Global Information Assurance Certification Paper

Road Warriors: Protecting Them from the Wolves - and the Organization from Them

James Babcock Hughes

GSEC Practical Assignment v.1.2f December 18, 2001

Introduction

Within organizations employees frequently attend conferences, visit remote subsidiaries, contact vendors, clients or partners [4]. Outfitted with laptops or PDAs, they use their organization's information infrastructure from within an environment over which the company's security team may have little or no control.

The security risk to an organization regarding these mobile users, the modern road warriors, is that their laptop or PDA may be lost or stolen, or become a vector through which malware can breach an organization's defenses, either during the trip or later when these devices are reattached to the corporate network [2]. Either way, the trip can quickly turn into a nightmare.

This article explores the security issues specific to traveling users, an often overlooked group for which an organization's security team must take extra care because they operate in a dangerous, changing and unpredictable environment. We will cover the special steps which should be taken with them and their computers before they sortie from the secure corporate castle out into a hostile world, the special steps when they access the home base while away, and the special steps which should be taken at the end of the trip to minimize the risk their laptops may pose to the organization should they return under the influence of the evil hacker.

Motivation

The proper architecture of an organization's information infrastructure, one which is to provide users confidentiality, integrity and availability of their data and applications, will also achieve defense-in-depth from a security breach. Reaching these goals involves careful planning and consideration of physical site security, the placement and operation of routers, stateful firewalls, DNS servers, network and host-based intrusion detection systems, modem banks, virus scanners, client computers, and servers for such things as WWW, FTP, email, databases, and other

information resources, not to mention the careful setup and security maintenance of the myriad software that runs on all of this.

Mobile users will not have the same defenses at their disposal unless they hire bodyguards and lug around a steamer trunk or two full of equipment (some companies probably do just that, or should, if the importance of the mission warrants the expense). For most organizations, traveling users simply are more vulnerable while they are traveling. That which is desired is to cover these users with as effective a layered defense as possible which still adequately protects them and the organization against security incidents.

The results a root exploit, remote administration trojan, worm, virus, or other malware can have on the traveler is a microcosm of the results such an incident might have on the main corporate network: a serious incident can precipitate a lost sale, a project slip, loss or theft of company intellectual property, web defacement or the publication of damaging information, legal liabilities, or, at the very least, time taken away from the trip's true purpose. The bottom line is that trips are very important ways that an organization gains or disseminates knowledge, and the stakes may be quite high in an economic sense - in terms of corporate prestige, or any other metric by which the organization measures its success.

One of the most important tasks for the security team is to get the upper management aware of these dangers, and to get them to decide what level of risk they are willing to accept, and to get them to support and fund a traveling user security program as an important component of organization wide general security policy that mitigates the risks associated with traveling users [3].

Achieving Security Consciousness

In an ideal world, users would not have to worry about security at all, with machines, software, or security specialists providing a safe cocoon protecting them from harm. In the real world, true security requires people to be on the ball, to apply common sense, and to avoid dangerous situations which may crop up even if there is a massive security infrastructure in place.

With upper management backing a general security policy, the security team must engender security consciousness among users of all types. Part of this is to integrate portions of the security policy into the larger organizational operational procedures, of crucial importance else security policies will end up largely ignored or at best unevenly applied. This extra visibility for security is crucial in

creating a security consciouness that will pervade all organization users, including those who are on the road.

Being in a policy manual, with however draconian sanctions for violating security rules, is clearly not enough to insure security consciousness since some users simply never bother to read any such policy. The security team must be more proactive in this sense: they should hold security talks (with free food!), publish periodic newsletters and email to raise the visibility of security topics, and in particular issues confronting the traveling user. The sale that has to be made by the security team is that being security conscious is in the user's best interest and will make the outcome of the trip more successfull.

The payoff in raising the security consciousness particularly with mobile users is to turn good security procedures into habits. The security team can tirelessly promote the security agenda to users, but real success requires the their active involvement and cooperation. If travelers always make sure the extra hardening and analysis of their equipment takes place, if they are careful when connected to a strange LAN, and if they make sure the post-trip checking of the equipment occurs to detect possible threats to the organization - *before* plugging the equipment back into the corporate network - then security incidents related to traveling users can become a rare event.

