Advanced Hacking Techniques: Implications for a Mobile Workforce

By Daniel V. Hoffman, CISSP, CWNA, CEH

August, 2006

FIBERLINK

CONTENTS

DEMONSTRATION ▶

Click here to view the demonstration: "Hacking the Mobile Workforce"

© 2006 Fiberlink Communications, Corp.

EXECUTIVE SUMMARY

Laptops are being deployed within enterprises at an increasing rate, mostly because of the flexibility and convenience they provide employees, and in turn, the productivity gains they provide for the companies.

It's impossible to go anywhere today without seeing people working outside the traditional office setting on their laptops - at the local coffee shop, while lounging in the park, standing at their kitchen counters, waiting at airport gates, and working in their hotel rooms. Gone are the days when people worked from 9:5 at the office. As John Girard stated in a report on Managing the Mobile & Remote Wireless Workforce[1], "during recent years, the volume of people working outside the settings of central offices has risen steadily. No matter where people are physically located, they are usually involved in remote work. Their outputs, collaborations, meetings and styles are characterized by interactions that are electronic, not face-to-face."

86% of employees in the United States will be working on laptops by 2007.
—Gartner Research

Some interesting market trends also support this same point:

- By 2008, 75% of the sales and services workforce worldwide will be mobile. (Gartner)
- In May 2005, notebook sales accounted for 53% of the total U.S. PC market, outpacing desktop sales for the first time. (Current Analysis, July 2005)

This shift in employee mobility has created a need to redefine the mobile worker. No longer can a mobile worker be defined solely as a "road warrior," the traveling salesperson who spends upwards of 80% of their time on the road going from airport, to hotel, to customer site, etc. It may also be a teleworker – someone who works mainly from their home office and uses either a laptop or sometimes even a personal PC. In today's business environment, a mobile worker can be defined simply as any user that has been issued a mobile computing device, such as a laptop.

With the growth in mobile laptop usage comes a new set of complexities for enterprises trying to make it simple and seamless for their end-users to connect, while at the same time, protecting their network, their assets and the reputation of their business.

In November 2005, a Boeing Co. laptop with personal information on 160,000 current and former employees was stolen and never recovered.

DEMONSTRATION

Click here to view the demonstration: "Hacking the Mobile Workforce"

© 2006 Fiberlink Communications, Corp.

THE CHANGING THREAT LANDSCAPE

When it comes to protecting data and devices, many IT professionals say that it has become too difficult to keep up. In other words, staying ahead of the security curve is overwhelming, and many feel like they are not leading, but rather responding or reacting. Conversely, there are others that feel like they have it all covered. Their end-users aren't complaining, their executives are happy, they haven't experienced any security breaches, and costs are under control. In our first video analysis, "Real World Security Threats: The Anatomy of a Hack" (12/2005), Dan Hoffman (Systems Engineer) walked through three primary network-based threats:

1. Credentials and data sniffing
2. Malware including viruses, worms, trojans, spyware and adware
3. Direct attacks to computer system or network as a result of deliberate action

The guide provided a thorough description of each type of threat, and best practices for how to protect your enterprise against that specific form of attack.

> *"The major Internet threat that is on the rise is the financially motivated, targeted internal attacks."*[2]
>
> —John Pescatore, Gartner Research

Gone are the days of random experimentation and information vandalism for the pure enjoyment of publicity and notoriety. Today's hackers are more motivated by quick financial gain – targeting specific industries or companies and going after their valued data and information. They are executing more cleverly than ever before to avoid detection. Therefore, enterprises need more sophisticated security processes, architectures and strategies to deal with these attacks today, and in the future.

A recent Gartner study shows that viruses and worms still top the list of threats that keep IT organizations up at night – with spyware and phishing in a close tie for second.[3]

Although most enterprises are aware of these sophisticated Web-based attacks, the threat is as daunting as ever.

> *More than 59 million cyberassaults originate in North America alone in an average 24-hour period.*[4]
>
> —Consumer Reports, July 2006

The Disconnected Threat

In a 2005 FBI Computer Crime Survey, US companies alone lost an estimated $67 billion due to computer crimes (e.g., viruses, spyware, PC theft and other computer crimes). This is despite the fact that virtually all of the organizations surveyed used anti-virus software (98.2%) and personal firewalls (90.7%). These losses are due to the fact that traditional Internet security solutions are not enough to handle sophisticated web-based threats. Malicious code can easily navigate open ports, disable a personal firewall and infect a network long before a signature-based anti-virus fix is available, or a software patch can be deployed.

