Constant vigilance:
physical security for notebook computers

THE THREAT TO YOUR PROPERTY AND DATA FROM PROFESSIONAL THIEVES HAS NEVER BEEN GREATER. SECURITY EXPERT MARC TOBIAS DETAILS THE QUESTIONS YOU SHOULD BE ASKING YOUR SECURITY PROVIDER.

The theft of notebook computers has dramatically increased over the past few years as the migration from desktops has become more pronounced. Today, virtually all hardware and software functions can be incorporated within a laptop, thus reducing or eliminating the requirement for fixed stations. The need to work in various environments has also contributed to their proliferation.

This article examines the problems involved in securing portable computers against high-level, expert theft, as opposed to opportunistic amateur pilfering (which is still, of course, theft). In these instances security measures are often bypassed by covert entry techniques, rather than forced entry methods such as cutting cables and prying the locks loose from the computer. We will also look at some of the practices that are employed to protect laptops.

By Marc Weber Tobias

YOUR LIFE IN A LAPTOP

The mobile traveller today may carry a portable computer containing everything from contacts, tasks, calendar, and spread sheets to highly secret corporate data, legal briefs, information relating to mergers and acquisitions, medical records, and every imaginable database.

Virtually all information on your laptop is confidential, therefore the ramifications are huge if the computer is lost or stolen. Not only can the compromise of information constitute an incredible inconvenience, it can create logistical and legal problems, to say nothing of potentially compromising your security and that of your company, family, friends, and everyone who is referenced in any file on your computer.

If you are a government employee, doctor, lawyer, banker, or other professional that works in a regulated industry where

there are privacy policies or statutes, you may also be at risk of civil or criminal prosecution if information has not been adequately protected. Another huge problem is identity theft. If a thief can access the information in your e-mail, contacts, and financial programs, then he may be able to cause serious economic damage.

JEOPARDISING LIVES

Everyone in your contact list could be in jeopardy, especially if there is confidential information with regard to where they live and work. The physical security of your associates could be at risk, to say nothing of the potentially disastrous results from the dissemination of privileged or secret information about you, your company, or others who you are dealing with. In addition, the potential for sending counterfeit messages and other data is of real concern.

SECURING A MOVING TARGET

Laptop theft is often a crime of opportunity. However, more and more, computers are also being targeted and stolen for the information they contain, not just for their hardware. Corporate and government espionage and intelligence gathering is clearly on the increase. The problem in securing a laptop is difficult, because they are a moving target and easy to secrete and transport, even from a secure area.

When securing a notebook computer or its contents software programs, hardware and physical security technologies should all be employed simultaneously.

SOFTWARE AND HARDWARE

There are many software-based programs that are designed to protect the compromise of information that is contained within a laptop. These include 'phone home' systems that will report the IP address every time the internet is accessed. These programs have been quite effective in retrieving stolen laptops. Password and encryption software can also secure the computer and its hard drives. Embedded chipsets, such as those utilised by IBM, can offer several levels of security for the laptop and its data. These devices and systems will not physically prevent the laptop from being stolen, but they may minimise the risk of compromise if theft occurs.

"How much time would a thief likely have to remove the computer?"

PHYSICAL DEVICES

There are two primary types of physical protection, locks and cables that secure the notebook to a work surface, and some form of cage or enclosure that anchors the computer to a specific location. Each approach has advantages and drawbacks.

Whatever the security device that is employed, it always has one critical and inherent weakness: the method by which the laptop is physically secured to its surroundings. If the design is too cumbersome, it simply will not be used. If it relies upon a method of affixing a cable to the computer, then we must rely upon the materials of which the computer and cable is constructed, and this too may be a problem.

All modern laptops and peripherals contain a security slot, measuring a few square millimeters. Unfortunately, this slot size does not provide much of a surface for an anchor or mode of attachment. Some computer slots are made of plastic, which makes the problem more complicated. To further complicate the matter, the cables that are employed with locking systems are generally quite thin and can easily be cut with small handheld tools.

FORCED REMOVAL

Manufacturers have tried many schemes for enhancing security, including screw-in anchors, expanding scissor-type interfaces, rotating T-bars, and other methods for affixing some form of secure cable to the computer security slot. In the final analysis, all rely on an extremely small contact surface, which must withstand pulling, wedging, and shearing stresses that can be caused by forced removal.

Most users employ cable locks. All of these devices consist of a key or combination lock that is affixed to a steel cable, which is anchored to a fixed surface. When attached, the lock interfaces with the security slot, making removal difficult. Or, so everyone thought, until we conducted an investigation into their efficacy.

