Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Basic Travel Security Revisited

The purpose of this paper is to survey and expand on the techniques put forth by other authors (1,2,3) to keep laptops "safe" while they are outside the protection afforded by a properly configured and maintained network. It is not what security professionals do when they travel because simply put they should know better, rather it is what employees do when they travel. Furthermore, if traveling employees are informed of security procedures in terms that they can understand and independently implement then they should ...

Copyright SANS Institute
Author Retains Full Rights

AD

Basic Travel Security Revisited

Thomas Palmer

August 6, 2001

Abstract

The purpose of this paper is to survey and expand on the techniques put forth by other authors (1,2,3) to keep laptops "safe" while they are outside the protection afforded by a properly configured and maintained network. It is not what security professionals do when they travel because simply put they should know better, rather it is what employees do when they travel. Furthermore, if traveling employees are informed of security procedures in terms that they can understand and independently implement then they should see that they have a stake in the fate of the laptop they carry. Ultimately, users are going to have to answer to federal or state authorities alone whether or not they comply with security procedures or not. When this process has come full circle users would be more willing to comply with other more technical procedures that they may not understand.

Therefore, it is my intent to show by example where possible, how various techniques have been and are still being utilized today. The specific areas that I will cover are maintaining a "security zone", cars and taxis, airports, airplanes, hotels and convention centers, lessons learned, and the need for user training. This paper is intentionally written to help administrators convey information to end-users who, unbeknownst to them, have the power to compromise even the most secure network. Users, for the most part, just want their mobile devices to perform as well as any other tool that they use to work. The trick is to allow them to be effective and secure.

For the sake of briefness and clarity I will use the term laptop to refer to any mobile devices we examine, be they notebooks, laptops, PDAs or any other future "mobile device" that has yet to be invented. The basic techniques set forth on in this paper can and should apply to all mobile devices.

Any time a device or tool becomes more portable it becomes more useful. The "tool" can be moved to the "job" instead of the "job" being moved to the "tool." Laptops and other mobile devices are exceptionally useful in allowing people to work where they will be most effective in doing their job. However, with this mobility comes a potentially catastrophic consequence; theft of not only a laptop, and the information it contains, but also the network connection identification. Once a laptop is stolen it is only a matter of time before the thief can gain access to the information on the laptop and, from there, any network identification information that the laptop contains.

An analogy to this phenomenon is identity theft. Identity theft occurs when a thief steals someone's private papers, mail, or even garbage and obtains enough information (credit card statements or offers for credit cards, bank statements etc.) to, at least to the outside world, become that person. Similarly, once the confidentiality and integrity of the laptop has been compromised, the thief/cracker's machine can then masquerade as that trusted machine and the confidentiality and integrity of the network can be breached. Once the network is compromised the cracker can do what he or she pleases. At this point, the cracker can expose to the world any confidential file or directory on the network or even launch an availability attack using the networked computers to bring down whatever server the person desires. He can open a back door into the network enabling him to virtually allow the whole world to poke around the company's network or even launch confidentiality, integrity, or availability attacks against a totally separate network(s).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

In order to limit the likelihood of laptop theft we will review seven issues that have been brought to the forefront where I work, for combating laptop theft. The first is maintaining a "personal security zone" around yourself. The second is cars and taxis and how to keep the laptop from being left behind. The third issue is how to safely traverse an airport. The next is how to safely work on an airplane. Fifth, we will examine how safe are hotels and convention centers. The sixth issue to be examined is what lessons we have learned where I work about preventing laptop theft. The seventh and final issue to be discussed will be the need for user training.

Other writers have covered these topics (1,2) however, little attention was paid to engaging the employee (via security experts) to take positive steps to ensure a safer network. To engage and motivate people they need to feel that they can take positive steps that are understandable to them. In turn, this brings them "on board" helping to ensure that their network remain free of compromise from the cracker trident of integrity, confidentiality, and availability attacks because so much of network security is dependent on what they do or don't do.

