The new encryption

Public key encryption is a vital enabling technology for Internet commerce that risk managers should understand, says David Rowe

Use of the Internet for commercial exchanges, exemplified by on-line equity trading, has dramatically expanded the need for secure electronic communication. Both the number and size of such transactions is growing rapidly, as is the number of distinct pairs of parties to such transactions. This gives rise to two increasingly urgent needs:

- Information security (assurance that only the intended recipient has access to the message).
- Sender verification (assurance that the message is from the stated source).

Traditional encryption methods are based on the principle of a reversible process for encryption and decryption using a common secret key. This is fine for a limited number of pre-arranged bilateral channels of secure communication, but it is inadequate to support the exponential growth in the number of bilateral pairs of communication points implied by the rapid increase in Internet commerce. A common key must be confidentially agreed in advance and communicated between the two parties. If this knowledge is compromised at either end, the communication link is no longer secure.

The basic concept of public key encryption rests on a process that is not reversible in the traditional sense of private key encryption and decryption. Nevertheless, under appropriate circumstances, the process is circular. An appropriate mental analogue is a car with no reverse gear on a circular track that is too narrow for the car to turn around. Having passed a given point, the car cannot shift into reverse and move back over the ground it has covered. It can, however, return to its starting point by continuing full circle around the track.

Public key encryption is based on modular arithmetic where results above the value of the modulus "cycle back" through the integers starting at zero. To extend the mental analogue, however, assume that after its first movement the car must advance in fixed increments as it travels around the track. It is very possible that all future stopping points will skip over its original location, making it impossible to land exactly where it started. In the same way, only some modular mathematical processes with selected parameters allow the original inputs to be reproduced.

Mechanics

To those not trained in modular numerical methods (myself included), the mechanics of public key encryption are quite amazing. The process begins with a plain text message, T, in numerical form. This message T is divided into agreed size blocks that are converted to encoded cipher text, C, as follows: $C = \mathrm{mod}(T^{PubK}, N)$. In plain English, take the original message T, multiply it by itself PubK times, where PubK is a large integer corresponding to the public key. Then divide the resulting value by N (known as the modulus of the transformation) and save only the remainder.

David Rowe is president of the Infinity business unit at SunGard Trading & Risk Systems
e-mail: david.rowe@risk.sungard.com

In effect, we perform an operation that results in a large number, then throw away all the significant digits, saving only the small residual fraction! The trick is then to reconstruct the original inputs based on only the remainders from this calculation. It turns out that for some values of PubK and N, there exists another value PvtK (the private key) such that $\mathrm{mod}(C^{PvtK}, N) = T$. That is, applying the same transformation used to encrypt the original message to the cipher text, but with a different parameter in the exponent, results in reconstruction of the original text!

Only special combinations of the values PubK, PvtK and N will allow this encryption and decryption process to work. Without going into excessive detail, assume that N is the product of exactly two prime numbers. Values for PubK and PvtK that work must have a special relationship to N. This relationship is intimately tied to the number of integers that are relatively prime to N. This number of relative prime numbers is known as Euler's Totient function of N, and is written J(N).

Finding the number of such relative primes is easy if the prime factors of N itself are known. For PubK to have an inverse that will reconstruct the original text, it (and its inverse) must be relatively prime to J(N). Finding pairs of invertible keys is fairly easy given J(N), but without the prime factors of N, it is a much harder task to determine J(N) itself. As a result, knowing only PubK and N, finding PvtK is a practical impossibility provided N is sufficiently large to make determination of its prime factors a computational nightmare.

The value

Public key encryption addresses the important shortcomings of private key encryption.

Only one public key/private key pair (and an associated modulus) is needed for every participant in e-commerce transactions, not a secret key for every possible pair of participants, as is the case with private key encryption.

The knowledge needed to decode messages can be more restricted, since senders of messages need not know how (indeed generally are not able) to decrypt their own messages. Knowledge of the private key is restricted to the recipient only, and is therefore less likely to be compromised.

No advance agreement on, or transmission of, a common private key is needed for participants to communicate securely. Party A encrypts with party B's public key, and party B encrypts with A's public key. Each is then easily able to decrypt.

Public key encryption is also ideal for establishing sender verification, as use of the public and private keys is interchangable. Just as a message encrypted with the public key can be decrypted with the private key, so a message encrypted with the private key can be decrypted with the public key. So, a message that can be successfully decrypted with a person's public key can only have been prepared by use of the corresponding private key. This guarantees that the message originated from the owner of the public key, since this is the only person with the necessary knowledge of the corresponding private key to have prepared the message in the first place.

Obviously, public key encryption is a major enabling technology in a globally wired world. It allows fully secure communication over public networks, since no one but the intended recipient can reconstruct the content of a message. Indeed, a genuine public policy worry is that public key encryption will facilitate criminal activity. This was the rationale for the long-standing US prohibition on the export of strong encryption software. However, knowledge of how to implement strong encryption is easily available, and those with the strongest incentive to use it had no trouble doing so despite the export embargo.

The bigger worry is whether the approach will continue indefinitely to provide an iron-clad guarantee of privacy. Unlikely as it is, if an efficient method for factoring the product of two large prime numbers was discovered, it would have devastating implications for the security of global commerce. Let us hope that this possibility remains in the realm of theory. ■