



MANUAL

Security Manual / FAQ

© Copyright 2009, UNIKEN Inc.

WHAT KIND OF SECURITY THREATS / ATTACKS DO WE NEED PROTECTION FROM?

Network Level Attacks

- Phishing: Fraudulent acquisition of sensitive information of Bank's users such as usernames, passwords etc. by masquerading as a trustworthy entity in an electronic communication.
- Pharming: Redirection of Bank's user traffic to another, bogus website using one or multiple fraudulent techniques.
- Man-in-the-Middle Attack (MITM): A form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection when in fact the entire conversation is controlled by the attacker.
- Replay Attack: A Replay Attack is a breach of security in which messages from an authorized user who is logging into an Application are captured by an attacker and resent (replayed) at a later time.
- Session Hijacking: Session hijacking is a method of taking over a Web user session by surreptitiously obtaining the session ID and masquerading as the authorized user. Once the user's session ID has been accessed (through session prediction), the attacker can masquerade as that user and do anything the user is authorized to do on the network.

Device Level Attacks

- Man-in-the-Browser Attack (MITB): A security attack where the perpetrator installs a Trojan horse on a victim's computer that's capable of modifying that user's Web transactions as they occur in real time.
- Man-on-the-Machine Attack (MOTM): Man-on-the-machine refers to malicious software in the user's access device such as Trojans, key-loggers etc. that have been installed to capture and transmit sensitive data.

The network level attack vectors apply to all e-channels while device level attacks vary from device to device, most of them targeted to steal or manipulate information. The security challenge is to protect the users from all of these attacks without hampering the usability of the solution.

WHAT ARE THE COMPONENTS OF SECURITY?

Security includes confidentiality, message integrity, identity and authentication. These protocols, developed over 40 years ago, still form the backbone of internet security today.

WHAT IS 'IDENTITY' AND 'AUTHENTICATION'?

A person's IDENTITY is based on, or determined by "What you know", "What you have", and "Who you are". Examples: Driving Car License, Passport, Voter ID Card, PAN Card, Social Security No. etc., which clearly shows a person's name, address, date of birth, etc. along with their photo. We're all aware that malicious elements regularly exploit loop holes in the system to create fake or duplicate IDs.

In addition, all this information or attributes can easily be stolen, compromised, or copied from genuine IDs and misused by fraudsters who assume the identity of the original person/entity. This is known as IDENTITY THEFT which has already resulted in huge losses – financial and of credibility.

AUTHENTICATION is a process by which one verifies a mutually agreed “SECRET” (login/password or biometric). If these credentials are compromised, then it is as good as giving the keys to your bank vault or safe to a thief yourself.

Both Identity and Authentication require ‘APRIORI’ knowledge. If Identity is localized, it can easily be stolen, no matter how many attributes/absolute labels are assigned to it.

WHY IS SO IMPORTANT TO IMPLEMENT TECHNOLOGIES TO SECURE INTERNET TRANSACTIONS?

All the resources or websites on the internet can be classified as either PUBLIC or PRIVATE.

We do not need security or users’ identity to access PUBLIC resources or websites – such as Google, Yahoo!, CNN, Wikipedia, etc. However, PRIVATE web sites allow access only on the submission of identity credentials (username / password) – e.g. Citibank, SBI, Gmail, Facebook, LinkedIn, etc.

If you are transmitting sensitive information on a website (such as credit card numbers or personal information), you need to secure it with some form of encryption. It is possible for every piece of data to be seen by others unless it is secured. Customers won't trust your web site without it.

As people use the Web for commerce, business, and social activities, they share personal and confidential information. High profile incidents of fraud and phishing scams have made Internet users very concerned about identity theft. Before they enter sensitive data, they want proof that the website can be trusted and their information will be encrypted. Without it, they might abandon their transaction and do business elsewhere.

Implementing security technologies provides a strong sense of confidentiality, message integrity, and server authentication to users. The business of e-commerce is tied closely to consumer confidence across the net.

