Interested in learning more about security?

SANS Institute
InfoSec Reading Room

Shopping for Security

As the internet evolves and organizations establish or enrich their web presences, people are interacting with an evolutionary, exciting, and efficient technological tool for conducting business. Today, the public enjoys shopping and banking from the comfort of their home while companies save money on processing transactions and hiring employees. However, with any innovation, there are obstacles to overcome before the venture is deemed successful. In ebusiness, encompassing any transaction via the internet, the informa...

Shopping for Security

Kimberly Lemieux
GSEC: Assignment Version 1.4b (August 2002)

Introduction

As the internet evolves and organizations establish or enrich their web presences, people are interacting with an evolutionary, exciting, and efficient technological tool for conducting business. Today, the public enjoys shopping and banking from the comfort of their home while companies save money on processing transactions and hiring employees. However, with any innovation, there are obstacles to overcome before the venture is deemed successful. In e-business, encompassing any transaction via the internet, the information exchange can be as simple as providing your name and mailing address or as confidential as releasing your banking information. One of the most overwhelming issues at either end of the transaction is security. Has the merchant clearly explained security on the site or application? How strong is this security? What are the associated risks of conducting business with the service provider? Ultimately, does the consumer accept these risks?

Essentially, e-transactional security is a compromise between the consumer and the merchant. First, if a merchant accepts all the online business security risks, they start developing an interactive web presence adhering to the security measures for meeting potential clients' expectations. Similarly, the consumer conducts a risk assessment of the merchant's policies and security before engaging in a transaction. If they are dissatisfied with the merchant's security efforts, whether the policies are too complicated or interaction requires extensive effort, this discouraged consumer continues shopping. Not only does the frustrated prospect continue seeking the good/service/information offered by the original site, but most importantly, they look somewhere else…somewhere presenting credible security. This guideline serves as a tool to assist users in establishing and testing some baseline security measures as described in the E-User's Security Concerns. In addition, the merchant section explains more technical details about protecting their business and the customer's information, either in transit or storage. Some concepts include the use of digital certificates and encryption.

Glossary

e-business (electronic business): "conduct of business on the Internet, not only buying and selling but also servicing customers and collaborating with business partners. E-Business can be said to include *e-service*, the provision of services and tasks over the Internet by application service providers." (Nelson)

SSL (secure sockets layer): "a commonly-used protocol for managing the security of a message transmission on the Internet. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate." (Cusack)

PKI (public key infrastructure): "enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority." (Brayton et al.)

AVS (address verification service): "a risk management tool for merchants accepting transactions in which neither the card nor the cardholder are present. AVS helps reduce the risk of accepting fraudulent transactions by verifying the cardholder's billing address with the card issuer." (Merchant Commerce)

Mod 10 Algorithm: "technique for checking the validity of credit card numbers. The process only checks to make sure that the credit card number is within a set of numbers which are valid for that particular credit card." (Barry)

CVV2 (card verification value 2): "a three-digit security code that is printed on the back of cards. The number appears in reverse italic at the top of the signature panel at the end. This program helps validate that a genuine card is being used during a transaction." (Atlantic Payments Systems, LLC)

The E-User's Security Concerns

Although consumers demand rigorous internet security standards, they often overlook the insecurities of their daily activities. For public acceptance of e-transactions, people desire the same assurances they feel during an "in-person, card-present" transaction. Did this consumer forget about this evening's dinner when the waiter took the credit card from the owner's sight to complete the purchase? How can the consumer guarantee the security of this financial information? Ironically, this same person is hesitant to provide the credit card details over the internet because they are unsure how or if the data will be intercepted during transit or will this information assist in a future malicious activity? In comparison, the waiter holding the card could have copied the information for himself or perhaps, he was interrupted while walking to the cash register and he accidentally left the card on another client's table. Surprisingly, the total number of items as well as the dollar value of internet purchases continues to rise despite the consumer's unchanging concerns about privacy or security. For instance, a Statistic's Canada survey concluded "About 72% of households that made payments online opted to ignore their (security) concern and use their credit card online anyway." (Statistics Canada)

Legitimately, consumers are concerned about the security of a financial transaction over the internet. Can the information be intercepted? How do I know the company accepting my payment information is authorized? How do I know what happens to my personal information? Is it being redistributed? What happens if I am unhappy with the service or product provided? Without a doubt, these are all valid concerns and fortunately, there are ways that consumers can learn to protect themselves from fraudulent companies and ensure their own privacy and security.

