

# Mobile Computing Security

## Protecting Data on Devices Roaming on the Perimeter

---

### Table of Contents

Executive Summary . . . . .	Page 1
The Expanding Network Perimeter . . . . .	Page 2
Securing the Device . . . . .	Page 3
Securing USB Ports . . . . .	Page 4
Improving Mobile Security with Microsoft Vista . . . . .	Page 5
Firewalls . . . . .	Page 6
Encryption . . . . .	Page 7
Protecting with Network Access Controls . . . . .	Page 8

### Executive Summary

Notebook computers were once reserved for the executive sales force or those that really, truly had an organizational need to be mobile. Today, the use of notebooks and other mobile computing devices has skyrocketed. In some organizations, the notebook has eclipsed the desktop as the standard issue computing platform in order to enable employees to take their work home with them and maximize productivity. In others, personal data assistants are the computing platform de jour. But organizations need to put the proper tools in place to ensure that their mobile devices and networks are not compromised as a result of this increase in mobility.

## Network Threats

In a recent CDW•G poll, IT managers stated that end-user data was the biggest threat to their organizations' networks.

Which layer of your organization's network security do you think is most vulnerable?

56%	<b>End-user data</b>
19%	<b>Application layer</b>
13%	<b>Network layer</b>
8%	<b>Transport layer</b>
4%	<b>Other</b>

SOURCE: CDW•G poll of 324 IT leaders.

## The Expanding Network Perimeter

The traditional network perimeter is eroding, or at least evolving. More and more users are relying on notebook computers and other mobile computing devices as their primary means of productivity. Organizations can realize efficiency and productivity gains by embracing mobile computing, but they also need to comprehend and defend against the unique security issues introduced by mobile computing.

Mobile devices such as notebooks, personal digital assistants, smartphones and USB storage drives have become ubiquitous, and for an increasing number of employees, their jobs would be challenging without the mobility provided by these devices. Nevertheless, poorly managed mobile devices greatly increase the potential for security failures and information compromise. Stolen or lost notebooks, BlackBerrys, USB sticks and other devices loaded with sensitive information, such as confidential e-mails, customer data and financial figures, can fall into the wrong hands. The loss of highly sensitive information and the potential associated media scandal is a huge problem in itself, but the impact might be greater — failure to protect certain information can be construed as a violation of regulations such as the Health Insurance Portability and Accountability Act.

Desktop systems that exist inside the network perimeter have the benefit of antimalware and firewall protection implemented at the network level, as well as the physical security present at the office site. For mobile computing devices, organizations have to ensure the device can protect itself. Administrators need to implement solutions at the device level to safeguard against infection and unauthorized access, and protect the data contained on the device.

In addition, administrators need to ensure that the organization's network is protected from potential compromise from the wandering device and wandering data. There are many ways that confidential or private data can leave an organization's network. Users may copy files to notebook PCs to take work home or copy data to portable storage devices, such as Universal Serial Bus flash drives, cell phones, digital cameras or MP3 players. Data can be intentionally or inadvertently sent out via e-mail, which makes it tough to protect against information leakage.

The best way to protect the ever-expanding network is to centralize data stores as much as possible, secure devices and USB ports, protect the network with firewalls and encrypt data. To maximize this, follow these simple, but practical mobile security best practices.

---

## Best Practices: Securing the Device

One of the first measures to protect a notebook computer is to set or enable a BIOS or hard drive password. This password is required when the computer is turned on and provides security at the hardware level before the operating system even begins to boot. Beyond that, antimalware, personal firewalls and wireless protocol encryption provide multiple layers of security for the mobile device.

Even on desktop systems inside the network perimeter, most organizations have some sort of client-level antimalware and personal firewall solution in place. For roaming mobile devices that have to protect themselves, these security measures become even more imperative.

**Download updates directly from manufacturers:** Administrators need to take into consideration that the mobile device may go days or weeks without connecting to the organization's, but it still needs to get the latest signature updates. For mobile devices, the software should be configured to download updates straight from the manufacturers' servers rather than relying on internal servers on the organization's network.

**Patch religiously:** Monitor security patches released by the manufacturers of the software installed on your mobile devices. Just like on the desktop, discovering and installing security patches as soon as possible can significantly reduce the number of security incidents.

**Manage connectivity mechanisms:** Turn off Bluetooth when you are not using it. Do the same with other connectivity mechanisms. Use the highest possible security settings for wireless connections.

