Global Information Assurance Certification Paper

Securing Remote Workers: The Forgotten Warriors

GIAC Security Essentials Certification (GSEC)

Practical Assignment

Version 1.4b

Option 1

Farhan Ashraf
SANS Scotland:
Feb. 9-14 in Edinburgh, Scotland

Table of Contents

Abstract

Just when you thought it was safe, a new challenge is facing IT security professionals. A growing number of remote users are demanding to have the same level of access to systems and data as those back in the office environment.

Users able to connect from anywhere while using corporate machines means one thing: security problems

Laptops are undeniably convenient, but they're also prone to malicious hacking and theft. We'll examine three facets of laptop security: protecting the hardware; protecting your data; and protecting the software and communication channel.

Introduction / Executive Summary

In the UK, the Government has introduced new legislation that enables eligible employees to apply for more flexible working hours, so the popularity of remote working is likely to increase.

The dangers are obvious. Laptops holding sensitive data can get lost, damaged or stolen. Data from wireless hotspots could be intercepted.

Mobile workers or remote users as I will refer to are often not protected as well as internal devices. A security policy for remote users should ensure that their systems and their data are as secure as your network. In order to reap the rewards of mobile technologies, an organisation must fully recognise both its capabilities and vulnerabilities.
When managing security within organisations, more emphasis is often placed on securing the network perimeter and protecting the internal devices from external and internal threats.

The same approach you would use to securing your network should be applied to remote users and having a layered defence will protect you from most attacks.

.
When looking at remote users' security we will look at a layered defence approach. Topics that we will discuss will fall into any of the 3 areas below:

1. Physical Security (protecting the hardware)
2. Network Security (protecting the software and communication channel)
3. Data Security (protecting your data)

Physical Security

Mobile computing has become a valuable part of everyday computing, allowing remote users to perform the same tasks as office workers whilst travelling all over the country. However the mobility, technology and information that make laptops valuable to employees and organisations also make them valuable to thieves.

Imagine if a senior director has lost his laptop with confidential company information on it. What potentially could be the implications of this indiscretion should it fall into the wrong hands? Share price could drops, customers could lose confidence in your company, or in the worse case scenario the director could be imprisoned for contravening the Data Protection Act.

So given the risk of laptop theft and the consequences of the potential losses that a stolen laptop can cause, we will be looking at steps that individuals and companies can take to prevent such threat.

One of the most cost effective ways to deter thieves is to attach a security cable to your laptop. By physically securing the laptop thus making it immobile could be enough to deter a potential thieve. Over 80% of the laptops on the market are equipped with a Universal Security Slot (USS) that allows them to be attached to a cable lock or laptop alarm.

However as is the case with any security measure, determined thieves are able to overcome such obstacle. Instead of breaking the strongest link which is the cable itself, thieves could instead try to break the desks to which the cables are attached.
Also a security cable is unable to protect any equipment attached to a laptop like external CD-ROMS or any device attached into their PCMCIA slots.

There are some pitfalls associated with security cables but overall it is an effective measure to deter most thieves. Another good solution is common sense itself, a laptop users can help to ensure the security of the device by following some simple steps.

1. Keep the laptop out of sight
If the laptop cannot be seen then opportunists on the lookout cannot steal what they can't see! When the laptop isn't being used, it should be safely tucked away in its bag or in a locked desk drawer.

2. Disguise your laptop with an ordinary carry case.
Keeping with the theme of keeping a laptop out of sight, an expensive looking carry case with the laptop's manufacturer logo splattered on the side might attract unwanted attention. By having a ordinary looking carry case will no doubt conceal the identity of the contents and therefore not attracted the eyes of a potential thieve.

3. Keep the laptop close by.
Remain in physical contact with the laptop at all times. A few seconds is all that is needed for a thieve to swipe your laptop, so don't leave it anywhere unattended even When travelling by plane or rail, do not ever place the laptop in checked baggage.

Reference 1

Protecting your data

Next we will be looking at several methods to prevent information loss and to protect valuable information even if you do lose a laptop.

There are a number of methods available to make a thief's life more difficult when trying to access a stolen laptop.

1. Set a system password.
Every remote user should protect their laptop with a system password. This way, a system password prompt will appear each time you start your computer before Windows even begins to load. It will prohibit any access to the computer at all, until a valid password is entered. However a determined thief could bypass this by physically opening the laptop and removing the CMOS battery or shorting some jumpers to reset the BIOS to a default state.

2. Set a Login Password.
The password is the cornerstone of all computer security. If you are running an operating system that supports proper logins like Windows or Linux then setting a password is required. *(Reference 1)*

Passwords are the weakest link in enterprise IT, concludes a new report by Secure Computing. The report found that business travellers run the risk of compromising their company network when they use public internet access points. At an airport internet kiosk for example, it was suggested in the report that an attacker could easily install a keyboard sniffer to capture all keystrokes entered in a hidden file.

The first and most common sense rule for passwords is not to give your password out. Another just as important but sometimes less obvious is not to write your password down or have it written somewhere inside your laptop case. Make sure you are not using your name, date of birth, favourite colour, or something else easily guessable as a password. This simple rule would save a lot of administrative headaches and potentially your data as well: Don't use an easily password. The stronger your password is, the less likely an attacker is to gain access to your machine.

(Reference 5

Some tips in selecting a stronger password.

1. Do not use password that are easy to guess and not based on words found in a dictionary.
2. Make sure your password contains a combination of upper, lower case characters. Include numbers and symbols.
3. Don't use the same password for everything.
4. Never tell anybody your password, even if they claim to be someone from your IT department.

By following some of these simple rules you could deter thieves from accessing your laptop and any confidential data on it. However passwords should not be relied upon as the only measure for security on your laptop.

Within Linux for example, a thief could use a brute force attack on your password file, or simply a boot and root floppy could be used to bypass your password and logins completely. The windows system is no better, if your laptop isn't using NTFS, accessing the data on your hard drive is a minor hurdle for an attacker.

Even if you are using NTFS doesn't necessarily mean you are safe. An attacker could use a utility like NTFSDOS which allows them to mount an NTFS drive, thus allowing the attacker to manipulate your information as they see fit.

Another vulnerability with windows NT/2000 is a program widely available called NTPASSWD. This program can create or modify existing logins and password without prompting for the original password. This is very dangerous as an attacker could change an Administrators password therefore allowing access to everything on your laptop.

Biometric authentication mechanism can be used to replace or supplement passwords on most operating systems. The methods used in biometrics is to use the uniqueness of certain features of a user such as fingerprints, retinal patterns, voice recognition and even typing characteristics to accurately identify and authorise persons.

Evidence in the use of biometrics is increasing as a means to identify and authenticate individuals.

Reference 3 + Reference 7

- The Home Office has announced that it is planning to install biometrics in 10 UK airports by the middle of next year to assist immigration control.
- The Nationwide Building Society is running extensive biometrics tests using iris scans in place of PINs at cash machines.

- Most recently, the Home Secretary announced that national ID cards – to be phased in over the next five years – will incorporate biometric data access via fingerprint recognition.

We have so far looked at a few vulnerabilities that a potential thief could bypass your password protection. Assuming that the thief has bypassed this line of defence, there are further means of protecting the information stored on your laptop. One method to protect is to advanced Encrypting File System (EFS) security feature available with the NTFS file system.

With EFS, you can choose to encrypt files and folders. If someone was to then someone gains access to the file, for example by stealing your laptop, they can't decrypt the file and see your information. Once you choose to encrypt a file, the actual process of data encryption and decryption is completely transparent and requires nothing on a user's part. *Reference 8*

We have so far looked at various measures to ensure the safeguard of devices vulnerable to outside attacks, thefts or losses. An organisation should therefore implement the same type of security strategy that would be for any other type of computing on the network. A good security process is implemented in layers, affording the maximum level of protection while still supporting the need of the remote work force.

Today's new mobile devices share many common vulnerability; devices are bought from shops with open operating systems, multiple connection ports and practically no peer to peer security. Installation of these devices is fast and easy, potentially creating an uncontrolled computing platform that can access a company's network. Further more, because such devices are small and portable the risk of theft or loss are greater, which potentially could put confidential data into the wrong hands.

