

## Step by Step Guide to the Advanced Mobile Hacks Video

[del.icio.us](#)

Discuss in Forums {mos\_smf\_discuss:Hoffman}

By Daniel V. Hoffman, CISSP, CWNA, CEH

Last year, Dan Hoffman created a highly successful hacking video of a laptop with an unpatched version of Windows 2000. Even the Department of Defense included a link to it in their security newsletter. This year Dan not only has 4 hacking scenarios for you, but each can victimize a laptop running Windows XP with SP2. The Hacking the Mobile Workforce Video on Fiberlink.com shows live hacks that illustrate why fundamental changes in security strategy are necessary. This video shows the exact steps a hacker would utilize to exploit mobile systems lacking the appropriate security protection.

This article in 2 parts is designed to be a compliment to the in-depth, step-by-step hacking video tutorial. Part 1, Step by Step Guide to the Advanced Mobile Hacks Video, will outline in detail the steps organizations and users need to take to prevent each of these hacks from taking place. Part 2, Engineering Guide for the Enterprise, details the fundamental changes in security strategy that enterprises and individuals need to implement in order to protect ongoing threats to mobile devices.

To watch the companion video, click the above banner.  
Part 1 - Step by Step Guide to the Advanced Mobile Hacks Video  
Hack #1 &ndash; AP Phishing, Evil Twin

With users increasing their mobility, more and more they are finding it necessary to connect to public Wi-Fi hotspots to remain productive. While sometimes these are pay locations and sometimes they are free, enterprises can no longer pretend that their end-users don't utilize Wi-Fi connectivity. Enterprises need to take the necessary steps to enable and protect their mobile users. In this hack, a fake public Wi-Fi hotspot is created. An unsuspecting user is tricked into entering their username and password into a fake Wi-Fi Hotspot Login Page, where those credentials are stolen.

#### Prevention

-

Control access by having a client help validate the authenticity of a public Wi-Fi hotspot.

-

Control access by having an end-user enter Wi-Fi authentication credentials into a client that encrypts both the username and password. This is preferable to having the user enter their credentials into whatever HTML page happens to be presented to them when they connect.

#### Hack #2 &ndash; Vulnerable by Simply Surfing the Internet

Every enterprise is aware of the plethora of security patches, Antivirus and AntiSpyware updates that are released on an almost a daily basis. Though aware, most enterprises lack the systems to ensure that mobile devices receive these updates in a timely manner. Also, enterprises lack the controls to prohibit a user from surfing the Internet if their security posture is deficient. This fact is taken advantage of by performing a hack on a mobile system that did not receive an Internet Explorer security patch in a timely manner. As a result, the mobile system is completely compromised.

#### Prevention

-

Have enforcement logic reside on the endpoint that prohibits a remote user from surfing the Internet if they are missing a security patch that leaves them vulnerable to exploitation.

-

Fix the security deficiency all the time by pushing security patches to the endpoint anytime it is connected to the Internet.

-

Layer security by utilizing an enterprise-grade personal firewall with IPS functionality that could stop a potential exploit from running on a mobile system, even if they were not patched.

#### Hack #3 &ndash; Unwanted Connectivity at 30,000 Feet

Working on an airplane is a great way for mobile workers to remain productive. Since domestic flights generally do not

provide Internet connectivity, most users feel quite safe working in this environment. Unfortunately, workers utilizing a Windows Operating System can find themselves at significant risk, because Windows does a poor job of controlling access. For this hack, HotSpotter is utilized to establish network connectivity to a mobile user's machine in an environment where no wireless network exists. From this point, the mobile device can be completely compromised.

#### Prevention

-

Control 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 on the mobile device which can prohibit a hacker from exploiting the machine.

-

Fix the security efficiency all the time by pushing patches to a mobile system anytime it is connected to the Internet. In doing so, the remote system will always have the latest protection and be less susceptible to exploitation.

#### Hack #4 &ndash; Modifying Malware to Pass Undetected by Antivirus Programs

Virtually all enterprises have antivirus software installed on their mobile systems. Most enterprises, however, do not have the systems in place to ensure that the antivirus program is always running and up-to-date. Regardless, this hack will demonstrate how malware can be modified to successfully pass undetected through 2 different antivirus programs. This hack will also show how important it is to protect all mobile endpoints, even if those endpoints only connect to the corporate network via SSL.

#### Prevention

-

Layer security by utilizing antispymware and a personal firewall with IPS functionality. Antispymware can catch modifications and installations that antivirus cannot. Personal firewalls with IPS can have similar functionality with the added benefit of prohibiting unwanted connections.

-

Fix the security deficiency all the time by ensuring that antivirus and antispymware applications are always running and have the latest definition files installed.

Part 2 - Engineering Guide for the Enterprise

It is clear that workers are more mobile than they have ever been. Last year presented the first time that sales of laptop computers surpassed that of desktops, and enterprise workers are increasingly working from airports, coffee shops,

hotels, home, etc. Mobile workers are also more frequently using their work computers for personal use and connecting less often to the corporate network. This change in how workers work requires a change to the very definition of a remote access user. No longer is a remote access user defined as one who utilizes company-provided remote dial connectivity, rather it is truly any user with a laptop. This change also exponentially increases the security risks to enterprise computer systems and requires enterprises to instill fundamental changes in their security strategy.

#### Fundamental Change #1

Protect the Endpoint with the Same Security as the Corporate Network. The reasons for this are simple: At some point that endpoint will connect to the corporate network, there is sensitive data on that endpoint that needs to be protected and the end-user relies upon a functioning laptop to remain productive. Enterprises would never think of removing hardware-based firewalls and IPS equipment from their WAN. At the same time, their mobile systems are connected directly to the Internet and public Wi-Fi hotspots often without personal firewalls containing IPS functionality and without the necessary security patches and antivirus/antispysware updates.

#### Fundamental Change #2

Enforcement Logic Needs to Reside on the Endpoint. Many companies are looking to Cisco NAC to protect their corporate networks. The problem is, that's exactly what NAC was designed to do: protect the corporate network not the mobile endpoint. Any checking of an endpoint's security posture and subsequent restriction needs to take place on the endpoint and not just when a mobile system attempts to connect directly to the LAN or VPN into the corporate network. If a mobile system is missing a security patch that makes it vulnerable to an exploit by simply surfing the Internet, then that endpoint should not be able to surf the Internet until it receives that security patch. Waiting until that mobile system connects to the corporate LAN to receive that patch is simply too late. To illustrate this point, the following two diagrams will show the traditional NAC Topology and the better, Agent-Based Topology:

Traditional MAC Topology (Click for larger picture)

Fiberlink Agent-Based MAC Topology (Click for larger picture)

#### Fundamental Change #3

Fixing Security Deficiencies Needs to Occur Automatically and All the Time. Often, remote systems need to connect to the corporate network to receive security patches and antivirus updates. That can leave the mobile system vulnerable to exploits for the majority of the time that they are physically away from the office. All antivirus updates and security patches must be pushed down to the endpoint anytime they are connected the Internet and without end-user interaction or approval. In addition, any security application that becomes disabled by malware or an end-user must be forcefully restarted to provide the necessary level of protection.

#### Fundamental Change #4

Layered Security is Essential. Antivirus alone, while important, is certainly not enough to protect a mobile device. Antispyware, personal firewall with IPS, proper endpoint configuration and robust patching and quarantining systems are all required on an endpoint.

#### Fundamental Change #5

Controlling Access is Crucial to Security. There are three main elements in controlling access:

-

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 remote system meets the minimum security requirements to establish this connectivity.

Hope this was informative and enjoy the hacking videos.