However, the current technologies need to evolve in order to ensure the security of sensitive information over the Web. This way, e-commerce will be able to continue to grow in popularity as users grow more confident in shopping and banking online, and embracing new online applications.

WHAT TECHNOLOGIES ARE AVAILABLE TODAY FOR INTERNET SECURITY?

- SSL
- Digital Certificates
- PKI (Public Key Infrastructure)
- OTP (One Time Password)
- 2 Factor Authentication
- Relative Identity (Rel-ID) Mutual Authentication & Encryption protocol

WHAT IS SSL?

SSL = Secure Socket Layer. SSL allows a secure connection between your web browser and a web server. This secure information 'tunnel' was developed by Netscape Communications and was based on encryption algorithms developed by RSA Security. SSL was widely adopted by numerous companies for other client/server uses other than web surfing.

SSL has two distinct entities, server and client. The client is the entity that initiates the transaction, whereas the server is the entity that responds to the client and negotiates which cipher suites are used for encryption. In SSL, the Web browser is the client and the Web-site server is the server.

Because SSL is built into all major browsers and Web servers, simply installing a digital certificate, or Server ID, enables SSL capabilities. However, in a SSL handshake the “verification” that happens is only to check the authenticity of the digital certificate.

WHAT DOES SSL MEAN TO THE INTERNET USER?

When the user comes across a web page that is secured, the browser will likely display a 'closed lock' or other symbol to inform him that SSL has been enabled. The web site address should also now start with "https://" rather than the usual "http://".

SSL apparently uses cryptography, digital signatures, and certificates to secure websites. However, this technology is almost four decades old, while cyber fraudsters and hackers are constantly evolving and using more sophisticated technologies with each passing day.

To top it all, many users who transact online are not even aware of what to look for or how to find out if the website is secure and whether it is genuine; and the fraudsters take full advantage of this. The scary part is that most banks and e-commerce sites are still secured by only SSL today.

WHAT IS A DIGITAL CERTIFICATE?

It is the key to starting the SSL engine, more like a driver's license. It's just an identification card that the server uses to prove that it is who it says it is.

Digital Certificates are issued by Certificate Authorities (CA). This is where it gets tricky, because anyone with the right software can be a certificate authority, just like anyone can make a piece of paper that says it's a driver's license. But just as only the state government can issue a license that a police officer will accept, there are certain trusted CA's that your web browser will accept (such as VeriSign, Inc.). Of course, you can tell your web browser to accept other CA's if you want to. In this case, you're the police officer that's accepting these certificates, so you should accept certificates from sources you trust.

Also note that, just like the SSL connection itself, a digital certificate does not vouch for the integrity of the company it is issued to. Users should be wary of who they send their credit card information to, regardless of whether the connection is secure or not.

WHAT IS PUBLIC KEY INFRASTRUCTURE (PKI)?

Public Key Infrastructure (PKI) is typically the network security architecture of an organization. It includes software, encryption technologies & services to enable secure transactions on the Internet, intranets, and extranets.

For example, VeriSign digitally signs each SSL Certificate that a Certificate Authority (CA) issues. Each browser contains a list of CAs to be trusted. When the SSL handshake occurs, the browser verifies that the server certificate was issued by a trusted CA. If the CA is not trusted, a warning will appear. When high security browsers recognise an Extended Validation SSL Certificate, they display the name of the CA next to the browser bar.

The VeriSign subscriber agreement prohibits customers from using a certificate on more than one physical server or device at a time, unless the customer has purchased the Licensed Certificate Option. When private keys are moved among servers – by disk or by network-accountability, and controls decrease, and auditing becomes more complex. By sharing certificates on multiple servers, enterprises increase the risk of exposure and complicate tracing access to a private key in the event of a compromise.

CAN ANYONE DOWNLOAD THE VERISIGN SECURE SEAL FOR THEIR WEBSITE?

The VeriSign Secured Seal is available for display on any Web page within a domain secured by a VeriSign SSL Certificate. Whether you are a new or existing customer, you can download and install the VeriSign Secured Seal on your server. A JavaScript verifies your common name and displays the seal. When site visitors click on the seal, they receive a dynamically generated verification page specific to your certificate. However, most internet users do not know how to check this or simply don't take the trouble of doing so every time they transact online. Going a step further, considering that the Secured Seal can be displayed on a website in less than an hour, what really prevents a cyber fraudster from altering the contents of his website immediately thereafter and launching phishing attacks on unsuspecting users.

WHAT IS SSL SERVER AUTHENTICATION & ENCRYPTION?

SSL server authentication allows users to confirm a web server's identity. SSL-enabled client software, such as a web browser, can automatically check that a server's certificate and public ID are valid and have been issued by a certificate authority (CA) listed in the client software's list of trusted CAs.

An encrypted SSL connection requires all information sent between a client and a server to be encrypted by the sending software and decrypted by the receiving software, protecting private information from interception over the Internet.

WHAT IS EXTENDED VALIDATION SSL?

Extended Validation SSL Certificates give web browsers information to clearly identify a Web site's organizational identity. For example, if you use Microsoft® Internet Explorer 7 to go to a website secured with an SSL Certificate that meets the Extended Validation Standard, IE7 will cause the URL address bar to turn green. But most users don't even know what this green band stands for and why some sites show it and some don't – which defeats the entire purpose of authentication. Further, a display next to the green bar generally toggles between the organization name listed in the certificate and the Certificate Authority, but even that disappears often within a few seconds if it does appear in the first place. So effectively, the problem of mutual authentication still remains unsolved. Besides, Firefox and Opera are yet to support Extended Validation SSL. Older browsers display Extended Validation SSL Certificates with the same security symbols as existing SSL Certificates (i.e. padlock icon).

No longer is identity absolute (based on individual entities alone), but defined in terms of a relationship of two entities with respect to a specific context & need. So in addition to the above three elements, we have introduced a fourth "WHO YOU KNOW" (Relative Identity – Mutual & Distributed Identity) element.

WHAT IS RELATIVE IDENTITY MUTUAL AUTHENTICATION & ENCRYPTION PROTOCOL?

Relative Identity (Rel-ID) Mutual Authentication & Encryption protocol, also called RMAP, is a revolutionary and cutting-edge technology (developed at Uniken's Innovation Centre in India) for secure communications and secure data exchange over the Internet. It is based on asymmetric encryption algorithms (that were born after the Diffie-Hellman paper on Cryptography was published in 1976).

No longer is identity absolute (based on individual entities alone), but defined in terms of a relationship of two entities with respect to a specific context & need. In addition to the three facets of IDENTITY (which can easily be stolen or compromised today), we have introduced a fourth element of "WHO YOU KNOW". This Relative Identity or Mutual and Distributed Identity framework IDs the link / relationship between two entities and splits it (mathematically) in to two or more parts. When you identify the link, you identify both end-points – hence, Mutual Authentication.

RMAP integrates IDENTITY with ENCRYPTION, making it one of the most robust protocols for internet security today that has the ability to ward off most known malware, spyware attacks and threats such as Phishing, Man-In-The-Middle (MITM) and Man-In-The-Browser (MITB) attacks, Key-loggers, Screen-scrapers, Trojans, etc. This is possible with the unique combination of a Secure Browser + Secure Desktop + Secure end-to-end encrypted channel between the users' PCs and the banks' servers.

WHAT'S THE DIFFERENCE BETWEEN REL-ID, A 40-BIT, AND A 128-BIT SSL CONNECTION?

Most banks require 128-bit encryption for online banking because 40-bit encryption is considered to be relatively weak. 128-bits is about 309 septillion times (309,485,000,000,000,000,000,000) larger than 40-bits.

As an analogy, sending information without encryption is like sending a postcard through post – the contents are visible to practically anyone who wants to see it. Using 40-bit encryption is like sending it in a plain white envelope. 128-bits could then be equated to using a security envelope that is printed to prevent it from being see-through. Relative to these strengths, Rel-ID encryption can be compared to encasing your data in a lead-lined, 12-inch thick titanium safe that is being transported by an armored tank with a convoy of a hundred armed guards. In other words, nothing short of military-grade security!

IS REL-ID ENCRYPTION REALLY STRONGER THAN 128-BIT SSL ENCRYPTION?

Absolutely! When a SSL handshake occurs between a client and server, a level of encryption is determined by the browser, the client computer operating system, and the SSL Certificate. In spite of having a 128-bit encryption, a hacker with the time, tools, and motivation can crack the code in a matter of minutes.

Besides, in a SSL handshake the "verification" that happens is only to check the authenticity of the digital certificate. And just like the SSL connection itself, a digital certificate does not vouch for the integrity of the company it is issued to.

LIMITATIONS OF VERISIGN 128-BIT SSL CERTIFACTES FOR USERS OF WINDOWS 2000 AND OLDER BROWSER VERSIONS

Many users are still using Windows 2000 and older versions of Internet Explorer which do not support VeriSign's SSL certificates using 128-bit encryption. Certain IE browser versions from 3.02 to 5.23 and Netscape browser versions from 4.02 to 4.72 fall in this category. IE versions prior to 3.02 and Netscape versions prior to 4.02 are not capable of 128-bit encryption with any SSL Certificate. With Rel-ID and TruBank, there is no such limitation as it uses an independent, stand-alone, dedicated and secure browser, which can only connect with the bank's servers and none other.

WHAT ARE THE BENEFITS OF IMPLEMENTING REL-ID TO BANKS & ENTERPRISES?

When you send confidential data using Rel-ID technology, the information is sent through a secure tunnel so that only the banks servers can view/ read it. It helps your visitors' complete secure transactions with confidence and puts your organization in a leadership position. If your site has the Rel-ID technology and your competitor's site does not, you appear to be more trusted and more legitimate. That's a competitive advantage in the world of e-commerce. For businesses with a high profile brand, using Rel-ID is an effective defense against phishing scams. When customers transact in a protected and secure environment (secure browser, secure desktop) and see other displays of trust, they can interact with you online, with confidence.

WHICH SITES SHOULD BE PROTECTED BY REL-ID?

Ideally, Rel-ID should be implemented by ALL security-sensitive intranets, extranets, and websites. However, it is mission-critical for large-scale online merchants, banks, brokerages, health care organizations, and insurance companies worldwide.

WHAT IS A VIRTUAL PRIVATE SECURE INTERNET (VPSI)?

A Virtual Private Secure Internet ("VPSI") is an on-demand private network for enterprises to enable its customers, employees and suppliers access to its online applications. It is an overlay virtual network over the public Internet that is available only for a limited set of users (viz. Bank's customers, employees and suppliers) and does not have access for anybody else apart from the defined set of users. The key characteristics of such a network are as follows:

- **Mutual Authentication:** Both the users as well as Bank (both at user level and device level) are authenticated before any connection is established. This ensures that the users connect only to the real Bank and vice versa.
- **Connection - Authentication - Encryption:** Unlike SSL-based protocols, the parties at the two ends of the connection first mutually authenticate each other, and then exchange keys and establish cryptographic ciphers. Hence, no unauthorized person/device can even get a connection without authentication.
- **End-to-end Encryption:** All the data travelling on the VPSI is encrypted using best-of-breed technologies. Additionally, any chosen encryption technology can be plugged into the VPSI to provide desired encryption levels.
- **Control:** Bank has control over who can access its VPSI. All business applications sit on this network and hence are protected from unauthorized access.

- **Device binding:** Device binding ensures that only authorized access devices (PCs & Laptops) can access Bank’s network blocking any other device not authorized for access.
- **Common Security Infrastructure:** The VPSI is a secure network infrastructure that can be used by Bank for its employees as well as its agents for connecting to any application of Bank securely without having to implement separate security infrastructure for each application or set of users.

Uniken offers a Virtual Private Secure Internet solution to banks and enterprises under the VPSI Core brand name. VPSI Core enables Bank to transform the user's PC/Laptop into a Secure Access Device and the normal Internet into a secure private network to provide a fundamentally new private communication channel.

	Network	Computing Environment	Application	User Identity and Privacy	Security
Private Application	Dedicated Private Network	Custom Hardware and Custom OS	Custom Application with strong end-user authentication	Biometric	Very High
Virtual Private Internet Application	Application level light weight highly scalable mutually Authenticated and encrypted tunnel created on demand over the internet	On demand virtual Private Computing Shell created on top of a standard OS and hardware	Hardened Application based on the standard components provided by the underlying OS	Standard and Multifactor	High
Semi-Private Application	VPN Networks – Heavy Weight, network level mutually authenticated and encrypted tunnel on the internet	Standard Hardware and OS	Standard Applications like IE , Chrome and Firefox	Standard and Multifactor	Medium
Public Internet Application	Internet with SSL (optional)	Standard Hardware and standard OS	Standard Applications like IE, Chrome, Firefox	Standard and Multifactor	Low

VPSI uses a secure tunneling infrastructure to create an On-Demand Secure Client Side Computing Environment, which...

- switches between secure and normal mode on demand
- is built-in with 2-Factor Authentication
- binds the user, device and software together

VPSI can be used for Mobile Banking, Secure Automated and Encrypted File Transfers, Online Credit/Debit Card Transactions, and deployment options can be either Cloud-Based or On-Premise.

WHAT IS TRUBANK?

TRUBANK is our custom-application based on the Rel-ID Mutual Authentication and Encryption Protocol that banks can use to offer secure internet banking to their customers. TRUBANK can be deployed either at the banks' premises or be cloud-based, and it can be offered for both corporate as well as retail customers. For more details about the product, please take a look at the TRUBANK brochure on our website (www.uniken.com)

HOW DOES TRUBANK CONDUCT MUTUAL AUTHENTICATION & OFFER END-TO-END ENCRYPTION?

Rel-ID Mutual Authentication Protocol is one of a kind True Mutual Authentication protocol, which is a zero-transmit protocol (where none of the information is transmitted in wire or otherwise). TRUBANK uses the same technology to ensure no confidential data is compromised during the transmission.

The Rel-ID framework ensures that the entire Network Traffic remains encrypted between all network nodes, including client, web servers, application servers and database servers, both over the Internet and within the bank's internal network.

HOW DOES TRUBANK LINK THE DEVICE TO THE INTERNET BANKING CUSTOMER ID & PASSWORD?

The user logs into his Internet Banking account using the browser and then the customer is notified to download the TRUBANK application (software) and activate it. The device activation key is sent to the customer using an out of band method such as a SMS or a PIN Mailer. This is a onetime activation process only. Once the device is activated, it gets bound to the hardware – e.g. laptop or USB drive.

The device Username and the Internet Banking Username are the same, and once the customer launches the device and logs into it the Internet Banking page is already pre-populated with the Username.

CAN TRUBANK BE 'CORRUPTED' OR 'POISONED' AT THE CUSTOMERS' PC TO RE-DIRECT TRAFFIC TO FRAUDSTER'S SITE?

TruBank cannot be 'corrupted' or 'poisoned'. Once TruBank is activated on the customers' PC, there can be no Man-In-The-Middle (MITM) attacks to re-direct traffic anywhere. Such an MITM attack is theoretically only possible during the activation process, where in addition to knowing the username, password, verification and activation keys, the hacker has to even know the exact time when the customer is activating the application for the first time – which is a rare possibility.

HOW DOES TRUBANK WORK IN THE SCENARIO THAT MULTIPLE CUSTOMERS USE THE SAME PC AND TRUBANK APPLICATION TO ACCESS THEIR SEPARATE INTERNET BANKING ACCOUNTS?

The same device (PC) can be allowed to be accessed by multiple users. Each user who will use the device would need to activate it individually using his Internet Banking Username. The pin for the device for each user could be different. The activation process is similar to individual user activation.

DOES TRUBANK WORK ON FIREWALLS AND BEHIND PROXIES?

Yes. TruBank works on all firewalls and behind all proxies – supporting BASIC, DIGEST and NTLM authentication methods.

M
A
N
U
A
L