Tools like L0pht that monitor IP traffic, locate IP addresses and other sensitive data on the local Ethernet segment, Netbios scanners like Legion and NAT to find and connect to exposed shares, and other tools provided in the NT/2000 resource kit are not something that they need to know how to use and interpret. Of course, these tools run in the hands of ethical security professionals or network administrators that have been given permission to utilize them are fine but run-of-the-mill users have no need of these tools. Even if users' laptops so much as contained these "tools" when attached to a different company's network it would at best cause deals to fall through. Users don't need to know that if a cracker is able to gain possession of their laptop the cracker can boot to a different OS, copy their SAM file to a floppy add a cracker "administrator account" to the SAM and then copy the forged SAM back to their laptop via the repair disk. They do need to know that once the OS has succumbed to these integrity and confidentiality attacks the cracker has stolen their identity and at some point they are going to have to answer for what the cracker has done in their name. In order to prevent this from happening they need to limit the likelihood of laptop theft to keeping these seven security issues in mind.

"Personal Security Zone"

Where I work we tell our employees, when they are in the airport or anywhere else, to maintain a "security zone" around themselves even if they feel safe. We define a personal security zone as an area around your person that is roughly arm's length. Naturally, the security zone is dependant on how crowded a particular area is at any given time. If someone they don't know violates this zone they should move away from them if they can. I like to use a personal example to illustrate this point. While on business in Europe I was at the Rome International Airport and was walking down a concourse to get to my plane when a young boy and girl (they must have been about 10 years old) approached me. The boy grasped my hand and was gently pulling on it while talking to me softly in Italian. The girl, however, had a newspaper that, after a second or two, I noticed was partially covering her hand and partially resting up against my stomach. Below the newspaper the girl was opening the fanny pack in which I had so cleverly stored my laptop's hard drive, passport, money, and plane ticket. Fortunately, I reached down and grasped the girl's hand under the newspaper and turned it over so that I could see what, if anything, was in her hand. When I did this, the boy immediately released my hand and ran off. The girl however, had a panicstricken look on her face as we stood there for a second or two staring at each other. Since my Italian is limited and there was no one else around, I threw her hand away and yelled for her to get away from me. She did so as fast as she could. That was the only thing we both agreed on that day.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Since that day I always maintain a security zone and generally take a few other precautions to ensure the safety of my equipment. For example, if I sit down and I am carrying a laptop case I put my foot through the strap of my laptop case. If I get anything out of my case I zip the case closed again and look around to notice if anyone is trying to see in my bag while it is opened. I also try to be discreet when I travel and avoid having any company logo appear on my luggage. My intent is to look like I don't have anything much to steal. I know, security through obscurity, but it is working so far. I also don't tell people that I meet in my travels where I work and especially what I do. If I am pressed to expose what I do I try to steer the conversation to my kids or the difficulties inherent in the other person's job.

Cars and Taxis

Cars and taxis seem to be a place where people seem comfortable and relax their guard. People appear to feel safer in a car, whether it is their own car or a taxi. Perhaps it is the familiar surroundings. The problem obviously occurs when they get out of the car or taxi and leave their laptop behind. For instance, a story that appears in a recent issue of Computerworld is a perfect example of how one person felt that leaving their laptop in their car was safe. www.computerworld.com/cwi/story/0,1199,NAV47_STO60994,00.html. This is an ongoing story of how a worker with limited computer ability becomes the prime suspect in the Federal Government's investigation of a financial institution that had suffered a confidentiality and integrity attack. The financial institution was hacked and the hacker gained access to a DNS (Domain Name Server) and from there to an Oracle database that housed credit card numbers via a trust relationship. The worker's original mistake was leaving his laptop in his car, the car was broken into and...

In taxis, people are either in a hurry or are often distracted and forget about their laptop and leave it behind. If a person took a second or two to put an arm through the loop of the case then no matter how "distracted" the person was the strap would "tug" on their arm when they went to get out of the taxi. Additionally, if the person filled out a luggage tag with a contact name and phone number and attached it so that it is seen from outside the bag, if an honest person found the case they would have the chance to return it.

Airports

Another prime location where people and problems walk hand in hand is the airport. In the airport there are several different areas that pose security risks; the check-in counter, the security checkpoint, laptop connection businesses, waiting areas, and luggage pick-up areas.

At the check-in counter is where your attention is focused on the counter person and not on your carry-on luggage. To illustrate this point to our leading salesperson I reached down and grabbed his laptop case and waited for him at the end of the check-in counter when we were flying together. The look on his face was enough for me to know that I had proven my point. Again I mentioned to him about putting his foot through the loop of his case to prevent someone grabbing his carry-on.