Choosing the Level of Allowed Access

In planning support for the trip, it should be precisely clear to the traveler and the security team what corporate resources will be needed, which devices need to be taken, and what remote administrative manpower may be required to support the trip. It should be made clear that the traveler is responsable for making sure that the hardening and checking procedures take place before and after the trip, and that the administration/security team is responsable for carrying out the procedures.

The above points, along with the procedures themselves, can and should end up in the security policy manual, so that answers to many of these questions and the issues they raise do not have to be worked out again and again.

Different means of access to the organization's information infrastructure exist, with varying levels of convenience, security, speed and expense. Each has different setup requirements and complications. Management, the security team, and the travelers themselves need to agree on this means of access, likewise which organization computers will be accessed, and which files on those

computers, over which ports. It is beyond the scope of this paper to describe all the possible ways a mobile user can connect back to the organization, but we discuss a few here and some of the important security issues involved.

The spectrum of access runs the gamut between completely transparent, dedicated and secure access such as that furnished by a managed security private DSL service provider (such as Isite), to "fend for yourself" access, where the mobile user is given NO extra access beyond that allowed to the web surfing general public, not even company email. In the first instance, the mobile user does not "touch" the rest of the internet, rather connects up into the parent organization via the private DSL service, typically using a modem with a level of performance, availability and security guaranteed by the secure service provider. In the other instance, the mobile user must find whatever connection is available: a LAN provided at a conference, hotel room DSL connection, airport "cybercafe" connection, etc.

The position of the security team, in keeping with the principle of least privilege, should be that, other than publicly available services, ALL other ports into the organization are closed to the outside by default, and it should not be necessary to open any new ports. The principal players involved with the trip can decide whether there are acceptable alternatives to each service. In many cases, the nature of the trip does not require much access at all, so seeking alternatives is a useful way to avoid creating additional security issues. Mobile users could for example receive email with a Hotmail or Yahoo!Mail account, and have their company email forwarded. The principals could agree to store data and files needed during the trip in certain locations on the public ftp server, properly encrypted with agreed upon keys, and retrieved by the traveler in an emergency or as needed.

In the cases where no viable alternative is available, the security team can open up the organization firewall just enough to allow through those services which are vital to the mission either by allowing individual services, such as those provided by secure versions of email, ftp or remote logon, or by providing a wider secure channel such as a VPN (virtual private network) which creates a safe connection based on encrypted PPP packets running over TCP/IP using the point-to-point tunneling protocol PPTP and X.509 certificates for authentication.

In either case, the security team needs to find out the particular IP addresses the traveling user's computer will have during the trip ahead of time, if possible, in order to make as narrow an access

control list as possible which still allows the hole in the firewall for the agreed upon resource. It is also important to have a mechanism in place to insure that this ACL is removed from the firewall ACL lists just as soon as it is no longer needed, so any hole is not only as narrow as possible in ports and IP addresses, but is temporally open for as short a period as possible.

Secure, encrypted remote logins can be provided using SSH Secure Shell. SSH packages frequently come with a secure FTP based on the same SSL libraries. Secure email access can be provided by IMAP/SSL. The Netscape email client, and Microsoft Outlook both support IMAP/SSL. The email server must also support this security protocol. Fortunately, Linux IMAP and Microsoft Exchange both support secure SSL SMTP transfers with clients.

Virtual Private Networks

VPN is touted as a great way to connect mobile users up to the organization since it provides full, reliable, secure and transparent access: when connected up via a VPN, the laptop actually becomes part of the organization network [13]. The network from which the VPN connection is initiated is "temporarily disconnected": all connections on the traveling laptop "appear" to be taking place from within the organization network. In truth however, the local connection is still very much alive (obvious since it must be tranmitting the encrypted VPN packets, but not so obvious is that the local connection is still vulnerable to probes and attacks).

