is established it will need to be implemented and enforced. With implementation the IT staff will need to be educated on wireless technology and updated regularly as the technology changes and advances. The IT staff will also need to understand the policy that is in place as well as who is effected by it. The entire IT staff should have an understanding of wireless technology and the policies to a certain extent. The IT security, network, and tech support staff must be able to recognize both authorized and unauthorized use of WI-FI devices. IT security and network

staff will need to be well versed in the use of network monitoring and analysis tools and wireless detection equipment. The entire IT staff needs to be able to recognize any device that may be used for wireless networking and have a procedure on reporting it when located in and around the workplace.

The level of physical security that is often overlooked in dealing with WI-FI is perimeter security. The security staff that monitors the facility grounds and the surrounding area needs to be able to recognize wireless equipment as well as have a fair idea of the extent of this technology. The facility security staff will need to watch for any unauthorized vehicles, unscheduled maintenance company vehicles and delivery vehicles that are in the area for a period of time. CCTV (closed circuit television) cameras should be setup to view all areas of the facility and surroundings without forgetting areas that are not always considered to be high traffic or high visibility areas. The facility security staff as well as the IT staff should conduct regular wireless detection sweeps of the area surrounding the property as well as areas within the facility with inconspicuous handheld devices[v].

As mentioned earlier, depending on the value and confidentiality of the items contained within your facility, this level of physical security may not be enough to protect you from a wireless intrusion. You may not even have any devices that are WI-FI enabled to possibly become victim of an attack. **EMR** or electromagnetic radiation is emitted by basically all electronic devices whether it is a PC, monitor, printer or even a phone. EMR moves through just about everything including power lines, air vents, and water pipes.

> "*The range in which an eavesdropper can monitor emanations varies tremendously according to conditions. In most cases, the emanations can be picked up with proper equipment from a distance of around 200-300 meters. However, in some cases where a signal has been captured by a conductive medium (such as a power line), monitoring can occur over a distance of many kilometers."* [vi]

Sometime around the late 50's to early 60's it was believed that there was a classified government project called Tempest that was focused on EMR use and detection. The term was later used to define a standard and classification for Telecommunications Electronics Material Protected from Emanating Spurious Transmissions (TEMPEST), which then evolved into EmSec or Emissions Security. To setup a facility that is protected from EMR detection you are basically attempting to build a room that nothing can enter or leave via air, water, or through electrical or communication lines. This becomes very expensive due to the materials and equipment required and may also require government approval depending on the equipment used. How much of a threat EMR detection truly is may be uncertain but if the value of what is inside you facility calls for this type of protection then EMR shielding may be a security measure to review.

Getting Inside

The ability for unauthorized personnel to enter a facility is generally dependent on the requirements established for the authorized staff to enter. Many facilities use a form of magnetic access badge or card that runs through a type of reader to identify the individual needing to enter then the door is unlocked. Some facilities may use a PIN (personal identification number) entry system on a keypad to unlock a door. Smaller facilities may just have a regular key to unlock a door. Any of the mentioned methods for a secure entry are only going to be as secure as the person walking in. Let us take a closer look at this. How often have you seen someone courteously hold the door open for someone else walking in behind him or her especially if the trailing person has his or her hands full? Do they always know who this person is? Are they willing to stop the person from entering and make them put down whatever they are carrying to show identification or swipe their badge? When someone simply follows behind somebody else to enter a facility is commonly referred to as **tailgating**. A facility that may be more stringent on entry would employ using a security guard to view anyone entering or exiting ether in person or by CCTV (closed circuit television) and confirm they are authorized to do so in this manner. Other options that are available are mantraps either as a turnstile or simply a small room with two doors that require an individual to be identified going into the mantrap as well as to exit in order to reach his or her destination. There has also been the development of tailgating detection systems[vii] that will sense when more than one person has passed the entryway.

What about the card itself? How easy is it to lose a card? Can you be certain that when a person loses his or her card they will immediately report that the card is out of their possession? What if that person were to lose the card on a Friday evening and does not even realize that the card is lost until they arrive to work on Monday morning and try to get in? Is that window of vulnerability something that can be accepted? Another scenario is that someone takes a vacation for a week or even just a few days. Their card is then lost or stolen. Some facilities require that when employees take time off that their card must be disabled until their return. Are the logistics in place to keep track of employee vacations within the security system? If not then this may be where the need for two-factor authentication comes in. The two forms of identification can be the use of the card or badge along with a PIN to enter on a keypad, or possibly the use of **biometrics.**[viii] (*Biometrics – Automated method of recognizing a person based on physiological or behavioral characteristics)*

There are a number of different methods used with biometric identification such as fingerprint, hand geometry, retinal, and voice recognition to name a few. Although the science of biometrics continues to make great strides it is still not without fault. Not everybody can be clearly identified with biometrics due to physiological limitations or simply changes that may occur naturally or unnaturally. Because of the margin of false positives or false negatives that

currently exists with the use of biometrics it would be best not to be rely on biometrics as a sole factor for identification or authentication.

