Get SET Go!

The advent of Internet ushered in an era of information sharing. Now, with the emergence of e-commerce, safeguarding information, specifically the user information has assumed greater importance. In the good old days of just cash transactions, all that one had to do was to secure greenbacks and treasure chests. And security was mostly restricted to strong rooms and alarm systems.

However, with advances in banking practices, technology and increased customer preferences, safeguarding paper money is no longer a need. The money is intangible and nothing more than a set of ones and zeroes in the cyberzone. That is where the real problem of security lies. How do you identify a user in digital transactions? If by some means you identify the user, how sure can you be that he is the same person that he claims to be? And if all these are taken care of, what is the guarantee that the data channel that carries your precious information is not vulnerable to attacks?

As an answer to these nagging questions consumers and businesses are looking to reproduce some of the safeguards they rely on for traditional face-to-face transactions. The first is a strong assurance of the identities of the transacting parties similar to the physical world identity through presentation of credentials. The second is the ability to ensure transactions are both confidential and unchanged by the medium. Most of today's Internet transactions fail to meet these requirements. Take for example a typical e-commerce transaction. The only mode of e-commerce at this point of time is through money cards (credit, debit etc.). The e-commerce cycle consists of three nodal points—the point where the user enters his credit card details, the point where the merchant establishment downloads these details and punches them into an electronic data capture (EDC) device and the third point where the captured data is sent to the issuing bank for approval through the established channel of acquiring bank and Mastercard/Visa gateways. At each and every point in this cycle there is a potential threat of data loss. Some of the advances recently have ensured that most of the loopholes are plugged in this cycle, well not completely!

For example data integrity over info-channels is now ensured by secure socket layer (SSL) systems and the threat of data pilferage at the merchant site is effectively warded off through the introduction of a payment gateway. But one of the most daunting challenges of securing e-commerce is authenticating the end-user (i.e., assuring that the e-commerce firm's suppliers, partners, and customers are who they say they are). The most common security measure in use today is SSL, which is at best an incomplete and partial answer to the needs of Internet commerce. These drawbacks, due to the impersonal nature of SSL transactions, are effectively addressed by Secure Electronic Transaction or SET. The SET specification is an open technical standard for the commerce industry developed by Visa and MasterCard as a way to facilitate secure payment card transactions over the Internet. Through cryptography and a trust chain of digital certificates SET verifies cardholder and merchant validity while maintaining confidentiality and security.

Using a combination of public and private keys the message data is encrypted and decrypted at either end of the transaction. This safeguard system appears to be the most reliable for Internet commerce, but only just. It may not be long before the next great cyber-revolution would render this redundant.

But for now get SET and go!

G.P .Vinaybabu
vinayg@mm.strategicnewspapers.com