Once you have secured the physical device, the next area to secure is the network, the applications and its data. Having a mobile workforce in a connected world requires securing devices a priority as they can potentially be left open for attack if not properly configured.

Over recent years the internet has been a valuable resource to mobile workers, enabling connectivity to the office from virtually any location. However even though the benefits are substantial, from a security prospective the drawbacks can also substantial if all vulnerabilities are not take into account and managed properly.

Personal Firewall

A device on the internet can be vulnerable from attacks by every worm, virus and hacker unless properly protected. Internal systems within a company are protected by one or more firewalls, a laptop attached to the internet should also be protected by a firewall.

Microsoft has included a basic firewall with Windows 2000 and XP suitable for performing the most crucial task required of a firewall. However there are limitations when using a built in firewall. With no decent GUI to manage the configuration, a typical user will need to really know what they are doing if they want to do anything beyond blocking all incoming packets.

Personal firewalls should be no different to company firewalls when it comes to functionality. Some of the features and functionalities a personal firewall should have are:

- Stateful packet filtering
  The ability to block incoming ports and protocols

- Robust protocol support
  Ability to support various protocols like UDP, TCP, ICMP etc.. Able to define custom protocols.

- Application Protection
  Filtering based on the application, ability to block certain applications that violate the security polices set by the organisation.

- Intrusion detection (IDS)
  Automatically block packets that meet well defined attack signatures. Automatic update of IDS signatures.

- Firewall rules
  Ability to support robust rule configuration with priorities and clear definitions of internal and external components. Dynamically update firewall rules depending on factors such as company network or remote access. *(Reference 2)*

A well configured firewall is an essential part of your line of defence, however even the greatest firewall can't entirely stop users from allowing their systems to be a target of a virus/worm attack.

Anti-Virus

A regularly updated virus scanner should be your next line of defence. An anti virus package provides remedy against viruses and worms but only if they have the latest virus definition and engine. Mobile devices are a bit more difficult when keeping virus definitions up-to-date compared with systems that are always connected to your network. Remote users may not connect for days or even weeks making virus definitions out of date and susceptible to the latest virus or worm attack.

Here are some points to look for when selecting an anti-virus product:

- Ability to support scheduled and multiple scheduled scanning, whilst not degrading system performance
- How frequent does the software vendor update virus definitions and engines. Check response time between virus outbreak and definition update.
- Ability to update internally (connected to your network) and externally (when connected to the internet only)
- Are there strong logging capabilities; how transparent is the software to the user, can it be disable by the user?

A good anti-virus should offer real-time e-mail and instant messenger scanning, it should also look for Trojans, ad-ware and key loggers, etc. It should also provide alerts when a virus attack is detected and provide detailed reports on virus detection and deletion.

(Reference 2)

Securing Communications

So far we have looked at physical security and methods to further secure a laptop and its data in an event of a theft or loss.

An important element for remote users is the ability to communicate back to the office to access company resources (e.g. e-mails, calendars, files etc) as part of their day to day tasks. However to do this securely you need to take steps to ensure the privacy of the communication between the remote user and the office network isn't compromised.

To do this we use a Virtual Private Network (VPN). A VPN is a private tunnel that connects two networks through a public network, usually the Internet. Using a virtual private network entails encrypting data prior to sending it across the Internet and decrypting it at the receiving end. There are many different methods to choose from, each with their own strengths and weaknesses. We will look and compare two main methods available today, which are IPsec and SSL;

IPSEC Strengths

- Client transparency – the client perceives they are directly connected to the network
- No limitation to the supported applications
- Access control generally tightly integrated with leading firewall vendors
- Leading vendors have personal firewall functionality in their clients

IPSEC Weaknesses

- Client installation required
- Support implications of remote clients
- Access limited to install base of client
- User education
- Poor extranet solution
- Lack of platform support I.e. Linux/Mac/PPC
- Lack of interoperability between vendors clients

SSL Strengths

- Ease of deployment
- No client to manage
- Ideal extranet solution
- Ease of traversing 3rd party networks
- Ease of use
- Access from any terminal with a web browser
- Securing web applications
- Application layer

SSL Weaknesses

- Network access is not transparent, however application level access can be expanded upon
- Loss of 'trust' of the client and the security implications this leads to
- Access control lacking from some vendors

(Reference 4)

Security in a Wireless World

The world today is going mobile, modern wireless networking products are reasonably priced, easy to setup and very convenient to remote users. Low cost remote access to a high bandwidth service is perhaps the biggest driver. However they are also full of security holes.