Another drawback to VPNs is that the way it is sometimes implemented violates a basic security commandment which is that "everything goes through the firewall", such that packets sent over VPN connections are NOT scanned by the firewall or by network IDS systems. It is a tremendous leap of faith for the organization to allow mobile Joe to hook up a VPN from the Bulgarian International Airport "cybercafe" to send any packets into the corporate network unchecked. The danger, of course, is that Joe's laptop has already been taken over by malware: the VPN just provides it with a reliable, secure and transparent path into the organization network [12].

It is up to the security team to make sure that the above does NOT happen, that VPN capability is designed into the organization information infrastructure and not added later ad hoc. The traffic flowing through a VPN needs to be checked at least as carefully as other traffic. Many modern firewalls will handle VPN connections and check their packets, the problems often arise with

older firewalls which were designed before VPN became so popular.

Additional encryption of packets sent over VPN can be achieved by using IPsec packages such as that provided by SSH Complete VPN However, VPN/IPsec does not address the issues raised above. It only insures data confidentiality, so sniffers at the home organization cannot capture these packets on the subnet at which the VPN emerges. If anything, IPsec makes security even harder since malware cannot be recognized as such if it is encrypted, should there be an internal network IDS (i.e. - a legitimate sniffer) on duty inside the company network looking for the malware's telltale signatures.

The security team needs to be aware of VPN weaknesses and try to work around them - a good personal IDS, for example, needs to protect the mobile computer from port scans coming from the local network even when the VPN is established.

Basic Hardening Procedures

An organization's security program should have hardening procedures in place which are applied to all devices (computers, laptops, PDAs, network printers, switches, routers, firewalls, etc) before they are connected to the corporate network. The should be reapplied periodically or when important patches are released.

The first step to harden travelling devices is to insure that they meet these basic security standards. Extra hardening may not help much if, for example, a laptop is open on the FTP port and it's operating system has unpatched buffer overflow vulnerabilities.

The following basic security list is probably a good starting point: it is condensed down from the vulnerabilities detailed in the SANS/FBI list of the twenty most critical internet security vulnerabilities [1] and other sources:

- *Services and Network Ports* - Minimize open network ports and remove all services not critical to the computer's usage. In particular, remove unnecessary servers which might be configured by the default installation, like IIS.
- *Software Patches* - Apply all pertinent operating system and application patches and service packs, particularly those dealing with security vulnerabilities. If a computer is running the infamously vulnerable Windows 95/98/ME then it should be "patched" by upgrading it in its entirety to Windows 2000!
- *Null Sessions and Network Shares* - Insure that null user sessions are not enabled and that there are not any open or

anonymous SMB network shares.

- *Passwords* - Insure that ALL accounts (particularly obsure ones that seem to have some maintenance function and show up from the factory) have passwords different from the factory defaults, are long enough, use letters, digits and symbols, and are changed regularly and are not easily crackable using password cracking tools like John The Ripper or crack.
- *Backups* - Make sure the computer can be restored to its functional state should it be trashed by a security incident, malfunction or accident. This will be harder to provide for traveling users, but can be accomplished with appropriately crafted restoration CD-ROMs for example and may save the trip should there be a hardware failure or security incident.
- *Logging* - Make sure there is adequate event logging such that a security incident, if not prevented, can at least be detected. Periodically run a tool such as Tripwire to get file signatures in order to know what "normal" files look like, and so detect exploited files when they appear.
- *Anti-Virus Software* - Download and apply updates to keep anti-virus software trained to detect the latest threats.
- *BIOS/CMOS Hardening* - Set up the laptop to boot the hard disk first. This will prevent the user from inadvertently booting a virus laden floppy or CD-ROM. Configure the BIOS password which must be entered before the device will boot. There are ways to bypass this protection with known universal passwords [11], but the thief may not know them. The point is to throw as many obstacles into the hackers path as possible: the hacker may be under time pressure and this step may increase it.

Travel Hardening Procedures

The basic steps given above result in a secure device ready to connect to an already secure network, but are not enough for the device to be connected to insecure one. Traveling devices are worse off even than the company servers that live outside the firewall in the DMZ, which even though exposed to the entire internet, are still typically protected by the firewall from many probes and attacks. Moreover, there is frequently a network based intrusion detection system scanning ALL incoming and outgoing packets before these even reach the firewall or DMZ.