This checklist is a guideline for users to consider before conducting online transactions. None of the features alone represent security, but use the list to determine a combination to suit personal risk tolerance: (Microsoft)

1. As a first choice, try shopping at well-known, reputable companies. Check if they are committed to a policy where they pay a deductible of $X (not covered by credit card companies) if your financial information is illegally used at their store.
2. Look for online seals including the Better Business Bureau or an authorized Certificate Authority (e.g., Verisign). These seals are only graphics and can be reproduced. Therefore, the seal alone does not exclusively constitute security but provides additional assurances.
3. Check the web site for accurate company contact details such as a physical address and phone number. If you feel more comfortable interacting with a sales representative, they will gladly assist.
4. Use a secure web browser. Thus, if the merchant's site has encryption available, the traffic between the client and the web server remains secret.

Before submitting any confidential information, check for encryption indicators shown in the diagram below. Each trait indicates the use of a server digital certificate to provide SSL (described in the merchant section).

a. HTTPS protocol: shown in the address bar
b. lock box: double click the padlock to retrieve valuable information about the certificate. A trusted authority such as Verisign, Thawte or Entrust should issue the certificate. Also, the expiration date should be valid.

(SANS, "Online Registration Form")

5. Review each web site's privacy policy. Look for details explaining if the company shares their data with other companies (e.g., Is your email address going to be sold to someone?). In addition, this policy should clearly state how the organization is protecting the information being submitted. For instance, the policy may state that credit card numbers are not stored on corporate servers. Thus, you must reenter the card information with each purchase. If there is no such policy or if it is unacceptable, the best idea is to take your business elsewhere.
6. Review each site's policies for security, shipping, and returning items. Watch for extra fees charged for shipping or restocking on returns. Again, if you are not completely satisfied, do not conduct business on a potentially unsafe site.
7. Be proactive and responsible for protecting your personal information. Do not provide social insurance numbers or bank account numbers without understanding why this information is being collected and how the company will process it. With the possible exception of government forms or completing a purchase, the numbers mentioned above are not

necessary for interacting with sites on the internet. If absolutely necessary, only provide this information in a secured area as mentioned in step 4.

8. Never share your passwords. Try using various passwords for different purposes in case one of them becomes compromised. Ensure passwords are difficult to guess and change them frequently.
9. Keep a printed invoice of all transactions made online. For instance, this future reference may be invaluable if there are fraudulent charges to your bank account. As well, to track these invoices, open important emails sent out by the vendor regarding the online activity.
10. Only open email or links that are safe. Unsafe clues are unknown email senders or web browser redirects into an unfamiliar areas. Do not proceed any further! Computers can be exposed to viruses or malicious code via these inappropriate links or emails.
11. Ideally, the consumer should obtain a credit card with a lower credit limit. The lower limit poses a smaller individual stake. Use this card exclusively for transactions via the internet.
12. Monitor the activity on this card carefully to detect its unauthorized use. Notify the appropriate personnel of any problems, including the bank and law enforcements. Notify the banking institution immediately if your card becomes lost/stolen or if there have been unauthorized purchases or cash advances.

The Secure Merchant

Obviously, people are interested in the convenience of shopping, banking, applying for jobs, etc from their personal computers. In turn, companies strive to attract or maximize consumer loyalty by implementing a safe location to engage in these activities. However, clients are frequently so preoccupied with their own security concerns that they consequently disregard the merchant's high stakes. As consumers, we think our personal stakes are high. But, developing, maintaining, hosting, and conducting business on the internet, with unfamiliar shoppers, is a far more risky investment undertaken by service providers. In parallel to users, e-businesses must also protect themselves from malicious users intending to commit fraud, misrepresenting themselves or stealing information either stored on a computer or in transit. These companies must take precautionary measures to meet or preferably exceed the public's expectations to provide a safe working environment for surfers and a profitable environment for themselves.

Starting with the fundamentals of any business, companies establish and follow comprehensive policies. Some of the necessary procedures, applicable to even an offline company, include processes to manage shipping, refunding, privacy/processing of personal/financial information, and security. On the internet, these policies strongly contribute to e-business success, especially if they are clearly documented and available to all potential customers surfing the web. Other forms of documentation needed for online transactions are invoices of the actions executed at a specified date or time. For example, some financial institutions require a statement to provide a tracking number while not recording any credit card numbers.

