Laptop Computer Security

White Paper

NOVEMBER 2001

Overview

In this paper, we describe the laptop security problem and current security technologies. There is a clear unmet need in the marketplace for a complete laptop security system that deters theft and protects both hardware and confidential information, while remaining convenient to the end user. Our product, Caveo Anti-Theft™, provides a critical missing link – threat detection and response – needed for enhanced security and user convenience.

Table of Contents

1.0 Introduction

Despite the slump in the overall PC market, growth in laptop computers continues. According to Gartner, worldwide laptop sales grew 21% in 2000, compared with only 2% overall growth in PCs (1). Early indications are that worldwide growth during the next few years will remain at least in the high single digits for laptops, despite the declining overall PC market.

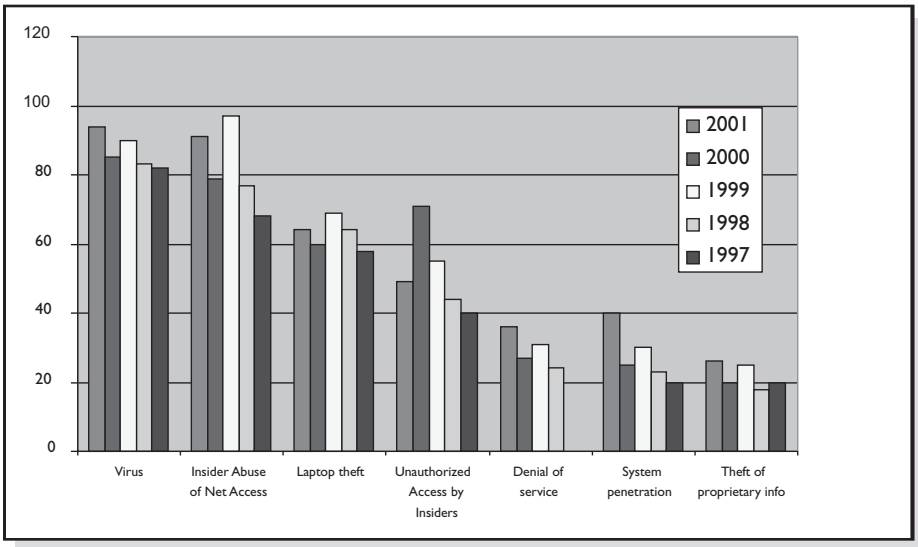
The laptop is increasingly the computer of choice for both business and consumer buyers. As laptops proliferate, laptop theft has become an ever more critical security issue. Safeware Inc., the largest U.S. insurer of laptops, projected that 387,000 laptop computers were stolen in the U.S. in 2000, up 21% from 1999 (2).

Laptop buyers in search of a security solution are faced with a wide array of products, systems, and services, each of which addresses a part of the problem. There remains considerable confusion about the extent of protection provided by each product, and the overall level of security that is achieved when a combination of approaches is used. As theft rates increase, it is increasingly evident that an ad hoc approach to laptop security is not adequate. An integrated solution is needed.

2.0 The Laptop Security Problem

The Computer Security Institute (CSI), in collaboration with the FBI's Computer Intrusion Squad in San Francisco, conducts an annual survey on computer crime and security in U.S. corporations and government agencies. For five consecutive years, CSI has reported the types of security attack and misuses experienced by its respondents. Laptop theft has been consistently reported by about 60%, as shown below.

MOST COMMON SECURITY BREACHES IN ORGANIZATIONS



Source: Computer Security Institute (Ref. 3).

A rash of recent news items has brought the laptop security issue to widespread public attention:

- In February 2000 a laptop computer with "highly classified" information disappeared from the U.S. State Department (4). The laptop was not password protected and the data on it were not encrypted. It was reported to contain several thousand pages of highly classified documents.
- Then in May 2000 two more laptops were reported missing from the U.S. State Department (5).
- In three separate incidents between March and May 2000, British intelligence and military agents lost laptops that were reported to contain state secrets. In the first, an intelligence officer for MI6 mislaid a laptop, which was recovered by police two weeks later. In the second, a laptop containing classified material on Northern Ireland was stolen from an MI5 security officer. In the third, a naval officer's laptop, containing details on a fighter plane being jointly developed by Britain and the United States, was stolen and later recovered by a British tabloid (6, 7).
- In September 2000 three laptop computers and a handheld device were stolen from a Democratic National Committee office (8).
- Also in September 2000, the laptop of Qualcomm's CEO, Irwin Jacobs, was stolen from a conference room in which he had just given a presentation. Jacobs told participants that the computer contained proprietary information that could be valuable to foreign governments (9).
- In April 2001 the British Defense Ministry reported 205 laptops missing since 1997, most of which contained classified material (10).
- In July 2001 the Federal Bureau of Investigation reported that 184 laptops had been stolen or lost. At least one and possibly as many as four contained classified information (11).

For the respondents to the CSI survey (3), average losses from laptop theft ranged from $32,000 to $87,000 during the past five years. The highest reported losses ranged from $500,000 to $2,000,000.

The asset loss associated with laptop theft is substantial. However, losing the computer and its installed software is often the least important worry among corporate and government users of laptops. Of far higher concern are:

- The risk that confidential and/or sensitive information will be lost or stolen. According to the Gartner Group, informal surveys indicate that 10-15% of laptop thefts are committed to obtain confidential data (12).
- The substantial business interruption losses and administrative costs involved in obtaining and setting up new systems, greatly compounded when employees have not recently backed up the information on the hard drive.
- The risk that a stolen laptop will be used to gain unauthorized access to private networks.
- The concerns about liability if confidential information from a third party such as a vendor or customer is lost. This is a particular issue in the health care industry, which must comply by April 2003 with new rules protecting patient information pursuant to the Health Insurance Portability and Accountability Act (HIPAA). The Act's Privacy Rule requires all healthcare organizations to implement security standards to protect the confidentiality and integrity of individuals' health information. Exercising reasonable due diligence in protecting laptops from theft can be assumed to be a necessary part of an acceptable set of security standards.

In recent focus groups, we found these risks to be foremost in the minds of IT managers in companies and institutions that are significant buyers of laptops:

> *"Once a laptop is out of IT's hands and out of our site, anything can happen to it and we have no control over it. I can't [be there to] tell that person that the laptop has critical information on it and they shouldn't leave it anywhere."*
>
> *"The interface between physical security and data security is the laptop. If that disappears, you lose the data on it, too, and if it is proprietary data then you are up two creeks."*
>
> *"We have had issues of laptops that were stolen. There is very confidential data because we have case managers who go out and visit patients."*

3.0 Approaches to Laptop Security

Within the much broader arena of IT security, there are five classes of technology that are relevant to laptops because they protect against the risks described above. These are summarized in the table below, and are described in more detail in this section.

Laptop Security Technologies

	TECHNOLOGY	PURPOSE
3.1	User authentication	Confirm the authorized user; prevent unauthorized access
3.2	Physical locking devices	Deter theft
3.3	Encryption	Protect data
3.4	Monitoring and tracing software	Locate and assist in recovery of stolen computers
3.5	Alarms	Deter theft

3.1 User authentication systems

User authentication (verifying the identity and authorization of the user) is a required component of all security systems. In a PC, different levels of authentication may be used: (1) pre-boot, done prior to boot-up (typically done with BIOS and/or hard drive passwords); (2) OS-level, done prior to operating system startup, and (3) user-level, done before granting access to networks or specific files, folders or applications.

It has often been written that authentication can be done three ways (e.g., Ref. 13):

- By something the user knows (e.g., a password),
- By something the user has (e.g., a token or card), and/or
- By a personal feature of the user (e.g., fingerprint, voice, eye scan)

Each approach has advantages, but each also has intrinsic limitations:

- "Something you know" can be forgotten, guessed by others, or inappropriately shared,
- "Something you have" can be misplaced or stolen, and
- "Something you are" can be difficult to distinguish reliably.

Combining two or more methods enhances the confidence level. This is common in situations where high levels of security are required; for example, a bank ATM machine requires both a card and a password.

The most common approaches to user authentication - password systems, smart cards and tokens, and biometrics -- are briefly profiled below.

