Against the Grain

Volume 10 | Issue 5 Article 10

November 1998

A Word About Data Encryption

James Williams
College of Charleston

A Word About Data Encryption

by **James Williams** (College of Charleston) <jwilliams@cofc.edu>

With the increased use of e-commerce and online banking, encryption is not only important, it is essential. "Encryption is the sending of a message, or the storage of data or software, in the form of a cipher." (*McGraw-Hill Encyclopedia of Personal Computing,* p.364) By "scrambling" and/or encoding data, one can "feel" fairly sure that one's data or transaction has been completed safely. The credit card number 123456789 would look something like (*&^%$#@! when encrypted. Using public key encryption is a highly secure method of transmitting data since it requires a registered public key to encrypt the data and can only be decrypted by a private key owned by the person receiving the data. The theory is that even if this information is intercepted, it is unusable to anyone other than the intended user. However, as with any technology, there are a few issues to consider.

1 Since the technology is new, there are bound to be flaws or "security holes" that leave a computer system or network vulnerable to attack and infiltration. In the past computer viruses used to be our biggest fear. But with new systems and software being produced almost daily, system vulnerabilities are much more popular. For 1998, the **CIAC (Computer Incident Advisory Capability)** for the Department of Energy identified 89 system vulnerabilities and only 3 viruses and worms. There have been reports of decrypted credit card files being visible behind an Internet Service Provider's (ISP's) "firewall." A firewall is security software setup to keep unwanted guests from entering your network. The problem is that unwanted guests use ISP's to access the Internet and if they are on the same network they are basically already behind the firewall.

2 Internet technology changes rapidly. People generally feel more secure about speaking their credit card numbers over the telephone primarily because telephone technology has been around for over 100 years. The technology has seen fewer changes on a slower more controlled basis, but phone technology is not 100% secure either. On the other hand, computer technology changes almost daily. If you think about it, 5 years ago we were saying how wonderful the "Gopher" was going to be. It is impossible to "guarantee" the security of any technology that undergoes a complete metamorphosis into something almost totally different every 2 to 4 years.

3 Computers and Internet technology are very complex and people are not perfect. Hardware performs specific operations, as does software. If improperly operated, there can be disastrous results or no results at all. The vast majority of all non-hardware-related problems with computers is operator error. These problems are generally easier to find and resolve. But, what about the "stray electron?" I was using my ATM card at a grocery store just before a storm hit. While the grocery store's machine said it could not process my transaction each time I tried, my bank was processing each transaction. Where did these "stray electrons" go on their way back to the store? When hardware and software go wrong, they usually go wrong in a big way.

4 What about identification and trust? Online, am I really who I say I am? If someone is using my PC and happens to find my encryption key, can he use my machine and information to impersonate me? I don't have a definitive answer for this one, but this is probably why there is so much work going on to develop digital signatures, certificates and fingerprints for proper ID verification.

5 And last, there is the human factor. There is a saying "you can't stop a good thief. The best you can do is slow him down enough to get caught." The same is definitely true of computer crackers. Most of our information or transactions are not important enough for anyone to go to a lot of trouble to try to obtain. But, if one is doing millions of dollars in transactions, then the payoff looks more worth the effort. If you add the availability of "super" technology to the human factor, it is not a matter of if the information can be compromised, but how long it will take to compromise it. In the article, "The Fed's Encryption Standard Cracked in Record Time" (http://www.thestandard.net/articles/article_display/0,1449,1115,00.html), the government's Data Encryption Standard or (DES) which is an "unbreakable" 56 bit encryption code, was broken in 56 hours using a $250,000 super computer. Considering the fact that the PC I'm using to word process this article has more power than the first mainframe that housed our online catalog a few years ago, I dare say there is a variety of "state of the art" gear in the corporate world that would worry me just a little. By the way, the standard code that us non-government types use is only 40 bit encryption.

The bottom line is that data encryption works, no doubt about it. People should still be aware that it is man-made technology and not perfect. It is also not invulnerable. One should be both practical and cautious in using any technology that involves finance.

Some interesting sites:

Computer Incident Advisory Capability
http://ciac.llnl.gov/ciac/CIACHome.html

CERT Coordination Center
http://www.cert.org/

Microsoft Security Advisor
http://www.microsoft.com/security

SC Info Security Magazine
http://www.westcoast.com/securecomputing/december/insight/commerce.html

McGraw-Hill Encyclopedia of Personal Computing, ed. Stan Gibilisco. New York: McGraw-Hill, 1995.

Krause, Jason and Weil, Nancy. "The Fed's Encryption Standard Cracked in Record Time," **The Industry Standard** 17 July 1998. 24 Sept 1998 http://www.thestandard.net/articles/article_display/0,1449,1115,00.html.

Pretty Good Privacy homepage for encryption software
http://www.nai.com/default_pgp.asp

Contains information about the Kerberos encryption system
http://www.cit.cornell.edu/computer/internet/security/kerberos.html

James Williams' site about Internet security
http://www.cofc.edu/~williamj/pcmission.html