

Securing Your Mobile Devices

In March 2005, while a restricted area of U.C. Berkeley's Graduate Division was momentarily unoccupied, someone slipped out with a laptop computer containing the Social Security numbers of more than 98,000 students and applicants dating back as far as 1976. In April 2005, a laptop containing the Social Security numbers of 16,500 MCI employees was stolen from an MCI financial analyst's car in Colorado Springs. The laptop was password-protected but, according to the Associated Press, MCI would not comment on whether the data itself was encrypted.

Almost everyone has heard a story about such a theft. The laptop stolen from the podium while the conference speaker answered questions outside the room. The PDA containing the company directory falling into recruiters' hands. With the general public paying so much attention to data privacy, and even reporters distinguishing between password-protected computers and encrypted data on them, it's surprising that organizations and their employees are so complacent, unaware, or uneducated about the security of their mobile devices.

The problem with complacency

Mobile devices – laptops, removable disks, USB memory devices, PDAs, BlackBerry® and Treo™ handheld devices – all represent risk that organizations and their employees need to manage. These mobile devices may contain information that allows access to internal enterprise networks. They may contain email, attachments, and documents that reveal product plans, financial information, or strategies. They may contain personal information about employees and customers. If this information falls into the wrong hands, there is a wide range of potential consequences:

- Lost passwords and VPN settings give away the keys to a company's networks and applications.
- Proprietary information can be sold to competitors or recruiters, posted on a Web site, or held for ransom. The results can include competitors obtaining secrets, embarrassment, a tarnished reputation, or financial loss.
- Stolen personal information can lead to a variety of consequences, including identity theft, violation of federal laws protecting health care information, and requirements of some states to inform customers of losses. Personal information has been held for ransom, probably more than we know.

An easy problem to solve

Securing the data on your portable devices is an easy problem to solve. Applied Trust Engineering recommends taking two

simple steps to prevent your mobile devices from being a thief's low-hanging fruit: leash and lock them, and use whole-disk encryption.

Leash and lock them

The easiest and most effective way to keep your data safe is to keep your mobile devices from being stolen in the first place.

Virtually every laptop comes equipped with a lock slot where you can attach a leash and tether it to something solid such as your desk, luggage, or car. Buy one and use it. The Kensington® MicroSaver® accessory is pictured, but just about any leash from



Photo courtesy of Kensington.

any manufacturer is good enough. The key is that you want to be sure that the one stolen is not yours.

Whole-disk encryption

What if someone does walk off with your mobile device? If you've set up a BIOS password on your laptop, kiss your data goodbye. Just about any high-school kid can boot your system with an OS install disk and access all of your information. Are you encrypting individual files? It's next to impossible to remember to re-encrypt them after you've edited them, and to destructively delete any decrypted versions that might be lying around in hidden, temporary, and cache files. Save individual file encryption for occasions when you send sensitive files in email. With whole-disk encryption, it will take a lot more than a fishing expedition to crack open your data.

Whole-disk encryption secures all of the data on your disk, not just your home directory or the files you remember to encrypt. This is key because applications may store temporary or cache files in locations that are not automatically encrypted and destructively deleted, leaving your data at risk. Whole-disk encryption decrypts every disk block when the operating system reads it, and encrypts every block before the OS writes it to disk. With encryption handled at the lowest level, even hidden, temporary, and cache files are secured.

Whole-disk encryption software also can handle your removable media including disks and USB storage devices. Other products can help you protect email and other data on handheld devices.

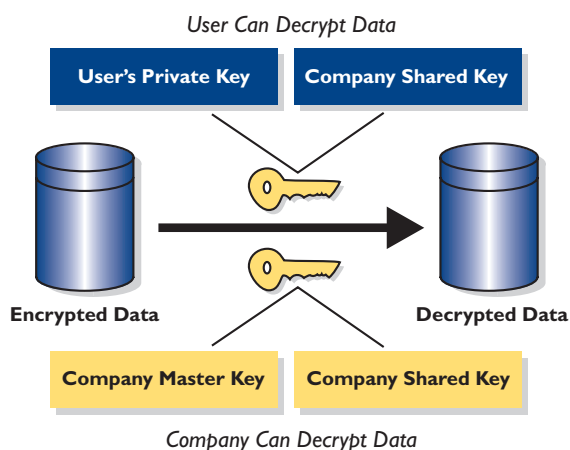
The value of enterprise solutions

By now you're ready to shop for a whole-disk encryption solution. Before you do, consider your requirements. If you're implementing whole-disk encryption in an enterprise context, think about how you will back up a device that's encrypted, and how you will access company data in the event that an employee leaves the company and takes her passphrase with her.