One of the greatest challenges that IT faces is the multitude of possible entry points for viruses, worms and other malware to enter the network – whether their mobile users are connected to the network, or not. These include: USB storage devices and iPods®, laptop usage outside the perimeter, non-network based wireless communication (e.g., Bluetooth) or careless acceptance of an End User License Agreement can all expose the corporate network to malicious code and jeopardize the safeguarding of corporate data.

And who can miss the headlines about the risks associated with the physical theft or loss of laptops? If a laptop is stolen or lost, corporate information and personal information can be compromised at potentially catastrophic levels - permanently damaging a business reputation and leaving behind the residue of gross financial repercussions.

© 2006 Fiberlink Communications, Corp.

LAPTOP THEFT STATS

- 97% of stolen computers are never recovered. *(FBI)*
- Veterans Administration: A laptop was stolen in May 2006, with Social Security numbers and personal information for 26.5 million veterans. The VA offered free credit monitoring services to those affected. (The laptop was recovered in June, with no evidence that the information had been copied.)
- Ameriprise Financial: In January 2005, Ameriprise Financial Inc. of Minneapolis had to notify 226,000 people that their names and other personal data was stolen from a laptop left in an employee's car.
- Boeing Co: In November 2005, a Boeing Co. laptop with personal information on 160,000 current and former employees was stolen and never recovered.

For more information on data breaches like these and others, go to www.privacyrights.org.

Bottom line: Network-based security applications can't protect mobile devices from all threats. A proactive and pervasive security strategy is required to protect valuable corporate assets against modern-day attacks.

DEMONSTRATION ▶

Click here to view the demonstration: "Hacking the Mobile Workforce"

HACKING THE MOBILE WORKFORCE

In Fiberlink's latest video analysis, expert ethical hacker, Daniel V. Hoffman, CISSP, CWNA, CEH demonstrates a series of four modern-day attacks:

Hack 1: Access Point (AP) Phishing, the "Evil Twin"
Hack 2: Vulnerable, Simply Surfing the Net
Hack 3: Unaware of Vulnerabilities at 30,000 Feet
Hack 4: Modifying Malware to Invisibly Bypass Anti-Virus Programs

Each demonstration takes the viewer through a series of steps that many hackers would follow to exploit mobile and remote systems that lack the appropriate security protection, and provides best practices on how to safeguard your network.

Hack #1 – AP Phishing, the "Evil Twin"

With the increase in mobile computing, more and more workers are taking advantage of public Wi-Fi hotspots to work anytime, anywhere they choose to stay productive. Sometimes these locations require the user to pay for Internet connectivity; others offer it for free. Enterprises can no longer ignore end-users who "bring their own" Wi-Fi connectivity - they need to take steps necessary to proactively protect the laptops (endpoints) that are being used to connect back to the corporate network for sensitive data and resources.

In this hacking demonstration, better known as the "Evil Twin," a hacker creates a fake public Wi-Fi hotspot by utilizing a readily available Access Point emulation program. At this point, an unsuspecting end-user is tricked into entering their username and password into a fake Wi-Fi hotspot login page, where those credentials are stolen.

© 2006 Fiberlink Communications, Corp.

Consider the following preventative measures:

- **Deploy an intelligent, software-based client** on all laptops that has the ability to validate the authenticity of a public Wi-Fi hotspot network.

- **Set policies** that require an end-user to enter Wi-Fi authentication credentials into an intelligent software-based client that encrypts both the user name and password, versus allowing the user to enter their credentials into whatever HTML page happens to be presented to them when they connect.

Hack #2 – Vulnerable, Simply Surfing the Net

It is virtually impossible for enterprises to keep up with the ever-changing threat landscape. Most enterprises are aware of the plethora of security patches, anti-virus and anti-spyware updates that are made available on a daily basis. However, the problem is that the highly reactive and "inside the LAN" defenses that are employed by most enterprises lack the systems necessary to ensure that mobile devices receive these updates in a timely manner. In addition, enterprises often lack the controls to prohibit a user from surfing the Internet if their security posture is deficient.

Hackers are highly aware of the gaps present in updating mobile workers in a timely and persistent manner, and they take advantage by performing hacks on mobile systems that do not receive Internet Explorer security patches quickly enough. As a result, the mobile system is completely compromised.

Consider the following preventative measures:

- **Have policy enforcement logic reside on the endpoint** that prohibits a mobile user from surfing the Internet if they are missing a security patch.

- **Remediate security deficiencies persistently and in real-time** by pushing security patches to the endpoint anytime it is connected to the Internet. Employing a system that supports seamless, real-time remediation of vulnerabilities prior to VPN connectivity will ensure your network will not be compromised, and your end-user will remain productive.

- **Layer security** by utilizing an enterprise-grade personal firewall with IPS (Intrusion Prevention) functionality that could stop a potential exploit from running on a mobile system, even if it was not patched.

