Chapter 23

Protecting Your Keys

New technology is on the horizon that will let people control processes in their houses and bank accounts using a hand-held computer, but this trend won't get very far without cryptography. Although modern cryptography has become more complex and in many ways more secure, you need to be very vigilant about your keys.

What you know, what you have, who you are

There are three currently accepted ways to protect your keys. You could use a password or passphrase ("what you know"), a smart card ("what you have"), or biometric identification ("who you are"). Or you could use some combination of the three.

Passwords, although the most popular approach, are the least secure. They're usually guessable by a wide variety of programs. Studies have shown that it is easy to successfully guess the majority of passwords.

Biometrics is better, but this science is still in its infancy. Voice recognition will falsely reject someone who has a cold, fingerprint identification will falsely reject someone who has a small scratch, and there are those who may not want laser beams in their eyes.[1]

As we explained in Chapter 22, even really big RSA keys aren't any more secure than 40-bit DES if BlackHat can easily find them in their storage place.

Smart Cards

Smart cards look like thin plastic bank cards, but they contain an embedded integrated circuit. In combination with some kind of reading and/or input device, they provide a variety of computer functions, including digitized communications. Smart cards easily store cryptographic keys and algorithms while limiting access to those keys. Smart cards are currently the most widespread commercial solution for key management. Although not foolproof, smart cards

1. Sign in a laser beam lab: "Don't look directly into laser with remaining eye."

are particularly valued for providing secure authentication by creating and storing keys someplace more secure than a desktop computer.

Smart cards have been more readily adopted in Europe than in the U.S.

First conceived in 1974, smart cards were put through their paces in 1984 during a trial by the French postal and telecommunications services to prevent vandalism and theft of public pay telephones. The trial was so successful that most French telephones now accept only smart cards. European banks have pioneered the use of these cards in the financial industry, and in Germany more than 70 million smart cards have been issued that carry health insurance information. Use of this technology is taking off in Asia, Australia, and New Zealand as well.

U.S. government GSA helps speed U.S. adoption.

A $1 billion purchase of smart cards by the General Services Administration of the U.S. government should help speed the spread of smart card technology in the United States.

Eventually, people will use these cards or something like them to prove identity. Currently, to use a smart card, you need a reader and software. The prices of smart card readers have been dropping and will most likely continue to do so as use of the technology becomes more widespread. American Express gave away readers with its trial of a new combination card called "Blue," which includes both a magnetic strip used on traditional credit cards and an embedded chip that can be used for online purchases. Because smart cards can be used in conjunction with a personal identification number (PIN) or even some type of biometric scan, theft of your identity becomes much more difficult.

Types of Smart Cards

Smart cards can be thought of as tiny computers that must be supplied with voltage, ground, and a clock by an external terminal. They come in two varieties: memory cards and microprocessor cards.

Some people believe memory cards should not be classified as smart cards.

Memory cards are not as "smart" as microprocessor cards. Memory cards are containers for information that can be read and modified. They are often used for temporary purposes, such as a prepaid telephone card, and then disposed of. If a memory card is lost, the finder can use the information it contains.

Microprocessor cards, on the other hand, contain more sophisticated chips and more memory than memory cards. Microprocessor cards can hold multiple applications and passwords, and some even contain co-processors that encrypt data stored in the chip. It's the co-processor that allows the private key to never leave the smart card. This means that cryptographic processing with the private key is done entirely on the microprocessor card, and that limits the exposure of the private key.

In terms of the mechanics of their use, smart cards can either be contact cards or proximity cards or both. *Contact* cards, as their name implies, are read by means of contact (such as insertion) with a device such as a card reader. *Proximity* cards contain a chip that is connected to an antenna and can be read from

a few inches to a few meters away. Proximity cards are intended for use in fast transactions, such as mass transit. A combination card combines both capabilities and offers even more versatility.

What's Inside a Smart Card

Having a microprocessor allows these cards to operate like tiny data processing systems. Typically, inside is an 8-bit central processing unit (CPU) and three types of memory—random access memory (RAM), electrically erasable programmable read only memory (EEPROM), and read-only memory (ROM). There's also an optional cryptographic accelerator to speed calculations.

Protections and Limitations

Obviously, if the card can be altered in an unauthorized fashion, it's not secure. So there are special epoxy coatings to protect the chip and special electronics to protect against other attacks. For example, the best-designed smart cards detect fluctuations in voltage, temperature, or clock frequency. If tampering is detected, the card can be programmed to erase your private key and other critical data. To avoid card cloning, an unalterable serial number is often burned into the chip's memory.

At the time of this writing, DES and Triple DES are commonly used in smart cards and can be used to verify message integrity through the use of message authentication codes (MACs). Bulk hashing is not feasible because the card has limited ability to quickly handle data input and output.

Smart Card Attacks

Any system is breakable, including those that use smart cards. As we've emphasized throughout this book, you must assess the cost of breaking the system and the value of the information to determine the kind of security measures you need. When choosing a smart card, you should ask the manufacturer for references to independent labs that have security-tested its system.

Smart cards can be attacked in various ways. Logical attacks examine the bytes going to and from the smart card in order to uncover the private key, and not all smart card manufacturers have implemented logical countermeasures. To cause a significant physical fluctuation, physical attacks usually require special equipment.

In the Trojan Horse attack, a rogue application has been planted on a workstation. The application waits until the user enters a valid PIN and then asks the smart card to digitally sign some bogus data. You should also be alert

to social engineering attacks, which have been used since the dawn of time. The idea is to trick you and steal what you know.

Technological advances affect smart cards, too.

As we've said before, just because a system was safe five or ten years ago, that doesn't mean it's safe now. For example, Cartes Bancaires (CB), which holds the monopoly on the supply of bank cards based on smart card technology in France, may have waited a little too long to begin replacing the 34 million "yes-cards." According to a Web-based report in *The Irish Times on the Web*, cryptologists had advised CB for the past 15 years that its 320-bit, 96-digit code needed to be longer because advances in technology were weakening it. For that reason, the report said, at the end of 1999 CB began replacing the cards with 792-bit cards, a process scheduled for completion in 2004.

But CB's actions were not in time to stop Serge Humpich, who worked independently for four years and determined that the retail terminals that dispensed small-ticket items, such as subway passes, were a weak link in the French banking system. Reports indicated that he managed to compromise the smart card system, in part because of factoring the public key.

Perhaps those 34 million "yes-card" holders will rest a little more at ease now that French smart card inventor Roland Moreno has offered a reward of one million francs (or about $150,000) to anyone who can demonstrate how to read a bank card's confidential code. French consumer groups spoke out for the immediate replacement of all the old, less secure cards and the payment terminals that Humpich was able to purchase, disassemble, and compromise. As of this writing, CB was waiting to see whether Humpich's discovery would result in any serious fraud before taking such drastic and expensive measures as called for by French consumer groups.

Smart cards could eventually replace all the credit cards and ID we carry in our wallet as well as the keys to all our valuables.

Review

No matter how strong any cryptographic system is, an identity thief could steal who you are (biometric scans), what you know (password), or what you have (smart card). One of the best ways to be vigilant about your keys is to store them someplace more secure than a desktop computer.

Smart cards, which are similar to credit cards, let you do that. Smart cards come in two varieties: memory cards and microprocessor cards. Microprocessor cards, the more sophisticated of the two types, can hold applications, passwords, and even a co-processor that encrypts data stored in the card's chip.

Manufacturers of smart cards design them in ways to protect against tampering. Although smart cards offer good security, they can still be attacked and are subject to technological advances that could weaken formerly strong keys.