A second place where trouble can happen is at the security checkpoint. Often the thieves snatch and grab from the conveyor belt while the target is detained at the metal detector (Reid). In Basic Travel Security Weissenfluh explains a very good way of having the laptop go through the metal detector without its hard drive, which is put in a jacket pocket and sent in separately. This, of course, can only work if the laptop has a removable hard drive. Another way that we have found to send a laptop safely through a security checkpoint is to hand the guard manning the metal

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

detector the laptop, then pass through the metal detector. It has been our experience that when you hand someone something they feel responsible for it and want to quickly hand it back to you as soon as you are clear of the metal detector. Additionally, handing a laptop to the guard at the metal detector may actually speed things up. We had a report just the other day that one of our salespeople was running late and the guards at the checkpoint wanted her to start her laptop in order to show that it worked and wasn't a bomb. If she had to fish her laptop out of her bag; re-insert her hard drive, and then powered up, she would have missed her flight. Naturally, we told her that sometimes security procedures can actually save time.

Admitedly, there have been a few times where the guard at the metal detector has insisted on having the laptop placed on the conveyor belt. We tell our people to hold on to the laptop until it is their turn to walk through the metal detector. Then after putting their laptop on the conveyor belt keeping a close watch on the laptop. If there is anyone loitering at the end of the conveyor belt say in a loud voice something like, "Is my gray Toshiba laptop ok to pass through your scanner?" What this does is interrupt everyone's routine expectations of what goes on at a security checkpoint and rivet attention on your laptop.

The third high-risk place at an airport is Internet connection businesses. These businesses appear to be prime locations for crackers to set up shop. I don't mean to imply that the people that own these businesses are crackers, but if I wanted somewhere to lie in wait for someone in order to obtain information, these places seem ripe for the picking. I have seen people rushing to get inside their cubicle and connect to the Internet. It is safe to assume that security policy and procedures are not foremost on these people's minds. We advise our people to only use these places in dire emergencies.

A fourth trouble spot is waiting areas. At the gate or at the bar, either place can lull a person into a false sense of security. People feel as though they had reached a sort of goal and could now relax a bit. This happened to one of our VP's. He arrived at the airport an hour early, maintained a discreet personal security zone, kept track of his carry-on at the check-in counter and the security checkpoint. After all this, he went to get an ice cream cone to bring it to the gate. After he finished his ice cream he went to throw the container away and when he got back to where he was sitting his laptop case was gone. Fortunately, he got the laptop back but we still made him change all of his passwords and pass phrases as well as ran intensive scans for viruses, trojans, and the rest. Naturally, we paid special attention to our logs and ids for any anomalies on the network side of things.

The last place we have found for theft is the luggage pick-up area. Here the person may walk away from his laptop case to get the rest of his luggage. This happened to colleague of mine that works at another company. He walked about three feet away from his case and someone snatched the carry-on that had his brand new laptop in it. He thanked God that he was too busy to configure it to access his network.

Airplane Travel

Weissenfluh's paper explains how he was able to obtain sensitive information from just sitting behind a diligent worker on an airplane. At Work we too discourage people from working with their laptops on an airplane because of the physical dangers and information loss that working on the airplane presents. Only on an airplane would you allow a person (the flight attendant) to pass at least one if not more drinks over your laptop and possibly short it out causing a nasty availability attack against yourself. We recommend to our people that they move the laptop out of harm's way. To prevent information loss we also recommend that people who "have" to work

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

on the airplane to request a seat change so that they can sit in the back row of the airplane, which eliminates the possibility of someone looking over your shoulder. We also remind employees that it gets harder to see a laptop screen when the angle that another person is viewing from exceeds 30°.

Another problem in airplanes is where to store the laptop on an airplane. Naturally, the overhead bin is not a good place for two reasons. First is the issue of the laptop dropping to the main floor and being damaged. Secondly, someone else can grab your laptop, either by mistake or by design. Logically the only other place to store the laptop is under the seat in front of you. This is what we recommend to our people, only with two modifications. We advise our employees to keep the bag zipped up so the laptop doesn't fall out and to stick one of their feet in the shoulder strap in order to keep the laptop case from sliding forward and crashing into something during a rough landing.

