Real World Security Threats: The Anatomy of a Hack

By Daniel V. Hoffman, CISSP, CWNA

FIBERLINK

CONTENTS

The increasing mobility of the enterprise workforce poses significant security challenges for the global enterprises. With mobile workers accessing corporate resources from a variety of networks, including Wi-Fi hot spots, hotel broadband, and home broadband, the need for a comprehensive mobile workforce security strategy is no longer an option, it's a necessity.

Today's mobile workforce no longer just refers to road warriors like traveling salespeople and business executives. Mobile technologies have given companies the flexibility to deploy workers in ways that allow the company to meet new business challenges and increase productivity, posing a new series of security challenges for IT. It's inevitable that keeping mobile devices connected often increases your company's exposure to Internet-based security threats.

The inherent complexity of the mobile workforce, emerging new security threats, and tightening security resources leave many security managers wondering where they should turn to protect their networks. Easier said than done since ensuring mobile endpoint device compliance with corporate security policy is an extraordinary challenge.

According to a study of more than 8,200 IT security professionals from 62 countries, companies experienced an average of 824 security incidents or events over the past 12 months with the majority of these events being the result of malicious code or unauthorized entry to information assets.[1]

The State of Information Security, 2005, CIO Magazine and PWC

Live Hacking Demonstration

Fiberlink has developed an on-demand video demonstration to accompany this guide. In it you can watch Fiberlink system engineer and mobile workforce security expert, Daniel V. Hoffman (CISSP, CWNA), show how a hacker can take complete control of a mobile endpoint system without the proper security protection and attack it. Hoffman reviews the more commonly used steps and procedures that hackers use to access mobile endpoint systems, and ultimately the corporate network.

Hopefully, this guide and its accompanying video demonstration will leave you with a better understanding of:

Common security risks and vulnerabilities that threaten today's mobile workforce;

Techniques, skills and tools used by hackers to exploit vulnerabilities on mobile endpoint systems;

Best practices and essential tools necessary to help protect your endpoints and corporate resources from attacks.

Understanding the Threats to Your Mobile Workforce

Prior to implementing a comprehensive mobile workforce solution, it is important to understand the risks that threaten your mobile workers everyday. The threats fall mainly into three categories: **network sniffing, malware and direct attacks.**

Below, you will find descriptions of each threat, and some examples of best practices for how to protect your enterprise against that specific form of attack.

Threat #1:

Sniffing – *a technique for capturing network traffic. Sniffing can also be used legitimately or illegitimately to capture data being transmitted on a network.*[2]

Mobile workers using mobile endpoint devices that are not compliant with corporate security policies are highly susceptible to the threat of data sniffing. Sniffing falls into two fundamental categories:

Credentials "Sniffing": As enterprises continue to adopt a model of using a single, unified client application to enable multiple forms of connectivity, including dial-up, wireless, and broadband, there are also certain advantages from a security perspective. With a single client comes the advantage of having authentication for all transports proxied back to a central location, commonly the corporate network.

However, along with these advantages also comes risk. Frequently, the authentication credentials are the same as the mobile user's network credentials, or have significant value to the end-user and/or the enterprise. Consequently, it is very important to ensure that credentials are protected during the proxy process. With standard RFC Compliant RADIUS Proxy (a commonly used authentication protocol), the username is always sent "in-the-clear" and the password is hashed with MD5, then un-hashed and re-hashed on each RADIUS server that the credentials pass through.

In order to maintain the integrity of the credentials, a truly secure solution must encrypt both the username and the password using 256-bit AES (Advanced Encryption Standard) on all forms of connectivity. This form of end-to-end credentials encryption provides significantly greater protection from sniffing than RFC Compliant RADIUS Proxy.

Fiberlink Extend360™ uniquely provides end-to-end encryption of all end-user credentials information, such as user IDs, passwords and other personally identifiable data.

Data "Sniffing": Data is under constant attack from a growing number of sources. With an increasing number of mobile workers using public Wi-Fi and hotel broadband networks, the threat of hackers sniffing application traffic exists.

In virtually all cases, public Wi-Fi and hotel broadband locations do not offer any form of inherent encryption for data leaving a system on these networks. At the same time, these networks are readily available to a number of simultaneous users. The best way to protect against the sniffing of data is to ensure that a VPN tunnel is active throughout the life of the public Wi-Fi and hotel broadband network connection. In addition, disabling split-tunneling will ensure that all data leaving the mobile system will be encrypted via the VPN client, which commonly uses DES, 3DES or AES encryption.

Threat #2:

Malware (Malicious Software): *software designed to destroy, aggravate and otherwise do harm to a computer. Malware includes computer viruses, worms, Trojans, and expanded threats like spyware, adware, and joke programs.*[2]

Deploying Security Software Alone is Not Enough

No single tool will solve all your security problems. In order to effectively manage the security of your mobile endpoint systems and corporate network, enterprises need integrated systems.

Anti-Virus Protection. When it comes to malware, people typically think of viruses. And erroneously, most IT managers believe that deploying a standard anti-virus software solution will protect the enterprise against the universe of malware threats. In reality, it is not enough to just *deploy* anti-virus software for your mobile workers. For an anti-virus solution to be effective, the software needs to be running and the virus definitions and signatures need to be up-to-date on each mobile endpoint device. With new malware threats being identified daily, this can present a significant challenge.

> Two-thirds of IT professionals and security administrators say spyware is the top network security threat of 2005. Viruses (23 percent) and Phishing (10 percent) were the next most popular threats.
> *(Watchguard, 2005).*[3]

Anti-Spyware Protection. In addition to anti-virus protection, the deployment of anti-spyware applications should not be forgotten as part of a comprehensive security strategy. Spyware installs itself without warning, opens dangerous security holes and reinstalls itself after its been deleted. The worst of these programs allow online criminals to hijack users' sensitive personal information at will. Keeping anti-spyware applications running and current on mobile endpoints is as important and as challenging as it is for anti-virus software.

Personal Firewall Protection: Anti-virus and anti-spyware applications are not sufficient enough. A third tool that is equally important in combating malware is a properly configured, enterprise-grade personal firewall with IDS/IPS capability. Enterprise-grade personal firewalls with IDS/IPS capability have the ability of performing zero-day protection, where malicious behavior can be intelligently identified and stopped as it is occurring. Alone, anti-virus and anti-spyware are unable to stop behavior as it is occuring because they are reactive in nature. This means that definition files are only updated once a piece of malware has been identified as a threat by the various anti-virus and anti-spyware vendors.

Patch Management Protection: An important element of a comprehensive corporate security strategy, and until recently an often-overlooked means to mitigating risk from malware, is an effective system for patching mobile endpoints. It is essential that all endpoints have the latest operating system and application security patches and that the mobile system is properly configured from a security perspective. Without the latest patches and proper configuration, malware will often take advantage of system and application vulnerabilities that would not be present if the mobile endpoint were properly patched.

> "...more than one in four impacted companies were hit by (the) Zotob (virus) because no firewall was in place or firewall policies were incorrectly set."
> *(TechWeb News, 10/26/2005).*[4]

Just When You Think You're Covered

There is always risk that certain malware will disable the security applications that enterprises have put into place to protect endpoint systems. Therefore, it is important to run frequent checks and scans to ensure that all security applications are up-to-date and running. If during the scan endpoint vulnerabilities are identified, the suspected machine or machines should be deemed "out of compliance" and denied access to the Internet and/or the corporate network until the deficiency is remediated.

According to Trend Micro, most malware programs (as observed in the majority of 2004 bot programs) will continue to employ anti-antivirus and anti-security routines to ensure infection, requiring the use of system cleaning services to ease the impact on system security.[5]

The logic for vulnerability scans and remediation should reside on the mobile endpoint, as today's systems need to be in compliance with security policies at all times. In the past, enterprises have relied upon VPN concentrators or NAC (Network Access Control)-type functionality to check the security posture of the mobile endpoint as it is gaining access to the corporate network. With today's mobile workers potentially spending more time directly connected to the Internet, than connected via an active VPN session to the corporate network, this method of checking the state of the system's security posture is inadequate.

What percentage of your users are in compliance with your information security policies?[1]

North America	74%
South America	60%
Europe	63%
Asia	66%
Middle East	54%

The State of Information Security, 2005, CIO Magazine and PWC

Threat #3:

Direct Attack – *an assault against a computer system or network as a result of deliberate, intelligent action.*[2]

The most malicious form of attack, is a direct attack on the network. This type of attack is most dangerous because it entails a hacker using their cognitive skills to exploit a mobile system, leaving it vulnerable for attack in the future by widespread vulnerabilities. In this case, the hacker can also consciously dissect and analyze data on the mobile system.

Some Best Practices to help protect against a direct attack include:

Personal Firewalls, Anti-Virus, Anti-Spyware. Not unlike other threats, the importance of security applications being up-to-date, properly configured, and always running on mobile endpoint devices is crucial in helping prevent against a direct attack. As stated in the section on malware, the use of personal firewalls not only prohibits a hacker from accessing the mobile endpoint system, but it also provides stealth capabilities that help make the endpoint invisible to scans that may be run by a hacker.

In addition, outdated anti-virus and anti-spyware applications will not provide protection against newly developed malware. Commonly, a hacker will place malware on a victim's machine to either further exploit the machine, or to provide a means to exploit it in the future. An endpoint that is in compliance with corporate security policy and is able to constantly scan for the existence of malware, will be able to detect when a hacker attempts to place malware on a mobile endpoint, and perform the necessary actions to address the threat.

Real-Time Remediation. Mobile endpoint systems that have up-to-date security patches and are configured properly help protect your corporate network from attack. Hackers gain direct access to mobile endpoints by running exploits that take advantage of vulnerabilities on mobile systems that would not exist if the systems were properly patched and configured in the first place.

Most patching systems and solutions available today simply quarantine infected machines versus providing a means to remediate the mobile system by pushing, in real-time, necessary patches or configurations to the system when the endpoint is not connected to the corporate network, or connected to the corporate network with a VPN.

Extend360™ provides an enforcement capability that prohibits an end-user from surfing the Internet or connecting to the corporate network if the mobile endpoint system is not up-to-date and properly configured with security patches. More importantly it also provides the capability of remediating the vulnerable system by pushing the necessary update or configuration change anytime the system is connected to the Internet, but not the corporate network. The ability to remediate in real-time inevitably increases mobile user productivity.

Click to view "The Anatomy of a Hack," a live hacking demonstration »

Anatomy of a Hack Video Companion Guide
Step-by-Step Hack of a Mobile Endpoint Device

1) **Footprinting and Scanning** – The first step in attacking a mobile endpoint is finding a live system. There are many tools available on the Internet to search for live targets. The one used in this demonstration is Foundstone's SuperScan.

How to Protect

- Your best means in protecting mobile systems from being seen during a scan is to run fully operational enterprise-grade personal firewall software on each mobile endpoint.

2) **Enumeration** – Once a target is found, more information needs to be uncovered to determine the best approach for exploiting the target system. Like scanning tools, there are many enumeration tools available for free use on the Internet.

How to Protect

- Ensure that the mobile operating system is properly patched and configured, so that information is not accessible through the "back door" of the corporate network.
- Employ fully operational enterprise-grade personal firewalls on mobile endpoint devices.

3) **Launching an Attack** – Once a live system is found through scanning and information is gathered through enumeration, a direct attack can be launched against the system.

How to Protect

- Make sure your mobile endpoint systems have the latest operating system and application security patches.
- Employ fully operational enterprise-grade personal firewalls on mobile endpoint devices.
- Ensure anti-virus and anti-spyware software is running, up-to-date, and utilizing real-time scanning. It is a common tactic for hackers to place Trojans and other malware on hacked systems. Real-time scanning programs will help catch malware as it is being transferred to the hacked machine.

4) **Leaving the Mobile System Vulnerable to an Attack** – Once a hacker has exploited the system, he or she will commonly take steps to leave it vulnerable to future attacks. This can be done by installing a Trojan or mobile control software, or installing a key logger that routinely sends all keystrokes from the system, etc.

How to Protect

- Ensure enterprise-grade personal firewalls are running, properly configured and up-to-date in order to stop a mobile intrusion, and sense when malicious activities are taking place.
- Anti-spyware and anti-virus applications that are running, and up-to-date are also able to find malware and address information left behind to further exploit the system.

In Summary: Ten Things You Can Do to Protect Your Enterprise from a Hacker

1. Deploy properly configured enterprise-grade personal firewall with IDP/IPS component;

2. Ensure anti-virus and anti-spyware agent software is active and up-to-date;

3. Make certain your mobile system is updated with the latest operating system and application security patches;

4. Only run a mobile system that is properly configured against vulnerabilities and configured to prevent disclosure of sensitive system configuration information;

5. Establish a means to provide authenticated and encrypted access to corporate resources, such as an IPSec or SSL VPN;

6. Lock down a process that requires end-users to utilize stronger and fresher passwords for authenticating to corporate resources (non-dictionary, combination of alpha-numeric, possibly two factor);

7. Set policies that disallow mobile access credentials from being stored in cache locally on the mobile workstation;

8. Configure endpoint machines so that local users do not have the ability to disable security components of the mobile workstation;

9. Ensure you have a means to easily report that all mobile endpoints are in compliance with corporate security policies at any given time;

10. Require an endpoint agent to ensure that all security applications are active, up-to-date, and have the ability to automatically remediate deficiencies, while prohibiting access to corporate resources. Quarantining, security application enforcement and remediation should not be dependent upon physical or VPN access to the corporate network.

Click to view "The Anatomy of a Hack," a live hacking demonstration

PROTECT YOUR ENTERPRISE FROM AN ATTACK WITH ROBUST MOBILE WORKFORCE SECURITY SOLUTIONS, FROM FIBERLINK

Fiberlink mobile workforce solutions eliminate the need to rely on a piecemeal strategy for mobile working because it brings together everything you need to protect, connect, and control the mobile enterprise. Fiberlink solutions combine a world-class collection of transport options with the industry's most robust security measures to keep mobile workers fully productive while protecting mission-critical assets. Fiberlink solutions also provide the industry's most comprehensive set of administrative tools enabling IT managers to efficiently push policy and security software updates to mobile workers throughout the enterprise.

Extend360™ (e360) is Fiberlink's proprietary, software-based service designed to keep mobile workers protected and connected while working outside of the traditional office setting – utilizing a single client interface.

At the core of Extend360 is an enterprise vulnerability management (EVM) security service designed to secure the mobile endpoint from unwanted intruders and hackers and ensure the highest levels of "always-on" protection for your mobile workforce. This service consists of an EVM agent that provides continuous assessment of the mobile endpoint from system start-up to shutdown – proactively identifying and remediating vulnerabilities as they occur. Services offered under the EVM suite include patch management, anti-virus, anti-spyware, managed personal firewalls and managed IPSec and SSL VPNs.

Fiberlink rounds out its mobile workforce solution suite with a single interface for one-click connectivity to a variety of transport options that include Wi-Fi, hotel broadband, wide area wireless (CDMA/EV-DO), dial-up, ISDN, PHS, etc).

With mobile workforce solutions from Fiberlink, it's never been easier for organizations of any size to deliver a full 360° of productivity, protection, and control.

Click to view "The Anatomy of a Hack," a live hacking demonstration

Mobile Endpoint Compliance and Remediation

Extend360™ can ensure that enterprise mobile systems are up-to-date with security patches, configured properly and that all required security programs such as personal firewalls, anti-virus and anti-spyware, etc. are operating. If a system does not meet the customized security policy criteria established by the enterprise, Internet access can be disabled, VPN sessions can be torn down and Extend360 can remediate the security deficiency by pushing down applicable patches and configuration changes, or by restarting the security application that has become disabled. Remediation can be accomplished anytime the mobile system is turned-on. Pushing patches and configuration changes can be done anytime the system has access to the Internet, NOT only when there is an active VPN session to the corporate network.

Managed Enterprise-Grade Personal Firewall

Fiberlink's integrated personal firewall & intrusion detection solution actively inspects all traffic going into – and out of – the computing device - searching for any suspicious or hostile activity. It prevents outside agents from compromising the mobile worker's system, keeping your corporate network safe and your mobile workforce productive.

Fiberlink offers ISS' Real Secure Desktop Protector as a turn-key managed service. In addition to inbound blocking of application ports, protocols, and IP addresses, the service supports a firewall feature known as "outbound blocking." If a worm infects a workstation, outbound blocking will prevent it from propagating further or delivering proprietary information back to the attacker. Outbound blocking can also prevent mobile workers from running applications like peer-to-peer or instant messaging programs that are notorious for their security shortcomings.

Outbound blocking can also be used to prevent malicious activity from hackers that use Trojans. By piggybacking on an open inbound port, even where there's already a restrictive inbound policy enforced, hackers can use Trojan modules to steal information or remotely control the mobile device. With outbound blocking, the desktop agent can isolate the infected device more effectively and prevent the hacker from receiving confidential information being transmitted from the Trojan module.

Managed Anti-Spyware and Anti-Virus

Fiberlink also integrates a turn-key anti-spyware solution that utilizes Computer Associate's Pest Patrol technology. With 1 in 15 corporate laptops being infected with spyware system monitors, such as key loggers, an enterprise-wide anti-spyware solution has become a requirement for global enterprises.[6]

The anti-spyware managed service, leveraging the EVM agent and infrastructure, will detect and remove spyware from the endpoint in addition to proving the necessary definition updates for the anti-spyware application.

Fiberlink also provides up-to-the-minute version control of integrated anti-virus technologies - ensuring that your mobile workforce is fully covered by the latest versions of our partners' virus protection. When updates become available, we install them automatically.

Fiberlink can monitor your anti-virus and anti-spyware software in much the same manner it monitors the personal firewall. Fiberlink's integration of leading personal anti-virus and anti-spyware products ensures that virus protection and anti-spyware software is active and properly configured . Based on the security policies set by IT, we can admit or restrict mobile user access to the Internet or corporate network based on whether or not that users' endpoint is compliant. If an updated version of software is required, Fiberlink will push the upgrade out to the endpoint before allowing access to the corporate network. This process is seamless and unobtrusive to the end-user.

Customer Control

Business intelligence and reporting are critical to every business and Fiberlink delivers this via its Customer Resource Center (CRC). The CRC provides secure access to support and services, documentation, reporting such as CostView, ConnectView, usage reports, managed services reports, security services reporting, account administration and downloads.

360° of Productivity, Protection and Control

Fiberlink mobile workforce solutions combine a full range of professionally managed enterprise security services and a full suite of connectivity options, resulting in a comprehensive solution that simultaneously empowers mobile workers, and the IT managers who seek to enforce compliance with corporate policies within and beyond the traditional enterprise perimeter.

To view the live demonstration, The Anatomy of a Hack, use the link below:

http://www.demosondemand.com/clients/fiberlink/002/page/index_new.asp

Fiberlink has been recognized by Gartner as a leader in their 2005 Magic Quadrant for U.S. Managed Remote Access and Mobility Services. Click here to view the report.

Sources:

1. The State of Information Security, 2005,
A Worldwide Study Conducted by CIO Magazine and PricewaterhouseCoopers

2. Definitions from SearchNetworking.com

3. Watchguard Technologies, February 2005, (http://www.csoonline.com/metrics/viewmetric.cfm?id=775)

4. TechWeb News, October 26, 2005, (http://www.techweb.com/wire/172900645)

5. Trend Micro 2004 Roundup (http://www.trendmicro.com.au/global/products/collaterals/white_papers/2004annual_roundup_final.pdf)

6. "State of Spyware," Webroot, November 2005 (http://www.webroot.com)

Real World Security Threats: The Anatomy of a Hack video demonstration and companion guide is published by Fiberlink Communications Corporation, 1787 Sentry Parkway West, Building 18, Suite 200, Blue Bell, PA 19422. Please direct inquiries to Kristen Muckleroy at 215-664-1690 or kmuckleroy@fiberlink.com.

Click to view "The Anatomy of a Hack," a live hacking demonstration