The method for identification that continues to maintain the smallest margin of error is also the least technical and oldest practiced. That would be the use of a manned security check-in. When you have one human identifying another it allows less room for mistake as well as reducing the likelihood of identity theft. Depending on the number of entry points the facility may have, this type of identification can become tedious and very time consuming. When you look at the fact that additional staffing will be required this identification method may not be the most cost effective solution for everyone.

On the Inside

So someone has made it into your facility. Whether they are authorized or not, what physical security threats and defenses are to be encountered? What methods can be used to counter something as simple as **shoulder surfing**[ix]? (*Shoulder surfing is the practice of looking over a user's shoulder to observe what he or she is typing. For example, a password may not be displayed on the screen, but it can be discovered by looking over the user's shoulders and observing which keys are pressed.)* Whether the snooping is for a password, account number or any other information that may be displayed on a monitor it can be captured by other means than just that of prying human eyes. If it is data theft or data damage that is being conducted there is technology available to just about anyone that makes any of these forms of attack easier. Let's take a look at some of these methods.

Everything from passwords to email and even Instant Message conversations can be logged and recorded via a keylogger. A keylogger is technology's version of shoulder surfing and can ether be a software program or hardware device designed to capture and log all the keystrokes made on a computer's keyboard. Often the program is kernel based and uses system calls to track the keystrokes and therefore it remains undetected by the user. The hardware models most often are physically attached between the keyboard connector and the connector on the back of the computer. In 2003 there were several cases where keyloggers were setup in a number of publicly used computers in businesses and school campuses in and around the world. The data that was stolen ranged from bank accounts and passwords to personal information.

Take an ordinary everyday cellular phone. Cellular phones currently posses the ability to capture voice recordings, take digital photos, and record video very discreetly. Because of the raise of personal rights infringement and lawsuits encountered with unauthorized photography, manufactures are starting to look at making the cellular-camera phones appear not so inconspicuous when they are in the camera mode. The PDA is incorporating digital voice recording and digital photography in one device and again can be accomplished very discreetly. Many

PDAs allow the addition of flash memory to increase the storage capability of the device. Digital cameras, whether it is still photos or full motion video, continue to improve on quality as well as the devices themselves getting smaller in size. There are digital cameras that are so small you can wear them as a pendant or attach them to your keychain. This brings us to our next little gadget that is taking the world by storm.

The ease of use, convenience and portability of the **USB flash drive** (also known as USB thumb drive or keychain drive[x]) has raised increased security concerns. The USB flash devices are getting smaller in size and the amount of storage available continues to grow past 2 gigabytes at the time of writing. There are USB based hard drives that are no larger than a pack of cigarettes yet they can store over 40 gigabytes of data and require no additional power source to run. Some of the risks that these types of devices can cause are data theft and data damage as well as another means for the introduction of viruses.

Something that we have all encountered and unfortunately may have guilty of doing ourselves is to walk away from his or her computer without logging off or locking it. So what can happen because of this? Somebody notices a computer is unattended so they approach the “open” computer and take out their keychain. On that keychain is a USB flash drive. What will happen next? For the most part anyone with a USB device can connect the foreign device to most Operating Systems (OS) without any need for additional drivers or need to reboot the computer for that device to be recognized. They can then gather large amounts of data in a very short period of time due to the available data transfer speeds of USB technology. They can modify or delete data to disrupt business or even introduce a virus or worm and remove the device without ever being noticed.

There is also the development of programs as well as bootable operating systems that can reside on these USB devices that will allow one to boot the computer straight to the USB device, eliminating any type of security authentication required by the OS on the computer or network. In most cases this gives complete access to the data on the computer’s hard drive for extraction, corruption, or deletion. Another use of the USB devices is that some have been designed to be used for multimedia recording and playback and therefore they have built into the device a small microphone to capture audio. Because there are no moving parts the device can be strategically placed in a discreet location and record any conversation in the immediate area for lengthy periods without ever being detected.

In an atmosphere that has information stored on computers or communicated in such a manner that will allow it to be displayed on a computer monitor or heard via a discussion over the phone or simply documents that may be left on top of a desk, it may be prudent to have a policy on the use of electronic devices in the area. A policy should be implemented for both employees and visitors. The issue with leaving a computer unattended can be addressed by several available

options. In the past when the common removable media for computers was a floppy disk or CD-ROM drive those were often removed or disconnected to prevent data form being removed or introduced to the computer. With the advent of USB devices the solution is not as easy. There lies the ability to disable the USB ports in the computers BIOS but this would prevent the use of many of the necessary peripherals such as a USB connected mouse, keyboard, scanner, or printer. There are software developers that are looking at programs that can restrict the adding of devices as well as log activity on the USB ports. A common practice used to protect data access due to someone leaving his or her computer unattended for a period of time is to enforce a strict screensaver policy that will force the computer to activate the screensaver and lock the workstation if it is not used within a designated timeframe.

Another increasingly popular method to use is smart cards[xi] *(A **smart card** is a tamper-resistant, credit card-like hardware token that can be used to add additional protection to security-enabled protocols and applications.)* to logon or authenticate on a workstation. The implementation of smart cards can be setup so that the card, which must remain on the person wherever they go, will be required to logon to any workstation. Removal of the smart card will cause the computer to lock itself until the card is re-inserted. An added benefit of using a smart card is that you can build your security infrastructure around the smart card, therefore it can be used with entry systems so that the same card used for computer authentication is required to open any doors in the facility. Smart card technology can also compliment the use of data encryption such as **EFS** (Encrypted File System) so that data cannot be accessed by anyone unauthorized to do so. The smart card would hold a certificate to allow the encryption and decryption of data.

Encryption of data is becoming a hot topic in the information security field due to the liability that can come into play. In the past year or so there have been several cases where an institution has had a laptop or workstation lost or stolen which contained valuable and confidential data regarding their customers. If the data is encrypted then the removal of this data becomes a very difficult and lengthy task. If no encryption is present, even with OS level file security in place, the data can be retrieved in a short period of time. Because of this there is an increase for institutes to look into encryption and smart card. Companies are enforcing policies that requires the storage of confidential data on any hard drive to be encrypted otherwise it cannot reside on the local hard drive and must reside only on a network drive or share that has security permissions applied. Some of the aforementioned “snooping” can and will be done not only by outsiders but also by people within you organization. Routine checks by IT security and facility security of workplace areas as well as checking behind workstations to make sure no foreign objects are present would be a good practice. In doing this there must be a clear policy on this action and the procedures that would follow on discovery of any suspicious items.

In Closing

The focus of this paper was technological advances and the effect on physical security. As mentioned several times throughout this paper, depending on the value and confidentiality of the items contained within your organization or facility will drive the amount of physical security measures placed within your organization. Along with this will be how well your staff is trained on the different attack and defense technologies. We didn't cover all the different technologies that are available but should have brought some new physical security threats and defenses into light or at the least reminded you of some that may have been forgotten or possibly overlooked.

List of References

[i] *http://www.littlepc.com/index.htm*

[ii] *http://www.microopticalcorp.com/Products/HomePage.html*

[iii] *War driving*
Security+ Certification Training Kit / Microsoft Corporation with Andy Ruth and Kurt Hudson - Chapter 5 -- Communications Security -- Lesson 3: Understanding Wireless Standards and Protocols - Copyright © 2003 by - ISBN 0-7356-1822-4)

[iv] *Sniffing*
Webmaster's Guide to the Wireless Internet – Ryan Fife, Wei Meng Lee, Dan A. Olsen - Page 454 – Copyright © 2001 by Sygress Publishing, Inc. ISBN 1-928994-46-6)

[v] *http://www.airmagnet.com/products/handheld.htm*

[vi] *http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci522583,00.html*

[vii] *http://www.koubasystems.com/productlist.htm*

[viii] *Biometrics*
http://www.biometricscatalog.org/biometrics/Biometrics_101_v3.pdf

[ix] *Shoulder surfing*
http://www.itsecurity.com/dictionary/shoulder.htm

[x] *http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci869057,00.html*

[xi] *Smart Card*
Microsoft Windows 2000 Server Administrator's Companion
Chapter 17 – Planning for Security; Section 1 – Smart Cards
Copyright © 2000 by Charlie Russel and Sharon Crawford

PUBLISHED BY
Microsoft Press - ISBN 1-57231-819-8

Last Updated: July 26th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 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
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
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 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 Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	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
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
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
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
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
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
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event