Below is a protection checklist for new merchants joining the online transactional ranks: (Merchant Fraud Squad), (Visa), (Strom)

1. Develop policies for shipping, refunding, personal/financial information processing, and security. Provide straightforward, descriptive navigational links from all interactive areas. Ensure the public understands the terminology within these documents.
2. Provide transactional documentation. Upon transaction completion, provide a printable invoice as a summary of the events. Include the date/time, tracking number, client's name and address, an itemized list of events or purchases, total cost (if applicable), and an email address or phone number to contact when problems arise.
3. As a minimum security rule, implement a firewall to protect the network. As well, an Intrusion Detection System (IDS) is beneficial for detecting unauthorized access or attempts to break into systems.
4. Stay current with security patches on all devices, operating systems and other software. Subscribe to memberships of security bulletin release programs offered by software vendors or generic security providers. Then, as new updates become available, the site administrator receives up-to-date problem assessments and resolutions. Carefully review the article and determine if enterprise systems are affected by the vulnerability. Take appropriate precautionary measures.
5. Log all daily activities. Confirm that IP addresses are being tracked in log files. Although these can be spoofed (forged), this is the most traceable piece of evidence gathered. Other important characteristics in logs include usernames, links, time and date stamps, and numeric server page return codes.
6. Monitor the site's daily usage and interactivity. Conduct trend analysis and usage reports on traffic and transactions. Investigate baseline deviations.
7. Get to know the clientele and their interests. In addition, carefully monitor orders for fraudulent indicators such as:
    a. Clients using free email services
    b. High risk, international shipping addresses
    c. Large total dollar amount orders
    d. Multiple, expensive items
    e. Multiple purchases within short time spans
    f. Rush delivery orders
    g. Single credit card attached to multiple shipping or billing addresses
    h. Similar credit card numbers being used (indicates automated number generator)
    i. Require identical shipping and billing addresses on each order

j. Invalid credit card numbers. Test each entry against the Mod 10 Algorithm before submitting it to the payment gateway. Not only does this prevent the acceptance of nonexistent cards but it also reduces chargebacks.

8. Contact law enforcements and financial institutions when criminal activity is suspected. Ensure there are log files as evidence to confirm your conclusions.
9. Protect stored data. Store client and transaction data in a database on a server that is not directly connected to the internet. If possible, encrypt this content on the server.
10. Use address verification (AVS) if it is available to your company. Cross referencing the order's billing address and postal code against the address details on file with the credit card issuer returns a match degree code. For example, 1 indicates a perfect match and 2 is a partial match (maybe postal code only). Each business selects an acceptable code for determining whether processing continues or if a rejection message is returned to the browser.
11. Require the card verification value 2 (CVV2). This 3-digit number on the back of credit cards aids in proving physical possession of the card.
12. Keep track of the "bad guys". Maintain a database of all problematic IP addresses, domain names, customers, addresses and use this information as an additional security check before fulfilling requests.

Aside from the consumer driven checks, the merchant needs to provide a few other complex services to ensure the customer's expectations can be reached. This includes special protocols for traffic scrambling techniques and merchant validation technologies.

Merchants need to promote security of transactions. Secure transactions comprise of the four characteristics listed below: (Curry, p.4), (Netscape)

1. Confidentiality: the content of the traffic remains private. Encryption ensures that unauthorized people cannot read it.
2. Authentication: confirms the identity of originator as a trusted source, which eliminates impersonation.
3. Non-repudiation: prevents denial of the information exchange process. Digital signatures provide accountability.
4. Integrity: enables recipient to confirm that information was not altered in transit. Use encryption and digital signatures to accomplish this goal.

Digital technology adopts PKI (public key infrastructure) to reinforce these prerequisites for safeguarding patrons. PKI utilizes digital signatures, certificates and cryptography techniques to provide special policies and software.

Encryption

Encryption scrambles plain text traffic, rendering it as unintelligible to anyone trying to intercept it, until the receiver decodes the message. There are two common types of encryption: symmetric and asymmetric.

Symmetric: sender and receiver share the same codes. The scrambling process uses a code to encrypt and the receiver uses that same code to descramble the content. This encryption exhibits faster performance but it is easier to break.

Original message → encoded message → decoded message
M i s s i s s i p p i → 7 4 A A 4 A A 4 N N 7 → M i s s i s s i p p i
Translator code: M=7, i=4, s=A, p=N

Asymmetric: This is the most commonly used cryptography. This type of encryption utilizes a key-pair consisting of a unique public and private key. The public key is published while the private key remains a secret (optionally password protected). Because the keys are different, data encrypted with your public key is only readable with your private key.

Encryption's strength is determined by the size of the keys being used. Most commonly, encryptions strengths are either 40-bit (low) or 128-bit (high). The larger the bit length, the more challenging the secret code becomes to break. To demonstrate the variability between high and low, the high encryption is trillions of times strong than its counterpart; it would take about a trillion trillion years to crack 128-bit encryption. For web page security, the functional strength of the encryption depends on a combination of the server and the browser. The table below outlines the results:

Client possesses:	**Server requires:**	**Resulting Encryption**
High encryption	High encryption	High encryption
High encryption	Low encryption	Low encryption
Low encryption	Low encryption	Low encryption
Low encryption	High encryption	No Access

Try this link to determine browser's encryption capabilities:
http://verisign.netscape.com/advisor/

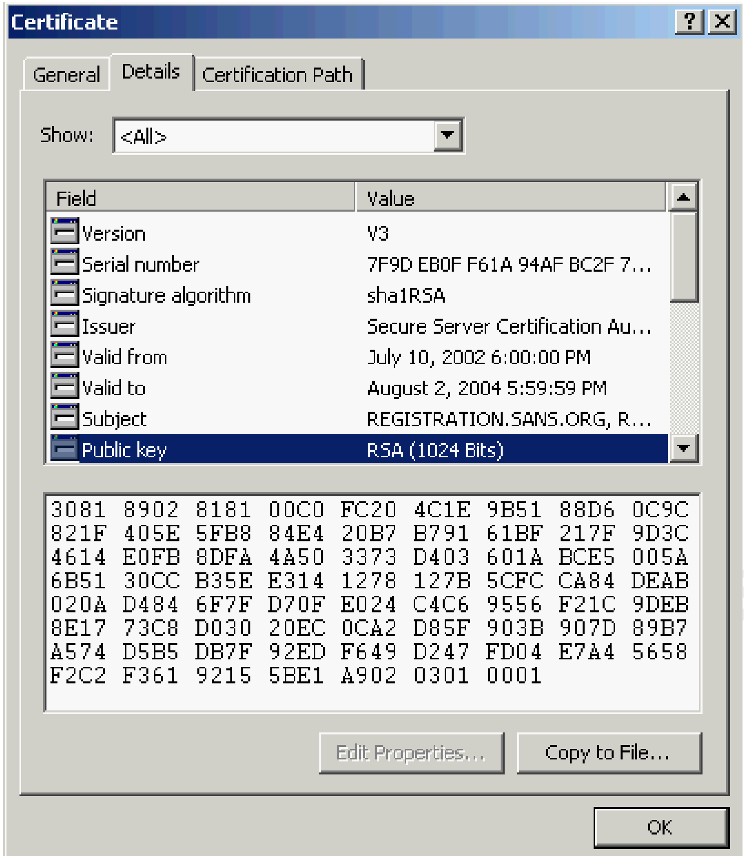
Digital Signatures and Certificates

To rectify impersonation, accountability, and integrity issues, use digital signatures and certificates. A digital signature is simply the signing of an electronic document. Just as a paper signature verifies that the signing party commits to the terms in a document, the electronic signature serves the identical purpose. However, an electronic signature is more beneficial than its paper counterpart because it is more easily verifiable and reliable, ensuring non-repudiation. As opposed to a paper signature, which is always identical, PKI enables an electronic signature to differ vastly, even with only a single, small change to the content being protected.

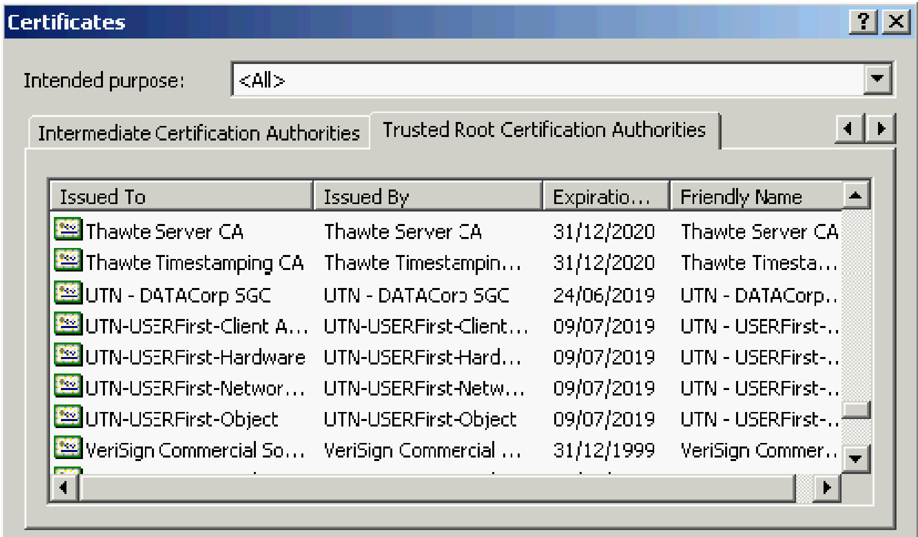
The digital signature process (with optional encryption for enhanced safeguarding) is as follows:

