Individuals Should Use Encryption to Secure Personal Data

By

Jim McCool

20 November 2003

Thesis: People now need to encrypt the personal data stored on computers or transmitted over the internet to protect against identity theft and fraud.

I. Computer crime, risk, and security
II. Personal data at risk
    A. Data stored on computers
    B. Data exposed through online activities
III. How personal data is compromised
    A. Direct access to computer files
        1. Hacking
        2. Viruses and Trojans
        3. Physical access
    B. Indirect access by network monitoring
        1. Email
        2. Instant Messaging
        3. Online commerce
IV. How personal data can be protected
    A. Protecting computer files
        1. Firewalls & their weakness
        2. Antivirus software & their weakness
        3. File encryption
    B. Protecting against network monitoring
        1. Email encryption
        2. Message encryption
        3. Encrypted channels (SSL)
V. Why encryption is the answer

The explosion of Internet services coupled with affordable high speed access has made online computing more attractive to home users than ever before. This phenomenon has also placed personal data at greater risk, by exposing unprotected computers and data to public networks. The home computer can be used to balance a checkbook, file tax returns, manage social calendars, and write a resume. It is also the gateway to a wealth of online activities such as shopping, managing investments, and online bill payments. Hugely convenient in today's fast-paced society, these activities threaten the security of personal information. However, many home computer users do not take the actions necessary to ensure the security of their personal data. Not doing so is a serious mistake. Each piece of information stored on a computer or transmitted across the Internet may be viewed by unwanted individuals. As if this simple invasion of privacy is not enough, much of this information can be used for identity theft or fraud. Identity theft is fast-growing; the risk is increasing as electronic systems of identification come into greater use (Schneier 26). In an interview, Special Assistant US Attorney Sandy Klein said the Internet is largely responsible for the growth in identity theft, and urges that personal information should not be posted on the Internet (Rosenweig B2). "As many as 700,000 Americans are targeted by identity thieves each year, the Justice Department says" (Block 1). Some may argue that home computers are not a target, or that the common precautions already in use are sufficient protection. Data on home computers are at risk, and the precautions commonly used are not sufficient to protect this data. The security offered by *encryption* technology is the final defense against data theft. (Italicized terms are defined in the glossary.)

A perusal of the software sold at stores shows the kind of data commonly stored on home computers. Home accounting programs are designed to store information about bank accounts, credit cards, investments, loans, and assets, often with the additional security data needed to manipulate these accounts online. Tax programs may store the social security number and financial details used in the return. There are personal appointment managers that tell when and where the user will be. Electronic address books contain names, addresses, and telephone numbers. Some contact managers may contain other personal information that users want to keep track of, such as birthdays and anniversaries, relatives, place of employment, manager, assistants, and job titles. Because of errors in medical records and problems with incomplete information, some doctors encourage people to keep their own medical records (Landro B1). Dr. Denton, a neurosurgeon in Huntington, Al., said that some patients are "showing up in other offices around town with printed summaries of PHR [Personal Health Record] information or even with their laptops" (Landro B1). Identity thieves can find a "goldmine" in all this personal information, which can be stolen by direct or remote access to a computer (Federal Trade Commission 4).

In addition to information stored locally on a home PC, online activities can expose further information. There are numerous online stores offering goods for sale at the click of a mouse. Online shopping usually involves sending credit card numbers over the Internet. In some cases, shoppers are asked to create personalized shopping accounts, providing ID information to build a user profile. Investments can be managed online. Forrester Research estimated $688 billion in assets managed online by 14.4 million accounts in 2002 (Littauer 22). Email, online chat, and instant messaging are other activities that can leak information. A single piece of data may be meaningless by itself, but valuable information may be obtained by organizing many small pieces (Parker 28).

Mistakenly, most users do not consider their home computer to be a target for *hackers*. An electronic break-in to a major corporation's computer is big news, but a break-in to a home

computer is not, even if the event is detected and reported. A study by the Defense Information Systems Agency found that "of 38,000 attacks perpetrated, 96 percent of the attacks went undetected" (Goodman 10). Now that home networks and computers can have continuous internet access via always-on wideband services, hackers also have increased access to the home PC (Johnson TNH2). Hacker software can scan the net, identifying machines that can be exploited (Mann, Mole 32). A computer's presence on the net does not need to be advertised or registered with a *domain name* to be a target. [1]

In addition to direct attack by hackers, data is vulnerable to indirect attacks through online activities. Malicious programs can be executed simply by loading a web page; without carefully examining the security settings, these programs can pass information from a computer to anywhere on the Internet (Schneier 164-7). Hidden programs can be a part of any *HTML* document downloaded to a computer. Browsing the web or opening HTML formatted email can run this intrusive software, which can then return information to the originator (Ryan 46). An undetected *virus* can bypass a computer's security, giving access to the data stored on it (Seiberg 3). Counterfeit software installed on a computer can bypass the protection of a personal *firewall* (Machrone 59).

Some users may feel their data is safe because they never connect to a public network. Again, this is a mistake. Even if a computer is not susceptible to online attacks, personal data still needs protection. Direct access to computer data by unauthorized users is something not often considered. Portable computers are "tempting targets for thieves" (Baig 164). Data stolen from PCs can be used by identity thieves to commit fraud (Johnson TNH2).
Old computers and hard drives that have been scrapped can be scavenged for data. Thousands of credit card numbers were able to be harvested from used hard drives purchased from EBay (Grahm D.09). When data is erased from a computer, it may still be recovered. Deleting a file does not delete the data; it simply makes the space available to be overwritten. Utility software is commercially available to retrieve such deleted information (Nickell 26). Even formatting the hard drive does not make the data irretrievable (Alexander E1-E2). Simson Garfinkel, security expert, MIT Doctoral candidate, and co-author of Practical UNIX and Internet Security, says "It's very difficult to be sure data is ever actually taken off a hard drive" (Mann Mole 34).

Passive techniques can be used to acquire personal data during online activities. The very nature of shared access on cable networks allows anyone in a cable group to monitor network traffic (Johnson TNH2). Email is commonly sent over the internet in plain text and can be intercepted and read (Wei 1). A youth broke into the network at Los Alamos labs by reading a password sent through email (Mann Mole 32). Special programs known as "*Sniffers*" monitor network activity, searching for information; through the use of this technology, "…tens of thousands of passwords have been stolen" (Parker 121). To an identity thief, "everyday transaction[s]" contain the kind of personal information that can be used to commit fraud (Federal Trade Commission 1).

There are many ways to protect personal data. Newer computers use operating systems that implement access control; a password must be entered to gain access. The next line of defense against external attack is the personal firewall. Firewall products can protect a computer from hackers attempting to break in (Johnson TNH2). These products are designed to lock down a computer's network connection, allowing only specified types of network activity. Unfortunately, a firewall can protect against simple attacks, but may not stop a determined hacker (McLure 62). It can be very difficult to set up an effective firewall, requiring knowledge of network protocols that many computer users lack (Bumback and Wolf 16). Even secure

military computers have been broken into, not by hackers, but by less skilled people using the tools built by hackers (Mann Mole, 35).

Antivirus software is generally considered a must-have for networked computers. New computers are sold with this software included. There are many virus protection programs available, and usually are sold with update subscriptions to keep them current. The problem with virus protection is that the programs can only protect against the viruses and *trojans* that are known; there is a continuous cycle of attack and defense: new viruses are created and found, cures are created and published, and then new viruses are created and found again. Few people update their virus protection daily; even then, they would still be vulnerable to the very latest viruses that have either not yet been found, or cures published, for the particular antivirus product in use.

In general, computer security requires a defense for each attack. The best way to ensure the security of data is *cryptography*. The power of cryptography uses mathematics to tip the advantage to the defender (Schneier 120). Cryptography provides a way to convert readable "plaintext" into unreadable "cyphertext", through a process called encryption (Wei 1). *Cryptographers* know that when strong cryptography is used, this data cannot easily be made legible without the key, often derived from a password or phrase, that was used to encode it. Thus, strong cryptography is usually not the subject of the attack; rather, the attack is performed by attempting to guess the key. The commonly used term for this type of attack is a brute force attack, since it uses the brute power of a computer to try all the possible keys until the correct one is found. As the key length gets longer, the number of guesses required grows exponentially. A strong key is a key that is long enough to make it difficult to guess. The futility of attempting to brute force a strong key is often described as taking long enough that by the time the correct key is found, the sun will have burnt out to a cold cinder. When a file is encrypted using strong cryptography and a strong key, it can only be read by a person with the correct key.

Considering the vulnerability of data on home computers, encryption of personal data should be routine. It might be argued that encrypting every file is too much work and too much bother for any but the most critical of personal data. With the availability of encrypting file systems, this argument is not valid. Unlike file encryption, hard disk encryption is easy and transparent to the user. The file is encrypted simply by saving it; there's no need to think about the process (Kutler 12). Encrypting file systems are included as part of some computer operating systems.[2] Using this technology, entire folders can be encrypted and decrypted transparently to the user, yet remain unintelligible to anyone not logged in as the user who encrypted it.

Similar techniques can be used to protect online communications. "Anyone can achieve absolute communications privacy by using strong cryptography… even [when monitored] by government efforts" (Parker 97). Although many people appear unconcerned, even telephone conversations can be overheard. It's now common to see someone in public carrying on a personal or business conversation on a cell phone. Statements sent by encrypted email are safer than telephone conversations (Littauer 22). Email encryption is built into some email programs, and encryption add-ons are also readily available (Wei 1).[3]

Instant Messaging (IM) conversations can be encrypted using a universal *client* (Machrone 2). Using such clients, users can enjoy complete privacy in an online chat, even though their messages are passing through vulnerable public networks.

SSL, an encryption technology commonly used to secure transactions with web sites, should be considered mandatory to protect credit card transactions (McLure 62). Fortunately, this technology is now commonly in use. Browsers such as Internet Explorer and Netscape

indicate a secure connection by displaying a small padlock icon. Any time a user is asked to complete an online form with personal information, or provide information for a financial transaction, he should always check for a secure channel.

The wealth of information stored on computers and exposed through online activities can be stolen without the victim even being aware of the theft. Much of this data can be used for fraud, or to steal one's identity; the damage is usually unknown until it is far too late. There are many avenues through which personal information can be stolen. Hacking, viruses, and spyware can often circumvent the protections set up to guard access to computers. Physical access is not even a consideration for stolen or scrapped computers; the data is completely unprotected. Unguarded online activities expose bits of information that can be useful to criminals. Given the proven vulnerability of personal data on computers, encryption should be considered essential. Strong encryption is proven to protect data from unwanted exposure, even when a criminal has physical access to a computer or its hard drive. Strong encryption products are now readily available, and are already installed on many home PCs. Encrypting file systems make using this type of security simple and transparent. Email encryption is an option included in some email programs, and can be added to others. The importance of encryption to secure online transactions is widely recognized, to the extent that most online commerce uses it. It is a simple matter for users to check the security of online transactions and choose not to use sites that do not secure the connection. Considering the risks to personal data and the security offered by encryption, computer users must insist on using this technology to secure their personal data.

Notes

[1]In my position as the network administrator at Slope Indicator Company, I register as many as 2 to 4 attacks daily on an unregistered computer connected to the internet. The nature of these attacks suggests automated software probing random internet addresses for known vulnerabilities.

[2]Windows 2000 and XP Professional include the capability to use encrypting file systems (EFS). Unfortunately, this option is not enabled by default, and must be explicitly enabled by the computer user.

[3]Among the email programs available that have built-in encryption capability are Microsoft Outlook and Netscape; however, PGP is the most popular (Wei 1). PGP is available as an add-on and can be purchased either commercially or downloaded for free. PGP also uses a widely supported, free public key server system, adding to its popularity.

Glossary

Client: A program that communicates to a server; for example, an email *client* sends and receives email to and from the email server. A web browser is a *client* that downloads web pages from a web server.

Cryptographer: A person who practices encryption.

Cryptography: The science of encoding and decoding messages such that the message can only be read by an authorized person.

Domain name: A human-readable name that is used to look up a computer address, similar to a person's name being used to look up a telephone number.

Encryption: The process of altering a file or text using a secret code to make it unintelligible without the secret code to read it with.

Firewall: Specialized security software that prevents unauthorized users from gaining access to a computer or network.

Hacker: A person who uses computer skills to gain illegal access to a computer or file.

HTML: HyperText Markup Language. The format that web pages are written in.

Sniffers: Software designed to monitor networks and copy data that meets specified criteria.

Spyware: Software that reports information about a computer or user activity, without the knowledge of the user.

Trojans: A counterfeit or modified program that appears to do one thing, but carries hidden code that is executed without the user's knowledge.

Virus: A program capable of replicating itself by attaching a copy of itself to other programs. When the infected program is run, the virus is able to propagate.

Works Cited

Alexander, Steve. "Clean Slate" Star Tribune (Minneapolis, MN 19 January, 1999. Online. SIRS Researcher 2 November 2003

Baig, Edward. "Making Your Portable Less Liftable" Business Week Jun 21, 1993: 164. Online. ProQuest. 26 October 2003

Block, Sandra. "States Pass Laws to Protect Identity" USA Today 14 July, 2003. Online. SIRS. 2 November 2003

Bumback, Jaclynn, and Mike Wolf. "Hardware Firewall Makers Eye Hot Consumer Broadband Market" Electronic News. Jul 23, 2001: 30. Online. ProQuest. 25 October 2003

Federal Trade Commission (FTC) ID Theft: When Bad Things Happen to Your Good Name Sept 2002. Online. SIRS Government Reporter 2 November 2003

Goodman, Marc. FBI Law Enforcement Bulletin SuDoc Number : J 1.14/8:70/8 August 2001. Online. SIRS Government Reporter 2 November 2003

Graham, Jefferson. "'Erased' hard drives can bite you ; Think you've deleted information? Think again; it's still there" USA TODAY Feb 6, 2003: D.09. Online. ProQuest abstract. 26 October 2003

Johnson, Dave. "Unauthorized Access Denied" Home Office Computing Dec 1999: TNH2. Online. ProQuest 25 October 2003

Kutler, Jeffrey. "A Focus on Protecting the Data in Stolen PCs" American Banker Apr 30, 1999: 12. Online. ProQuest 26 October 2003

Landro, Laura. "Tools That Can Help You Keep Your Own Accurate Medical Files" Wall Street Journal (Eastern edition) New York. 26 May, 2000: B1. Online. ProQuest. 25 October 2003

Littauer, Stephen. "What to Consider About On-Line Investing" Consumers' Research March 1999. Online. SIRS Researcher 2 November 2003

Machrone, Bill. PC Magazine Jul 1, 2002: 59. Online. ProQuest 26 October, 2003

Mann, Charles C. "The Mole in the Machine" New York Times Magazine. Jul 25, 1999: 32. Online. ProQuest 25 October, 2003

Mann, Charles C., Ernest R May, Bruce Schneier and Thomas C Schelling. "Homeland Insecurity" The Atlantic Monthly. September 2002: 81. Online. ProQuest. 25 October 2003

McClure, Dave. "Guarding your Gateway" Association Management. Aug 2001: 60. Online. ProQuest 26 October 2003

Nickell, Daniel B. "Computer Security: Networked for Crime" Security Management Dec 1991: 26. Online. ProQuest 26 October, 2003

Parker, Donn B. Fighting Computer Crime New York: Wiley, 1998

Rosenzweig, David. "ON THE LAW; Educational Video Helps Curb Identity Fraud; U.S. attorney's outreach program shows people what they can do to avoid becoming Victims" Los Angeles Times Aug 15, 2003: B2. Online. ProQuest. 25 October 2003

Ryan, Dan J. "Warding Off PC Spies" Federal Computer Week. Aug 7, 2000: 46. Online. ProQuest 25 October 2003

Schneier, Bruce. Secrets & Lies New York: John Wiley & Sons, Inc. 2000

Seiberg, Jaret. "Anti-Fraud Experts Urge Strengthening Shields Against Hackers, Thieves" American Banker Oct 22, 1998: 3. Online. ProQuest. 25 October 2003

Wei, Raphael Phan Chung. "Simple Way to Protect E-mail Privacy" Computimes Malaysia.Oct 11, 2001: 1. Online. ProQuest 26 October 2003