**Password-protect the device:** Most devices come with basic password protection for device use. Turn it on. If possible, install third-party applications that implement stronger authorization mechanisms than basic login passwords.

**Use physical locks for notebooks:** Physical locks will prevent miscreants from picking up your notebooks and walking away with them. Provide physical locks to your employees, and instruct them to use the locks whenever they use the notebooks outside the organization's premises.

**Securely wipe devices before retiring them:** Confidential information has been recovered from mobile devices sold through online auction sites. Needless to say, most of those cases have been media disasters for the organizations involved. It is not enough to just delete the files before retiring devices — deleted files can be recovered easily. Destroying data completely from disks and making it unrecoverable is a difficult job. Use enterprise-grade disk-wiping software for all mobile devices before retiring them.

**Use software designed to recover or destroy lost or stolen devices:** Software applications are available that "phone home" or connect to monitoring services and report their location whenever they are connected to the Internet. Such applications can help in tracking, locating and recovering stolen or lost notebooks.

Some devices have a remote-wipe feature that lets you remotely delete all data or perform a hard reset if they are lost or stolen.

## The Perfect Storm

Ben Rothke, a New York City senior security consultant with International Network Services, calls it the "perfect storm" — curious people, ubiquitous high-speed Internet access and overall poor security on the servers storing that information. "When you put those three factors together, they combine to create the situation where confidential data can be quickly leaked and shared with an enormous amount of information. Once the data is shared in such a manner, it is effectively impossible to get it back in a secure state."

## Unauthorized Devices

"Make sure your employees understand they shouldn't plug 'foreign' — nonauthorized — devices into [organizational] computers," suggests Eric Ogren, security analyst with Enterprise Strategy Group.

Does your organization currently use USB flash drives?

55%	Yes
44%	No
1%	Don't know

SOURCE: CDW•G poll of 560 IT leaders.

## Securing USB Ports

Portable media has always been an issue when it comes to securing data. If you do not have control over the data once it is stored on the portable media, how can you monitor or control where it goes or who has access to it? From a security perspective, the confidentiality and integrity of the data are both at risk once it becomes portable.

When portable media meant 5.25-inch-wide square floppy disks that only stored 360KB of data, the risk wasn't quite as big. Not that 360KB isn't enough to store some sensitive or confidential information, but portable media today increases the risk exponentially. Now, users can store 8GB on a USB drive smaller than their thumb. This increases the risk both from the perspective that a user can house significantly more data on portable media, and from the perspective that the small thumb drives are easier to lose or misplace.

USB flash drives also pose a malware risk. Users may bring in USB flash drives that have been compromised and unwittingly infect the network with a virus, worm or other malware. Allowing users to bring in unauthorized storage devices and attach them to computer resources on the internal network exposes your organization to threats that bypass most, if not all, of the layers of security in place to protect the network.

In addition to the risk of compromising data or transporting malicious code, regulations such as Sarbanes-Oxley, HIPAA or the PCI Data Security Standards require that certain types of information, especially personally identifiable information and customer data, be protected. Noncompliance or breaches of these requirements can be quite costly.

It is important for organizations to understand the risk posed by USB flash drives and other removable media, and take proactive steps to manage users' ability to use them. The list below details some things you can do to lock down access for USB flash drives and protect your data from the risks of portable media.

**Written policy:** The first step in reigning in the use of USB flash drives and other portable media is to define your policy in a written document. Letting users know when, or if, or under what conditions the use of USB flash drives is acceptable will raise user awareness of the risks and reduce your exposure.

**Restrict access:** You can use Group Policy to restrict or deny access to prevent the computers on your network from reading data from or writing data to USB flash drives or other removable media entirely.

**Antimalware:** You should have desktop-level antimalware software in place and ensure that it is updated regularly to detect current threats. Antimalware software will scan and detect threats before allowing a file on the USB flash drive to execute, and it provides protection against rogue USB flash drives infecting your whole network.

**Encrypt data:** To prevent the compromise of data in the event that a USB flash drive is lost or stolen, implement security measures on the USB flash drive itself, such as encrypting the data.

**Rights management:** By implementing Windows Rights Management Services (WRMS), you enable a much higher level of control and flexibility in managing access rights for the data on your network. WRMS allows you to control not only whether groups or individuals are able to view or modify a file, but also whether they can forward or print the file. In addition, these rights can be changed even after the data has been downloaded and taken offsite.

The technology options for securing USB ports and drives is growing, and includes manufacturers such as GFI EndPoint Security, Pointsec Device Protector and Media Encryption.

In addition to controlling access to USB ports, port management tools may also control a combination of FireWire, serial, printer and infrared ports, floppy/CD/DVD drives, and USB-connected Wi-Fi or Bluetooth adapters. Some of the tools also let you restrict access for MP3/media players, handhelds, and CompactFlash and SmartMedia, as well as USB flash drives.

With port-blocking software, you don't need to physically remove, change or block any of your computer hardware. Instead, simply install the software — which may install small "agent" programs on each computer to be controlled — and assign appropriate privileges to each end user. You shouldn't need any new hardware to run the administrative software, as one of your current Windows computers should be sufficient. The cost is likely to be in the \$30 to \$100 range per computer — far less than the impact of any security breach.

---

## Improving Mobile Security with Windows Vista

Using Windows Vista as the operating system for mobile devices also provides additional security. Malware typically executes with the privileges of the logged-in user. In many cases, organizations have allowed users to have local administrator privileges under Windows XP in order to enable them to be able to make system and configuration changes that they are unable to do as standard users.

With Windows Vista, Microsoft addressed many of the issues that standard users encountered in Windows XP, enabling organizations to enforce users logging in as standard user rather than local administrator. In addition, one of the features of UAC (user account control) protects the system from being compromised by malware even for users who are logged in as administrator. Malware that would simply execute for an administrator in Windows XP will result in a consent prompt in Windows Vista, alerting the user that something is attempting to perform actions that may impact the system.

The whole point of UAC is to protect users and their computer systems from themselves. The standard user often does not have broad enough permissions for many purposes, which leads to users running with administrator privileges. Without some other control or security measure

in place, a user running as administrator can install software or make system changes that have an adverse impact. Malware that compromises the system typically runs in the same context as the logged-in user, meaning that the malware could also install software and make system changes with administrator privileges.

With UAC, even administrators are greeted with the Consent User Interface, or Consent UI. Consent UI is just a catchy name for the pop-up box that appears to confirm that you really want to execute the program in question. Most of the time, you will see the Consent UI alert message immediately after you try to execute or install some software. Because you initiated the action, the Consent UI seems more like an annoyance than a security measure.

In addition, Windows Vista includes additional features that render virtually all existing malware powerless. Most malware attacks rely on either being able to identify where in memory certain functions or processes are stored, or the ability to exploit buffer overflows in data to execute malicious code, or both. ASLR (Address Space Layer Randomization) and DEP (Data Execution Prevention) combine to eliminate these common attack vectors. ASLR randomizes the memory location of system functions, and DEP prevents any code to execute from within file areas designated for data.

## Vista Encryption

Microsoft Vista relies primarily on AES (Advanced Encryption System), using it as the encryption algorithm for both EFS (Encrypted File System) and BitLocker drive encryption. BitLocker can be configured to use either 128-bit or 256-bit AES encryption. IPSec encryption uses DES (Data Encryption Standard) or 3DES, but provides the ability to use a standard MD5 hash or an SHA-1 (Secure Hashing Algorithm) hash for the integrity algorithm.

## Firewall Options

Three popular firewall options include SonicWall's Pro 2040 Standard, Cisco's Adaptive Security Appliance 5510 and WatchGuard's Firebox X 550e. Cisco offers a Secure Sockets Layer VPN option.

All three options inspect the network layer, opening and closing ports like any router would. But they also each perform stateful filtering, which works at the transport layer and inspects packets for their intended destination. If that destination did not request that particular packet, it gets rejected. This type of stateful inspection lets the systems administrator block any information to or from a particular address. At the application layer, these products also will inspect entering and departing packets for inconsistencies and patterns in the application layer, which would indicate problems such as potential network attacks.

## Restrict Access with a Personal Firewall

Mobile devices should also be protected by some form of personal firewall. Many security suites include a personal firewall component that can be used for mobile devices as well. As with the antimalware component, the firewall software on mobile devices should be configured to download updates from a publicly accessible source rather than relying on a connection to servers on the internal network.

All data entering or leaving your organization will pass through the firewall. It can keep out unwanted intruders but also hamper critical connectivity. For example, your firewall may interfere with links to your website (if hosted locally or not), access to other websites, remote virtual private network users, wide area network connections, Internet updates and Voice over Internet Protocol telephone calls. It may also interact with server certificates, web e-mail, handheld device connections and domain name system requests.

To make sure you understand what you want your future firewall to keep out, thoroughly catalog and prioritize all your needs. There may not be a system within your price range that meets all of your diverse needs, and ultimately some things may need to be left out or more money must be budgeted. But there is another dark and insidious reason: maintaining VPN services.

Once a VPN is available, users expect it to work at all times from all locations, yet not all firewalls will accept a connection from the built-in Microsoft Windows client. Additionally, some firewalls on the remote end will block VPN connections. Meanwhile, your remote users may instinctively seek out locations around the globe where a VPN connection is nearly impossible and then call in asking that you remedy the situation.

Today unified threat management firewalls add a range of security functions that have typically been available piecemeal as separate programs or devices, from virus protection to spam, phishing and spyware blockers. On the menu of UTM features, buyers can find intrusion prevention systems (IPS); content filtering functions; programs to block spam, spyware and phishing attempts; and even vulnerability

scanning — software that probes for potential security gaps based on a network's defenses and known vulnerabilities. Yet every manufacturer offers a different mix of services in their UTM cocktail, and the mix can vary within a single manufacturer's product line. For example, WatchGuard's Firebox X family of security appliances can run either the standard Fireware or Fireware Pro operating systems, but IPS and antispymware capabilities are only available on the Pro version. Figuring out the menu of available services isn't hard, but anticipating future as well as current needs is critical. In many cases with the smallest devices, UTM features and expansion capabilities may be severely limited.

In all its various flavors, UTM carries a clear promise: more security that is easier to manage, requires fewer boxes and provides higher reliability. It's an obvious advance that has pushed every significant firewall manufacturer to jump on the UTM bandwagon. Calculating security return on investment is a difficult game: Estimating money saved by not suffering a network breach or other security meltdown can be next to impossible. But the new generation of UTM firewalls offers a better deal, combining a range of services into a single box that's economical to purchase and easy to manage.

Even if there is not a third-party personal firewall solution, mobile devices using Windows XP or Windows Vista include the Windows Firewall. The Windows Firewall in Windows Vista restricts both inbound and outbound access and provides more granular control than its predecessor, but given the alternative of using nothing at all, even the Windows Firewall in Windows XP affords some protection for mobile devices.

All three products inspect the network layer, opening and closing ports like any router would, but they also each perform stateful filtering, which works at the transport layer and inspects packets for their intended destination. If that destination did not request that particular packet, it gets rejected. This type of stateful inspection lets the systems administrator block any information to or from a particular address. At the application layer, these products also will inspect entering and departing packets for inconsistencies and patterns in the application layer, which would indicate problems such as potential network attacks.

## Encryption

Encrypting the entire disk or other storage is probably the most important thing you can do to prevent the theft of confidential information from a mobile device. An encrypted disk will be the final layer of defense in case a device falls into the wrong hands. Good encryption makes the data inaccessible to illegitimate users. Many commercial software applications do this automatically while remaining completely transparent to the user. Another, albeit weaker, approach is to encrypt individual sensitive files and folders instead of encrypting the entire disk. This tactic can be used in situations where encrypting the entire disk is not an option.

Configure the devices to always use the highest available encryption standard for wireless connections. All connections to the internal organizational network must be over a virtual private network.

### Encrypting Wireless Communications

Mobile devices are commonly used to connect to wireless networks. The wireless network may be at the office, at home, in a hotel, or at the coffee shop on the corner. Wireless networking is convenient but also represents unique security concerns. Namely, anybody within range can intercept the data as it is beamed through the air.

To protect the data being transmitted to and from the mobile device, a wireless encryption protocol such as WPA2 should be used whenever possible. In addition, any connections from outside of the network should only be allowed via a secured connection such as an encrypted VPN tunnel. At public hotspots that are not configured for encryption, users must be aware that their data is unprotected and exercise caution in the types of sites they visit and the information they transmit across the network.

### Encrypting the Data

If you read the news headlines, it seems as if there isn't a week that goes by without some security breach resulting from a lost or stolen notebook. The rise in the use of mobile computing devices brings with it a rise in the number of lost and stolen mobile computing devices and a need to implement some protection for the data contained on the mobile device in the event it falls into unauthorized hands.

Many organizations have implemented or are looking to implement drive encryption to protect all of the data contained on the mobile device. This is especially true for those organizations in specific industry segments like the financial or health sectors which have more stringent compliance regulations.

Checkpoint and McAfee offer two of the more widely known disk encryption solutions. Checkpoint's disk encryption was formerly known as Pointsec, and McAfee's solution was previously SafeBoot. Again, organizations that have deployed Windows Vista for their mobile devices have an advantage because it comes with BitLocker Drive Encryption built in so there is no need to invest additional money in an add-on third-party product.

BitLocker works with the Trusted Platform Module, a chip used to provide additional security functionality that's permanently attached to a system's motherboard. Tying the encryption key to the hardware and the validation process of TPM means hackers cannot modify or bypass the encryption — a problem with other encryption tools Microsoft has offered. Previous Windows versions have included data encryption features, such as Encrypted File System (EFS), but the tools protected only files and folders. An attacker could boot another OS, such as the Knoppix Linux distribution, to access and crack a system's password store. Once the system authenticates a hacker, EFS cannot provide protection.

Other Windows encryption tools have relied on the user to decide what should or should not be encrypted. Even if a systems administrator creates a special encrypted folder on a drive specifically to hold confidential or sensitive data, there's no way to be sure that users put all appropriate data in the folder. In the event of a notebook theft, the organization would still be unable to guarantee that private or personally identifiable information was not exposed. But encrypting the entire drive removes the guesswork.

## Network Access Controls

Whichever NAC option your organization selects, it's important that they consider standards. The three competing standards — Microsoft's Network Access Protection (NAP), Cisco's NAC and Trusted Computing Group's Trusted Network Connect (TNC) — have begun to merge, but users may find some early compatibility gaps when they mix products from the more than 200 vendors that have licensed the three technologies. But compatibility is the goal. In October 2006 Microsoft and Cisco announced they had developed an interoperability architecture that lets NAP- and NAC-compatible products work together. Then, in May 2007, Microsoft said it would make NAP compatible with TNC, which is an open standard. NAP is built into Microsoft Vista and is available in Windows Server 2008.

---

## Protecting the Network

Eventually the wandering mobile device will return to base and want to connect with the home network directly. In order to protect the internal network from any system compromises or nasty malware infections the mobile device may have picked up while it was away, it is a good idea to have some sort of NAC (Network Access Control) solution in place.

NAC products will analyze the mobile device (and any other device connecting to the network) and ensure that it is patched, has the appropriate security software installed, running and up to date, and that it otherwise meets the organization's security policy requirements before allowing it to connect to internal network resources. Most NAC solutions offer an option between simply rejecting connections from noncompliant clients, or redirecting them to a site or server with information and resources to enable the device to become compliant.

NAC is more than a mere firewall that grants recognized computers access, or a password scheme that lets privileged members log on. At its best, NAC ensures that any notebook computer, server or handheld device trying to access the network has up-to-date antivirus software and meets specified security standards. This is done by software agents sent by the NAC to check approaching machines for antivirus, antispymware and installed patches, as well as complex system characteristics, such as registry entries and file attributes. Computers that aren't deemed safe are barred entry or are redirected to a quarantined site where network administrators can update the computer's software or tell its user where to do so.

## Network Attacks

Mobile devices must also be protected against network-based attacks. Mobile devices (notebooks running off-the-shelf operating systems, for example) are vulnerable to the same varieties of attacks as any other computer system.

Because they need to operate in foreign networks, such as coffee shops, airport kiosks or other hotspots, mobile devices have extra-stringent security needs. They can't rely on the organization's firewall for protection. And the organization needs a means of managing security configuration, patch deployment and antivirus updates on their devices in the field.

Even systems running special-purpose operating systems have some vulnerabilities. Forced de-authentication attacks, in which an attacker transmits packets intended to convince a mobile end-point to drop its network connection and reacquire a new signal, can insert a rogue infrastructure device between a mobile device and the legitimate network.

Another security concern is the ability of many mobile devices to operate utilizing multiple protocols. They may primarily use one of the 802.11 family protocols or a cellular provider's network, but chances are good that they can also communicate via infrared or Bluetooth.

Even if those protocols aren't in active usage, many devices have these interfaces set "active" by default. Attackers can take advantage of this vulnerability and connect to the device, allowing them access to extract information from it or use its services. It's important for mobile device users to take the step of securing each of their device's communications interfaces. ♦