Hotels and Convention Centers

After calling several different hotel chains Hilton, Marriott, Ramada, etc I was informed that the security of the internet connection in the rooms was something that was left up to the individual hotels, and that there was nothing chain-wide to enforce. So the only advice I can give is to encrypt the laptop and any messages with PGP, have a good personal firewall in place, as well as an up-to-date virus scanner. As far as convention centers are concerned the same advice applies.

Lessons Learned

In each of the aforementioned instances, we handled some of the potential threats very well while others were learning opportunities. In keeping with my company's security policy, I am unable to go into great detail, but there are some basic things I can mention. In securing the information contained in our laptops we applied a multi-tiered approach depending on the information the laptop contained. For example, we:

1) Encrypted all hard drives & installed/Upgraded a personal firewall

2) Provided motion detecting alarms for laptops

3) Provided security cables for laptops

4) Additional VPN access controls

The most contentious issues we still are dealing with are what information to put on luggage tags and the use of luggage locks. The sticking point on the tags are should the company name and main phone number be on the tag or should the person provide an unlisted phone number. It is my belief that if the employee's name and a phone number that connects to an unlisted phone number located in our department be on the tag. This gives away the least amount of information and still provides a way for someone to get in contact with us even if the user hasn't yet. This can increase the likelyhood that we need to disable the dial-up account and prevent a possible intrusion as well as return the laptop.

Others in the company contend that the laptop and its case are company property and the company name should be on the tag with the main company phone number. Additionally, the company needs to know that a laptop has been lost and this would be accomplished if the company name and phone number were on the tag. I have come to the conclusion that if the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

company name is on the laptop case with the main company phone number and if the person that finds the laptop has an axe to grind against the company at best they won't return it. At worst, the person that finds the laptop will get whatever information they can get and use it for ill. Our working solution for right now is to have the person's name and an unlisted phone number that is hooked up to a phone answering machine located at the security desk on the tag.

The other contentious issue is the use of luggage locks. Admittedly, they won't keep a determined person out of the carry-on, but it would keep the curious from opening the carry-on. The person would have to resort to calling the phone number listed on the luggage tag. Others in the company point out that the locks can't keep everyone out and that they are inconvenient. Whether or not the use of luggage locks is made part of our security policy or not has still to be decided.

User Training

Perhaps the most difficult and time-consuming addition to our security procedures was the implementation of additional user training (Cartwright, Weissenfluh, and Wilson) to not only provide information on the proper use of laptops, but also why they need to use the laptops in a secure fashion. In an attempt to convey to our employees the need to use laptops securely, we had law enforcement agencies come in and talk with employees about what will happen to them when their machine is used to hack into any network not just ours. We told them that we were proceeding under the assumption that they had no connection to the hacking event. However, they would still have to at least meet with law enforcement officers and be questioned about their connection to the incident.

Additionally, we post at various places where people tend to congregate; the printer, the cafeteria, pod secretaries' cubicles, company news bulletin boards, etc., any information about companies being hacked into. We especially like to post what happens to workers that get caught up in these hacking incidents. We also encourage people to submit any questions that they may have to us.

We also verify that the person taking a laptop on a trip perform the following check list:

- Back up data and programs prior to leaving the building.
- Ensure that the virus software is up to date
- Check to ensure that the laptop has the employee's name and the "company's" phone number on it and if the laptop has a removable hard drive that the same information is placed on it as well.
- Make sure that any passwords/pass phrases that may be needed are in force for the length of the trip
- Record the serial and model number of the laptop
- Test to make sure that the laptop is in good working order
- Users have good removable media to bring with them
- Ensure the employee is up to date with the latest company procedures on laptop security

Conclusions

In this paper we explored how laptops are very effective tools that allow for company personnel to have access to information be it stored on the laptop or via a connection to the network. Because laptops are so good at information gathering and storage they are continually under threat by unscrupulous people. These people seek to exploit the mobility vulnerability inherent in

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

laptops in order to snatch them away from unsuspecting personnel. These workers' only mistake was momentarily being distracted, but that is enough to have the laptop stolen.

