Part I

Understanding the Threats and Devices

CHAPTER 1

Understanding the Threats

A phone is no longer a phone and a BlackBerry is no longer a BlackBerry. All of these devices now need to be considered *enterprise mobile workstations*. As such, they need to be protected like mobile workstations and contain the very same protections (and more) that are afforded to LAN-based desktop workstations. Remember, these devices are on the front lines and they require in-depth protection — not providing it would be ridiculous.

Take a moment to think about all of the sensitive information that can be contained on these devices. Emails, confidential documents, and contact information are commonly stored on mobile devices. Now think about how small these devices actually are and how easy it is to have them lost and stolen. Then, realize that lost and stolen devices are just the tip of the iceberg.

Another important realization is that mobile devices don't stop being used once the user enters the corporate office. These devices are routinely connected to PCs to be synched and to download or upload all types of data. What is protecting that data? What is protecting your PCs from these mobile devices? The truth of the matter is that the threats to mobile devices extend far beyond the obvious situation of a BlackBerry getting lost or stolen. Fortunately, these threats can be categorized.

Quantifying the Threat

Regardless of the type of device being used, the threats are pretty much the same. This goes for laptops and desktops, as well as for BlackBerrys, PDAs, and cell phones. To really understand how to protect these types of devices, it is imperative to grasp the categorical threats that will be discussed in the upcoming sections.

The Malware Threat

Malware is the most well-known security threat to computers today. Even casual everyday users know something about viruses and understand that antivirus software is needed to protect against them.

If a device runs a computer program and additional data can be loaded onto the device, it is susceptible to malware — period. BlackBerrys, PDAs, and cell phones are no different.

There's not an enterprise out there that doesn't have antivirus software installed on their LAN-based desktop computers. The main reason for this is that everyone knows malware is bad, it can easily infect computers, and the next malware threat is only a day away. Even though antivirus software does an extremely inefficient and poor job of catching malware, it is the most standard security application out there today. Why then, don't enterprises ensure all of their mobile computer devices have antivirus software?

It's for two reasons. The first is that they simply don't know any better. Why would a BlackBerry or cell phone need antivirus protection? The second is that they don't know of the appropriate solution to implement; the malware threat is realized, but what can be done about it on mobile devices? Fortunately, this book will address these two points directly.

Understanding the malware threat is important, as is understanding how antivirus programs operate. Let's take a moment to consider how antivirus programs attempt to protect against these threats.

Antivirus programs rely on the signature (a unique identifier) of the particular virus, worm, or other threat to detect that a piece of code actually is a threat. If a piece of malware contains the actual and unique text `c: <ENTER> Jamie 3363` as part of its code, then it makes sense to look for that text to determine if a threat is present. It's pretty simple, and that's the problem — it's too simple. If the text in that piece of malware were changed to `c: <ENTER> Izzy 2006`, the threat would go undetected.

Another issue with signature-based antivirus is that it is reactive instead of proactive. For the threat to be detected it needs to be known first. To become known, the malware needs to have already infected enough machines to garner the attention of the antivirus software vendors. That seems like a bit of a Catch-22 — you'll be protected once enough computers have become infected.

Figures 1.1 and 1.2 illustrate a simplified version of how antivirus programs work and the process by which malware is detected.

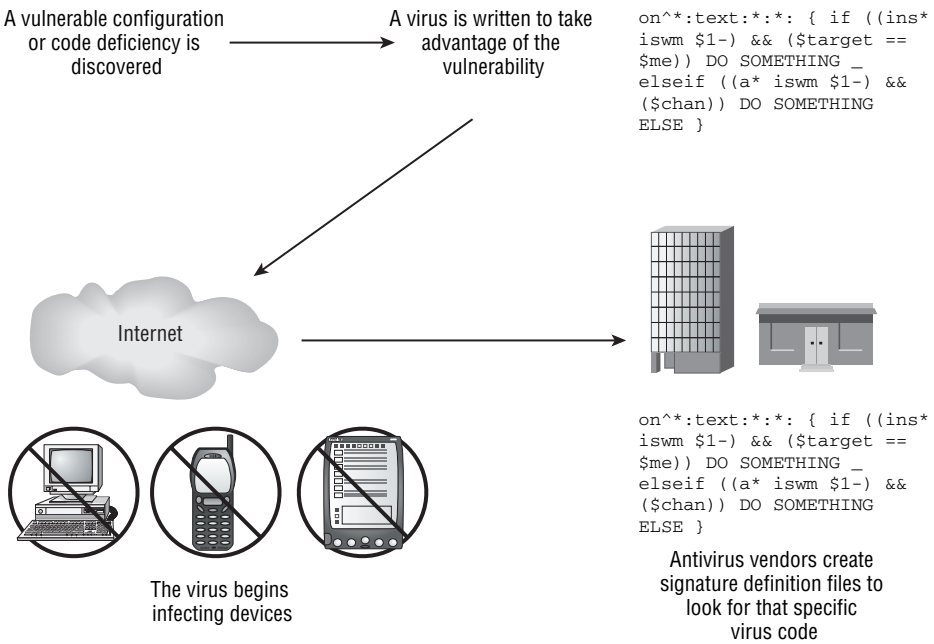


Figure 1.1: Creating a virus and an Antivirus

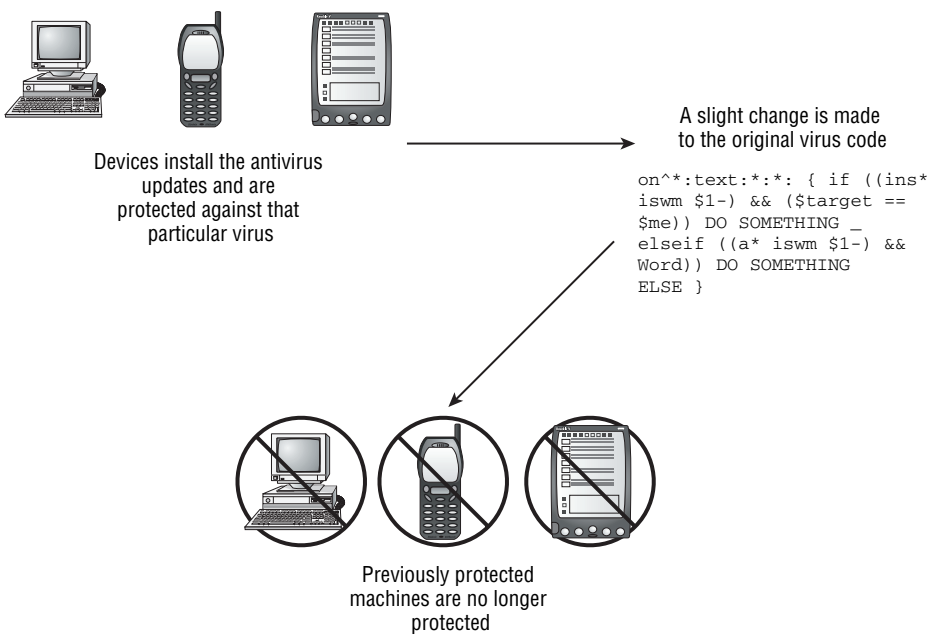


Figure 1.2: Applying the Antivirus

Given the obvious shortfalls of antivirus software, it is easy to understand why zero-day protection is becoming such a hot item. Zero-day protection can identify malware by what it does, not just by how it looks. Protecting against the unknown is certainly the wave of the future when it comes to malware protection. Keep in mind, though, that protecting against malware requires a multifaceted, layered approach. In addition to antivirus software, mobile devices should

- Be equipped with personal firewalls, which can directly help prevent malware, as well as deter its propagation and the extent of the damage
- Have the latest updates, as malware will often take advantage of vulnerabilities that may not be present if the proper updates are installed
- Be configured securely
- Possess available non-traditional antivirus programs, such as zero-day protection, antispyware, etc.

This is very similar to how you would protect a laptop or desktop computer. That's really the point! BlackBerrys, PDAs, and cell phones need to be protected with the same types of software and services as laptops and desktops. Later in this book, specific malware threats and specific preventative security solutions will be covered in detail.

Direct Attack

One of the most dangerous ways a mobile device can be exploited is by a direct attack, in which a hacker finds the device and takes deliberate actions to exploit it.

Mobile users employ their devices in a variety of venues and under a variety of circumstances. To attack the devices directly, a hacker needs to find the device, which can be done a number of different ways.

Perhaps the easiest way to find the device to exploit is to simply see it. If someone is checking their email with a BlackBerry or PDA, or simply speaking on the phone while sitting on a train, all a person with ill intent needs to do is see the device being used. Sounds simple, and it is. Once the device is found and identified, a hacker can determine which exploits to use against it.

Another way is to see the person using the device while actively connected to a network. In some cases a mobile user is more vulnerable when connected to the Internet while in a public Wi-Fi hotspot. If a user is checking their email with a PDA at Starbucks, then a hacker knows there is someone on the network and they can run utilities to determine the device's IP address and launch an attack. I've participated in a number of security videos that show in great detail how to attack a mobile user in a public Wi-Fi hotspot. There are few scenarios in which a mobile user is more vulnerable to attack than this one.

It's not necessary to see the device or the user to attack the device directly. If the device is connected to the Internet, it has an IP address. If it has an IP address it is on a network and anyone who can get on that network could find that device. If a hacker can determine the IP address of the device and can access that IP address, the device can be attacked from anywhere in the world. A mobile user could be connected to the Internet with their EvDO (Evolution Data Optimized) card while traveling in a taxi in New York, and a hacker sitting on the beach in LA can scan a range of IP addresses and happen to find their device. That's one of the very good and very bad things about the Internet. It enables different devices to be interconnected all around the world, though not everyone connected is acting ethically.

Figure 1.3 illustrates how a hacker can find a mobile device from anywhere in the world. The hacker can use any number of free tools to quickly and easily scan hundreds of thousands of IP addresses. These IP addresses can be assigned to networks and devices anywhere in the world. The scan will then show the hacker which IP addresses have devices attached, and the hacker can then attempt to find more information about the device and launch an attack.

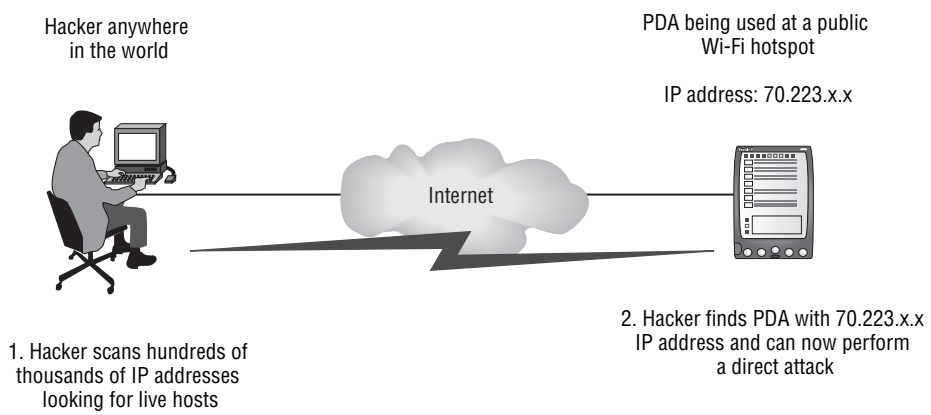


Figure 1.3: Finding a target

Another method for finding a device is to identify the signals being emitted from the device. Bluetooth is a good example of this. If a Bluetooth-enabled device is in use, a Bluetooth-sniffing tool can find and identify that signal. Once discovered, all types of bad things can be done to exploit the device. I will cover Bluetooth exploitations in detail later in this book.

I've covered how devices can be discovered, but what can be done to devices once they are found? This depends on the particular device and the technologies the device is using. Examples of things that can be done include

- Removing data from the device
- Altering data on the device

- Uploading data (including malware) to the device
- Modifying the device's configuration
- Utilizing the device in an unauthorized manner
- Rendering the device useless

Figure 1.4 illustrates the different direct attack threats to a mobile device.

Neither of the examples in the figure bodes particularly well for enterprises. In later sections of this book, specific examples of direct attacks will be illustrated, as will specific applications and actions that can be taken to protect the devices. In a general sense, the following tactics can protect mobile devices from direct attack:

- Personal firewalls can prohibit unauthorized access, as well as help devices become stealthier to avoid detection.
- The latest operating system and application antivirus updates will remove vulnerabilities, preventing direct attacks from taking advantage of ones that may not be present if the proper updates are installed.
- A secure configuration can leave fewer exploits open.

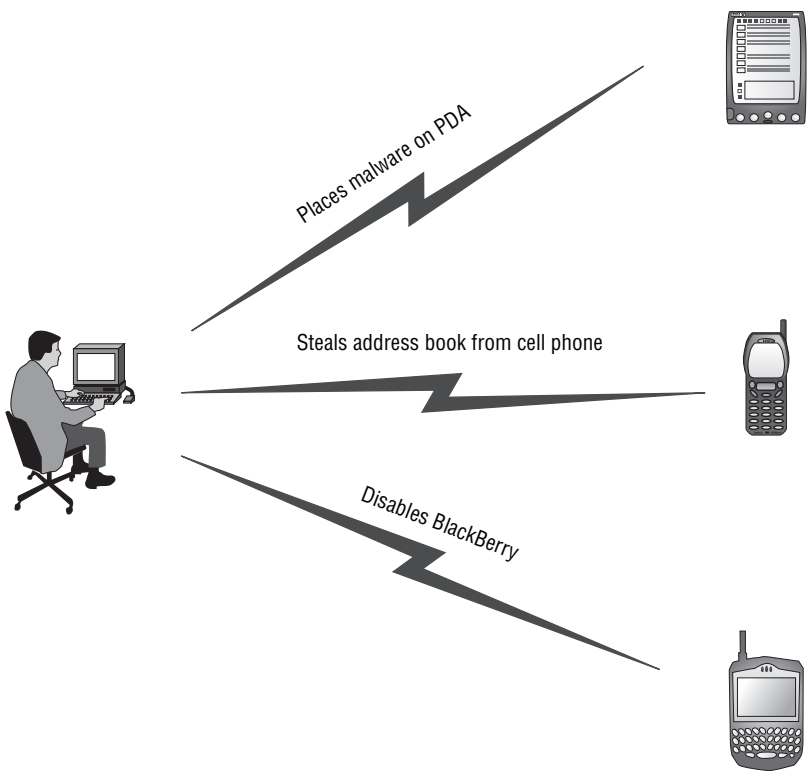


Figure 1.4: Examples of direct attacks

Data-Communication Interception

Sometimes the easiest and best means of attacking a device is indirect. Many devices are now capable of connecting to other devices and networks. Often these devices can connect via a number of methods. It's this communication that can be hacked and used for malicious intent.

One quick trip to an electronics store will yield a plethora of devices capable of connecting via Wi-Fi, EvDO and other 3G (third-generation) technologies, infrared, and so on. Enterprises are challenged to get their hands around these different types of connectivity and ensure that these connections are secure and that the info being transmitted over these devices is secure and encrypted.

Believe it or not, there are still enterprises out there that do not allow their mobile laptop devices to utilize wireless technology. They view Wi-Fi as simply too dangerous and too difficult to secure. But these companies really don't have a good way to stop their laptops from utilizing Wi-Fi — it's a written policy that they have no way to enforce. When it comes to nontraditional mobile devices such as PDAs, the threat is largely ignored.

As stated previously, mobile devices need at least the same protection as desktop and laptop computer systems. The fact that enterprises will attempt to prohibit Wi-Fi on laptops and have no strategy for PDAs and other devices is quite disturbing. These mobile devices will be used with no enterprise-provided protection or strategy, but they contain the same data and perform the same functions. This is explicitly true when it comes to data-communication threats.

A good way to protect a laptop or desktop computer that utilizes Wi-Fi is to implement WPA2 (Wi-Fi protected access 2) technology. That way, there is authentication to the wireless network that is encrypted and the data being transmitted and received is encrypted as well. Companies implement this technology on their wireless LANs, though 802.1x technology generally isn't used at public Wi-Fi hotspots.

One good way to address this with mobile laptops is to ensure — via technology not written policy — that VPN tunnels are up and running when the laptop is connected via wireless. With split-tunneling disabled, all communication leaving that interface will be forced to go through the VPN tunnel and be encrypted, commonly with IPSec via 3DES or AES, or via SSL. This is a good approach, but not rarely thought of with mobile devices.

When mobile devices connect to public Wi-Fi hotpots, enterprises generally ignore the threat and pretend there really isn't any of their data being transmitted from mobile devices over unprotected wireless networks. Clearly, not admitting there is a problem doesn't make it go away. Without question, mobile workers will use their PDAs and other devices for tasks such as checking email and sending instant messages. As with a laptop, this information can be easily

sniffed and is therefore susceptible to exploitation. You'll learn exactly how later in this book

Figure 1.5 illustrates the sniffing of data in a public Wi-Fi hotspot. In this example, a PDA is connected at the hotspot and the user is sending instant messages to a coworker. Because the data being transmitted wirelessly is not encrypted, it can be viewed by anyone within range. The data shown in the figure is actual data sniffed from a Yahoo! Messenger session.

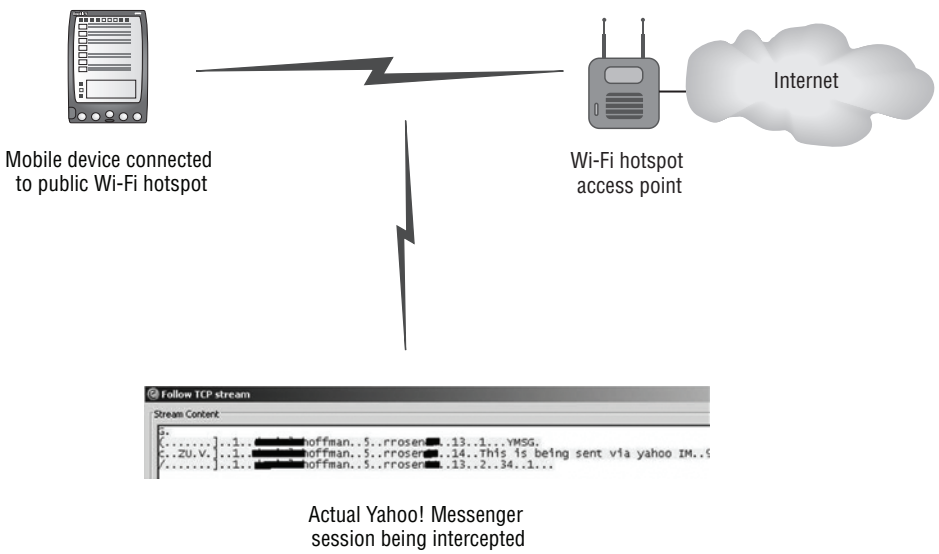


Figure 1.5: Sniffing data in a public Wi-Fi hotspot

Another consideration is that new mobile devices are coming with Bluetooth technology. This can be particularly helpful when using wireless headsets for phone conversations and for synching Bluetooth-enabled devices with other Bluetooth-enabled devices. As with Wi-Fi technology, this information is flying through the air and can be sniffed.

Often people think of Wi-Fi and are aware and concerned that the data is flying through the air. Sometimes, though, they overlook another threat associated with Wi-Fi: access point (AP) phishing. If a user attempts to be productive by using their Wi-Fi enabled PDA while standing in line to board a plane, what mechanism do they have in place to ensure that the Wi-Fi hotspot to which they are connecting is valid and not malicious? AP phishing is an attack in which a hacker configures a fake wireless access point (WAP) and attempts to trick users into connecting to it. Users may think they are connecting and entering authentication or credit card information into a valid hotspot, but they are actually doing so into the hacker's hotspot. I cover this in greater detail later in the book.

Protecting against data-communication interception includes

- Ensuring that data being transmitted to and received by a device is encrypted
- Ensuring that best practices are implemented when utilizing Bluetooth and other technologies
- Ensuring that network/connection interfaces are disabled when not in use

Authentication Spoofing and Sniffing

Whether you're logging into a T-Mobile Wi-Fi hotspot or accessing Yahoo! Mail, authentication takes place. This authentication verifies the identity of the person attempting to get access to the resource, which makes perfect sense. You don't want just anybody checking your email. You also don't want just anybody using your T-Mobile account for Internet connectivity, as you can incur additional charges. With mobile devices, the threat of authentication spoofing becomes considerably more prevalent.

When I worked at UUNET (an ISP) there were issues with dial-up fraud in Russia. Basically, groups would steal usernames and passwords from mobile users and use them to gain dial-up access to the Internet. You could just create a Microsoft Dial-Up Network Connection, enter the stolen username and password and get free Internet access. The problem was that this was done on a massive scale, where victimized companies would incur charges of thousands and thousands of dollars for Internet access that was being used by unauthorized people. The problem was very serious.

This threat is just as real now as it was back then. Some things have changed from a technological standpoint, but groups still can steal credentials for Internet access — these days it's mostly for public wireless hotspot Internet access. Credentials for means of access still need to be protected.

These days people use their BlackBerrys, PDAs, and cell phones to log into quite a few different systems. These can include webmail sites such as Yahoo! Mail, corporate intranet/extranet sites, and online banking. The authentication for these needs to be protected. All too often, enterprises and users operate under the assumption that protecting this authentication is the responsibility of the service provider — that is, they assume Yahoo! will protect their authentication; after all, they use SSL. It is true that the provider needs to do their part, but so do the enterprise and mobile users. You'll see later in this book exactly how not protecting authentication on the mobile device can lead to exploitation.

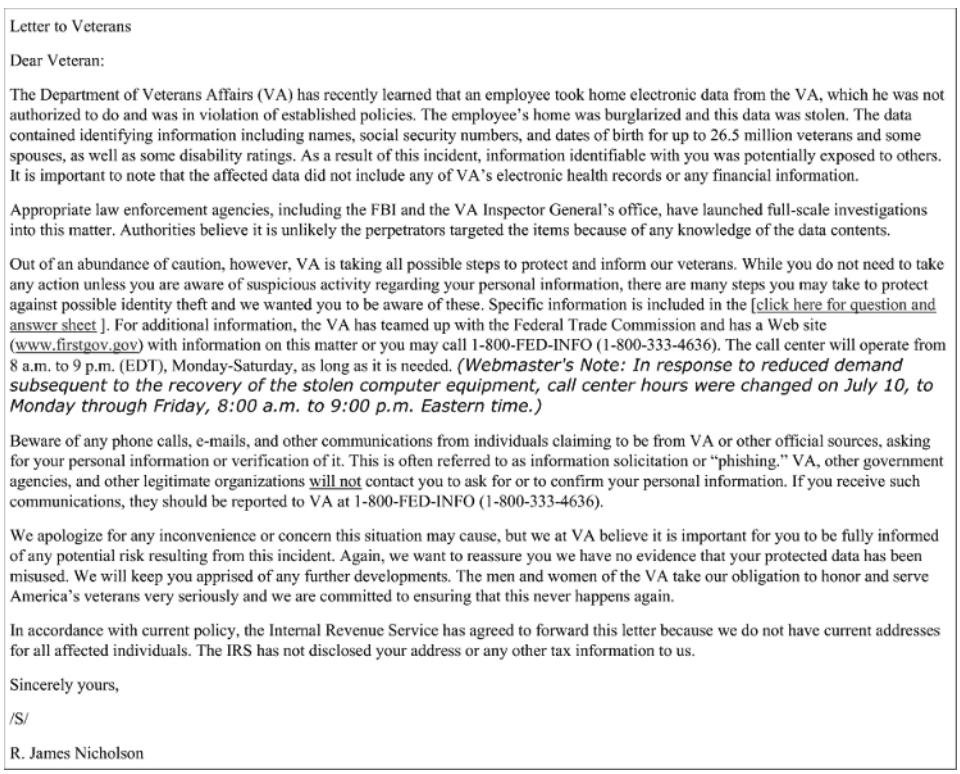
Protecting against authentication spoofing or sniffing includes

- Ensuring that authentication is encrypted

- Ensuring that authentication credentials are being given to the intended system — that is, authenticating against a *real* hotspot location
- Providing protection for credentials that are being stored on a mobile device
- Controlling what credentials are being stored on a mobile device

Physical Compromise

Recently there have been reports all over the press about sensitive data being lost or stolen. As a veteran of the United States Coast Guard, I received the letter from the Department of Veterans Affairs stating that my personal information was taken home and that the device on which my data resided was subsequently stolen. Figure 1.6 shows the letter.



Letter to Veterans

Dear Veteran:

The Department of Veterans Affairs (VA) has recently learned that an employee took home electronic data from the VA, which he was not authorized to do and was in violation of established policies. The employee's home was burglarized and this data was stolen. The data contained identifying information including names, social security numbers, and dates of birth for up to 26.5 million veterans and some spouses, as well as some disability ratings. As a result of this incident, information identifiable with you was potentially exposed to others. It is important to note that the affected data did not include any of VA's electronic health records or any financial information.

Appropriate law enforcement agencies, including the FBI and the VA Inspector General's office, have launched full-scale investigations into this matter. Authorities believe it is unlikely the perpetrators targeted the items because of any knowledge of the data contents.

Out of an abundance of caution, however, VA is taking all possible steps to protect and inform our veterans. While you do not need to take any action unless you are aware of suspicious activity regarding your personal information, there are many steps you may take to protect against possible identity theft and we wanted you to be aware of these. Specific information is included in the [click here for question and answer sheet]. For additional information, the VA has teamed up with the Federal Trade Commission and has a Web site (www.firstgov.gov) with information on this matter or you may call 1-800-FED-INFO (1-800-333-4636). The call center will operate from 8 a.m. to 9 p.m. (EDT), Monday-Saturday, as long as it is needed. *(Webmaster's Note: In response to reduced demand subsequent to the recovery of the stolen computer equipment, call center hours were changed on July 10, to Monday through Friday, 8:00 a.m. to 9:00 p.m. Eastern time.)*

Beware of any phone calls, e-mails, and other communications from individuals claiming to be from VA or other official sources, asking for your personal information or verification of it. This is often referred to as information solicitation or "phishing." VA, other government agencies, and other legitimate organizations will not contact you to ask for or to confirm your personal information. If you receive such communications, they should be reported to VA at 1-800-FED-INFO (1-800-333-4636).

We apologize for any inconvenience or concern this situation may cause, but we at VA believe it is important for you to be fully informed of any potential risk resulting from this incident. Again, we want to reassure you we have no evidence that your protected data has been misused. We will keep you apprised of any further developments. The men and women of the VA take our obligation to honor and serve America's veterans very seriously and we are committed to ensuring that this never happens again.

In accordance with current policy, the Internal Revenue Service has agreed to forward this letter because we do not have current addresses for all affected individuals. The IRS has not disclosed your address or any other tax information to us.

Sincerely yours,

/S/

R. James Nicholson

Figure 1.6: Letter from the Department of Veterans Affairs regarding theft of personal information

It's an interesting scenario. The person taking home the data wasn't purposely doing anything wrong. To the contrary, they were actually trying to do something good — working from home. This type of thing happens all the time. Why not be productive out of the office?

Almost every day in the press you read about similar scenarios taking place. We all know that the days of working only from 9A.M. to 5P.M. are gone; rather than stay in the office and work late, it's much more appealing to bring the work home.

Now, throwing jet fuel on to the fire, there are mobile devices. Sensitive information is not just being taken home to be worked on; it's being conveniently carried in the pockets of mobile users. Enterprise-sensitive data is now being taken to places like the airport, on fishing trips, to the ballgame, and to the bar.

Convenience is a really good thing — sometimes too good. I know of people that constantly have their BlackBerrys. While it may be annoying to have a dinner conversation with a friend who refuses to stop checking their email, the threat posed to enterprises is even higher. I know of an actual instance in which an individual took a mobile device along on a business trip out of the country. It made perfect sense to stay connected and productive while being mobile. On that trip and after a day full of meetings, the person decided to go to a bar and have a few drinks — then to have a few more. By the next morning there were stories that certainly wouldn't be appropriate for printing in this book (think of the movie *Bachelor Party*). There was also one missing mobile device.

Clearly, the need to protect data transcends the confines of the brick-and-mortar office. Anywhere data goes it needs to be protected and frankly its dissemination needs to be controlled. Enterprises sometimes understand this but don't feel that controlling the data is possible. This book will show exactly how it can be done.

On a trip earlier this year, I witnessed one of the most outlandishly ignorant disregards for security I've ever seen. I was on flight and noticed a person in front of me working on a mobile device. This mobile device had a fairly large screen, and even though I tried not to look it was difficult not to. It didn't hurt that I was sitting in a middle seat and didn't have the space to open my laptop and get some work done, so I was bored. The person with the mobile device was actually organizing all of his different usernames and passwords. Right there, in clear sight, was his name, his company's name, usernames and passwords to various computer systems and applications, and key codes to different keypads to enter various company locations.

There really is a danger to the widespread expanded use of mobile devices. It goes for mobile computers and for mobile phones. I can't tell you how many sensitive phone conversations I have overheard in airports, or sensitive information I've seen on other people's screens — all without any real desire on my part to see or hear it.

We can do a number of things to protect against physical compromise:

- Ensure all data on a mobile device is encrypted
- Mandate that all mobile devices require authentication to be accessed
- Control and audit data that is copied and downloaded onto mobile devices
- Educate users on the dangers of using mobile devices in public

Mobile Device Enterprise Infrastructure

BlackBerrys, PDAs, and cell phones are cool devices and you can do a lot with them. The ability to check the score of the Cubs game from a cell phone is certainly useful, and fairly simple. But taking it to the next level — utilizing a mobile device for corporate activities — often requires that an infrastructure be implemented or modified back at the corporate location. This possesses its own set of problems.

I know of a company that didn't really embrace the idea of using mobile devices. They provided their remote users with laptops and Internet connectivity from just about anywhere, and that was it. But a number of employees wanted (and some needed) to use PDAs.

At first, these users simply bought their own PDAs and synched them up with their laptops continually. This enabled them to carry certain documents, contacts, and emails with them wherever they went. The company officially didn't support this, but there wasn't a lot they felt they could do. As long as the company didn't have to pay for the PDAs, they didn't really care. The company's concern was with cost, not security.

Armed with their new PDAs, the employees used them to connect to the Internet. At first it was to wireless LAN, then to public Wi-Fi hotspots. The advent of code division multiple access (CDMA) and EvDO cards enabled these users to employ their PDAs to get on the Internet from just about anywhere. There still wasn't a huge security concern even though sensitive data was undoubtedly on these devices and they were routinely being connected to the Internet without any enterprise security policies, controls, or technologies.

It didn't take long for people to want to use their PDAs to actively check their company email. The company was approached and due to security concerns, the idea was squashed. The company just wasn't ready to support PDA email access.

The users were discouraged, but not thwarted. They simply had their company email forwarded to a personal email account. They could then modify that personal email account to send email messages to look like it was coming from their corporate email account, and they were all set.

At this point, the company officially didn't support PDAs because they didn't want to spend the money on the devices and they felt the devices were a security risk. At the same time, company email was being automatically forwarded to these devices and sensitive company documentation was being used.

Soon somebody had a real good idea. Even if the company wasn't going to allow PDA email access, they could simply set up their own server on the company premises, have it talk to the official corporate email server, then open up that unauthorized server to the Internet. That would save the users the trouble of using multiple email accounts to access company email from their PDAs. So the server was set up. Figure 1.7 shows a simplified example of this topology.

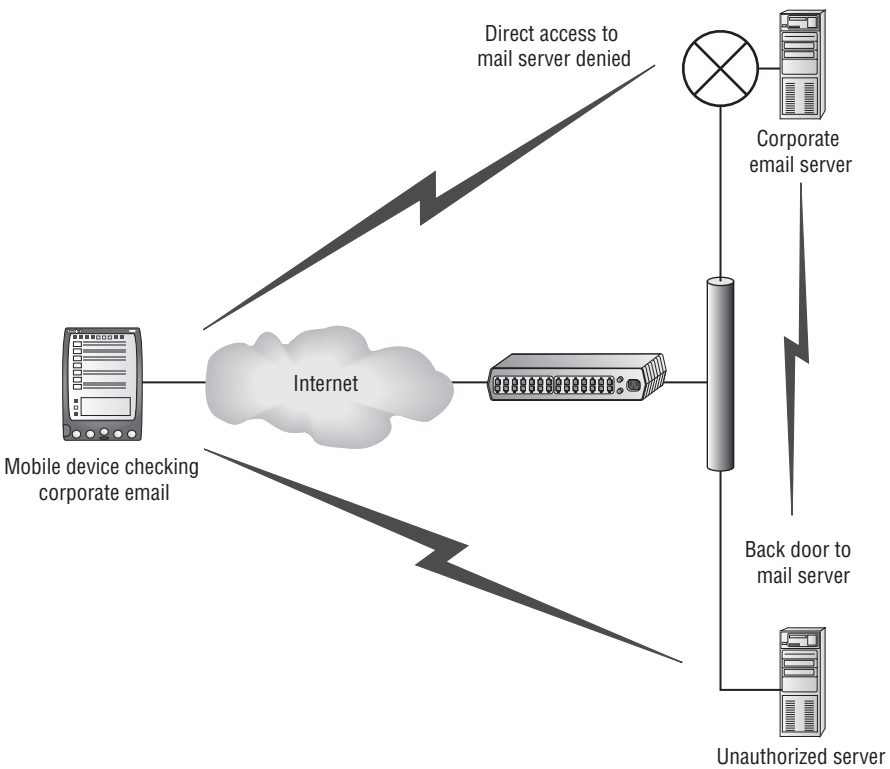


Figure 1.7: Accessing corporate email through an unauthorized server

Everyone was happy. The users had access to their corporate email, the company didn't have to worry about securing PDAs because they officially weren't supported, and the company didn't have to bother to buy the PDAs — the employees were doing it themselves! Perfect!

I hope I don't have to go into detail about why this scenario is so bad! Clearly, ignoring the problem didn't make it go away, and the company ended up being much more insecure as a result. The employees who set up the server probably broke quite a few rules. That being said, their intention certainly was not malicious. The point to be learned is that if new technology is not recognized, embraced, and controlled, it can lead to mavericks taking it upon themselves to implement the technology. This implementation will almost certainly be less secure than if it were done by the security department.

The company in the previous scenario eventually moved to using BlackBerrys. They opened up their infrastructure to accept this and put into place various supporting servers. They had to embrace the fact that users wanted to be productive and check their emails from mobile devices. They eventually complied and everyone was happy…and secure!

Not all of the infrastructure-related threats are linked to maverick employees and their rogue servers. Sometimes security personnel themselves implement the technologies in a manner that is not secure. Also, there can be vulnerabilities to the servers themselves.

Anybody who has ever set up a server knows that one of the real challenges is to set it up so that it is secure. It's not very difficult to get it up and running, but knowing what you can disable to make it more secure, configuring it so it is secure, and keeping it patched are all challenges. Add the variables of loading proprietary software for mobile devices and opening it to both the Internet and the corporate LAN, and the security can become a challenge.

Whether realized and officially supported or not, there are systems within the corporate infrastructure that facilitate connectivity to mobile devices. It is important to both know about these devices and to have them under complete control.

Consider that any system on the LAN that connects to a mobile device is potentially a conduit from that device into your infrastructure. It's really that simple. If that mobile device is compromised, then a direct connection to a system on the LAN can be achieved.

Enterprises have been using hardened VPN concentrators for years and these devices serve a very similar function to appliances that allow mobile devices access to the LAN. The VPN concentrator sits between the Internet and LAN and enables someone with Internet connectivity to securely access resources within the LAN. The vulnerability is both the conduit and the device itself.

NOTE **The name-brand VPN concentrators that are found in most enterprises are bastion hosts, hardened and protected to withstand connections directly to the Internet. While it is common and a best security practice to place one of these systems behind a firewall, they are specifically designed to withstand relentless attacks from the Internet.**

Now consider a Windows server. Few would say that a Windows server on any hardware has the same type of inherent security as VPN concentrators. To the contrary, Windows exploits are very well known and available. If you are implementing a mobile-device connectivity solution that runs on a Windows server and has connectivity directly to the Internet and your LAN, then you have a unique set of challenges in just ensuring that the server itself is secure. Again, throw on some proprietary connectivity software and the solution can become difficult to secure.

Protecting the infrastructure that supports your mobile devices is commonly done by

- Ensuring that all exposed servers are configured as securely as possible and that they contain all necessary security patches
- Utilizing firewalls on both the LAN and Internet side of the exposed server
- Having indisputable knowledge of the devices on your LAN and how they are being accessed (to prevent the installation and use of unauthorized servers)

Later in the book, I will detail specific examples of how the infrastructure can be exploited and illustrate best practices to help prevent that from happening.

PC and LAN Connectivity

The days of the stand-alone mobile device are passing quickly. For many years now, it has been possible to synch mobile devices with PCs and Macs and to connect these devices to the LAN. These simple acts actually pose significant security threats.

The first PDA that I recall buying was very simple. I don't think it could even synch to my PC. I used it for keeping track of my schedule and for holding a few phone numbers. Now just about anything you buy — including iPods and other music devices — can synch with your PC and Mac.

This is a problem because any time you connect devices together or transfer data between devices, you run the risk of unwittingly transferring malware.

Virtually all enterprises have antivirus software and similar technologies running on their mail servers. Many have also implemented appliances that sit between their LAN and the Internet that are designed to catch viruses and other malware before they enter the LAN. That way, they are able to catch these threats before they to get to the LAN-based desktops.

Let's say a user has a home PC, a work PC, and a mobile device. Before leaving for home, the user synchs some files from his work PC to his mobile device. The user goes home and then synchs the mobile device with his home

PC. Unbeknownst to the user, his home PC has a nasty worm on it. During the synching process, that worm takes up residence on his mobile device. He goes to work the next day and synchs his mobile device with this PC. His work PC now has the nasty worm. Because it's a worm, it doesn't require any human interaction to spread. The worm propagates to other PCs on the network and before long, the corporation has a major outbreak.

Figure 1.8 illustrates how this process takes place.

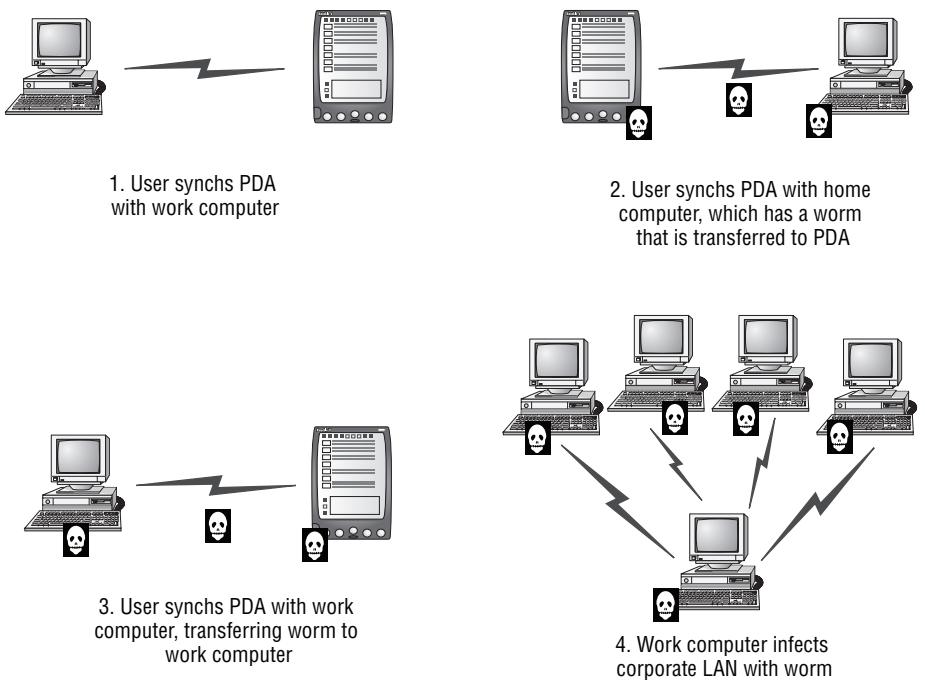


Figure 1.8: How a single PDA can infect a network

The scenario in Figure 1.8 is very common and bypasses the aforementioned network-based antivirus solutions. It essentially gives malware a back door to the enterprise and renders the networked-based solutions useless.

Another problem with connecting mobile devices to PCs and the LAN is that data can be taken off the LAN and PC and be placed on the mobile device. The common way that enterprises determine who has access to data is by assigning users rights and permissions to different network drives, servers, etc. This is nothing new.

Although controlling who has access to what on the LAN isn't much of a challenge, the needs are becoming more granular. It's no longer acceptable simply to dictate who has access to what data, but rather you must indicate what the user can do with that data.

Take for example the following scenario. A corporation may give a specific individual access to sensitive information. The user may have every right to access and modify that data and in essence, the corporation wants the end user to work with that data as part of their job. At the same time, that corporation may not want that end user to be able to take the data and place it on a mobile device or USB drive. Perhaps the corporation would like to allow the data to be copied, but only if the data is encrypted. The reasons for this are many. Human resources data, intellectual property, pricing information, customer contact information, and other sensitive data all need to be protected. If this information is copied to a mobile device or USB drive, it can easily be lost or stolen and made public. Devices with sensitive data on them get lost or stolen every day.

The problem is that many corporations don't have the systems and technology in place to enforce controlling their data. Consequently, they need to rely solely on written policies to stop employees from copying data to mobile devices and USB drives. That is an ineffective solution to a serious problem.

Not long ago I spoke with an insurance company that had a written policy that no non-company–issued and –authorized devices could be connected to company devices. This essentially means that employees were not allowed to connect mobile devices or USB drives to their work computers. They put this policy in place to stop end users from copying sensitive data to devices that could be lost or stolen. The company did not have any technical means to enforce this policy; they simply relied upon the written policy for enforcement. The written policy clearly stated that any employee caught breaking the rule would be fired — period. The security department at the company was gravely concerned that they had a serious problem and that they needed a technical means to enforce the security policy. Protecting their sensitive data was paramount.

The security department approached their senior executives with their concern. The senior executives did not feel there was a threat. How could employees possibly copy sensitive data to mobile devices if there was a specific, clearly stated written policy against connecting unauthorized devices to company computers? Doing so would get the employee in question fired!

Undaunted, the security guy decided to run a pilot program with a technology that was able to report and audit when devices were connected to their laptops. The data showed that 80% of users were connecting unauthorized devices to their corporate PCs!

The moral of the story is that written policies are not enough. Sure, these employees could have been fired, but they weren't setting forth with the intent to break company rules; they simply wanted to be more productive. In reality, many of the users probably didn't even know they were breaking a rule that could have gotten them fired.

You can protect against PC and LAN connectivity by

- Putting policies and technical systems in place to ensure that data is controlled at all times
- Putting policies and technical systems in place to control the devices that can be connected to company-owned computer systems
- Ensuring that every computer system contains appropriate and up-to-date antivirus and anti-malware solutions.

Fundamental Changes in Security Strategy

The recent change in how users employ mobile devices and technology requires a fundamental change in security strategy. The old way of thinking doesn't work any longer.

In the beginning, enterprises put all of their time and effort into protecting their LAN from the outside. It made a lot of sense at the time: place as much protection as possible between yourself and the threat. In doing so, companies spent millions on firewalls, intrusion detection and intrusion prevention systems, antispam appliances, antivirus appliances, etc. They essentially built a fortress between the LAN and the Internet, and they did so for good reason.

With the present change in how workers work and the technology that they use today, this old way of thinking simply doesn't apply to mobility. Certainly, the LAN still needs to be protected and that will not be denied. However, these LAN-based systems cannot be relied upon to protect mobile devices.

This means that two fundamental shifts needs to take place:

- Enterprises need to change their strategies from protecting only their LAN to putting policies and systems in place to protect the mobile devices.
- Enterprises need to put into place policies and systems to protect and control their data, wherever it may reside.

These shifts are quite simple to comprehend at a high level and they really make sense. If devices are mobile, you need to take action to protect them, as the LAN-based systems won't be able to do so. Also, controlling and protecting data seems like common sense. Though these changes are easy to state and easy to comprehend, many enterprises have yet to adopt and implement them.

The reasons why these shifts haven't taken place include the following:

- Mobility presents unique challenges that many enterprises simply do not know how to address.

- Common perception is that it's cheaper to do nothing than to address the threats. While it may be easier, it certainly is no longer cheaper. Numerous studies are able to quantify the costs of inaction when it comes to security, and with companies losing millions to clean up the mess from security mishaps, it only verifies that the idea that easier is cheaper is a myth. In addition to the actual man-hours it takes to address a security breach, there are now significant soft costs. If a CEO of a company were asked what amount of money he would be willing to spend to remove his company's name from the press after sensitive data was made public due to a security mishap, it would likely be considerably more than the cost to implement the appropriate security policies and technologies to prevent the breach from having happened in the first place.
- Apathy. This one drives me nuts. Security personnel and executives understand the threat, realize it can be addressed, and do nothing. In my job, I see it all the time. Their apathy is due partly to personnel being too gun-shy to implement the systems, in fear that they won't work and they themselves will look bad. Not too long ago, the IT job market really was bad — it was hard to get a good job, as many companies were forced to lay people off and there were more IT people than jobs. Those who had jobs wanted to do everything they could do keep them. Unfortunately, apathy and security don't work very well together. When somebody is afraid to do the very job for which they are being compensated, there can be very serious problems. Today the job market is good and security personnel can still be apathetic. This is out-and-out negligence.

Throughout this book, there will be specific examples of technologies that can be put into place to address the threats. The fundamental shifts require a tactical change in security strategy. The fundamental shifts are critically important to understand, accept, and implement. The following sections cover the necessary changes in security strategy.

Protecting the Mobile Device Itself

As devices leave the confines of the protected LAN, they need to be protected as if they were still on the LAN. Doing so means that the various LAN-based systems and technologies now need to be extended and reside on the various types of mobile devices. This includes antivirus software, personal firewalls, IPS/IDS, VPN, etc. Remember, these devices are on the front lines — directly connected to the Internet and other networks. These devices are more vulnerable than any other systems you have. They need to be protected accordingly.

Enforcing Compliance on the Mobile Device

Just as with PCs, it is important to keep mobile devices compliant. Compliance can mean different things to different companies. For example, if antivirus software is running on a PDA, that may be enough to meet one company's security requirements. At the same time, another company may need to ensure that a personal firewall and encryption software are installed and running. In any event, there needs to be a technical means to ensure that the devices meet the minimum security posture set forth by the company. A written policy alone will not suffice.

Addressing Security Deficiencies Automatically

If a mobile device does not meet the minimum security-posture requirements as set forth by the organization, then those deficiencies need to be remedied automatically and without having to connect to the corporate LAN.

Implementing Layered Security

As with any type of a security, a layered approach is essential. Protecting mobile devices from malware doesn't mean simply installing antivirus software on a mobile device. We'll go over this in great detail later in the book.

Controlling and Protecting Data

Regardless of where data resides, it needs to be protected. Because data can be copied to mobile devices easily and mobile devices can be exploited a number of different ways, the focus is on protecting the data itself.

Things to Remember

The threats that mobile devices bring to the enterprise are significant and complex. Many enterprises are operating under the assumption that these threats consist solely of having mobile devices lost or stolen. As you now know, the threats are much more complex than that.

In a nutshell, the threats consist of

- Malware
- Direct attack
- Data-communication interception
- Authentication spoofing and sniffing

- Physical compromise
- Mobile device enterprise infrastructure compromise
- PC and LAN connectivity

As I go into detail about and relate specific threats to each type of mobile device, I will concentrate on each threats for each device. I will then illustrate specific products and services that can address these threats

Understanding the threats is an important first step in securing mobile devices, as is changing security philosophy and strategy to adapt to the increase in mobility. If security departments, executives, and end users are unwilling to accept that change is necessary, protecting the mobile devices will prove impossible. The threat has changed, and how each of these parties operates must adjust to address this change.

Up to this point, I have discussed the threats to mobile devices and the necessary security-strategy changes to protect those devices. I will now discuss the plethora of devices available.