New Media

D. John Doyle MD PhD FRCPC

Internet security issues

Part two: Encryption and cryptograhy

We live in an age of electronic information. Information technology is quickly transforming society, creating new businesses, new jobs and new careers but also new concerns about privacy and crime, since information technology also creates new opportunities for law-breakers. That is, these developments may also lead to new problems in investigating and prosecuting crime. As a result, electronic information, be it corporate trade secrets, pre-release government crop statistics, VISA numbers or a patient's medical records, must have strong protection from uninvited modifications or disclosure. Cryptographic and encryption technology provides that protection.

Cryptographic and encryption methods provide a set of techniques for encoding data, messages and other forms of digital information such that they can be stored and transmitted securely, i.e., without the possibility of data being intercepted and understood by the wrong people. This section of this month's New Media section introduces the basic terminology of cryptography and encryption and identifies some of the common methods used.

Cryptography can be used to achieve secure communications, even when the transmission media (such as the ordinary Internet) is ordinarily quite untrustworthy. You can also use cryptography to encrypt your sensitive files, so that an intruder cannot read them. Using cryptography, it is also possible to verify the origin of data and messages, using a technology known as "digital signatures".

When using cryptographic methods, the only part of the process that must remain secret are any cryptographic "keys". The algorithm designs, the key sizes, any file formats, etc. can all be made public without compromising security (but usually are kept secret anyway in military settings).

The two fundamental operations of cryptographic systems are encryption (with decryption as its inverse) and signing (with verification of signature as its matching operation). Encryption is analogous to enclosing data in an opaque envelope. Decryption is analogous to removing the message from the envelope. Signature is similar to signing a document physically, and initialing each section to show that no portion of the document has changed. Verification of signature is the rough equivalent of matching the signature to a "signature on record" card, and verifying that no portion of the document has changed. Certificates may be viewed as signed documents which match public keys to certain information.

Encryption techniques that could stump even the NSA and the CIA are available to anyone with a little money and a modest understanding of computer cryptography. Most systems fall into one of the categories described below.

Single Key Encryption

In this system there is one key used to encrypt and decrypt the message. This key must be given to the intended recipient of the message in order to have then message decrypted. If a person knows how to intercept e-mail en route to its destination, then any keys sent via the Internet may also be caught. If this happens, the message can be decoded. The only way to prevent this is by physically exchanging keys, a method that is often impractical, and carries its own security burden.

Address correspondence to: Dr. D. John Doyle MD PhD FRCPC; New Media Editor, Canadian Journal of Anesthesia, Department of Anesthesia, The Toronto Hospital, 200 Elizabeth Street, Toronto, Ontario Canada M5G 2C4 Voice pager: (416) 375-0565, Fax: (416) 423-0452, e-mail: djdoyle@inforamp.net

DUAL KEY ENCRYPTION
Under a dual key system, the key to encrypt can be safely transferred across a network. This is because the key that is sent (the public key) can only encrypt, not decrypt messages. The situation is like a safe deposit box where anyone can put something in (encrypt) but only one person can remove objects (decrypt). The public key can be transferred, uploaded, posted on the web - whatever is easiest. It's only use is to encrypt messages, and thus does not present a security hazard if stolen. By contrast, the private key must always be guarded carefully.

ENCRYPTION SITES (for more information)
Frequently Asked Questions about Cryptography.
http://www.rsa.com/rsalabs/faq/

Privacy Place - Information "Self-Defence" for the Common User
http://maxpages.com/privacyplace/Encryption

Encryption Privacy and Security Resource Page
http://www.crypto.com

Internet glossary

Part 4. Glossary of security terms

ABUSE OF PRIVILEGE
When a user performs an action for which they have neither privileges nor authorization.

ACCESS CONTROL
The most common form of access control is the use of passwords or passcode. Almost certainly, the most common form of security breach is the compromising of these passwords. Other forms of access control include passcards, fingerprint readers, retinal scanners, etc.

AUTHENTICATION
The process of determining the identity of a user that is attempting to access a computer system or network. Authentication procedures ensure that you are indeed who you say you are and not an imposter or fraud, and also ensures that the sender identified by the source address in any messages truly is the sender of any data. Authentication is important for facilitating banking transactions, making purchase orders and conducting commerce over the Internet.

AUTHORIZATION
The process of determining what types of computer activities are permitted to a given user. Usually, authorization is in the context of authentication: once you have authenticated a user, they may be authorized for different types of access or activity. Some users, for instance, may be granted read-only file access, while more powerful users such as the system administrator would also have write-to-file privileges.

CHECKSUM
A one-way function applied to a file to produce a unique "fingerprint" of the file for later reference. Checksum systems are a means of detecting file system tampering.

CONFIDENTIALITY
Confidentiality is the concept that information should be made unavailable to those persons who are unauthorized to access it. Strict controls must be implemented to ensure that only those persons who need access to certain information receive that access. Many computer crimes involve compromising confidentiality and stealing information. The concept of allowing access to information or resources only to those who need it is called access control.

DATA DRIVEN ATTACK
A form of attack in which the attack is encoded in innocuous-seeming data which are executed by a user or other software to implement an attack. Transmission of viruses via e-mail attachments are one example. In the case of firewalls, a data driven attack may get through the firewall in data form and launch an attack against a system behind the firewall.

DIGITAL CERTIFICATES
These are digital IDs or passports to present credentials online. Digital certificates are issued by companies that act as "trusted third parties." In a secure electronic transaction (SET), the buyer, the merchant and banks for these parties all have digital certificates. Verisign is the dominant certificate authority on the Internet. Current versions of the Microsoft & Netscape browsers have the facility for users to add new certificate authorities.

FIREWALL
Firewalls are hardware / software systems configured to protect against unauthenticated logins from the "outside" world. This helps prevent vandals from logging into machines on your network.

INTRUSION DETECTION
Detection of break-ins or attempts either manually or via software systems that operate on logs or other information available on the network.