The next point that we looked at was the importance of maintaining a "security zone" and not allowing anyone that they don't know to violate that zone. I don't mean to imply that a person should look or act as though they are afraid of the situation, just to discreetly move away from a potential threat. If anything, I would encourage everyone to walk confidently as though they owned the place.

We next examined several places that people tend to drop their guard because they feel safe for the moment or they get distracted. We discussed cars and taxis and how people, either through feeling that the car is theirs and therefore whatever they leave in it will be fine or, people just being in a hurry, forgets about the laptop and leaves it behind. We examined airports and airplanes and how to always be aware of where your laptop is either by being able to see it or be in physical contact with it at all times. We also took a look at hotels and convention centers.

Lastly, we examined lessons learned and user training. The two subjects are open-ended and need to be delicately handled. At my company it seems to be mainly a balancing act of giving enough information/access to employees to do their job, and not too many restrictions to alienate them to the point where they go out and cause more problems; I have enough already, thank you.

In closing I would like to reiterate an important concept that as Mr. Cole pointed out in Security Essentials; that networks should have a layered defense like a medieval castle. A layered defense that is comprised of firewalls and other perimeter defenses, such as virus scanners to protect from trojans, worms, and the rest of their ilk. In addition, having an ids in place to detect anomalies in the network thus allowing for learning how to stiffen your defenses. Having skilled people that know their systems and how to analyze what the information that these defensive systems are telling them is vital. Exercising due diligence in keeping up to date with patches, alerts, virus software while always scanning at different places in the network architecture. The castle of your business can be kept "safe" from the three prongs of confidentiality, availability, and integrity attacks.

It is disheartening that after all of this time, effort, and expense all it takes is one person who experiences a few seconds of inattention to potentially bring down a network. In order to prevent this, company personnel need to be made aware of simple ordinary things that they can do or shouldn't do, so that they can help prevent such catastrophic consequences from happening.

References

1) Weissenfluh, Aaron. "Basic Travel Security". October 26, 2000 URL: www.sans.org/infosecFAQ/travel/travel_sec.htm (30 June 2001).

2) Reid, Frank. "Securing the Mobile Businessman". October 24, 2000 URL: www.sans.org/infosecFAQ/travel/mobile.htm (30 June 2001).

3) Cartwright, Warren. "Managing Security in a Mobile Environment". February 17, 2001 URL: www.sans.org/infosecFAQ/travel/managing_sec.htm (30 June 2001).

4) Thurman, Mathias. "What to Do When the Feds Come Knocking". Computerworld. Volume 35, Number 23 (2001) 62

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

5) Thurman, Mathias. "Manager Locks Down As The Feds Move In". Computerworld. Volume 35, Number 25 (2001) 44

6) Wilson, Zachary. "Hacking: The Basics". April 4, 2001 URL: www.sans.org/infosecFAQ/hackers/hack_basics.htm (30 June 2001).

7) Cole, Eric. "SANS Security Essentials Conference" May 23-25, 2001 Minneapolis, Minnesota.

8) Paul, Brooke. "Building an in-depth defense" Network Computing. July 9, 2001

9) Electic Consulting, Inc. "Laptop Security". (1998) URL: www.laptopsecurity.com/ls (30 June 2001).

10) Carnegie Mellon University. "Eliminate all means of intruder access" (30 April.2001) www.cert.org/security-improvement/practices/p050.html (30 June 2001)..

11) @stake, Inc. "Humans Are The Weakest Link In The Security Chain – Say 'Goodbye' To Your Business" (1 May 2001) www.atstake.com/events_news/press_releases/index.html?europe/050101 (10 July 2001)

12) Elkins, Monta. "Anatomy of a Break In" Linux Journal. (1 May 2001) http://www2.linuxjournal.com/articles/culture/0022.html (31 June 2001)

13) Hilton Hotels and Resorts. Hilton Reservations Worldwide. 1-800-445-8667 (31 June 2001)

14) Marriott Hotels Resorts Suites. Out-of-Town Reservations. 1-800-228-9290 (31 June 2001)

15) Ramada Nationwide Reservations. 1-800-272-6232 (31 June 2001)

16) Scambray, Joel. McClure, Stuart. Kurtz, George. "Hacking Exposed Network Security Secrets and Solutions Second Edition". Berkley. Osborne/McGraw-Hill. 2001.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced