using a private-key encryption algorithm.

To implement this kind of algorithm, both sides must have a single private key, which is generated by the browser. Rather than simply using the public key to encrypt this master key for transmission to the server, however, the browser sends a premaster secret key instead. Based on a predetermined protocol and using the random numbers exchanged during the handshake protocol, the server can use the premaster secret key to determine the true master key. This avoids the necessity of transmitting the actual master key. Once this process is complete, both browser and server have copies of the master key and can communicate securely.

INTERNET EXPLORER SECURITY

As mentioned earlier, Internet Explorer 3.0 supports both SSL and PCT. Like SSL, PCT uses public-key cryptography to encrypt a private key, which is used for the rest of the session between the browser and server. The major difference between SSL and PCT is in the handshake protocol phase. According to the Internet draft proposal written by Microsoft and presented to the IETF, PCT requires fewer messages to negotiate a compatible set of protocols, supports more encryption algorithms, and provides additional security by using different keys for authentication and encryption. Microsoft evidently plans to continue to support both SSL and PCT in future versions of Internet Explorer.

In addition to supporting these security protocols, Internet Explorer 4.0 uses its security zones to let users configure their browsers' security levels at different sites. Each zone is assigned a security level that allows only certain activities to take place. For example, you could assign your company's intranet site to the trusted zone, in which case you could surf the site without encrypting transmissions. On the other hand, you could assign Internet sites you are visiting for the first time to the untrusted zone, which would require the server to provide SSL authentication before the browser uploaded any information.

Internet Explorer 4.0 ships with four defined zones: local intranet, trusted sites, Internet, and restricted sites. Using the Options dialog box, users can alter a zone's security level or create new zones (see Figure 1). A fourth option allows the user to configure a custom security zone.

THE FUTURE OF INTERNET SECURITY

The Transport Layer Security protocol derives its name from the IETF working group charged with developing an Internet standard for a secure, authenticated channel between hosts. Version 1.0 of the TLS protocol was presented to the IETF in May. The protocol is currently based on SSL, but the differences that have been introduced make it incompatible with SSL 3.0.

According to Netscape, the IETF is close to according TLS the status of an Internet standard. This doesn't mean that vendors will be obliged to implement it, of course. But at least there will be a standard for secure transactions against which other protocols can be compared.

The major credit card companies have been developing another standard, called the Secure Electronic Transaction standard (SET), which may have an important effect on the security of Internet transactions. SET wouldn't eliminate the need for protocols such as TLS; rather, it focuses on confidentiality and authentication. SET-compliant software not only will make sure that thieves cannot steal a credit card number; it will also keep a merchant from seeing the number while still providing assurances that the card is valid. The transmission will pass through the merchant's hands directly to the credit card issuer, which will then decrypt it and credit the merchant's bank account.

FIGURE 1: *The security dialog in Microsoft Internet Explorer, Version 4.0, lets you set security levels for four types of Internet and intranet sites.*

But SET's significance goes beyond its ability to protect credit card transactions from prying eyes. That known and trusted companies like MasterCard and Visa created it may instill more confidence among consumers than any strong encryption.

SO IS IT SAFE?

When creating a new algorithm, a cryptographer has no way of knowing for sure that it is airtight against thieves. The only way to increase confidence in any encryption algorithm is through trial and error: Confidence improves as the number of people who try and fail to break it increases. This is why only a few algorithms, such as RSA and DES, are used in most business and government applications; they have stood the longest test of time. But even these algorithms may have weaknesses that cunning hackers can exploit.

Apart from using any weakness in the algorithm, the only way to decrypt encrypted data without the key is a brute-force attack. This method is similar to trying to open someone else's padlock by trying 0-0-0, 0-0-1, 0-0-2, and so on, until the correct combination is found. The longer the combination, or key, the harder it is to find the right number.

This is why so much debate centers around the issue of key length. The large majority of keys range from 40 bits to 1,024 bits; obviously, it's a lot easier (though still not easy) to find the right combination of 40 ones and zeros than to find the correct string of 1,024 ones and zeros. There have been several cases in which people have successfully identified 40- and 48-bit keys. DES 56-bit has also been cracked, but only with an immense brute-force effort by tens of thousands of people. This kind of resource is *not* going to be available to Joe Hacker. Your swimwear purchase at Land's End is almost certainly still safe.

Although encryption techniques continue to improve, cryptographers emphasize that strong encryption isn't the answer to every security issue. Buggy software, human error and greed, and poor server administration leave the door open wide for unscrupulous hackers. On the other hand, a recent review of Internet security breaches indicates that most systems will never experience a break-in and those that do will not be severely damaged. Rather than taking heart in these results, though, one leading cryptographer points out that as long as little valuable data is on the Internet, thieves will stay away; when electronic commerce picks up steam, it's likely that more people will be tempted to try their hands at cracking.

So if the Internet is relatively safe now, what's stopping consumers from buying? Fear of the unknown and the tenacity of old habits are two factors. But like the tortoise, electronic commerce will slowly but surely accelerate. Whether it wins the race depends in part on how well software developers and system administrators protect the process.

Michele Rosen is a freelance technical writer.