Computer locks that utilise keys can be set for individual codes, keyed alike, or master keyed. Key locks mostly utilise what is referred to as axial pin tumbler mechanisms. That is, the key appears round, and generally has from four to seven pin tumblers spaced around their circumference. Various keyway sizes in part determine the difficulty in picking the lock (see the security issues checklist). Some are easy, and some more difficult. The question you will be asking yourself is: how easy?

TERRIFYING EASE

In one extremely popular lock that was tested, we were able to open the mechanism with the end of a ballpoint pen, or the cardboard material from a roll of toilet paper. The procedure to open these locks took less than 30 seconds, and often they could be bypassed in under 10 seconds with terrifying ease.

In the case of combination locks, there are many different models, but most work in basically the same way. Generally, three or four different thumb-wheels are employed, with a maximum of 10,000 different combinations for a four wheel lock. In the case of combination locks, we found that most were extremely easy to decode, either by visually inspecting or feeling each wheel.

For one major manufacturer, we utilised a piece of paper and were able to

decode the four-digit combination within seconds with virtually no skill required. In another instance, the lock could be opened in less than 30 seconds with no tools at all; just look at the lock and feel it. In the end, such products are simply a deterrent to a thief with no expert knowledge.

So, what about the systems that employed some form of enclosure or cage that surrounded the computer? The advantage to these devices is their structural integrity in comparison to the cable locks that provided an extremely small contact surface to link the laptop to a cable. However, even though the enclosures appeared strong, they too can be easily defeated within seconds by a determined professional. In addition they are more cumbersome and less likely to be used by the consumer.

It is clear from our inquiry that extremely common implements can be used to defeat locking mechanisms quickly and without any real skill. If the only thing standing between the thief and your notebook computer is a ballpoint pen that costs less than one dollar, then other security measures must be implemented. Companies and individuals must invest in a comprehensive programme that includes software, hardware and physical security measures.

Some security devices are quite expensive. Can the consumer expect any real measure of security for the price they pay? I think they can, but they have to understand the issues, evaluate the environment, and run relevant tests in an attempt to defeat their mechanisms and therefore understand their own security weaknesses. ■

Marc Weber Tobias is an investigative attorney and security expert in Sioux Falls, South Dakota. He has written five police textbooks, including the treatise entitled Locks, Safes, and Security, published in 2001, with a 14 volume multimedia edition published in 2004. He works as a security consultant for both private and government clients throughout the world, mainly dealing with the bypass of high security locks, safes, and alarm systems. Marc is a member of ASIS, IAI, and is a technical advisor to the Association of Firearms and Tool Marks Examiners. His website can be found at **www.security.org** and his e-mail address is **mwtobias@security.org**. He welcomes feedback from readers.

SECURITY ISSUES CHECKLIST

The following issues should be considered when evaluating the threat level and requisite hardware for protecting laptops.

ENVIRONMENT

Is the laptop left unattended for long periods of time?
Is there any surveillance of the area where the laptop is stored?
Are there any physical controls with regard to removing the laptop from the facility?
Does the laptop contain any RFID tag, transponder, or proximity device that would alarm if it left the area or building?
Is there 'phone-home' software in the event the laptop is stolen?
Are critical files encrypted?
Are passwords required to access hard drives?
How much time would a thief likely have to remove the computer?
What is the computer or peripheral to be physically attached to in order to secure it?
Would a thief have unrestricted access to the computer, and if so, for how long a time?
Are locking devices routinely utilised in your facility?
How valuable is the information that is stored within the computer?
Is the security slot made of plastic or metal? If it is plastic, is it reinforced?

SPECIFIC SECURITY DEVICES

Are key locks or combination locks employed presently? If key locks, are they master keyed, and if so, what is the security of the master key system?
If a key lock is employed, how many pin tumblers are present?
Has the lock been tested by an expert with regard to covert methods of entry?
If the key lock is an axial pin tumbler device, does it use a standard diameter keyway, such as .25" that can easily be replicated with plastic tubing or a ballpoint pen?
How difficult are the keys to duplicate or obtain from the manufacturer?
If the mechanism is a combination lock, how many wheels are utilised? There should be a minimum of four, with 10,000 possible combinations.
Can tension be applied to the lock in order to allow decoding of each wheel?
Does the lock allow any of the wheels to be 'read' in order to derive the combination?
How does the cable attach to the lock? Can leveraged force be applied to the lock to easily force its removal?