Hack #3 – Unaware of Vulnerabilities at 30,000 Feet

Airplane travel allows mobile workers to remain productive, even when they are not able to communicate with their co-workers and customers on the ground. Today, most domestic flights don't generally provide Internet connectivity, leaving most IT managers feeling fairly confident that mobile workers are safe when working in the air.

Unbeknown to most, however, workers utilizing a Windows Operating System can find themselves at significant risk because Windows does a poor job of controlling non-network based access. For this hack demonstration, HotSpotter passively monitors probe frame requests automatically being sent by Windows XP anytime the machine is powered ON. It then identifies the preferred networks listed in Windows XP Zero Config and utilizes that information to establish network connectivity to a mobile user's machine, in an environment where no previous Internet-based network exists. At this point, the mobile device can be completely compromised by the hacker.

> *"During recent years, the volume of people working outside the settings of central offices has risen steadily."*
>
> —John Girard, Managing the Mobile & Remote Wireless Workforce

© 2006 Fiberlink Communications, Corp.

Consider the following preventative measures:

- **Control network access** by preventing mobile devices from connecting to Wi-Fi networks unless specifically initiated by the end-user.
- **Layer security** by utilizing an enterprise grade personal firewall with an intrusion prevention system (IPS) on every mobile device. This will prohibit a hacker from exploiting the machine.
- **Remediate security deficiencies in real-time** by pushing patches to a mobile endpoint anytime it is connected to the Internet. Following this practice will ensure that mobile systems will always have the latest protection and be less susceptible to exploitation.

Hack #4 – Modifying Malware to Invisibly Bypass Anti-Virus Programs

Virtually all enterprises have anti-virus software installed on their mobile systems. Most enterprises, however, do not have the systems in place to ensure that the anti-virus program is always running and up-to-date prior to allowing an endpoint access to the corporate network. Regardless, this hack will demonstrate how malware can be modified to invisibly bypass two different anti-virus programs. This hack will also demonstrate how important it is to protect all mobile endpoints, even if those endpoints are only connecting to the corporate network via SSL VPN.

Consider the following preventative measures:

- **Layer security** by utilizing anti-spyware and a personal firewall with IPS functionality. Anti-spyware solutions can catch modifications and installations of malware that anti-virus systems might miss. Personal Firewalls with IPS have similar functionality, with the added benefit of prohibiting unwanted connections. Also, the use of two-factor authentication for SSL connectivity is becoming essential. A keylogger that captures every key an end-user enters will not be able to re-use those credentials to login themselves, if two-factor authentication, such as RSA tokens, are utilized.
- **Remediate security deficiencies in real-time** by ensuring that anti-virus and anti-spyware applications are always running and have the latest definition files installed prior to VPN connection back to the corporate network.

> *US companies alone lost an estimated $67 billion due to computer crimes (e.g., viruses, spyware, PC theft and other computer crimes.) This is despite the fact that virtually all of the organizations surveyed used anti-virus software (98.2%) and personal firewalls (90.7%).*
>
> —FBI Computer Crime Survey, 2005

DEMONSTRATION

**Click here to view the demonstration:
"Hacking the Mobile Workforce"**

© 2006 Fiberlink Communications, Corp.

SECURITY FUNDAMENTALS: RETHINK YOUR SECURITY STRATEGY WITH THE MOBILE WORKER IN MIND

Fundamental Change #1

Require your mobile endpoints to have the same level of security as those devices that are connecting to the network from inside the network perimeter.

The reason for this is simple: at some point that endpoint will connect back to the corporate network. Most IT enterprises spend most of their time making sure security is up-to-par on the machines that they see everyday (those machines inside the perimeter), versus mobile laptops which may leave the perimeter and not come back for months.

Not unlike desktop PC's, laptops need comprehensive mobile inspection systems to determine whether a device seeking a network connection is really an authorized device. It also requires that they are requesting tools that monitor a device to see if it has up-to-date firewall, anti-spyware and anti-virus settings, and all current software patches. This level of security should be applied to reduce risk, ensure business continuity and comply with government regulations, irrespective of the actual threats.

Most enterprise IT departments would never dream of tearing down hardware-based firewalls and IPS equipment from their WAN. While at the same time, their mobile systems are connected directly to the Internet and public Wi-Fi hotspots, often without up-to-date personal firewalls containing IPS functionality and without the necessary security patches and anti-virus or anti-spyware updates.

> *97 percent of stolen computers are never recovered.*
>
> —Federal Bureau of Investigations

Fundamental Change #2

Security policy enforcement logic needs to reside on the endpoint.

Many companies are looking at solutions like Cisco Network Admissions Control (CNAC) as the single source to protect their corporate networks against threats. Although a very strong solution for devices that are connecting from inside the corporate perimeter, the good and bad news is that's it – NAC was designed to only protect the inside: the LAN users, the corporate network; not the mobile endpoint.

