

Internet Security: "Knowing me, Knowing you"

Chris Gledhill, Managing Director of PDMS Advanced Systems Group

May 1999

One of the main issues in the growth of e-business is undoubtedly security. There are of course many different aspects to security in a wired world, but they can be divided into two simple categories the first is "securing your premises". Businesses and individuals need to secure their internal systems and data from intruders. Just as with physical premises, the level of security required depends on the value of the contents and the likelihood of attack. Securing your premises in the context of the Internet is all about network security, firewalls, proxy servers and "de-militarised zones". These are essentially infrastructure issues for individual businesses and will be the subject of a future article.

The second category, and the subject of this article is "doing business with confidence". As a buyer you want to know you are dealing with a real organisation, and as a seller you want to be sure that any transaction is verifiable. Also all parties want to avoid the fraudulent use of personal information by third parties.

In practice, the issues of authentication (knowing who you are dealing with) and encryption (hiding information from prying eyes) are very closely related in that they both rely on the same technology for their solution.

The basis of virtually all transaction security initiatives on the internet is a digital key; this is a unique code used by the encryption functions built into many forms of internet software such as web browsers. The key is used to encrypt (lock) a message before it is transmitted, the message can then only be decoded (unlocked) by someone who has the corresponding key.

Digital keys come as matched pairs, a private key and a public key, any message sent using one key requires the other to decipher it. The private key is always retained by you whilst the public key can be given to anyone with whom you wish to communicate securely. All messages which can be unlocked with your public key must have been locked with your private key, therefore they must have come from you. All messages returned using your public key can only be unlocked using your private key and are consequently unreadable by anyone else.

Digital keys can be issued manually as part of the process of establishing a trusted business relationship or automatically under the control of a software package. A good example of this is the communication between a web browser and a secure web server. In this case a secure channel of communication is established between the browser and the server for the duration of a transaction through a two stage exchange of keys. First the secure server sends its public key to the browser. This is used to encrypt a 'session key' generated automatically by the browser. The session key can then be sent securely to the server. The session key is then used to decipher subsequent messages from the client.

This process provides two important safeguards; message privacy because the information exchanged is encrypted, and message integrity because the contents cannot be altered once it has been encrypted. Even an accidental corruption of a single character will render the whole message unreadable.

Secure Sockets Layer (SSL) technology, which is the standard protocol for secure, Web-based communications, protects the information exchanged during a transaction using encryption as described above. In addition it requires a digital certificate to authenticate the identity of the server. A digital certificate is a text file containing information about the identity of the certificate owner together with a digital signature from the certification authority. The certification authority is an organisation which acts as a trusted third party by checking the identity of an applicant before issuing a certificate. The certificate is validated with the digital signature of the certification authority.

A digital signature is simply a piece of information encrypted with an organisation's private key. This can only be read using that organisation's public key. Successful decoding with the public key proves the origin of the information.

In effect a digital certificate is very much like a passport. When you apply for a passport the government acts as a trusted third party; it verifies you are who you say you are and issues a physical document to that effect. The passport is then universally accepted as proof of your identity. There are a number of established certification authorities such as VeriSign whose role is to provide the equivalent independent validation of the identity of an organisation or individual.

A business may also wish to issue its own certificates to its business partners. The analogy here might be with a bank account and associated plastic cards which are issued once a new customer has been accepted. Such certificates could be exclusive to a specific business or shared between a group of organisations. Again there are clear analogies with existing systems within the financial services industry.

Most of the processes described in this article are already well established at a technical level and can operate almost invisibly as we go about our business in cyberspace. The challenge is for business and government to work together to create an environment where Internet security is as well understood and common place as the use of a cash-point machine or a credit card is today. And for those who rise to this challenge the prize is a piece of the world's fastest growing market place.

The next article in this series will focus on the subject of Internet payments.

Published in Money Media, May 1999