Global Information Assurance Certification Paper

Public-Key Infrastructure And Online Banking

Blair Campbell
November 13, 2000
GIAC Security Essentials

Introduction

An Angus Reid Group finding points out that while those in the Canada and the U.S. have not been as quick to embrace online banking as compared to Europeans, that number is growing. However, a recently released survey by the American Express Company states that although at least three out of every five North Americans have access to the Internet, many are still reticent to utilize online services to make purchases or execute financial transactions. Almost 79% of those queried expressed concern with regards to security and privacy issues. Are these apprehensions warranted?

Background

A private-key or symmetric system requires that both the information sender and receiver share a single key that is used to encrypt and decrypt data. Securely distributing the key is cumbersome and difficult with its greatest pitfall being the loss or compromise of the key makes the information it encrypts vulnerable. In 1976, Whitfield Diffie and Martin Hellman published a revolutionary paper titled, "New Directions in Cryptography," which introduced the concept of public-key or asymmetric cryptographic keys. A public-key system utilizes two complementary keys: a public-key, which is designed to be shared, and a private-key that is secret. They created a formula, the Diffie-Hellman algorithm, that allowed a practical public-key cipher for both confidentiality and digital signatures, based on the difficulty of factoring large numbers. Considering that "New Directions in Cryptography" was released almost a quarter of a century ago, the concepts found in Diffie and Hellman's paper allow today's e-commerce, Internet, and intranets to operate with a high degree of integrity.

Public-Key Infrastructure (PKI)

The function of a Public-Key Infrastructure is to simplify the use of public-key exchange and to protect information assets by including the following essential elements:

Privacy – the ability for confidentiality

Authentication – the capacity to establish identity

Integrity of data – to ensure that data has not been altered

Non-repudiation – to provide irrefutable evidence that an action has occurred

Keep in mind that Public-Key Infrastructure isn't a physical object or software program; it encompasses public-key technology, supporting applications, policies, practices, standards, and law. Completing the critical components of PKI are digital certificates and certificate authorities. The best definition regarding both can be found at Netscape's "Understanding PKI" page.

> Digital Certificates – Digital certificates are electronic files that act like a kind of online passport. They are issued by a trusted third party (i.e. Verisign), a certificate authority (CA), which verifies the identity of the certificate's holder. They are tamper-proof and cannot be forged. Digital certificates do two things: Authenticate that their holders - people, web sites, and even network resources such as routers - are truly who or what they claim to be. Protect data exchanged online from theft or tampering.
>
> It's important to note that there are two separate digital certificates: a server certificate for the user and a personal certificate for the host.
>
> Digital certificates utilize the following standardized protocols which have been adopted for electronic communication: SSL (Secure Sockets Layer) for web browser and server authentication, and secure data exchange, Secure Multipurpose Internet Mail Extensions (S/MIME) for e-mail and electronic data exchange (EDI), Secure Electronic Transactions (SET) for electronic payments, and Internet Protocol Secure Standard (IPSec) for authenticating network devices.
>
> Certificate Authorities - Certificate authorities (CAs) are the digital world's equivalent of passport offices. They issue digital certificates and validate the holder's identity and authority. CAs embed an individual's or an organization's public key along with other identifying information into each digital certificate and then cryptographically "sign" it as a tamper-proof seal, verifying the integrity of the data within it and validating its use.

A Banking Case Study - Scotiabank PKI (Public-Key Infrastructure)

Scotiabank (Bank of Nova Scotia) was founded in 1832 and is a full service financial institution that provides retail, commercial, corporate, investment, and international banking services to customers around the world. Scotiabank employs approximately 41,000 people in their 1,600 branches and offices in more than 50 countries.

In September 1997, Scotiabank teamed with Entrust Technologies, who are widely regarded as leaders in cryptographic security, to launch its Scotia OnLine service. The service avails their customers an ability to bank 24 hours a day using either Microsoft's Internet Explorer or

Netscape.

The following is an excerpt form Scotiabank's Fall 1998 VAQ Newsletter : "Last month, a 1998 Canadian Information Productivity Award was given to Scotiabank for Scotiabank PKI (Public-Key Infrastructure), a program that has set global standards for Internet security. Acceptance of the program has exceeded expectations and has made Scotiabank the largest certificate issuer on the Internet."

How It Works

Prior to banking online, the client of the bank must possess four items: a ScotiaCard (think ATM), a password which they control, Internet access, and Internet Explorer 4.0 or higher or Netscape 4.08 or higher because of their built in security measures.

Once the user has connected to the Internet, they then proceed to Scotia's OnLine service sign-on page. There, they enter their ScotiaCard number and password in the given fields and enter the site's secured area. From this point clients can receive current account balances, pay bills, transfer funds, view latest credit card transactions and statements. Another feature of Scotia OnLine lets users move between banking and brokerage transactions during the same session without having to enter separate passwords. After the transaction is complete, the connection with Scotia OnLine is closed by clicking the "Sign-Off" link at the bottom of the page.

Safeguards

Scotia OnLine's service outlines the following significant components it has incorporated into their PKI: Scotiabank issues its own public-key certificates which can only be used with Scotia OnLine services and are not transportable to other systems. By using a unique public-key certificate for each customer this gives assurance that what is sent is what is received. Passwords are verified at the customer's computer thus not transmitted over the Internet, minimizing the risk of "identity theft" as the customer has control of their electronic identity. The PKI is controlled end-to-end and directly secured by the bank greatly reducing web site spoofing of Scotia OnLine and ensures that the customer is only communicating to Scotiabank. All customer transactions and information is encrypted for privacy and confidentiality, as well as, being digitally signed, creating end-to-end integrity of the data. A reference number is provided after every online transaction.

Client's Responsibilities

Scotiabank has gone to great lengths to ensure the online session is private and secure but, as the saying goes, the chain is only as strong as its weakest link. The customer must also follow simple but important computer security procedures to protect their information. The bank strongly recommends that its clients "install and keep up to date a proven anti-virus product, only accept or download software from a source that you believe to be trusted, and keep passwords and pass-phrases secret (even from family members)." They also provide useful computer security links to these sites: Home Hack-Ins Article at Canoe.ca, The "Lines of Defense" feature at ZDNet, High-

Speed Security Issues at Sympatico.ca, and Network Architecture And Security Issues at rogers.home.com. Security can be taken one step further by verifying the site's certificate. Clicking on the padlock icon at the bottom of the browser allows the user the ability to view its security information. Finally, upon closing their session, the client is taken to a page that suggests that they clear their browser's cache. If the user is unsure how to do it, Scotia OnLine provides clearly outlined directions on their site for both Microsoft and Netscape browsers.

Conclusion

While the majority of North Americans that have Internet access express reservations about using online services to execute financial transactions, more and more are are begining to understand and trust those that are available. Paul K. Wing, Vice-President, System Security and Controls at Scotiabank states, "As of April 28, 1998 Scotiabank had issued 40,000 public-key certificates, making it the largest digital Certification Authority in Canada…As of January 2000 the bank reached 150,000 active customers." When proper security measures are implemented and utilized by both the financial institution and its clients, online banking is effortless and safe.

References

[1] "Canada Among World Leaders In Adopting On-Line Banking." Ipsos Reid. 20 June 2000. URL:
http://www.angusreid.com/media/content/displaypr.cfm?id_to_view=1049 (24 October 2000)

[2] "21 Per Cent Of U.S. Internet Users "Very Likely" To Try Online Banking." Ipsos Reid. 20 June 2000. URL:
http://www.angusreid.com/media/content/displaypr.cfm?id_to_view=1050 (24 October 2000)

[3] "The World Is A Small Place When It Comes To Online Attitudes And Actions." American Express. 24 October 2000. URL:
http://home3.americanexpress.com/corp//latestnews/gis2000.asp (24 October 2000)

[4] "Understanding PKI." Netscape. Last updated 17 May 2000. URL:
http://verisign.netscape.com/security/pki/understanding.html (24 October 2000)

[5] "Corporate Overview." Verisign – Corporate Overview. URL:
http://www.verisign.com/about/index.html (24 October 2000)

[6] "MS Windows 2000 Public Key Infrastructure." Microsoft TechNet. Last updated 12 January 2000. URL:
http://www.microsoft.com/TechNet/win2000/win2ksrv/prodfact/2000pk.asp (24 October 2000)

[7] Ellison, Carl. "Cryptography Timeline." 2 June 1996. URL:
http://world.std.com/~cme/html/timeline.html (24 October 2000)

[8] Palmgren, Keith. "Diffie-Hellman Key Exchange – A Non-Mathematician's Explanation."

Security Portal. 6 June 2000. URL:
http://www.securityportal.com/topnews/dhkeyexchange20000706.html (24 October 2000)

[9] "Entrust And Scotiabank - Securing the Future of Internet-based Electronic Commerce." Entrust Technologies. Last updated 27 September 2000. URL:
http://www.entrust.com/success/scotiabank.htm (28 October 2000)

[10] "All About PKI…What is a Public Key Infrastructure?" Entrust Technologies – Security Product Solutions – Public-Key Infrastructure (PKI) - All About PKI…What is a Public Key Infrastructure? Entrust Technologies. Last updated 20 September 2000. URL:
http://www.entrust.com/products/pki/pki.htm (28 October 2000)

[11] "Security With Entrust." Scotia Online - Security With Entrust. Scotiabank. URL:
http://www.scotiabank.ca/FAQSec1.html (28 October 2000)

[12] "Top 10 Advantages of Scotia Online Security with Entrust." Scotia Online - Top 10 Advantages of Scotia Online Security with Entrust. Scotiabank. URL:
http://www.scotiabank.ca/FAQSec2.html (28 October 2000)

[13] "About Security." Scotia Online Internet Banking – About Security. Scotiabank. URL:
https://www.pcbanking.scotiabank.ca/pcbanking?reqOption=AboutSecurityPage&action=display&token=0000000000000000D19&language=English (28 October 2000)

[14] "Simplify Your Life with Scotia OnLine." Scotiabank. URL:
http://www.scotiabank.ca/simplify/index.html (28 October 2000)

[15] "Technology: The Key to Internet Commerce - Security and Scotiabank PKI." VAQ Newsletter - Technology: The Key to Internet Commerce - Security and Scotiabank PKI. Scotiabank. Number 2, Fall 1998. URL :
http://www.scotiabank.ca/ctms/VAQNewsletter/1998-2.html#3 (28 October 2000)

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor