Securing the mobile device

Bruce Potter

Much of the information available about wireless security revolves around securing the actual wireless communications; insuring the confidentiality, integrity, and availability of the data on a wireless network. However, what often goes overlooked is the wireless device itself. These devices are wireless for a reason; they are mobile and generally designed to be used in any location a user has access to a network. Phones, laptops, and PDA's are all purchased primarily for their mobility, not their stunning good looks.

However, the extra security required by a mobile PC such as a laptop is generally an afterthought. From a policy perspective, the extra protection provided for a laptop may be as rudimentary as "do not let it get stolen." From a technology perspective, the popular operating systems provide more power management utilities for laptops than security utilities.

Security mechanisms for mobile phones and PDAs are almost non-existent. Until recently, these devices were deemed to be too computationally lightweight to provide any serious security protection. However, now that PDA's have the power of many desktop computers from just a few years ago (and many phones are simply PDA's with a GSM interface), real security protections can be put in place.

Terminal protection

The first step in protecting a mobile device is preventing an unauthorized entity from interacting with it. A mobile device is likely to spend time in relatively uncontrolled environments such as coffee houses, conference rooms, and hotels. While an attacker may not be interested in stealing the device outright, they may utilize time when the device is unattended to view or modify data stored on the device or access any resources the device has access to such as the network.

Many phones and PDA's have PIN-based locking for access to the phone functionality. Windows Mobile and PalmOS has the capability for users to enter in alphanumeric passwords to access the device. On the laptop front, the major operating systems have screen lock capabilities like their desktop counterparts. However, non-NT based versions of Windows' and Mac OS X's screen locking are not exceptionally robust; an attacker can bypass these screen locks in most situations without much effort.

Security mechanisms for mobile phones and PDAs are almost non-existent

Biometrics are an up and coming terminal protection mechanism. Fingerprint authentication is popular because fingerprint scanners can be produced inexpensively and require very little space. Unfortunately, there are ways to defeat most of these scanners.[1] While fingerprint authentication is an easy-to-use solution for the mobile device user, it does not provide the high-levels of security many people believe it does.

Data encryption

Protecting data on the mobile device is another common security mechanism. The idea is that even if an attacker has access to the device, sensitive data is encrypted to prevent unauthorized viewing and modification of data.

No major phone or PDA operating system provides persistent data encryption by default though many third party products exist that fill this void. Products such as PDA Defense[2] and Point Sec[3] provide enterprise-aware transparent encryption on supported mobile devices. However, without integration of this feature into the core operating system, many users will not encrypt data stored on their PDA or phone.

Since Windows 2000, the Microsoft operating systems have provided transparent filesystem encryption through EFS. EFS allows users to encrypt files or whole directories. Information is decrypted through the use of the user's credentials so that all cryptographic operations are transparent. If an attacker obtains access to a laptop that the user has not locked or logged out of, they also have transparent access to the encrypted data. However, when the user is not logged in, their data is safe from local attackers.

Theft protection and mitigation

Theft of a wireless device is an extreme compromise of the security of the device. Once an attacker has unfettered physical access to a device, generally any security mechanisms that the device has in place can be bypassed. An attacker can pull the hard drive out of a laptop and subvert OS-level access controls. Similarly, an attacker can pull a memory card out of a phone or PDA and copy it to a workstation.

To prevent theft, a user can anchor the device to a large, immovable object like a desk. Many laptops have special lock interfaces that can be attached to a cable on a desk. These lock interfaces are designed in a manner that destroys the laptop in the event an attacker attempts to break the lock. Unfortunately the locks can be difficult to use and require cables or harnesses anywhere a user puts the laptop. Outside of a corporate environment, these locks generally are never used. Further, locking a PDA or phone to a desktop makes them basically unusable.

Vendors have created proximity sensors to detect when a mobile device is removed from your immediate surroundings (or when you forget your mobile device). For instance, Caveo's Anti-Theft PC Card[4] uses motion and proximity detection to protect your laptop while you are away. If an "attacker" is sensed, it secures locally stored cryptographic material and sounds an audible alarm. While this is not the same level of protection afforded by bolting a laptop to a desk, an attacker who is carrying a laptop which is making a terrible noise is much less likely to go unnoticed.

Of course, the best way to not have your mobile device stolen is to never leave it in a location where it can be stolen. When not in a corporate environment, this may mean carrying the device with you wherever you go. "Never leave your baggage unattended!"

Policy

Phones and PDA's are generally the property of the user, not a corporation. As such, they are under little if any centralized control and management. Laptops are more likely to be centrally controlled. However mobile users (ie: road warriors) may be granted more permissions on their workstation in order to facilitate their mobile lifestyle.

When a user has complete control over a device, there is no technical solution that can prevent them from acting in an insecure fashion. Corporations need to have policy to guide the users to ensure data is encrypted, screen locks are used, and devices are not left in an uncontrolled environment. The policy then needs to be enforced through manual examination to ensure that users are acting appropriately.

Parting shot

The security mechanisms discussed here are not the be-all and end-all of mobile device security. Especially on the phone and PDA front, the operating systems that run the devices are still finding their footing. They do not have the robust security mechanisms that their desktop and server counterparts do such as users and roles, effective cryptographic service providers, and rogue code protection mechanisms. Even the desktop and server operating systems that run on laptops are not without fault. See the recent SoBig and MyDoom worm outbreaks as examples of the state of the desktop operating system environment.

All is not lost. It will just take time. As mobile security continues to become a higher and higher priority with the purchasing public and vendors adding more security mechanisms to these mobile devices, the bar that attackers need to jump over will be raised. Until then, we have to use the tools at our disposal to defend ourselves the best we can.

References

[1] A Case Study for User Identification – http://www.itu.int/itudoc/itu-t/workshop/security/present/s5p4.pdf
[2]PDA Defense – http://www.pdadefense.com/
[3]Point Sec – http://www.pointsec.com/
[4]Caveo – http://www.caveo.com/

About the author

Bruce Potter has a broad information security background that includes deployment of wireless networks. Trained in computer science at the University of Alaska Fairbanks, he served as a senior technologist at several hi-tech companies. Bruce is the founder and President of Capital Area Wireless Network. In 1999 he founded The Shmoo Group. Bruce co-authored 802.11 Security published through O'Reilly and Associates and has co-authored Mac OS X Security. He is currently a senior security consultant at Cigital.

Is malware wrecking your computer?

Andrew Miller, Consultant, Insight Consulting

Don't you just hate it when you get pop-ups for no reason whilst accessing Web pages and your Internet browser seems to have a mind of its own – throwing new screens open left and right. All of the links on the Web page are suddenly re-programmed to go to some pointless shopping site no matter what you do.

You try to delete the cookies files, your page history and your off-line temporary Web files, even to the extent of hitting the 're-set Internet Explorer Settings to default' button. All you end up doing is perpetually changing your home page back to the one YOU wanted at every reboot with the problem persistent as ever.

"Ah", you think, "I'll update and run my trusty AV scanner — that'll get rid of it". But your AV scanner, having spent as much time scanning your 20Gb hard disk as it takes to make coffee and drink it, merrily tells you that your computer is not infected.

Yet it is obvious from just starting up your browser that all is not well.

As you may have already suspected, all is indeed not well. It is likely that you are amongst a growing number of Internet users who are experiencing the effects of some type of malware – an increasingly common threat that operates aside from the traditional types of virus attack.

Whilst legitimate sites regularly capture and use information to track or collect browser data to create Internet behaviour profiles, more malicious sites can use the same methods to modify your homepage to one of their choice and override the