1. Start with the original information.
2. Use signing software to produce a one-way hash (A hash is a mathematical formula producing a unique fixed length string which cannot be computed).
3. Encrypt the hash with your private key.
4. Send detail to recipient to be validated.
5. Recipient decrypts message via public key.
6. Use the identical hash function (math formula) to produce another one-way hash.
7. Compare the new hash to the original. If they are the same, the data was not altered in transit. However, determining the identity belonging to the signature via a digital certificate remains unresolved thus far.

Next, obtain the corresponding digital certificate. This certificate associates a person, company, server, etc with a public key. Basically, the certificate verifies the identity of the "Issued To" entity thereby preventing impersonation. Certificates include an issue date, expiry date, the name, address, and public key of the certificate applicant, and the digital signature of the certificate authority. When a consumer clicks on the lock box , these attributes appear as shown in the example from SANS's online registration area (SANS, "Online Registration").



Now that the certificate's attributes are clearly displayed, decide whether or not to accept the document as originating from a trusted source. The prospect trusts the certified entity based on the trust of the third-party that issues the certificate, the Certificate Authority (CA). The certificate authority investigates all applicants to consequently guarantee their credibility and legitimacy of business operations. By default, web browsers accept certain Certificate Authorities as automatically trusted, including Verisign or Entrust. Users can freely add new trusted authorities to their browsers or remove any questionable sources. Nevertheless, to securely communicate, the user must accept the authority as reliable and ensure they possess the CA's public key within their browser's trusted authorities list pictured below.



<u>Secure Sockets Layer</u> (SSL) (Verisign, "Building an E-Commerce Trust Infrastructure")
The most popular infrastructure for protecting e-commerce sites is through the implementation of SSL, a protocol originally designed by Netscape Communications. SSL encrypts plain text and later decrypts unintelligible traffic to provide secure, unreadable communication between a client and a server. Not only does SSL provide confidentiality of this information, but it also provides authentication (using certificates) and protects the integrity of data. The process begins as a handshake to negotiate the keys and algorithms to be used during the session, resulting in common data computations. Once the communication channel is established, all passing data is secret. This includes usernames, passwords, data on form submissions, and confidential URL requests.

The SSL process for secure data exchange where the server authenticates itself to the client is as follows:

1. User connects to a web site on a secured URL that begins with *https://.* For instance, this may be a registration web page where the commerce site accepts a credit card number and password as authentication.
2. The client's browser sends its encryption information to the hosting server. This information outlines the browser's capabilities for SSL, including SSL versions, encryption settings and some randomly generated data.
3. To continue with the negotiation process and hopefully generate a communication channel, the server responds with its digital certificate, SSL versions and encryption capabilities.
4. Next, the client authenticates the server by:
    a. Examining the certificate for a valid date
    b. Determining if the certificate authority is included in the browser's trusted list (or the digital certificate needs to be manually approved)
    c. Verifying the domain name requested matches the one in the certificate

If all criteria are satisfied, the client's browser establishes a unique session key for future secure data exchange. Otherwise, the client receives a warning message that a secured channel cannot be established.

5. As an initial test of the communication channel, the client's browser encrypts test data with the public key originally transmitted in the server's certificate. This message is sent to the server where it is decrypted with the server's private key.
6. The client and server each exchange messages stating that the future communications will be encrypted with this session key generated in the previous step. As well, each entity sends a separate message stating that its portion of the handshake process is complete.
7. The SSL negotiations are complete and transmissions continue using the one-time symmetric session key.
8. When the session terminates, the session key is discarded.

(Verisign, "Guide to Securing Your Web Site for Business", p. 3)

<u>Secure Electronic Transactions</u> (SET)

SET protocol, a less popular alternative to SSL, was developed as a joint effort by Visa and MasterCard. SET is based on digital certificates to confirm all the identities, consumer and merchant, involved in a transaction. Again, it provides encryption of internet traffic. SET uses the strong, 128-bit encryption for things such as financial information. Because this protocol is exempt from the US

Export Restrictions (in cryptography), this transmission encryption cannot be used for something like the description of goods being sold. Unlike SSL, SET also authenticates the user to the business. Therefore, it is more difficult to use stolen credit cards. And, with SET, the protocol completely restricts access to financial information. For example, in SET, any data destined to a financial institution is encrypted with the bank's public key while information about the purchase that pertains to the merchant, is encrypted with the merchant's public key. This eliminates a third party risk such as a hacker breaking into a corporate server and stealing client's credit card numbers since the merchant never sees this. Because SET is more complex and costly, it is not becoming as popular as other methodologies.

Merchants wishing to use SET must purchase special software to accept this payment. In addition, they need a merchant certificate from their bank where their digital account resides. Consumers desiring SET's protection require a digital wallet and a personal digital certificate. Currently, users download and install wallet software. During installation, the product collects details about credit cards available, client's name, a PIN number, and a password. In the future, internet browser developers wish to provide a built-in wallet available in their software. Next, the user needs a digital certificate for each credit card they wish to use on the internet. The bank issues this personal certificate to their clients based on successful answers to personal questions. Now, the bank validates you are who you say you are and that you are the rightful owner of the credit card. Finally, at time of purchase, the user selects to pay via SET. Then, their wallet opens and they choose which credit card to use as payment. Although SET provides an additional layer of security, it is an increasingly complex technology for potential shoppers to understand, hindering its growth.

<u>What's Next?</u>
Now that some of the current basics of security online have been discussed, we need to consider what the future brings to the internet. Since technology improves so rapidly, we need to consider these updates and determine how technology can continue to be secure.

1. How is changing hardware and communication channels affecting online business?
Since handheld devices and cellular phones are becoming smarter, I thought the next big commerce move would be towards "m-commerce", mobile-commerce. However, after researching, I discovered Visa's futuristic concept of "u-commerce", universal-commerce. Of course, their prospect is even more encompassing than wireless networks, including everything from television to infrared communications in their business model. With data traveling on so many new, open channels and devices, there needs to be strong developments in the protection of personal information and authenticating all those involved in virtual transactions. Visa's ultimate goal is to produce an interconnected, interdependent world where consumers can pay for something electronically and

at the same time, update a personal bank book and budget, receive an electronic receipt, and update the financial institution's data. How does the security of all the parties involved in this single transaction affect one another when they are so tightly linked?

2. How can the internet achieve uniformity and universality in online shopping, banking or forms submissions sites?
To make security easier for consumers, there needs to be uniformity. Adopting non-technical, universal terms for speaking about e-commerce and security is a great start.

Another idea for extended functionality is implementing personal digital certificates. Since setting up a client certificate is challenging for users, perhaps the certificate could serve a more universal purpose. It could enable people to access a mall where they can shop at multiple stores for different needs, such as food and clothing. Or, for example, the use of personal certificates may enable users to access only various areas of a site based on identity verification for online banking situations. Also, technology can perhaps minimize security complexities by using this same certificate to manage a user's digital wallet. Finally, with personal certificates, users can expand their communication from a web site to secure email. Now, at your convenience, you can discuss personal matters over email, shop online, and merchants can offer restricted accessibility.

Microsoft has started looking into uniformity with their MS .NET Passport functionality. The sign on service allows users to sign into participating sites using only a single set of logon credentials. For example, Microsoft's .NET Passport's extensibility enables user authentication to web sites across various devices and applications. In addition, people can access multiple vendors using this same authentication. Undoubtedly, this means fewer usernames and passwords to remember, promoting using a complex password to offer increased protection. The passports also support the Express Purchase functionality with similar wallet functionality as described in SET but it uses SSL encryption.

3. What can other organizations do to aid in security enhancements?
Establish a government agency or a government partnership with a reputable company to assist users and companies in learning about security. Education is the most important asset to grow online commerce. Teach users about insecurities, problematic companies and people that may have been involved in previous international fraudulent activities. Maintain a central portal of scams conducted through web or email campaigns. For example, the econsumer.gov site is trying to develop this centralization scheme. The involvement of consumer-oriented agencies, such as Federal Trade Commissions and Better Business Bureaus, can use their established trusts to help people make informed decisions about security.

Also, the law needs to play a more prominent role in dealing with insecurities. There will never be a time where security is a guarantee; risks will always exist. Thus, there needs to be processes to determine what constitutes electronic illegalities. Aside from identifying problems, legislations must address these occurrences with punishments or penalties.

Finally, if I speak of the informed consumer, they not only need to be aware of security within their control, they also need to be informed about insecurities beyond their access. The law needs to adopt policies stating that companies must report successful break-ins to enterprise systems. How can users protect themselves when they are unaware of the misuse of their personal information? It should be mandatory to report security breaches such as gaining accessing to corporate databases or exposing financial information without regard to a company's reputation. For instance, California is working on state legislation to mandate the report of any computer security breaches.

These are only some ideas of how to take safe data exchange into the future. Consumers need to offer more input on how effective existing security measures are and what types of improvements will allow them to more comfortably enjoy their online ventures. Without a consumer willing to conduct business on the internet, there is no economic drive to develop the e-commerce initiative.

References

Atlantic Payment Systems, LLC. “Card Verification for Card-Not-Present Sales”. 13 January 2003. URL: http://www.atlanticpayment.com/cardterms/index.htm (20 January 2003).

Barry, Wayne. “Mod 10 Credit Card Check”. URL: http://www.15seconds.com/issue/970101.htm (20 January 2003).

Brayton , Jim, Finneman , Andrea, Turajski , Nathan, Wiltsey , Scott. SearchCIO.com Definitions. 4 August 2001. URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214299,00.html (13 December 2002).

Curry, Ian, “An Introduction to Cryptography and Digital Signatures”. V 2.0. March 2001. URL: http://www.entrust.com/resources/pdf/cryptointro.pdf (9 Dec. 2002).

Cusack, Brendan. SearchCIO.com Definitions. 5 September 2001. URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci343029,00.html (13 December 2002).

MasterCard. “Here’s How SET Works”. New Technology: E-Commerce Security. URL: http://www.mastercardintl.com/newtechnology/set/howsetworks.html (26 January 2003).

Merchant Commerce. “Online Commerce Suite”. 2002. URL: http://documentation.innuity.com/faq.htm#faq1 (20 January 2003).

Merchant Fraud Squad. “Fraud Fighting 101”. URL: http://www.merchantfraudsquad.com/Members/membpages/fighting.asp (22 January 2003).

Microsoft. “.NET Passport Review Guide”. November 2002. URL: http://www.microsoft.com/net/downloads/passport_review_guide.doc (25 January 2003).

Microsoft. “Take a Few Precautions when Shopping Online”. 13 November 2002. URL: http://www.microsoft.com/security/articles/holiday_shopping.asp (15 December 2002).

Nelson, Tim D. seachCIO.com Definitions. 26 July 2001. URL: http://searchcio.techtarget.com/sDefinition/0,,sid19_gci212026,00.html (13 December 2002).

Netscape. “Introduction to Public-Key Cryptography”. DevEdge Online Documentation. 09 October 1998. URL: http://developer.netscape.com/docs/manuals/security/pkin/ (25 January 2003).

Salkever, Alex. “Computer Break-Ins: Your Right to Know”. 11 November 2002. URL: http://www.businessweek.com/technology/content/nov2002/tc20021111_2402.htm (24 January 2003).

SANS. Welcome to SANS Orlando Registration. 2002. URL: https://registration.sans.org/cgi-bin/Orlando_register (25 January 2003).

Schapp, Stephen, Cornelius, Richard. “U-Commerce: Leading the New World of Payments”. URL: http://corporate.visa.com/av/ucomm/u_whitepaper.pdf (26 January 2003).

Statistics Canada, “Electronic commerce: Household shopping on the Internet.” The Daily. 19 September 2002. URL: http://www.statcan.ca/Daily/English/020919/d020919b.htm (9 Dec. 2002).

Strom, David. “E-commerce Security, Locking Up Your Web Storefront”. Searchseacurity.com Webcast. 21 May 2002. URL: http://searchsecurity.techtarget.com/webcastsTranscriptSecurity/1,289693,sid14_gci809032,00.html (29 December 2002).

Treasury Board of Canada Secretariat. “PKI for Beginners”. 20 June 2001. URL: http://www.cio-dpi.gc.ca/pki-icp/beginners/beginners_e.asp. (26 January 2003).

Verisign. “Guide to Securing Your Web Site for Business”. 2002. URL: http://www.verisign.com/resources/gd/secureBusiness/index.html (24 January 2003).

Verisign. “Building an E-Commerce Trust Infrastructure: SSL Certificates and Onine Payment Services”. 2002. URL: http://www.verisign.com/resources/gd/buildEcommerce/index.html (25 January 2003).

Visa. “Visa E-Commerce Merchants’ Guide to Risk Management: Tools and Best Practices for Building A Secure Internet Business”. 2002. URL: http://usa.visa.com/media/business/ecomm_merch_guide.pdf. (12 January 2003).