In 2003 alone the following devices were shipped;

- 516 million mobile phones were shipped worldwide
- 11.46 million PDA were shipped
- Around 26 million mobile PCs were shipped
- 3.1 million WLAN Access Points, 5.1 million broadband gateways and 16 million WLAN add-on adaptors were sold.

The future of the Hot Spot market is hotting up too;

- By 2005 over 80% of notebook PCs will have an 802.11 WLAN interface
- By 2005 10% of broadband Internet access will be through public and campus WLAN hot spots
- By 2007 there will be 31 million frequent users of public WLAN hotspots, and over 35 million infrequent users.
- By 2007 revenue from WLAN hotspot users will surpass $9 billion.
- The average enterprise will have 80% more mobile application in the field by the end of 2004 than in 2003.

(Reference 8)

The world of 802.11 has a number of standards, many of which are incompatible. The process of designing and implementing a secure WLAN is something of a minefield.
Increasingly remote workers have WLAN implementations at home on their broadband connected network, which will in doubt raise questions from a security prospective.

Generally out-of-the-box configurations of WLAN hardware by default have security features turned off. Remote users buying these products are more concerned with the product working and therefore often security is overlooked. This could be a risk as an attacker could easily access devices within WLAN environment if the security is poorly configured or not al all. It is an even bigger risk if you allow remote users to access a company network via the WLAN as an attacker could penetrate to the company network.

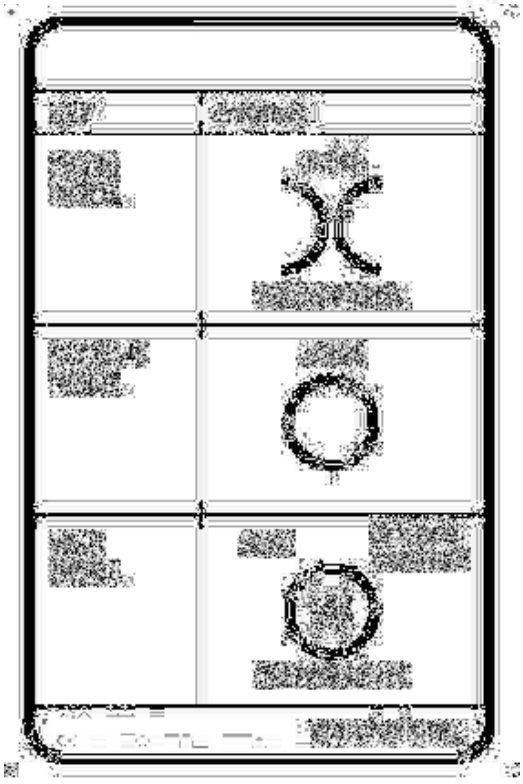
There are many tools available on the Internet for would be hackers to use to access WLAN devices. Here are some tools and their uses:

- **NetStumbler** Basic WLAN finder
- **WINC** Basic WLAN finder
- **Aerosol** Basic WLAN finder
- **Wellenreiter** Another WLAN finder / traffic sniffer
- **Kismet** The best WLAN finder / traffic sniffer
- **AirSnort** Sniffs WLAN data and extracts the WEP key values
- **WEPCrack** Takes'sniffed' WLAN data and extracts the WEP key values
- **WopAP** WLAN jammer – emulates thousands of Access Points

(Reference 4)

If you have a WLAN, you should beware the trend to identify its existence to the all using "Warchalking" In London this practice is apparent. Usage of the information may be hostile – or just for some free surfing by someone external.

Symbols below could be found on walls or pavements near WLAN environments.



(Reference 4)

Information can be found on websites and bulletin boards that identify WLAN sites providing details for others to use to access a WLAN even including pictures.

James Street, London

by Anonymous Hero, Wed Dec 10th, 2003 at 08:32:06 AM EST (Pictures and Locations)

Looks like there's a hottie somewhere on James Street, adjacent to Selfridges. SSID jre-wireless-4 and numerous Rendezvous contacts popped up near to the Lamb pub and also nearby the courtyard. Patchy reception, but good speed - managed to get a handful of audios downloaded before I got cut.

Comments >>

Access point in London

by Anonymous Hero, Thu Apr 22nd, 2004 at 01:13:27 AM EST (Pictures and Locations)

Plant yourself in The Lemon Tree just off Trafalgar Sq and access the interweb for free, sitting at the window. There is an open access point that hasn't been chalked yet. It has nothing to do with the pub but thought you'd may as well have a pint! Enjoy. n.b. This point was open on friday night 16th April.

Comments >>

(Reference 4)

.

After identifying some of the vulnerabilities associated with WLAN and the ease to which unauthorised access could occur. We will now look at some options available to secure WLAN points as Do's and Don'ts;

Do's

- Use at least WEP encryption , the in-built security for WLAN data.
- Gateway or Firewall ALL Access Points – treat the WLAN as untrusted.
- Regularly MONITOR gateway or firewall LOGs.
- Ensure the wireless channel(s) you use are reasonably clear.
- If possible, use directional antennas on Access Points.
- If possible, configure your WLAN as a CLOSED system.

There has been a lot of bad press regarding WEP encryption, the algorithm used to encrypt is weak. Encryption keys and data can be extracted given time by using some of the tools mentioned earlier. There are other forms of stronger encryption to use including:

- WiFi Protection Access (WPA)
  This is a new improved WEP that include a TKIP key refresh process,
- IPSEC
  Very secure, but its use limit client type
- SSL
  Secure, with a wide choice of client hardware.

For really secure connection it is recommended to use a combination of the above two, e.g. WEP + IPsec or WEP + SSL.

Don'ts

- Don't use any WLAN hardware 'out of the box'. Security is off by default.
- Don't connect Access Points anywhere on the internal wired network.
- Don't allow any staff members to install WLAN hardware.
- If you broadcast an SSID, don't make the name too obvious.
- Don't use the default manufacturer SSID (e.g. tsunami)
- Don't allow Laptop and mobile PC hardware to have WLAN clients configured ON if they are not used.

(Reference 4)

Creating a sound policy is the first step to implementing effective WLAN security for your remote users. Good security starts with understanding your potential areas of vulnerability. Controlling WLAN hardware for a remote user is almost impossible as the nature of their location is remote therefore knowing what they have is difficult.

Provide configuration help or guidelines to your remote users so if they do purchase WLAN hardware some guidelines are available. An inexpensive yet equally essential security measure against all computer threats is of course, user education

References

Reference 1
Ryder, Josh. “Laptop Security, Part One: Preventing Laptop Theft” July 30, 2001
URL: http://www.securityfocus.com/infocus/1186

Reference 2
Rudis, Bob. “Protecting Road Warriors: Managing security for Mobile Users”
April, 2004
URL: http://www.securityfocus.com/infocus/1777

Reference 3
Ryder, Josh. “Laptop Security, Part Two: Preventing Information Loss”
August 13, 2001
URL: http://www.securityfocus.com/infocus/1187

Reference 4
Integralis. “Mobile Security Seminar Series” June 2004
Attended the seminar in Manchester, United Kingdom.

Reference 5
Claburn, Thomas “Mobile Working Leaves System Passwords Vulnerable to Attack” Computing Magazine, March 2004.

Reference 6
Goodman, Tom. “Embracing Mobility: Three Steps to an Effective Mobile Security Policy”
SC Magazine November 2003

Reference 7
Biometric Security: “More Bottom-Line Benefits Less James Bond”
SC Magazine December 2003

Reference 8
Gartner Dataquest, IDC, Strategic Analytics

Reference 9
Microsoft, “Encrypt Your Data to keep it safe” August 2001
URL:
http://www.microsoft.com/windowsxp/using/security/learnmore/encryptdata.mspx

Last Updated: July 27th, 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
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
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
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
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 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
SANS Baltimore Fall 2017	Baltimore, MD	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