Global Information Assurance Certification Paper

SET for e-commerce security?
Nick Main

In today's world of computers, electronic commerce, and the enormous range of products made available to us by the prevalence of online shopping facilities, most consumers are still shy of the technology used to make it all possible. Why are people so hesitant to embrace this amazing technology that can bring such a world of possibility to our fingertips and front doors?

Security.

More particularly, it is the common perception that such technology has an intrinsic lack of security, and that perception prevents many consumers from accepting it as a safe transaction, and therefore it is not seen as a safe way to shop.

According to the CyberSource Fraud 2000 Survey [1], 81% of responding e-commerce businesses believe that online sales would increase significantly if online shoppers were not as concerned about fraud.

In the same survey, it was also revealed that an average of 4% of total transactions carried out by the respondent companies was fraudulent in nature! That means if a company were to process 100 transactions, 4 of them would likely be fraudulent. It doesn't sound like much, but when put into real terms, it becomes scary.

Imagine if a company sells a product at $110 per item. Assume their markup is 10%, so the cost to them is $100 per item. If the company takes in 100 orders, their theoretical net profit is $1000. If 4 transactions are fake, the loss from those transactions is $440, or 44% of their operating profit!
How many businesses would be happy in writing off 44% of their operating profit to fraud?

This paints a bleak future for the world of e-commerce without some significant changes to the way vendors authorise and process their online transactions. The fact that most companies can see the need for some sort of fraud mitigation system is a great place to start from, but getting to the point where all online business transactions are almost completely protected against fraud will be a long and arduous task.

Already big credit companies such as Visa, American Express and MasterCard are bringing their considerable size and influence into play and starting to require online vendors to comply to a strict set of security controls in order to accept payment methods from that institution.

It is only as recently as May 2000 [2] that these financial institutions have started to differentiate between "card-present" (eg swiping your card at the counter) transactions and the so-called "card-not-present" (eg telephone or internet) transactions. From this change the institutions are able to identify with greater precision the sources of the highest fraud. According to one report [2], while overall fraud is as low as 6 cents per

$100, the "card-not-present" fraud was significantly higher at 15-20 cents per $100.

To address this exact issue, Visa, in collaboration with other companies such as MasterCard, has developed an open standard that can be used by online merchants to enhance their operational security to a point where most of these fraudulent transactions can and will be prevented.

This technology standard, called Secure Electronic Transaction (SET) provides multiple layers of authentication and protection at every step of the purchasing process, and is maintained by a company called SETco [3]. All vendors and financial institutions must pass a strict security audit before becoming authorised to accept SET payment methods. Once accredited, the vendors must also regularly pass rigorous audits to maintain that accrediation.

SET is based on a number of major technologies, including multi-level (symmetric and asymmetric key) encryption, and digital certificates from a CA or Certificate Authority for absolute verification.

The process works as follows [4].

Note: This is an extremely simplified representation. For more detail please see the document "Secure Electronic Transaction Specification" [4] linked below.

1. The cardholder registers with Certificate Authority (CA) in a 7-step process that absolutely verifies the cardholders' identity and computer. An encrypted certificate is stored on the cardholders' computer, and if the cardholder wishes to use another computer, registration and validation must take place again for the new location.
2. Merchant / Vendor registers with CA in a 5-step process that also absolutely verifies the identity, location and legitimacy of the merchant. When successful, this step means that the merchant can now accept payment by the SET standard methods.
3. When a purchase request is made from a cardholder (ie, at a vendor clicks the Process Order or equivalent button):
    a. The cardholder software sends a digitally signed request to initiate a transaction to the merchant server.
    b. The merchant server verifies the cardholders certificate with the upline CA. The server then replies to the cardholder software with a digitally signed response, which includes the certificate for itself and its Payment Gateway.
    c. The cardholder software verifies the merchant and Payment Gateway certificates with the upline CA. There is now a trusted dialogue between the three parties, authenticated by the Certificate Authority.
    d. The cardholder software sends an encrypted message with a digital signature "purchase request", containing "Order Information" (OI) and "Payment Instructions" (PI). These fields are used by the merchant server to process the order and payment.

e. The merchant server decrypts the Purchase Request, and verifies the signature from cardholder.
f. Signed, encrypted message is sent to the Payment Gateway, including the Payment Instructions from the Purchase Request.
g. Payment Gateway decrypts and verifies message, verifies cardholder certificate with CA, and then sends signed, encrypted authorisation to financial institution. The Payment Gateway then responds to the merchant server with a Authorisation Response.
h. Merchant server decrypts and verifies the Authorisation Response.
i. The merchant server then sends an encrypted, signed Purchase Response to the cardholder computer.
j. Cardholder software decrypts and verifies the Purchase Response, and if verified stores the Purchase Response for future records (just like a receipt from a card-present transaction).
k. If the Payment Authority authorises the transaction, the merchant completes processing of the order, goods / services are then delivered to the cardholder.

This process is very secure, due to the implicit distrust that it requires. No single point unquestioningly trusts another, and requires authentication to proceed. This provides total accountability for the merchant, the Payment Gateway, and the end consumer. The merchant is protected against almost all fraudulent purchases, the Payment Gateway is protected because it only communicates with verified merchants, and the consumer is protected against misuse of his/her details.

This style of security is becoming more and more attractive to the small / medium e-commerce vendors. Businesses have to wear the consequences of any fraudulent transaction their system processes. When this powerful monetary incentive is combined with companies such as Visa implementing additional financial penalties on businesses that do not implement secure procedures, it becomes a motivation too strong to ignore.

There are other methods of secure payment, for instance token-based or hardware based authentication devices [5], but in terms of minimal impact to the consumer, a system such as that outlined above is one of the most appealing, despite the overheads in initial set-up.

E-business can not exist without good security. This is a reality of today's e-commerce environment, and all vendors must at least become aware of the implications of not securing their systems. Unhappy customers, litigation, and inevitably financial ruin are on the horizon for those that do not. If you work for or consult to an e-commerce business, ensure they understand the gravity of what could happen if they fail to secure the way they do business, and this type of solution may well be the one you suggest.

REFERENCES:

[1] CyberSource, "CyberSource Fraud 2000 Survey", 11/09/2000, URL: http://www.cybersource.com/fraud_survey/ (9/11/2000)

[2] Blankenhorn, Dana, "Visa Launches Web-Merchant Crackdown", 14/08/2000, URL: http://www.clickz.com/cgi-bin/gt/print.html?article=2222 (9/11/2000)

[3] SETco, URL: http://www.setco.org/ (9/11/2000)

[4] SETco, "Secure Electronic Transaction Specification", 31/05/2000, URL: http://www.setco.org/download/set_bk1.zip (9/11/2000)

[5] PaymenTech, URL: http://www.paymentech.com/ (9/11/2000)