Security and the Basics of Encryption in E-Commerce

The success or failure of an e-commerce operation hinges on myriad factors, including but not limited to the business model, the team, the customers, the investors, the product, and the security of data transmissions and storage. Data security has taken on heightened importance since a series of high-profile "cracker" attacks have humbled popular Web sites, resulted in the impersonation of Microsoft employees for the purposes of digital certification, and the misuse of credit card numbers of customers at business-to-consumer e-commerce destinations. Security is on the mind of every e-commerce entrepreneur who solicits, stores, or communicates any information that may be sensitive if lost. An arms race is underway: technologists are building new security measures while others are working to crack the security systems. One of the most effective means of ensuring data security and integrity is encryption.

Encryption is a generic term that refers to the act of encoding data, in this context so that those data can be securely transmitted via the Internet. As Professor Lawrence Lessig of Stanford Law School put it, "Here is something that will sound very extreme but is at most, I think, a slight exaggeration: encryption technologies are the most important technological breakthrough in the last one thousand years." Encryption can protect the data at the simplest level by preventing other people from reading the data. In the event that someone intercepts a data transmission and manages to deceive any user identification scheme, the data that they see appears to be gibberish without a way to decode it. Encryption technologies can help in other ways as well, by establishing the identity of users (or abusers); control the unauthorized transmission or forwarding of data; verify the integrity of the data (i.e., that it has not been altered in any way); and ensure that users take responsibility for data that they have transmitted. Encryption can therefore be used either to keep communications secret (defensively) or to identify people involved in communications (offensively).

The basic means of encrypting data involves a symmetric cryptosystem. The same key is used to encrypt and to decrypt data. Think about a regular, garden-variety code, which has only one key: two kids in a tree-house, pretending to be spies, might tell one another that their messages will be encoded according to a scheme where each number, from one to 26, refers to a letter of the alphabet (so that 1 = A, 2 = B, 3 = C, etc.). The key refers to the scheme that helps match up the encoded information with the real message. Or perhaps the kids got a little more sophisticated, and used a computer to generate a random match-up of the 26 letters with 26 numbers (so that 6 = A, 13 = B, 2 = C, etc.). These codes might work for a while, managing to confuse a nosy younger brother who wants to know what the notes they are passing mean, but the codes are fairly easy to crack. Much more complex codes, generated by algorithms, can be broken by powerful computers when only one key exists.

Public Key Encryption, or asymmetric encryption, is much more important than symmetric encryption for the purposes of e-commerce. The big improvement wrought by Public Key Encryption was the introduction of the second key - which makes a world of difference in terms of protecting the integrity of data. Public Key Encryption relies on two keys, one of which is public and one of which is private. If you have one key, you cannot infer the other key.

Here's how it works: I have a public key, and I give that key (really, information about how to encode the message) out to anyone with whom I wish to communicate. You take my public key and use it to encode a message. You send that message, in coded form, over the network. Anyone else who sees the message cannot read it, because they have only the public key. The message only makes sense when it gets to me, as I have the only copy of the private key, which does the decoding magic, to turn the zeros and ones (bits of information) into readable text.

The most common use of PKE for e-commerce involves the use of so-called Digital Certificates issued by "trusted" third parties. Here's how this one works. Say you are a customer of Big Safe Bank and you would like to communicate with your bank. If you sent the bank some information (for instance, "please wire the contents of my savings account to a new account in Switzerland"), you might worry that the information could get intercepted en route but you might also worry that the bank would not know it was you who sent the information. You and

Big Safe Bank agree to use a trusted third party to help you communicate in an encrypted manner to one another over the Internet. The bank contracts with VeriSign or another provider of a Digital Certificates. When you send a message to the bank, you send your message about wiring funds encrypted twice: once with your own private key, and once with the bank's public key, along with a certificate, encrypted using the institution's private key. Once the bank gets your message, they use the institution's private key to decrypt the certificate, which in turn gives the bank your public key. The key in the certificate can decrypt the message you sent to such an extent that all the bank then needs is its own key to read the message. After all those keys have worked their magic instantaneously, the bank can be certain of two things: that you were the one who sent the message and that the message was not read along the way. And you know that the only one who could have read the message was the bank. The funds get transferred, as requested - probably using another encrypted data transmission.

Public Key Encryption ostensibly creates a world in which it does not matter if the physical network is insecure. Even if - as in the case of a distributed network like the Internet, where the data passes through many hands, in the form of routers and switches and hubs - information could be captured, the encryption scheme keeps the data in a meaningless form, unless the cracker has the private key.

Public Key Infrastructure (PKI) refers to the notion that the best way to establish a system of secure communications over networks is to establish an infrastructure that will support public key encryption. The PKI would create an environment where any Internet user could "carry" certificates around that identify them in a variety of ways. Authentication of parties could become very cheap and easy. Some e-commerce proponents suggest that creation of a seamless and robust PKI would have enormous implications for speeding the growth of e-commerce.

There are non-technical limitations to PKI. It is said that it simply shifts the security risk to the certificate authorities. They wonder who will certify the certifier and how safe their key data will be in these hands. Some governments have demanded access to such key repositories in the interest of national security.

Other interesting issues worth pursuing for further information related to encryption include:

- secure sockets layer (SSL) protocols, which allow for the transmission of encrypted data across the Internet by running above the traditional TCP/IP protocols;
- the effectiveness - and occasion flaws - in easily-accessible (freeware) security technologies such as PGP;
- other uses of encryption, such as the closely-related notions of digital signatures (very broadly defined), access controls, and watermarks;
- the technical means by which keys use hash tables to achieve the encryption and decryption process;
- regulation of Ceritificate Authorities (CAs), Registration Authorities that validate users as having been issued certificates and the directories that store certificates, public keys and certificate management information;
- policies that identify how an institution manages certificates for its own personnel, including legal liabilities and limitations, standards on contents of certificates, and actual user practices;
- the history of codes, from ancient times through the second World War to present day, including the recent controversy over whether encryption methods of a certain force should be treated as "armaments" illegal for export by the United States government and the debate over the so-called "Clipper Chip."

Web sites of interest for further information on encryption and related topics:

PKIguru.com's PKI Nutshell Tutorial:
http://www.pkiguru.com/nutshell.htm

Greg Shipley, Certificate Authorities: How Valuable Are They? TechWeb News (March 25, 1997):
http://www.networkcomputing.com/806/806f1.html

Internet2's collection of sample certificates:
http://middleware.internet2.edu/certprofiles/

RSA Security's cryptography resource center:
http://www.rsasecurity.com/rsalabs/faq/

Prof. Lawrence Lessig's site for CODE AND OTHER LAWS OF CYBERSPACE
http://www.code-is-law.org/

Electronic Privacy Information Center's Clipper Chip page
http://www.epic.org/crypto/clipper/

Francis Litterio's Cryptography resource center:
http://world.std.com/~franl/crypto/info.html

Internet Law & Policy Forum, The Role Of Certification Authorities In Consumer Transactions(1997):
http://www.ilpf.org/work/ca/draft.htm

The Web site dedicated to Neal Stephenson's book, CRYPTONOMICON:
http://tombstone.epiphyte.com/

For more information contact:
John Palfrey