Global Information Assurance Certification Paper

Basic Travel Security
Aaron Weissenfluh
October 26, 2000

As I sat in the terminal waiting for my delayed flight, I read through Stephen Northcutt's book on Network Intrusion Detection. Earlier in the week, I was a bit worried about choosing the subject of my practical when I read a brief section on laptop security. It then hit me that I had found the subject matter for my practical assignment, where a good amount of information was contained on the Internet. As I travel quite a bit in my current job, I am exposed to all sorts of situations which call for a heightened awareness in the area of "travel security." In this brief writing, I will describe situations that I have seen and experienced and how to counteract the possible security breaches which could have devastating effects to a company that allows users to reconnect to the network following travel periods. This paper is written in three sections, airport security, airplane security, and hotel security. Each section will list a specific instance in which security was compromised and how to counteract that situation. This is not intended to be a complete guide to "travel security" but to point out the main areas of concern and how I deal with these areas. Also, as a security professional, I point out some examples that could be misconstrued as information gathering for the purpose of illegal activity, but they are just experiences and examples to emphasize the lack of security among travelers. When researching for this topic, I found that my experiences were not unique.

Airport Security

Although I have never been the victim of a quick snatch and run while walking through the metal detector, I truly understand the need for physical security while traveling through any airport both domestic and international. There are a couple of quick actions that I personally take prior to arriving at the airport when traveling. The first thing I do when traveling is to remove the hard drive from my laptop. This may appear time consuming and an extreme measure, but should a theft of my laptop occur, then my hard drive is not in the same location as my laptop. The most difficult part of removing a hard drive is where to store it once it has been removed. The second part of securing my laptop is to put the hard drive in my jacket pocket and put my jacket through the x-ray machine. That way, my laptop and hard drive are never in the same location. Placing a hard drive in your luggage creates another problem as luggage is often lost and locks on these pieces are close to useless. The most secure action is to purchase a small non-metal lock-box to place your hard drive and your personal effects in during your travels. Since most airlines allow two pieces of carry on luggage, this is usually acceptable.

One neat trick a friend taught me about going through security at an airport is to place all of your metallic items in the front flap of your laptop case so that you can immediately pass through security while keeping your eyes on your laptop and personal effects case. After making sure that I wore the light metal belt buckle, I pass through security without incident and wait for my laptop without taking my eyes off of it.

Once through security and into the waiting area (I usually get to the airport plenty early) I usually sit and read. A question that may have been asked during the previous couple of paragraphs is "How do I work on my computer if the hard drive is out?" The answer is simple, you don't. This may lean to the side of the super-paranoid, but when I am in airports, I consider my surroundings to be unsecured. Although this will be covered in the next section on airplane security, I will touch on it briefly here. How many of you remember the television show that was run about those people that hang out around airports video taping people on public phones? There were two methods that these criminals used to get calling card numbers: they videotaped those who were dialing the numbers and they mounted tape recorders under the pay phones so that the tones could be replayed later. In regards to computer security, whether your back is to a wall or you are sitting in a corner, someone may be watching your every keystroke or even worse, video taping what you write. Kevin Coffey, a security expert and undercover police officer reported in a recent ABC News online session, that "Crooks use cameras with zoom lenses to record this info. The best defense is to use calling cards or pre paid phone cards so numbers do not have to be punched in." (Coffey, 2000)

To counteract shoulder surfing, I do all my work on a notepad since my writing is awful. I transpose all information at a later time to my laptop or desktop computer. If you must do work on your laptop while in an airport, it is good not to display any secure or company proprietary information. When I return from a trip, I always change my passwords in the event that someone captured it while I was working.

Airplane Security

Once on the airplane, everything is controlled and safe, right? Not exactly. When entering an airplane with my two bags, I always place my computer and special hard drive box underneath the seat in front of me. The reason I make most of my trips very uncomfortable is that I don't need someone pulling my laptop down from an overhead bin while

I am sleeping. On my recent trip to New York, I was sitting behind a young, hard working individual that was catching up on some work before getting back to her home city. She was a consulting working on a major project in Kansas City which dealt with large amounts of information about a database that contained the inventory of a retail store. This young lady had a relatively short password on her laptop, but one that must have been relatively difficult to type in the small airplane space. She was fairly creative about two of her other passwords, one for the company database and one for email. I know that her director and other managers, whose names I will not include, would be proud of her for working so diligently during her travel time. Finally, I can call her anytime at work, home, or on a cell phone number to check up and see how she is doing.

Here's the information that was passed to me while on the airplane:

- First and Last Name
- Position in Company
- Hometown
- Home Phone Number
- Work Phone Number
- Cell Phone Number
- Company Name of Employee
- Company being consulted
- Logon password
- Email password and email address
- Database password
- Director's Name
- Manager's Name
- Vice President of Marketing

Although I don't intend to use any of the information for illegal purposes, I gained this information not through a conversation with this young lady, but just by sitting behind her and watching her work. Computers continue to grow more complex and more difficult for the masses to comprehend, but people will continue to be the weak link in the security system. Computers are not as easily manipulated as people. Most people in companies want to be helpful to both internal employees and customers. Regardless of the technological level of security, humans will always be the weak link in chain. With the above information, one can imagine the security holes that have been opened.