Last Updated: May 26th, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Atlanta 2018	**Atlanta, GAUS**	**May 29, 2018 - Jun 03, 2018**	**Live Event**
SEC487: Open-Source Intel Beta Two	**Denver, COUS**	**Jun 04, 2018 - Jun 09, 2018**	**Live Event**
SANS Rocky Mountain 2018	**Denver, COUS**	**Jun 04, 2018 - Jun 09, 2018**	**Live Event**
SANS London June 2018	**London, GB**	**Jun 04, 2018 - Jun 12, 2018**	**Live Event**
DFIR Summit & Training 2018	**Austin, TXUS**	**Jun 07, 2018 - Jun 14, 2018**	**Live Event**
Cloud INsecurity Summit - Washington DC	**Crystal City, VAUS**	**Jun 08, 2018 - Jun 08, 2018**	**Live Event**
Cloud INsecurity Summit - Austin	**Austin, TXUS**	**Jun 11, 2018 - Jun 11, 2018**	**Live Event**
SANS Milan June 2018	**Milan, IT**	**Jun 11, 2018 - Jun 16, 2018**	**Live Event**
SANS Cyber Defence Japan 2018	**Tokyo, JP**	**Jun 18, 2018 - Jun 30, 2018**	**Live Event**
SANS Oslo June 2018	**Oslo, NO**	**Jun 18, 2018 - Jun 23, 2018**	**Live Event**
SANS Philippines 2018	**Manila, PH**	**Jun 18, 2018 - Jun 23, 2018**	**Live Event**
SANS ICS Europe Summit and Training 2018	**Munich, DE**	**Jun 18, 2018 - Jun 23, 2018**	**Live Event**
SANS Crystal City 2018	**Arlington, VAUS**	**Jun 18, 2018 - Jun 23, 2018**	**Live Event**
SANS Minneapolis 2018	**Minneapolis, MNUS**	**Jun 25, 2018 - Jun 30, 2018**	**Live Event**
SANS Cyber Defence Canberra 2018	**Canberra, AU**	**Jun 25, 2018 - Jul 07, 2018**	**Live Event**
SANS Paris June 2018	**Paris, FR**	**Jun 25, 2018 - Jun 30, 2018**	**Live Event**
SANS Vancouver 2018	**Vancouver, BCCA**	**Jun 25, 2018 - Jun 30, 2018**	**Live Event**
SANS London July 2018	**London, GB**	**Jul 02, 2018 - Jul 07, 2018**	**Live Event**
SANS Cyber Defence Singapore 2018	**Singapore, SG**	**Jul 09, 2018 - Jul 14, 2018**	**Live Event**
SANS Charlotte 2018	**Charlotte, NCUS**	**Jul 09, 2018 - Jul 14, 2018**	**Live Event**
SANSFIRE 2018	**Washington, DCUS**	**Jul 14, 2018 - Jul 21, 2018**	**Live Event**
SANS Malaysia 2018	**Kuala Lumpur, MY**	**Jul 16, 2018 - Jul 21, 2018**	**Live Event**
SANS Pen Test Berlin 2018	**Berlin, DE**	**Jul 23, 2018 - Jul 28, 2018**	**Live Event**
SANS Cyber Defence Bangalore 2018	**Bangalore, IN**	**Jul 23, 2018 - Jul 28, 2018**	**Live Event**
SANS Riyadh July 2018	**Riyadh, SA**	**Jul 28, 2018 - Aug 02, 2018**	**Live Event**
Security Operations Summit & Training 2018	**New Orleans, LAUS**	**Jul 30, 2018 - Aug 06, 2018**	**Live Event**
SANS Pittsburgh 2018	**Pittsburgh, PAUS**	**Jul 30, 2018 - Aug 04, 2018**	**Live Event**
SANS August Sydney 2018	**Sydney, AU**	**Aug 06, 2018 - Aug 25, 2018**	**Live Event**
SANS San Antonio 2018	**San Antonio, TXUS**	**Aug 06, 2018 - Aug 11, 2018**	**Live Event**
SANS Boston Summer 2018	**Boston, MAUS**	**Aug 06, 2018 - Aug 11, 2018**	**Live Event**
SANS Hyderabad 2018	**Hyderabad, IN**	**Aug 06, 2018 - Aug 11, 2018**	**Live Event**
Security Awareness Summit & Training 2018	**Charleston, SCUS**	**Aug 06, 2018 - Aug 15, 2018**	**Live Event**
SANS Amsterdam May 2018	**OnlineNL**	**May 28, 2018 - Jun 02, 2018**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**