Applying these extra steps will try to restore some of the protection not available to traveling computers while on the road:

- *Verify the Basic Hardening* - Insure that the hardening steps

itemized above actually took place on the traveling device. Good records should detail the dates when this occured, version checks and file signatures (from Tripwire) can confirm that the device is up to the current basic hardening standard. If software and patches are not current, this is a good time to make them so.

- *Install and Configure Access Software* - This includes the software to support the access previously agreed to. This could be SSH, IMAP/SSL, VPN client software, IPsec software, Public Key Infrastructure software, or special software required by a secure private DSL network provider. The mail reader (e.g.- Outlook, Netscape) which will be used by the traveler needs to be configured, in particular, to use IMAP/SSL.
- *Personal Intrusion Detection System* - Install and configure an up-to-date personal IDS such as ZoneAlarm Pro or Black ICE Defender, and instruct the traveler how it works. The personal IDS is very important for the mobile user as this software must substitute for the organization's firewall and IDS systems [7]. It will warn the user when there is an attack and hopefully shutdown the attacker's attempts to connect. The personal IDS should be configured at the highest security setting to provide maximum protection. If the laptop runs Linux, the ipchains package is a very powerful substitute for a personal IDS.
- *Get Baseline File Signatures* - Run Tripwire on the traveling computer just before the trip to have a baseline to compare its files when it returns, in order to detect exploits. Store the results in a safe place at the home organization.
- *Secure the Data* - Remove data from the notebook which is not needed during the trip [8] and encrypt the vital data that will be carried on the device. Consider taking critical data separately from the laptop, on a removeable USB memory device, CompactFlash, or even burned into a calling card sized CD and carried along with a traveler's most valuable items (passports, credit cards, etc).
- *Install Physical Security Hardware* - Invest in hardware locks for securing the laptop to fixed objects. These will clearly *not* stop a determined thief but may slow them down long enough to prevent the theft.
- *Consider Biometrics or Digital Keys* - SSH, VPN clients and other software will often support specialized authentication devices which verify digital identity combining something the user has and something the user knows. These devices range from a simple USB based digital key to fancier thumbprint or retinal scanners [6]. These devices can provide an additional layer of security against unauthorized access

from a stolen or "borrowed" laptop.

- *Other Software Installation and Configuration* - You may want to consider theft deterrent software like ComputracePlus which will silently dial out over the modem or connect up via a LAN to allow tracing the whereabouts of a laptop, making it easier to catch the thief and recover the laptop. This software purports to survive a full disk format and reinstallation of the OS!
- *Check the Procedures* - Run vulnerability scanners such as Nessus or Nmap against the traveling device to make sure the hardening has taken effect. Evaluate the results and improve the hardening if need be. As a final step, set up the personal IDS to lock out these scans!

Out in the Cruel World

On the road, the warriors must fend pretty much for themselves, armed with whatever protection the security team manages to assemble. The key concept on the road is - *extreme paranoia*. Physical security of the mobile device is paramount, along with common sense to not do things like type in ones American Express card number into a random terminal at an airport "cybercafe" - the computer could easily be running a KeyKatcher or similar device.

The traveling user needs to keep the following risks in mind while on the road:

- *Loss or theft of the laptop/PDA.* - Notebooks are highly prized by thieves and will disappear in a minute from an airport xray scanner, from a hotel room or from a conference terminal room [10]. The key defense is to never let it out of ones sight, and always carry it as hand luggage, never checked as baggage. It should be locked up in the hotel safe at night, if possible [9].
- *The Risk of Prying Eyes* - Someone may be watching over the traveler's shoulder, (shoulder surfing), or even video taping the user from a hidden camera, capturing each and every keystroke. The user should look around a bit and take extra care when typing in passwords or other sensitive data.
- *The Risk of Being Sniffed* - Someone may be capturing all the user's network packets, over a conference LAN, over a hotel cable hub, or anywhere between a user's laptop and the home institution. If anything the user has typed is in cleartext, then the hacker can see it and may use it to mount a more serious exploit. The user needs to make sure the personal IDS system is engaged and make sure that all

access to the home organization is over secure encrypted applications or channels.

- *The Risk of Being Hacked* - Someone may probe the user's laptop for open ports or unprotected file shares, prelude to an attack and deposit of malware. The security team should have these closed off, and the user must help by not running software that might defeat these protections (e.g.- Napster, ICQ, mIRC). The user should not leave the device unattended at all: someone could install a remote administration trojan from a floppy disk in less than the time it takes to come back from the bathroom.
- *The Risk of Downtime* - The traveler needs to have the telephone number or beeper of the organization administration/security team should he or she run into a problem, whether hardware malfunction or a security incident. The team can fill out a hardware trouble report or a security incident ticket to help keep track of the event, and try to solve the problem remotely and help the traveler get back on track. The administration/security team likewise should have the telephone number of the traveler!
- *The Risk of not Detecting an Exploit* - While the traveler is on the road, the security team needs to monitor organization security log files with particular care to verify that accesses from the traveler are legitimate, and are as agreed to. If it appears the traveler is trying to probe the system in unexpected ways, it is quite possible that someone else is spoofing his machine or has taken it over. The security team should call the traveler to check out these incidents.

Back to Safety

The portable computer used by the traveler needs to be sanitized before being hooked back up to the corporate network. Should this mobile computer be infected with NIMDA for example, malware can quickly propagate over the company LAN onto vulnerable machines, silently and without warning. Clearly, the security team is supposed to set in place a security program so computers on the company network will resist such attacks, but there are occasional rogue computers on the network with no basic hardening. These pop up on the net from time to time and the security team may not even know they exist until stumbling upon them during an IDS analysis session. The objective is that the mobile computer back from a trip not become one of these rogue computers.

In another nightmare scenario, a mobile user's laptop may return infected with a remote administration trojan like Back Orifice,

NetBus, or SubSeven: it is not enough to depend upon the corporate firewall to shut down outside access to these remote trojans, as they are constantly mutating and could use a covert channel to receive instructions over allowed ports (the infected machine for example could initiate an ftp connection from inside the network and receive covert commands encoded in ftp packets or files transfered by the hacker).

The following steps should be performed on the returning device to minimize the risks to the company network. The security team would be well served by setting up an isolated subnet which is shut out from the rest of the network, where computers in an unknown security state can be checked out without threatening the rest of the network.

- *Run Malware Scans* - Run scans to detect viruses and/or malware. Run it from some other media: assume the virus software on the laptop has already been compromised, so run your own copy burned into a CD.
- *Expire the Passwords* - Change any passwords on accounts that were accessed by the traveler during the trip.
- *Analyse File Signatures* - Rerun Tripwire on the traveling computer (also from your own CD), and compare its output to the previous baseline to detect files (particularly system executables, startup files and libraries) which may have been compromised.
- *Reapply Basic Hardening if Applicable* - If new patches or service packs have shown up while the device was on the road, this is a good opportunity to apply them. Similarly, make sure the anti-virus software has been brought up to date.

Conclusion

Of major importance in setting up security guidelines for traveling computers is to realize that the number of laptops is quickly increasing as their prices plummet and their features continue to improve. I type these words in from a laptop that is far more powerful than my main computer at work, and I lug it around almost everywhere. My office is not where I work so much as where I synchronize my PDA, leave my finished documents and tasks and get new ones.

The organization's security environment is changing because of these laptops: I know of several users at work who have had their main computer removed from their office, and work entirely out of the laptop, which now travels with them between home and office, and even follows them on vacation. The security slant on this is

that a fixed perimeter defense is no longer enough...the computers that make up the corporate network move around now, and things will get worse. The security team must project the security envelope out to cover this cloud of wandering machines or pay the consequences when they come back to infect the main network.

If there is a trend where laptops are replacing workstations on the desk, there is a similar trend where handhelds are replacing laptops, particularly amongst the seasoned road warriors who are tired of lugging around a five pound laptop and associated paraphernalia, when a six ounce handheld can store a large number of Autocad files, surf the Internet, run a full Powerpoint presentation, run a spreadsheet or create a Word document, or send email via Outlook. Any road warrior who has had a laptop stolen will appreciate that handhelds can easily fit in a hotel room safe, and are small enough to carry around everywhere.

With a collapsable keyboard, full length documents and reports can be created on a handheld almost as easily as on a laptop. It used to be that PDAs where strictly downloadable devices. The newer generations, however, perform as fully connected computers on a network, via modem, ethernet or 802.11 wireless, or via software like Microsoft ActiveSync using IR, USB or a serial based cradle. VPN software for handhelds is available, with IPsec even, and there are even WWW *servers* available for these devices!

As a result, from a security standpoint one needs to treat these devices as what they are: full featured computers. As hackers become more aware of handhelds, they will increasingly become the targets of their attention [5], particularly if they correctly gauge that the software on these devices tends to be a bit more rudimentary and immature than that of larger computers, hence their defenses easier to breach. Fortunately, McAfee, TrendMicro and other security specialists are starting to pay more attention to these devices and to provide full featured anti-virus products for them. Personal Intrusion Detection Systems are not yet available for these devices but their arrival cannot be far off.

The guidelines presented here for road warriors are just a mixture of security common sense, practical advice for travelers, and the application of technologies which did not exist at all a few years ago (personal IDS software first appeared in 1999). Many of the points discussed apply equally well to other situations: users working from home, turnkey computers provided as part of a larger system, or visitors hooking their laptops up to the corporate network. Each of these situations provides a way for hackers to get

into the organization's network.

The proper job of the security team is to provide ALL users, including road warriors, with acceptable confidentiality, integrity, and availability of their data and applications, without allowing any group to put the organization's information infrastructure at risk. The objective of this paper has been to put together a set of procedures and policies which will help with that job. The topic of traveling users, however, is an enormous one and this paper merely scratches the surface of the issues involved.

List of References:

[1] SANS/FBI Top 20 Vulnerabilities
http://www.sans.org/top20.htm (18 Dec 2001).

[2] Protecting the Portable Computer Environment - 1997 Handbook of Information Security Management
http://www.cccure.org/Documents/HISM/699-703.html (18 Dec 2001).

[3] Managing Security in a Mobile Environment Warren Cartwright
http://www.sans.org/infosecFAQ/travel/managing_sec.htm (18 Dec 2001).

[4] The Security Challenges to Offshore Development - Rob Ramer 26 sep 2001
http://www.sans.org/infosecFAQ/code/offshore.htm (18 Dec 2001).

[5] Pocket PC Secure or Insecure - Darrin Murriner 96 jul 2001
http://www.sans.org/infosecFAQ/PDAs/pocket_pc.htm (18 Dec 2001).

[6] Laptop Security - past, present - Andrew Mueller 10 jul 2001
http://www.sans.org/infosecFAQ/travel/laptop_sec.htm (18 Dec 2001).

[7] Protecting Your Corporate Laptops from Hackers while they are on the Road Darrell Keller
http://www.sans.org/infosecFAQ/firewall/corp_laptops.htm (18 Dec 2001).

[8] PDQ Reference: Travelling with a Laptop
http://www.pdqwebdesign.ca/lib/laptop.html (18 Dec 2001).

[9] Notebook Computer Security: Loss Prevention Tips
http://www.secure-it.com/newsletters/security_advice.htm (18 Dec

2001).

[10] Basic Travel Security - Aaron Weissenfluh
http://www.sans.org/infosecFAQ/travel/travel_sec.htm (18 Dec 2001).

[11] Securing Information on Laptop Computers Jim Purcell
http://www.sans.org/infosecFAQ/travel/sec_info.htm (18 Dec 2001).

[12] Securing the mobile Businessman Frank Reid
http://www.sans.org/infosecFAQ/travel/mobile.htm (18 Dec 2001).

[13] Demystifying Virtual Private Networks by Michael Busby
ISBN 1-55622-672-1 Copyright 2001
Wordware Publishing, Inc., Plano, TX