The solution for such a problem is to not do work on the airplane. A time crunch may not permit this, but I would restate my method of writing everything on paper and transposing it to my computer later. Also, I want to make it very clear that I have never undertaken illegal actions using information gained from the above methods and I never intend to do so, but use this example as a clear example of what could happen.

Hotel Security

These days, hotels are providing everything from high speed Internet access to cafes with Internet provided free of charge. Recently, I was at a conference in Washington DC staying at a great hotel with high speed Internet access in my room. After the conference, I began logging into my computer to get email, read security updates and keep in touch with my company. Two things came to mind when I was logging into this foreign, "unsecured" network:

1. This is Ethernet and everyone on this network can view the information that I am viewing.
2. I am on a large subnet so there are several hundreds of hosts that can view my information.

The following are the steps that a very low-level hacker would take to break into a computer on a hotel LAN.

Step 1: While on the hotel LAN, activate a sniffer program.

Step 2: After locating the IP addresses of unsuspecting hosts, run a netbios scan to see which of these hosts are running on Windows platforms and which of these hosts have open shares.

Step 3: Map a drive on your Windows machine to one of the open shares, preferably one that has a default password or no password. If this is not possible, use a password cracker to find remote passwords.

Step 4: Copy the custom Java or Perl script that you wrote that performs some malicious task such as sending your passwords through an email program to a remote mail server or starting a world wide macro virus contagion from your computer.

Step 5: Since most Windows NT users never lock down or log events happening in their registry, remotely connect to the unsuspecting user's registry and add the following value to the "HKEY_LOCAL_MACHINE on *remote machine* Software/Microsoft/Windows/Current Version/Run key: C:*openshare**maliciousssoftware.exe*

With the previous five steps, anyone could start the next Melissa virus. The most frightening thing about the above example is the anonymity of the attacker. Checking into a hotel with a stolen credit card is no more difficult than finding the right credit card number on the Internet.

The methods I use to counteract these and other hotel methods are to install a host based IDS system on my laptop. I have this running at all times, even when logged in at work. I am immediately notified of any port scans or any connect attempts from remote hosts. When traveling, I always turn off sharing on my Windows based computers so that none of my hard drives are shared. I have also set permissions within my registry so that only my system and I have access to the registry. I also log all activity to my registry keys with the correct user access…ie myself and my system. I always use my digital signature and PGP when sending email and use SSH rather than clear text telnet.

I would like to make a point on physical security in regards to hotels. Most hotels offer safety deposit boxes, but I prefer to take my computer(s) with me wherever I travel due not only to the high level of paranoia, but also to the fact that some people will not be very cautious when cleaning and could destroy my laptop. Get a smaller bag with a strap and carry your laptop with you on your travels. Also keep in mind that when traveling abroad, the US State Department advises that "Many hotel rooms overseas are under surveillance. " (US State Department, 2000)

As technological advances force hackers to become more intelligent and also to share information with each other. The simplest way past security is always through the human factor. As the cold war faded, a new war between corporations, governments, home users and malicious hackers emerged. The spies of yesterday could easily become the social engineers of this era. The overall solution is complete training of all employees on the methods of social engineering. When traveling, laptop users need to take extra precautions to ensure that they are maintaining secure computing practices. Whereas floppy disks and bulletin boards once were the carriers of viruses, today foreign networks and trust relationships between networks form the majority of technological security holes. Social Engineering will remain the quickest and easiest method of penetrating networks. The end solution is employee training and enforcement of security policies.

References

Carnegie Mellon Software Engineering Institute, "CERT® Advisory CA-1991-04 Social Engineering" September 18, 1997, URL: http://www.cert.org/advisories/CA-1991-04.html

Coffey, Kevin "Learning How to Travel Smarter" 12 August 2000 URL: http://www.abcnews.go.com/onair/DailyNews/kevincoffey081299_chat.html

Lowe, Richard and Claudia Arevalo, "Social Engineering" October 2000. URL: http://internet-tips.net/Security/social.htm

Northcutt, Stephen **Network Intrusion Detection: An Analyst's Handbook** Copyright 1999 Osborne/McGraw-Hill ISBN: 0-07-212127-0

United States State Department, "At The Airport" State Department Electronic Research Archive Documents on Security 26 March 1996 URL: http://dosfan.lib.uic.edu/ERC/travel/security/security_airport_concerns.html

United States State Department, "Selecting a Secure Hotel and Security Tips" State Department Electronic Research Archive Documents on Security 26 March 1996 URL: http://dosfan.lib.uic.edu/ERC/travel/security/security_hotels.html

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event