The checking of a laptop's security posture and subsequent remediation needs to take place on the endpoint, whether the laptop is connected or not. If a mobile system is missing a security patch that makes it vulnerable to an exploit just for simply surfing the Internet, then that endpoint should not be able to browse the Internet until it is remediated with the proper security patch. Waiting until that mobile system connects back to the corporate LAN to receive that patch is simply too late – by that time, your network may have already been exposed.

Fundamental Change #3

Fixing security deficiencies needs to occur automatically and persistently, in real-time.

Most of the time, mobile systems need to connect to the corporate network to receive security patches, and anti-virus, personal firewall updates, etc. This policy can leave the mobile system vulnerable to exploits the majority of the time they are physically away from the office. All anti-virus updates and security patches must be pushed down to the endpoint anytime they are connected the Internet, as soon as they are tested and authorized by the enterprise, and without end-user interaction or approval. In addition, any security application that becomes disabled by malware or an end-user must be automatically restarted to provide the necessary level of protection.

© 2006 Fiberlink Communications, Corp.

Fundamental Change #4

Layered Security is Essential.
No single countermeasure can protect a network from all threats. Deploying multiple, integrated security measures throughout the enterprise is your best bet to protect your systems against threats to the enterprise. And don't be fooled by claims made by SSL service providers, who tout that browser-based VPN access back to the corporate network provides all the security IT needs to protect your network. VPNs (SSL or IPSEC) alone, while important, certainly do not provide the security necessary to protect a mobile device. Anti-spyware, personal firewall with IPS, proper endpoint configuration and robust patching and quarantining systems should all be required, and current, on an endpoint.

Fundamental Change #5

Controlling Access is Crucial to Security.
Controlling access falls into three essential categories:

- Ensuring that the access being provided is valid; (i.e., Evil Twin, AP Phishing).
- Ensuring that connectivity to Wi-Fi hotspots occurs only when desired and initiated by an end-user.
- Ensuring that Internet and VPN connectivity only occur when a mobile or remote system meets the minimum-security requirements to establish this connectivity.

DEMONSTRATION ▶

Click here to view the demonstration: "Hacking the Mobile Workforce"

FIBERLINK: SIMPLE. SECURE. MOBILITY.

Fiberlink delivers the software and services that make mobile working simpler and more secure for today's global enterprises. Since 1994, Fiberlink has earned a reputation for being the trusted mobility expert for demanding customers like GE, Bloomberg, and Continental Airlines, as well as over 675 other mid to large-sized companies.

Fiberlink has a legacy of offering solutions that compliment the access component of mobile connectivity. Though access remains an important service, Fiberlink solves the challenges of securely managing mobile and remote workers for IT, while simplifying the end user connectivity experience.

Fiberlink developed Extend360™ mobile access software and its Dynamic Network Architecture Platform™ (DNA) to extend security, command and control over mobile devices. This established a foundation for offering broader solutions that deliver both access and endpoint security and allowed Fiberlink to differentiate itself from competitors.

With the demand for dial services declining and trends towards "free" access, Fiberlink has focused development on enabling and securing all forms of access and offering valued-added services. Fiberlink created the first solution that allows end users to "bring their own access" but remain protected and connected to the enterprise.

Customers are asking for IT solutions that provide the ability to control who and how mobile users get connected, along with better business intelligence, through a control center portal. Fiberlink services are focused on providing the avoidance of reputation risk, asset risk, and network risk, using the command and control features of the DNA Platform technology.

© 2006 Fiberlink Communications, Corp.

In addition, endpoint vulnerabilities are on the rise. Fiberlink has created the ability to isolate and remediate identified vulnerabilities before the user "touches" and potentially exposes the LAN. With each new innovative service offered, Fiberlink creates competitive advantages over access providers, security point solutions and direct competitors.

To view the live demonstration, Hacking the Mobile Workforce, use the link below:

DEMONSTRATION ▶

Fiberlink has been recognized by Gartner as a leader in their 2006 Magic Quadrant for U.S. Managed Remote Access and Mobility Services for the 5th consecutive year. **Click here to view the report.**

SOURCES:

1) "Managing the Mobile and Wireless Workforce," John Girard, 28 April 2004

2) Augment Security Processes to Deal with the Changing Internet Threat, John Pescatore, 2 March 2006

3) Excerpt from Gartner RAS Core Research Note G00129419 "User Survey: Security Summit Reveals Spending Patterns Worldwide, 2005" Vic Wheatman.

4) Consumer Reports.org. State of the Net 2006, July 2006

© 2006 Fiberlink Communications, Corp.