PASSWORD SYSTEMS

"Something you know" is usually manifested as a password or by providing correct answers to previously established questions. Password or personal identification number (PIN) systems require the user to type in a sequence of characters. They are the most common of the user authentication methods, and the least expensive in initial cost.

Password systems are vulnerable to various forms of attack. Brute force and dictionary attacks are carried out by readily available "crack" programs that simply try all possible passwords, starting with the most likely choices, such as words in the dictionary. Other methods of password attack include keystroke monitoring, "social engineering" methods (snooping or trying to trick people into disclosing passwords), and network "sniffing" (14).

To reduce the risk of password attack from brute force or dictionary attacks, many companies require employees to use relatively strong passwords containing 8 or more digits, combining random upper and lower case letters, numeric and punctuation characters. Policies requiring frequent password changes are also used, as are policies that employ different passwords for access to the computer or operating system, the network, and specific files and applications.

These added complexities are inconvenient and burdensome to users, and they substantially increase the administrative burden. By some estimates, as much as 30 percent of internal help desk calls are related to forgotten passwords (15).

Burdensome password policies are also self-defeating: users faced with trying to remember a number of complex passwords give up, and write them on sticky notes posted near or on their computers, or program their computers to remember their passwords, thereby eliminating any protection.

SMART CARDS AND TOKENS

"Something you have" can be manifested in a number of form factors - most common are smart cards and tokens. These provide the advantage of storing robust authentication information that the user does not have to remember - he or she just has to possess the smart card or token.

A smart card is a plastic card with an internal memory chip or microprocessor. Memory smart cards are used to store confidential data such as personal information and encryption keys. Microprocessor smart cards are used in applications that require manipulation of data, such as data encryption.

Smart cards have gained widespread use, especially in Europe, for telephone calling, electronic cash payments, and similar applications. Gartner reported that worldwide smart card shipments grew 45% in 2000, to 628 million units. Two vendors, Gemplus and Schlumberger, dominated, with 66.7% of world market (16).

In computer security applications, smart cards are most often used for authentication at the user level, and particularly for network access. Most systems require two-factor authentication - i.e., both a typed-in PIN as well as possession of the card -- thus providing very robust security. Windows® 2000 offers authentication with smart cards as an alternative to passwords (17).

Smart card systems are somewhat inconvenient for the users. In addition to requiring that the user have the card in his or her possession, most systems today require separate smart card readers. Gemplus and Schlumberger offer smart card readers as external serial port or PCMCIA devices at prices ranging from about $50 to $100. Pricing of the smart cards themselves starts at about $12 per card, when purchased in bulk (18, 19).

Acer began offering notebook PCs with smart card slots in the first quarter of 2001 (20).

The IT managers in our focus groups cited the robust security provided by smart cards as an important advantage, especially for network access. However, they noted that users are prone to lose them, creating a cost and administrative burden associated with replacing lost cards. Compliance with good security practices was also cited as a problem: as one participant noted, users often carry the smart card in the same bag with the laptop to avoid losing or forgetting it.

Smart tokens differ from smart cards in form factor and interface but operate on the same premise - they can store robust authentication information, and their presence is required for access. An example is Rainbow Technologies' iKey™, a token that plugs into the USB port on the computer. Rainbow's tokens operate on two-factor authentication, i.e., the user is also required to enter a password (21).

Other tokens such as RSA Security's SecurID® products display a unique code that the user must then enter as a PIN to gain access (22).

Ensure Technologies' offers XyLoc™, a system consisting of a token ("key") that communicates via RF with a serial-port or USB-based peripheral ("lock") on the computer. The lock and key communicate up to 50 feet. When the authorized user approaches the computer, the key transmits verification information, and the lock enables access to the computer's keyboard and screen (23).

BIOMETRICS

Biometric technologies rely on a personal feature of the user ("something you are"). Approaches include fingerprint recognition, hand geometry, face recognition, eye scans, and voice verification. The most commonly used in PC applications is fingerprint.

