Overcoming pre-encryption security threats through a complementary SSL solution

An introduction to Dynamic SSL: true endpoint-to-endpoint security

APRIL 2009

DYNAMIC SSL

NetSecure
Securing the Internet

TABLE OF CONTENTS

1) EXECUTIVE SUMMARY

While traditional SSL encryption has proven very effective in transferring sensitive data over the internet, new hacker technologies are exploiting vulnerabilities at the client's computer to obtain sensitive data prior to encryption. The ability for hackers to circumvent SSL encryption undermines the entire internet security infrastructure. This has profound implications for legitimate businesses collecting sensitive data via the Internet, as consumer trust and confidence in the security of their private information is vital to maintaining the integrity of this system.

To address this concern, NetSecure Technologies has developed **Dynamic SSL**: a client-side technology that works seamlessly with **existing SSL-enabled systems** to provide true endpoint to endpoint security. Sensitive data is secured at the point of origin before it even reaches the computer and is transferred securely to an organization's secure server. No cumbersome and expensive changes are required to existing client and server systems.

Dynamic SSL allows organizations to retain all the benefits of SSL (low-cost/interoperable/proven) while at the same time addressing its endpoint vulnerabilities. In addition, organizations do not need to change any of their server side encryption infrastructure to benefit from the extra layer of data security that Dynamic SSL provides.

2) TRADITIONAL SSL: STRENGTHS & WEAKNESSES

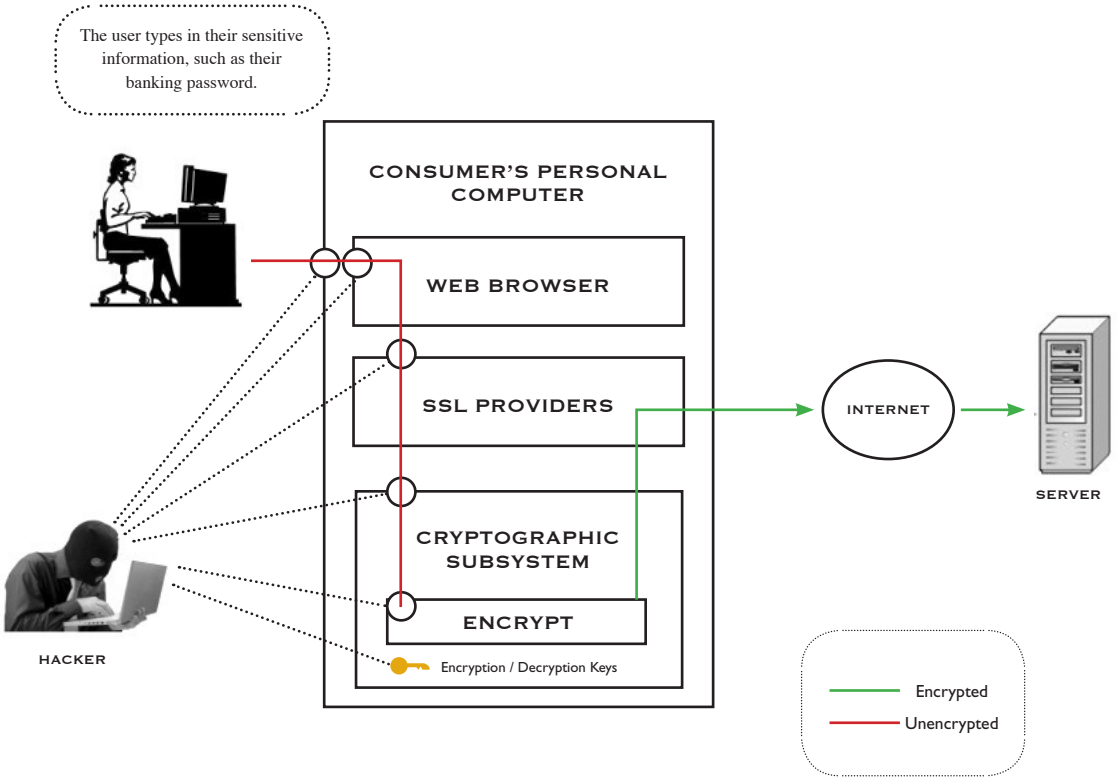
Since its introduction in 1994, SSL (Secure Socket Layer) has been the de facto standard for internet transaction security. It is a low-cost, widely accepted technology that does not require elaborate customization. Furthermore, once data has been SSL encrypted it has proven to be virtually impossible to crack[1]. For example, it would take approximately 10^{22} years on a corporate computer network (at a billion keys searched per second) to crack current commercially available SSL encryption algorithms[2].

SSL was specifically designed to protect information in transit only at the point where information leaves a computer. Therefore, one of its inherent weaknesses is that it leaves information vulnerable and unprotected while it resides on the personal computer prior to encryption[3].

Exploiting the Endpoint: The SSL Security Chasm

Given the tremendous effort required to break in to modern corporate networks, organized cybercriminals have shifted their focus away from highly protected corporate servers and focused instead on the weakest link in the online security chain – the end user's personal computer.

Figure 1: Hackers can access sensitive information prior to encryption by monitoring the data flow between system components in a transaction.



1. Based on typical processing power of the average personal computer.
2. Web Security, Privacy, and Commerce, S. Garfinkel & G. Spafford, O'Reilly, 2002
3. Keyjacking: the surprising insecurity of client-side SSL, John Marchesini, S.W. Smith, Meiyuan Zhao, 2004

While corporations have invested millions of dollars securing their network infrastructure against cyber attacks, the same cannot be said of the personal computer user. The typical computer user's failure to install and maintain even basic security measures such as antivirus software and security updates has made it increasingly easy for organized cybercriminals to steal their sensitive data for financial gain.

Cybercriminals have developed a number of sophisticated hacking tools to circumvent SSL encryption and steal sensitive information at the endpoint, including:

- **"Man in the Browser":** Exploiting lack of security at the browser level on the user's PC, information is stolen as it is being entered into a web form.
- **Keylogging:** User keystrokes or mouse movements are captured and recorded. These attacks can be hardware or software-based.
- **Memory Sniffing:** Malicious software is secretly installed on a user's PC. The software gains access to the computer's memory in order to steal sensitive information.
- **Spyware/Crimeware:** This is malicious software that appears to be a benevolent program (such as a software update). These programs are able to monitor user actions and collect sensitive information, which is then sent to a third party.
- **Viruses:** A virus can infect a program or operating system to steal data.
- **Keyjacking:** A scary attack whereby malware or viruses on the local PC silently export the SSL session keys used to protect the transaction.

While SSL is essentially secure, the potential for security breaches at the personal computer endpoint undermines the entire SSL infrastructure on which many systems are built. This poses a grave problem to those who conduct business online – in particular those who are required to guarantee the security of an online transaction.

Traditional solutions to endpoint security rely on custom protocols or proprietary authentication architectures that are not interoperable with SSL. In many circumstances, particularly in anonymous or distributed environments (such as online commerce) where interoperability with SSL is a requirement, synchronization of client and server systems with a proprietary security protocol is simply not feasible.

3) DYNAMIC SSL: A PRACTICAL SOLUTION FOR ENDPOINT TO ENDPOINT ENCRYPTION

NetSecure Technologies has developed an innovative solution for endpoint-to-endpoint security that is fully compatible with existing SSL-enabled systems: **Dynamic SSL**.

Dynamic SSL works seamlessly to complement and enhance the existing SSL encryption standard providing endpoint security without fundamentally changing the protocol or process. With Dynamic SSL, organizations can continue to receive information in the widely accepted SSL encrypted format without requiring a synchronized change between the organization and the end user. The fundamental difference in the process of implementing Dynamic SSL is that data is encrypted before it even enters the computer, thus eliminating the typical endpoint vulnerabilities and pre-encryption attacks at the personal computer.

What is Dynamic SSL?

Dynamic SSL consists of a simple software component that is installed on a personal computer or workstation, which interacts with the computer's existing SSL engine to eliminate endpoint vulnerabilities and provide comprehensive protection of sensitive information during an SSL transaction.

Dynamic SSL can be implemented as a software-only solution, or enhanced with a Dynamic SSL-enabled secure hardware device, such as a USB key, Smart Card, or mobile phone. Hardware-based implementations of Dynamic SSL provide an additional layer of security by offloading the SSL cryptography from the client machine to the secure hardware device, ensuring complete immunity against advanced cryptographic attacks such as Keyjacking.

Dynamic SSL is the most cost-effective way to deploy endpoint security. The advantage of Dynamic SSL is that it requires absolutely no changes to existing server systems or infrastructure. It works with your existing web infrastructure and SSL-enabled systems out of the box.

The Holy Grail of Endpoint Security: SSL Offloading using Dynamic SSL-Enabled Hardware

The underlying principle in Dynamic SSL is that encryption of sensitive information cannot be performed in an untrusted environment, such as most personal computers, where the security of the encryption process could be compromised. Rather, encryption of sensitive information must be done outside of the personal computer.

In other words, when paired with a secure cryptographic hardware device, such as a USB Token or Smart Card, Dynamic SSL acts as an "SSL offloader". Instead of having the SSL key negotiation take place on a personal computer (which is vulnerable to keyjacking and memory-sniffing attacks) – it occurs on the secure hardware device attached to the computer. Keys are securely stored within the hardware device bypassing all endpoint vulnerabilities and therefore cannot be intercepted or stolen.

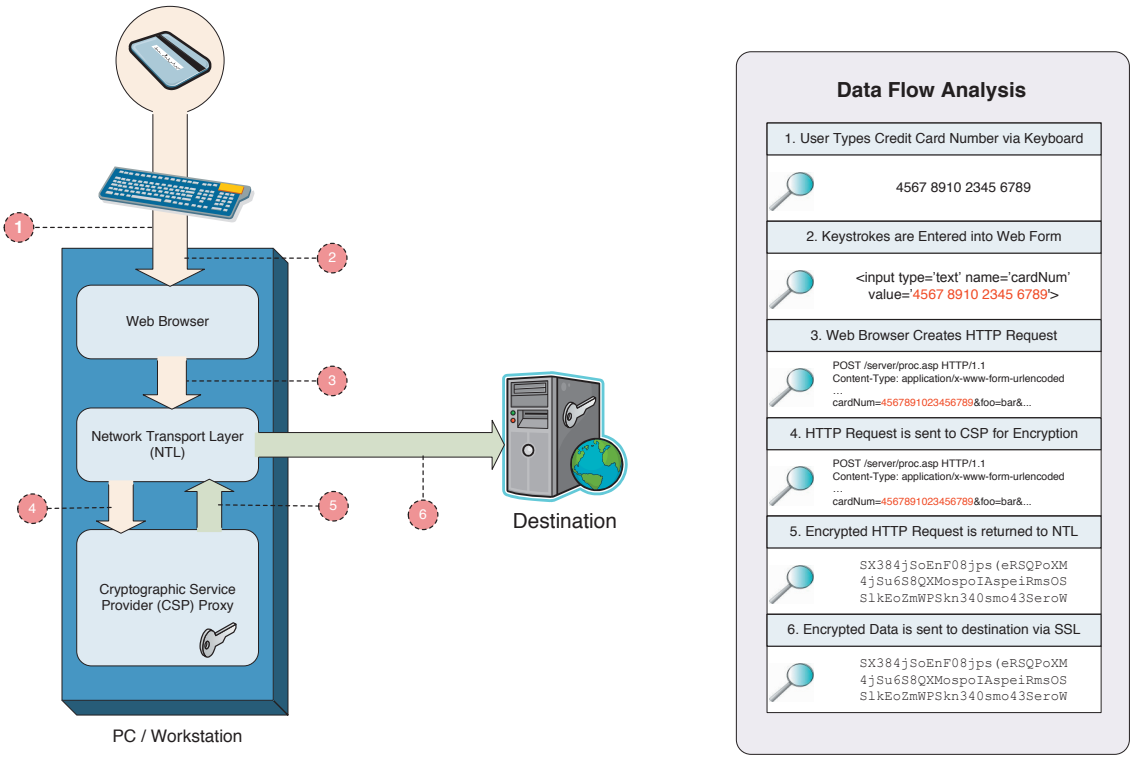
Secure cryptographic hardware that implements Dynamic SSL can guarantee complete security of a transaction[3]. Using a combination of SSL offloading and variable-based encryption, neither the sensitive information, nor the keys used to encrypt the sensitive information, ever exist on the user's personal computer. Complete immunity against virtually all client-side vulnerabilities can be achieved, without requiring any changes to server systems or infrastructure.

How does it work?

In a typical SSL session, a data stream containing the end user's sensitive information is sent to the computer's SSL engine for encryption prior to transit across the internet.

Figure 2 shows how this approach is problematic. Since the data exists in plaintext until the point of encryption, a malicious user can intercept this data stream before it reaches the SSL engine, harvest the sensitive information, and send it through to the SSL engine virtually undetected. Neither the sender nor the receiver knows that the transaction has been compromised.

Figure 2: In Traditional SSL, sensitive data exists in plaintext until the point of encryption, leaving it vulnerable to interception or tampering.



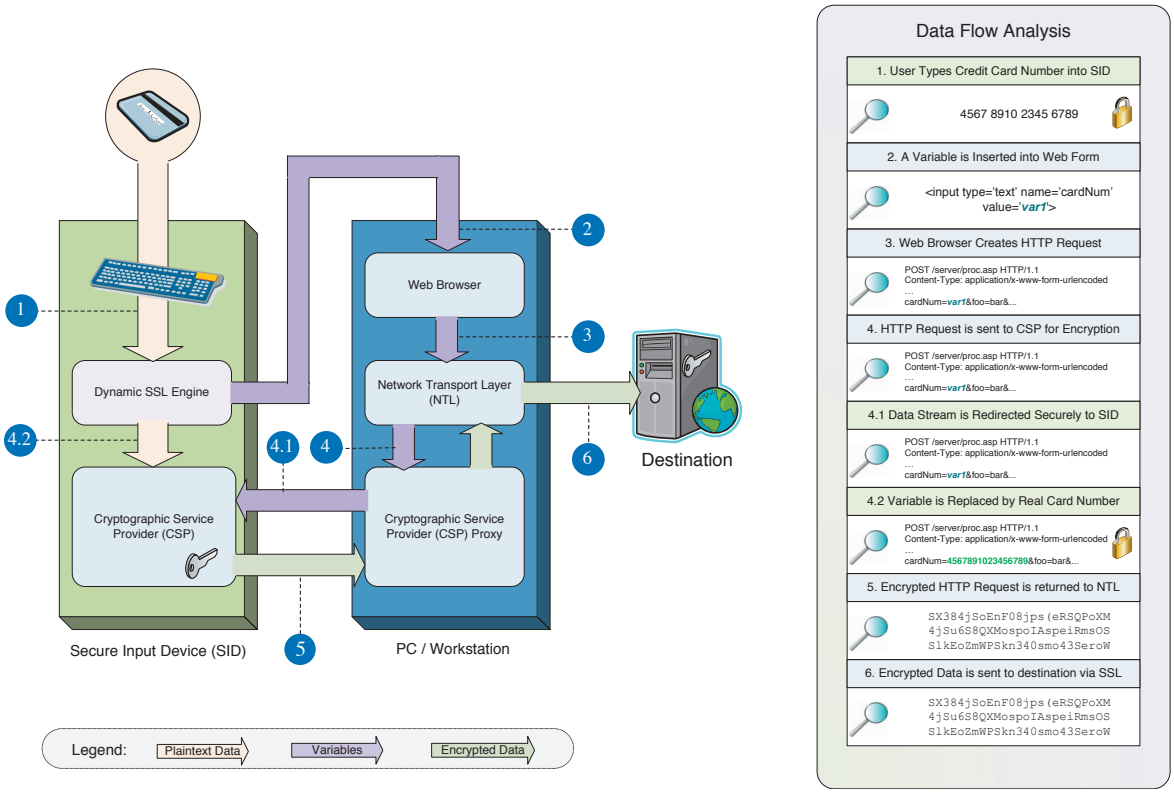
3. Dynamic SSL contains advanced Man-in-the-Middle protection to ensure the authenticity of the SSL session. Discussion of this feature is available in the supporting document, *Using Dynamic SSL to Prevent Man in the Middle Attacks*.

Figure 3 shows how Dynamic SSL avoids this problem by ensuring that sensitive information is never present in the data stream until the point of encryption. The Dynamic SSL engine inserts variables, rather than the unencrypted sensitive information, into the data stream at locations where the remote server is expecting the sensitive information.

Next, the Dynamic SSL engine securely redirects the data stream to a secure location where the sensitive information is stored. (For example, a Smart Card, USB device, mobile phone, etc.., or a software location such as network server or protected storage area).

Inside this secure location, the Dynamic SSL engine replaces the variables with actual sensitive data (e.g. credit card number, usernames and passwords, etc.) and encrypts the data stream using the SSL session keys negotiated with the remote server.

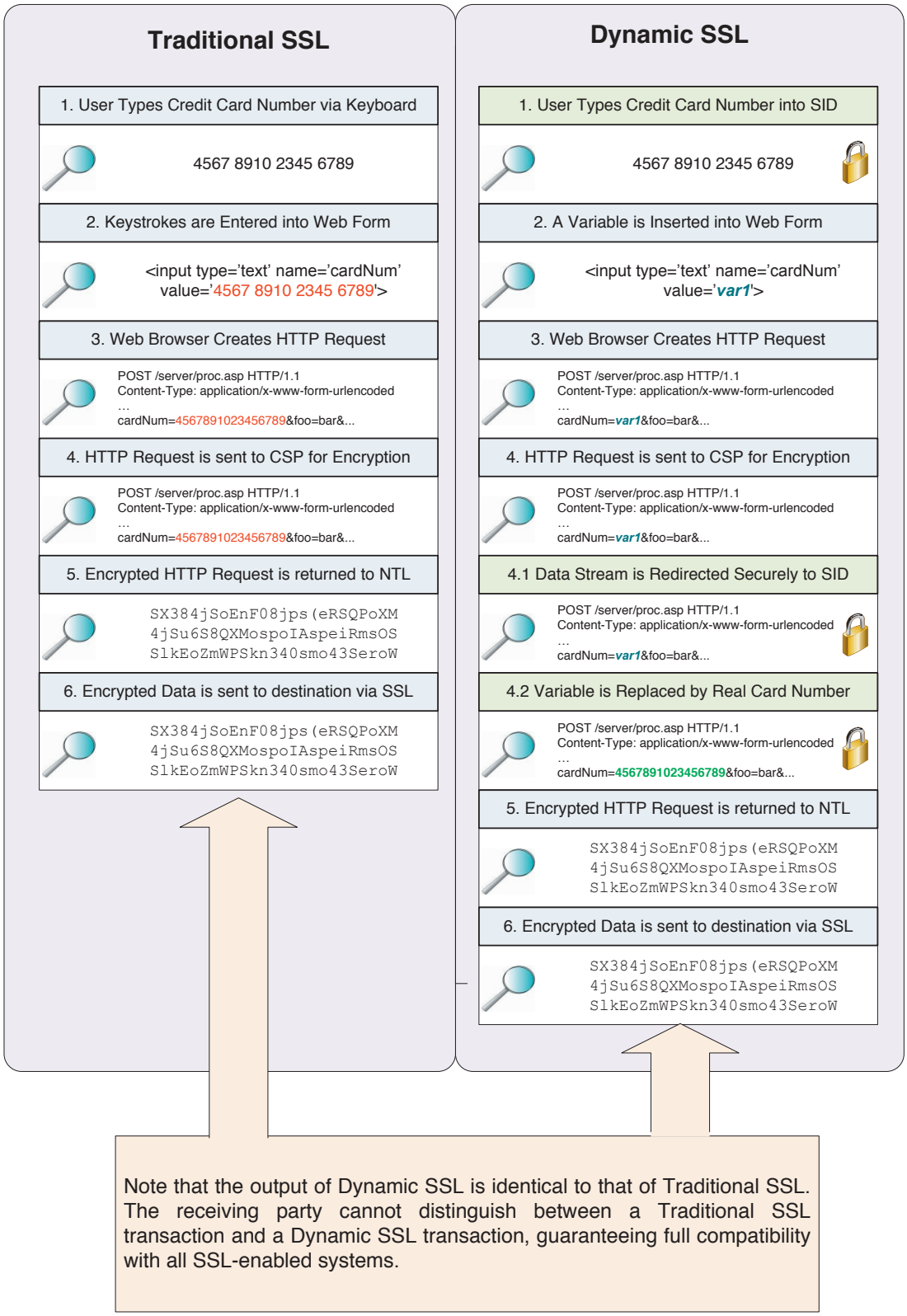
Figure 3: In a Dynamic SSL transaction, sensitive information is never accessible to the endpoint computer.



Finally, the encrypted data stream, containing the sensitive information in the format expected by the server, is then passed to the remote server via the SSL protocol. It arrives in the standard SSL format expected and can be decrypted with the same SSL keys used to protect the web session. (See Figure 4)

Since the sensitive information was not present in the data stream until the point of encryption, any attempts to intercept the data stream and harvest the data would be useless. Rather than obtaining the sensitive information, a malicious user would only see meaningless variables.

Figure 4: Dynamic SSL solves the endpoint vulnerabilities inherent in traditional SSL implementations, without requiring changes on the server end.



4) KEY BENEFITS OF THE DYNAMIC SSL SECURITY SOLUTION

1.) Eliminates the weak link in the security chain by bypassing the endpoint security vulnerabilities. Dynamic SSL Encryption guarantees that unencrypted information is never available at the personal computer endpoint.

2.) Allows merchants and organizations to offer an unprecedented level of security to customers – a competitive advantage when conducting business online.

3.) Fully compatible with existing SSL encryption processes – no software or hardware changes are required at the organization/server side. Secure SSL keys are still negotiated with the organization's server.

4.) Fully compatible with virtually all existing SSL enabled websites.

5.) A low cost, commercially viable, easy to implement solution.

6.) Ideal for situations where infrastructure changes are unfeasible, such as secure online commerce.

Who is it for?

NetSecure Technologies is offering its Dynamic SSL solution as a licensed technology or a turnkey solution. It is for any organization entrusted with protecting sensitive financial, strategic or personal information online, including:

- E-commerce merchants
- Banks and financial institutions
- Government
- Healthcare providers
- Charitable organizations
- Online service providers

5) CONCLUSION

The need to secure sensitive data from endpoint to endpoint is vital if our current system of global information transfer is to remain viable and universally available.

The SSL security protocol has been widely recognized as the de facto standard in online data security - despite its inherent endpoint security vulnerabilities. Given the vast logistical and financial effort that would be required to overhaul the current infrastructure and implement a new system, SSL is likely to remain the standard in online data security for the foreseeable future.

However, the evolving threat of organized cybercriminals, targeting the end user with increasingly sophisticated hacking tools, means that the status quo protection of SSL for online data security is no longer sufficient. It is clear that an enhancement, rather than a replacement to SSL is needed.

Dynamic SSL by NetSecure Technologies provides an innovative solution to these problems:

1. It provides a more secure endpoint-to-endpoint online data security system.

2. It does not require an overhaul of the current global online security standard.

3. It does not require any synchronization between an organization and the end user thus increasing the ease and likelihood of wide acceptance.

In an increasingly vulnerable environment, online merchants, banks, governments and organizations offering the Dynamic SSL security solution will have a strategic advantage over those who do not offer a true endpoint-to-endpoint security solution.

About NetSecure Technologies

NetSecure Technologies is a technology company dedicated to providing endpoint data security systems.

Its patented Dynamic SSL technology forms the core of its flagship online security product – the SmartSwipe – the secure credit card reader for your home computer.

Visit **smartswipe.ca** or contact us for more information:

NetSecure Technologies
info@netsecuretechnologies.com
Office: (306) 205-3226
Fax: (306) 205-1927

6) CASE STUDIES

The following scenarios demonstrate how Dynamic SSL enhances existing SSL encryption by eliminating its endpoint vulnerabilities, offering a superior online security solution.

A. Securing credit card information in an eCommerce transaction with a Personal Payment Device

In a typical online shopping scenario, an end user navigates to an online shopping website using the HTTPS prefix in the address bar of their browser. When a lock icon appears in the browser, this signifies that the ecommerce server and the end user's browser are using the SSL protocol to encrypt and secure all communications between the two endpoints.

But when the end user types his credit card number into the computer to make a purchase, the number, along with other sensitive data, is not yet encrypted at this point. Hackers, using a keylogging application installed on the computer, or a Man in the Browser attack masquerading as a 'free utility' – are able to steal the user's unencrypted credit card number and use it to make thousands of dollars of fraudulent purchases and cash advances.

Virtually every commerce website expects that the users credit card number will be keyed into a web form in plain text. Any deviation from this process on the client side will break the transaction in an unexpected format. Any deviation from this process on the server end will eliminate the possibility of attracting new customers that don't use their "proprietary" system. Therefore, implementing endpoint security using any approach that fundamentally changes the process is unfeasible.

The Solution: The SmartSwipe Personal Card Reader

In the scenario above, instead of typing the credit card number on the keyboard, the end user swipes his credit card using the SmartSwipe Personal Card Reader connected to the personal computer.

Dynamic SSL software, running on the computer and within the SmartSwipe device, encrypts the credit card information before it even gets to the computer. In this scenario, any hacking tools residing on the computer will never have access to unencrypted credit card information – keeping the transaction completely safe and secure from endpoint to endpoint.

The SmartSwipe Personal Card Reader makes use of the Dynamic SSL's variable-based encryption process to ensure that no changes are required to the traditional purchase process. The online merchant receives all transactions from the end user in the expected SSL encrypted format and no changes are needed to the merchants infrastructure to enable this extra layer of security. Therefore, the user may use the SmartSwipe Card Reader on any website, enjoying complete protection of their personal information from endpoint attacks, without limiting their choice of merchant.

The *SmartSwipe* plugs into the USB port of a home computer and scrambles the user's credit card data before it reaches the computer or Internet.

B. Preventing Access to Sensitive Personal Data in an Electronic Health Records System

Many government jurisdictions are implementing electronic health record systems allowing access to a patient's complete medical history to a variety of health care providers such as doctors, pharmacies, hospitals, emergency care providers, etc.

In this scenario, the patient's master health records and corresponding personal health number are stored on a secure server at a central Registry. Typically, a doctor's office would access the health record using the personal health number of the patient via a SSL-secured web interface to the Registry. Also, the patient themselves can review their medical history by using the same SSL-secured web interface.

Unfortunately, accessing health records with a personal health number leaves this system vulnerable, as unscrupulous employees at a doctor's office who should not have access to a patient's personal health number can steal the number and use it to access the confidential records of the patients.

Eliminating the use of the personal health number is not a feasible option given that the Registry uses a standard web interface which requires the personal health number for all their clients. The Registry cannot change their SSL-enabled system for one client without breaking it for all the other clients. Therefore, if a particular doctor's office wants to eliminate the use of the personal health number for privacy reasons, they are unable to do so.

The Solution: Using Dynamic SSL to eliminate internal access to the health number.

A doctor's office decides they will eliminate the internal use of the patient's health care number for privacy reasons. However, they still require access to the central Registry. To accomplish this, they randomly generate a "Patient ID" number that is used only within their office. They map each Patient ID to the patient's health care number, and store the real health care number in a secure Dynamic-SSL enabled Token server that office staff do not have access to.

When a health care provider needs access to sensitive health records for a patient, they log on to the web interface of the Registry, but instead of entering the health care number (which they no longer have access to), they input the Patient ID for that patient. (Note that the web interface still expects the health care number, and does not have any knowledge of the Patient ID).

During the SSL session, the Dynamic SSL software then redirects the data stream, containing the Patient ID instead of the health care number, to the secure Token server. Inside the secure Token server, the Patient ID is replaced by the corresponding health care number for that patient. The data stream is then encrypted with the SSL keys of the Registry, and returned to the health care provider's PC, which then forwards the encrypted information to the Registry.

The Registry decrypts and processes the information, which contains the health care number, and returns the patient's health care record.

In this scenario, the health care worker was able to access the Registry's web interface without ever having access to the patient's health care number, yet no changes were required to the Registry.

For more information on DynamicSSL and licensing opportunities, please contact NetSecure at:

NetSecure Technologies, Ltd.
info@netsecuretechnologies.com
Office: (306) 205-3226
Fax: (306) 205-1927
www.netsecurecanada.com

DYNAMIC SSL

NetSecure
Securing the Internet