Enterprise-grade, whole-disk encryption packages make it easy to apply encryption policies uniformly across a large number of mobile devices, and they ensure that the company can obtain access to encrypted data even if the employee isn't around. Enterprise solutions for mobile devices can revoke access rights on laptops and some handheld devices if they are lost or stolen or if the employee leaves the company.

Enterprise solutions typically employ strong public-key encryption to protect a weaker (but more efficient) secret key used to encrypt data on the disk. Now that it's possible to securely protect every user's secret key, it's possible to store them on a server where they can be unlocked if there's no other way to access the mobile data. This is called key escrow, and it's like giving a trusted friend a key to your car just in case you lose yours. Like key escrow, a Public-Key Infrastructure (PKI) also supports key revocation. What happens if an employee is fired and his laptop is at home? You can deny access to that person's data through the PKI mechanism, preventing unauthorized access to what's really the company's data.

Along with a central server to support the PKI, enterprise solutions include management capabilities such as authorizing data decryption for backups and enforcing specific security policies, for example specific filesystem encryption settings or handheld email access procedures.



Both the employee and the company can decrypt data using PKI. The company can revoke access by denying access to its shared key.

First steps to take

Remember that security is an amalgam of people, policy, and technology. Without all three working together you won't be successful in securing your mobile devices.

Policy

Determine the right policy for your organization. Make sure that you include physical security through laptop leashes, data security through whole-disk encryption, and additional protection for handheld devices. Recognize that handheld devices present just as much risk as laptops. Make it clear where employees can take their laptops and where they can't. (Leaving one in a car is usually a bad idea.) Consider whether employee or customer data should ever be taken off-premises on a laptop. Spell out how employees must comply with the policy, and what happens if they don't.

Technology

Give your employees the tools they need to implement the policy. Buy them laptop leashes and make sure they have adequate anchor points on their desks and in conference rooms. Consider the products mentioned on page 4 and set up an enterprise-quality, whole-disk encryption system. Make sure that every device's encryption settings are in compliance with the policy. Be sure that you back up all data before installing whole-disk encryption, and set up procedures for performing backups once the encryption software is installed. Are handheld devices, PDAs, or flash memory devices part of your fleet? Incorporate them into your strategy as well.

People

Now that you have a policy and the technology to support it, get your employees signed up. Make sure they know their devices contain information that, in the wrong hands, could damage them, their peers, the company, or their customers. Teach them how to comply with the policy, and give them incentives. Enterprise-quality tools can help enforce uniform settings and standards, but what about laptop leashing? Make it fun. Award a bounty when one employee can swipe another's laptop, encouraging them to leash their devices everywhere, including conference rooms. Give them a bonus for surviving walk-through audits. Once you've established good habits at work, encourage them to continue them at home and while traveling. ■

SECURITY PRODUCTS TO CONSIDER

CompuSec® Software

Whole-disk, enterprise-grade encryption for laptops, flash memory, and removable media.

<http://www.ce-infosys.com.sg/>

FreeOTFE

Disk-partition or volume-in-a-file encryption, USB device, removable media.

<http://www.freeotfe.org/>

SafeGuard® Easy

Whole-disk, enterprise-grade encryption for laptops, flash memory, and removable media.

http://www.utimaco.com/content_products/sg_easy.html

ThinkVantage™ Technology

Hardware encryption embedded into IBM laptops.

<http://www.pc.ibm.com/us/think/thinkvantagetech/security.html>

TrueCrypt

Disk-partition or volume-in-a-file encryption, USB device, removable media.

<http://www.truecrypt.org/>

Secure push e-mail from Microsoft Exchange Server

Microsoft Exchange Server 2003 SP2 will support push e-mail and remote security management of mobile devices.

<http://www.microsoft.com/exchange/downloads/2003/sp2/overview.mspx>

GoodLink™ Wireless Messaging

Push e-mail and application access for wide range of devices, can revoke access remotely.

<http://www.good.com/>

This article was reprinted from the Q3 2005 issue of The Barking Seal, a publication of Applied Trust. You can subscribe to The Barking Seal online at <http://www.appliedtrust.com/barkingseal>. “Applied Trust” and the “Seal on a Rock” Applied Trust Engineering logo are registered service marks of Applied Trust. All other trademarks are registered to their respective owners.