Fingerprint technology today is able to achieve very low false acceptance rates (FAR) of 1 in 10,000 or better (13). A much greater issue with most current fingerprint products is the false rejection rate (FRR), i.e., the probability of rejecting the authorized user. Statistics vary, and depend on whether the user is trained on proper fingerprint placement on the reading device, and how many fingers are used in the attempt. In practice, there are still significant levels of false rejections; therefore, most systems provide users with smart cards or other tokens for access

in the event of rejection. Further, about 2.5% of people do not have fingerprints of sufficient quality to allow for authentication (13). For these users, an alternative authentication technique (e.g., a password) is necessary.

Acer and Compaq both offer laptop PCs with integrated fingerprint scanners - Acer with Veridicom technology and Compaq with Identix. According to a review in PC World (24), both were finicky about finger placement and required practice and patience to reduce false negatives.

Fingerprint technology remains expensive to purchase and implement. Individual fingerprint scanners range from a low of about $100 for peripheral devices to $150-250 for PC Card readers. Server software for 25 users is $1500 plus $50 per additional user (25, 26). Installation and integration into enterprise systems, and training end users, are substantial additional costs.

Template storage is one of the complex aspects of biometric systems. Most solutions rely on one or more centralized databases. Since biometric templates require large storage capacity, these can become quite substantial for systems with many users. They must be absolutely secure and resistant to remote attack, of course, because an attacker who recovers the data can use it to create false credentials. Systems that store templates locally on hard drives or on smart cards avoid the problems of large central databases but have the disadvantage of creating local vulnerabilities that are susceptible to loss or theft (27).

3.2 Physical locking devices

According to a survey conducted by Kensington (28), two of every five laptop thefts occur from within. Because of this, many companies adopt increased building security (guards, gates, badges, video surveillance systems) as a means of reducing laptop theft.

Also in fairly widespread use are physical locking devices, e.g.,

- Cable locks (e.g., Kensington's) - used by 20% of organizations, according to the above-cited survey
- Docking stations and lockdown enclosures - used by 14%

Devices such as cable locks are generally inexpensive (<$50), and they are good deterrents. The main disadvantage of physical locking devices is that they are cumbersome, and especially inconvenient to the mobile laptop user.

3.3 Encryption

User authentication systems prevent unauthorized access to the laptop's operating system. However, if the hard drive is removed to another machine, or if boot-up from a floppy disc is enabled in the stolen machine, the files can be accessed. Unless a hard drive lock option is available and implemented, the only way to protect files from this type of attack is to encrypt them.

Encryption systems require the use of a digital key to encrypt and decrypt the data. In "symmetric" systems, the same key is used for both encryption and decryption. In PKI (public key infrastructure)-based applications, asymmetric encryption is used, with two keys: a public key for encryption and a private key for decryption.

In many current encryption products, the key is stored in a "secure" location on the hard drive. Keys stored inside a computer can be vulnerable to attack. Encryption experts such as RSA Security recommend protecting keys by storing them in tamper-resistant hardware devices that can handle cryptographic functions internally and do not permit the keys to be exported outside the hardware (29).

3.4 Monitoring and tracing software

Monitoring and tracing software keeps track of the location of the laptop and, if it is stolen, assists in its recovery. These products work by making a call into a monitoring service regularly when the laptop is logged onto the internet. If the laptop has been reported stolen, the service activates a caller-ID system, identifies the IP address of the computer, and notifies authorities.

Products that fall into this category are Compu-Trace™ (Absolute Software), Cyber Angel™ (CSS), MobileSecure™ (Lucira Technologies), zTrace™, and Solagent™(30-34). In most cases, the cost of the software plus a one-year monitoring service is about $50. These prices have declined considerably, and continue to drop, as competition increases in this segment.

The benefit of monitoring and tracing software is that it offers the possibility of recovering a stolen computer. Another important benefit to enterprise customers is that the monitoring service can be used for routine asset tracking.

The major disadvantage of trace and recovery products is that they require the stolen computer to be logged onto the internet before the recovery operation can be enabled. A stolen computer that is not logged onto the internet will not get recovered. Another disadvantage is that tracking down the physical location of a computer from an IP address can be quite difficult and time-consuming.

Although the software is difficult to remove from the computer (simply reformatting the hard drive won't do it), it can be done by a sophisticated thief.

Some products offer features for retrieving, encrypting and/or erasing files on the stolen laptop once it is logged onto the internet. Of course, such files would be accessible to the thief up to that point.

3.5 Alarms

Alarm systems, such as the Defcon™ unit marketed by Targus (35), detect motion and sound an alarm. One version, which costs about $50, attaches to the computer via the security slot, and also comes with an integrated cable for physical locking. Another version, priced at about $130, is integrated into a carrying case. Arming and disarming is done by entering a combination or with a remote controller. The systems offer two levels of motion sensitivity before the alarm is tripped.

TrackIT™ markets a two-piece alarm system with a keychain token that communicates with a receiver that is carried in the bag with the laptop. If the signal is lost between the two units, the alarm sounds. The product costs about $60 (36).

Alarms serve as deterrents; however, these devices are somewhat cumbersome because they are external peripherals. They are not integrated with the computer system and, therefore,

cannot provide user authentication or data protection. Products based on RF communication have the added disadvantage that signal strength varies considerably. The signal can be lost in certain environments - e.g., in buildings with metal infrastructures - or because of a change in orientation between the token and the receiver's antenna, or simply when the user's body comes between the token and the receiver. This results in many false alarms.

4.0. The Unmet Need

In two focus groups conducted in the Boston area in the summer of 2000, and in dozens of conversations since, we've asked IT and security directors to define the features of an "ideal" security system. Here is what they say:

1. The ideal system addresses multiple security risks, not just one - i.e., it prevents unauthorized access, protects confidential information, and protects hardware.
2. The ideal system is easy to install, use and administer. For the user, the best of all worlds would be a completely transparent system. For the IT administrator, user transparency translates to fewer calls to help desks, thus decreasing administrative burden.
3. The ideal system is configurable, with options that enable users and their organizations to configure the system to their particular needs.
4. The ideal system deters theft, but if deterrence fails, detects theft and responds accordingly. We have found unanimity in the notion that deterrence is necessary. If deterrence fails, detection and response become vitally important. However, systems that focus on detection and response without deterrence ignore the substantial costs and aggravation associated with simply dealing with a laptop theft.
5. Last but not least, the ideal system would be inexpensive.

5.0. An Analogy and a Model: Automobile Security

It has been written that one's laptop is the second most likely personal possession to be stolen, after the automobile. Actually, auto theft rates have declined dramatically in recent years, while laptop thefts have soared - so unless you own one of the two or three cars most vulnerable to theft, your laptop is now far more likely to be stolen than your car (37).

Nevertheless, auto theft has been a problem for a much longer period, and the sheer number of automobiles -- and therefore auto thefts -- is still far greater. It is useful, therefore, to consider the evolution of automobile security systems and the parallels with laptops.

In auto security, the earliest approaches focused on deterrence alone. Using a lock and key (in essence, a token-based "user authentication" method) -- has been long established as a necessary, but not sufficient means of preventing theft. It deters the casual or opportunistic thief, but barely slows down the professional thief.

Physical locking devices gained some use as auxiliary deterrents by a small fraction of automobile owners. They have advantages in some situations, but are too unwieldy and inconvenient to gain widespread use.

Alarms also gained some use for their value as deterrents, but accidental alarms are a nuisance. When they occur frequently, they are ignored.

The relatively low acceptance of physical locking and alarm-only devices illustrates the importance of minimizing user inconvenience and aggravation. If the deterrent is a hassle, it will not be used.

Next, auto security systems evolved to include the a particular kind of response - initiating steps to recover the stolen vehicle. The LoJack™ system, introduced in Massachusetts in 1986, is an example of this approach. LoJack relies on a hidden transmitter that is activated when a vehicle is reported stolen, enabling police to locate the vehicle.

This approach is effective in areas where prompt response from law enforcement agencies is available. Establishing regional police support has proven time-consuming, though. LoJack has gradually expanded its service area over its 15-year history, but is still only available in 21 states (38).

The most recent - and most effective - development in auto security is the passive immobilizing anti-theft system. Usually factory-installed by the manufacturer, these systems are based on the use of motion detection technology to detect threats. When a threat is detected, the system invokes an alarm, but more importantly, it also invokes an immobilizing device that keeps the vehicle from being driven.

Thefts of vehicles containing immobilizing systems have declined dramatically. The Nissan Maxima provides an example: 1998 models, without factory-installed antitheft devices, had overall theft losses more than seven times the average for all cars. After standard immobilizing antitheft devices were introduced in 1999, theft losses for the Maxima declined by more than 60% (39).

Cars containing passive immobilizing anti-theft systems use simple stickers and warning lights to communicate the presence of the system to the potential thief. [1]

Overall insurance losses for vehicle theft have been reduced an average of about 50 percent for vehicles with passive immobilizing antitheft devices. As a result, insurers offer significant discounts to owners of vehicles with these systems.

6.0. Caveo Anti-Theft™

Caveo Anti-Theft™ is a laptop security system that is based on the same principles as today's most sophisticated auto security systems: (1) use of motion detection technology to detect threats, (2) implementation of strong responses (including "immobilization") when theft is detected, and (3) incorporation of known deterrents - stickers, warning signals, and an optional alarm.

Threat detection is key to an ideal security solution because it enables the system to implement strong responses. In the case of the car, the vehicle is rendered immobile. In

[1] LoJack, on the other hand, has not traditionally provided stickers or warning signals, and has long maintained that its system is not intended to be a deterrent - that there is major benefit in not disclosing its presence to the thief, in order to make rapid recovery more likely and minimize damage to the vehicle. Recently, though, LoJack has begun offering "full-featured" systems including intrusion detection, warning signals, and immobilization (see www.lojack.com).

the case of the laptop, Caveo Anti-Theft blocks access to the operating system and protects confidential information.

Threat detection is also key because it enables the system to remain convenient and virtually invisible when a threat does not exist, i.e., in normal everyday use.

Caveo Anti-Theft is available in the convenient PC Card (Type II PCMCIA) form factor. Suggested retail price is $99. There are no external peripherals. The PC Card is a stand-alone system containing a motion sensor, processor, secure storage, sounder, and a rechargeable battery. The system operates independently of the PC and works whether the laptop is on or off.

In normal everyday use, the Caveo Anti-Theft system is either armed or disarmed. Arming and disarming can be done easily via the taskbar, or with Caveo's proprietary Motion Password™, which provides a quick and simple way to arm and disarm when the computer is off.

The system can also be set to automatically arm upon specific events if the user so desires: when the operating system starts up, when the screen saver comes on, and/or when the system enters suspend/hibernate mode.

Caveo Anti-Theft labels are provided and can be affixed to the laptop to alert the potential thief that the laptop is protected.

In initial setup, the user sets the "theft perimeter," which defines the range of motion that the Caveo Anti-Theft system will interpret as non-threatening. An armed computer issues an alert sound if it is moved, transitioning to more insistent warning signals if movement continues. These sounds serve as further deterrents to theft, and also serve to remind the user to disarm the system if he or she wishes to carry it beyond the specified perimeter.

If an armed system is carried beyond the perimeter, Caveo Anti-Theft assumes theft and invokes strong responses, including: (1) preventing access to the operating system, (2) securing passwords and encryption keys in its secure storage, and (3) sounding an audible alarm (optional). Caveo Anti-Theft is also designed for easy add-on of a BIOS boot block and hard drive lock, which require cooperation from PC manufacturers.

If a stolen computer is recovered, a robust 16-digit master code (emergency PIN) is required to regain access to the operating system and the information in secure storage. Administration of the master code can be controlled within the IT department or by the end user.

In addition to the auto-arming options, the user-selected perimeter, and optional alarm settings (high, low, off), Caveo Anti-Theft offers other convenient user options such as a browse feature that enables the user to select her own sounds for the alert and warning signals, arm and disarm confirmation, etc.

Like a smart card or hardware token, Caveo Anti-Theft™ enhances the security of file encryption by providing secure storage off the hard drive and by securely managing operations involving encryption keys, user information and passwords. The beta version of Caveo Anti-Theft includes two integral encryption options: E4M™ (a convenient on-the-fly encryption product developed by Paul Le Roux of Software Professionals) and RSA Security's Keon® Standalone Desktop system, a powerful security system that includes not only encryption but also a number of other security features enabled by a sophisticated public key infrastructure (PKI). (Encryption options in the commercial product will be determined after beta testing.)

The PC Card contains a rechargeable battery that powers Caveo Anti-Theft for more than three weeks when the computer is off. The battery automatically recharges when the computer is on.

Caveo Anti-Theft incorporates the critical elements of deterrence, detection, and response. It offers a robust, complete, and very convenient security system for the laptop user.

References

1. Gartner Group, cited in Iwata, Edward, "PC makers may face grim future," USA Today, June 15, 2001.
2. Safeware, Inc., "Accidental damage poses biggest risk for PC owners, insurance survey shows," press release, www.safeware.com, February 26, 2001.
3. "2001 CSI/FBI Computer Crime and Security Survey, Computer Security Institute, www.gocsi.com, Spring 2001.
4. "Highly classified State Department computer missing," CNN, Associated Press, and Reuters, April 17, 2000.
5. "Two more laptops missing from U.S. State Department," CNN and Reuters, May 5, 2000.
6. "British officer's laptop recovered by tabloid," APB newswire, May 22, 2000.
7. Sharkey, J., "Business Travel" column, New York Times, March 29, 2000.
8. "Stolen DNC laptops located, three men arrested," APB newswire, October 6, 2000.
9. "Qualcomm secrets gone along with CEO's laptop," Associated Press, September 18, 2000.
10. Delio, Michelle, "The spy who lost me," Wired news, April 17, 2001.
11. Vicini, James, "FBI finds weapons, computers missing or stolen," Reuters, July 18, 2001.
12. Malik, William, Gartner Group, cited in Ryder, J., "Laptop Security, Part One: Preventing Laptop Theft," www.securityfocus.com, July 30, 2001.
13. American Biometric Company, "Discussion Paper: Biometric User Authentication," January 1999.
14. Lobel, Mark, "The case for strong user authentication," Price Waterhouse Coopers, reprinted by RSA Security, 2000.
15. "Client Security in the Enterprise Network: Dell's Perspective," Vectors Dell Highlight, February 2000.
16. Gartner Group, "Gartner Dataquest says worldwide smart card shipments grew 45% in 2000," Gartner Dataquest press release, www.gartner.com, May 14, 2001.
17. "Smart Card Logon," www.microsoft.com/windows2000/techinfo, June 22, 1999.
18. Gemplus, www.gemplus.com
19. Schlumberger, www.schlumberger.com
20. Uimonen, T., "Acer unveils notebook PC with smart card slot," InfoWorld, October 13, 2000.
21. "Two-Factor Authentication - Making Sense of all the Options," Rainbow Technologies, www.rainbow.com.
22. RSA SecurID authenticators, www.rsasecurity.com.
23. Ensure Technologies, www.ensuretech.com.
24. Fenton, Jamie, "Security at your fingertips - new notebooks offer biometric protection," PC World, March 2001.

25. Deitch, Joel, "Body language: the new security," ZDNet Tech Update, August 22, 2001, www.zdnet.com.

26. Raikow, David, "Pick a finger, any finger," ZDNet Security News, March 12, 2001.

27. Raikow, David, "The myth of fingerprints," ZDNet Security News, March 12, 2001.

28. "Most reported laptop thefts occur inside the office," news release by Kensington, January 26, 1999 (www.kensington.com).

29. RSA Security, www.rsasecurity.com/rsalabs/faq.

30. Absolute Software, www.computrace.com.

31. CSS, Inc., www.sentryinc.com.

32. Lucira Technologies, www.lucira.com.

33. zTrace Technologies, www.ztrace.com.

34. Solagent, www.solagent.com.

35. Targus, www.targus.com.

36. TrackIT, www.trackitcorp.com.

37. Highway Loss Data Institute, press release, May 23, 2001, www.carsafety.org.

38. www.lojack.com.

39. Highway Loss Data Institute, press release July 19, 2000, www.carsafety.org.

Caveo Technology
411 Massachusetts Avenue
Cambridge, Massachusetts
02139-4102 USA
www.caveo.com

CATWPLCS 11-2001 2