The SSL Protocol

– Authenticating Websites Reliably

ODYSSEY
cryptic by intent

ODYSSEY TECHNOLOGIES LTD.

The SSL Protocol

– Authenticating Websites Reliably

Introduction

The SSL protocol was originally designed by Netscape as a way of providing a secure, encrypted channel between a web server and a web browser. For some reason, the first published version of this protocol was termed version 2.0. As the primary purpose was to provide a secure channel, an elaborate handshake mechanism was specified for agreeing on a 'session key' that was essentially a symmetric encryption key that was used in all subsequent data exchanges for encrypting the data.

Man-In-The-Middle Attacks

The problem with Diffie-Hellman Key Exchange

The handshake mechanism initially relied on an algorithm known as 'Diffie-Hellman' key exchange though a digital certificate based exchange was also recognized. The Diffie-Hellman key exchange was found to have serious flaws in that it allowed a hacker to place himself between the web server and the browser (Man-In-The-Middle) and have access to the data. The hacker essentially did that by having two different sessions – one with the web server and another with the user and piping the data from one session to the other and vice versa. This gave him unencrypted access to the data that was being exchanged. Because of this, most web servers have now phased this out and exclusively use a digital certificate and the public key found in the certificate for a secure session key establishment.

The problem with Certificate-Based Key Exchange

In the certificate-based model, the server, when contacted by the browser, sends its own certificate to the browser. The browser extracts the public key from the certificate, creates a random session key and then encrypts the session key with the server's public key and sends it back to the server. Since the server has the private key corresponding to its own public key, it is able to decrypt the random session key. Thereafter, the server and the browser use that session key for encrypting the data stream for that particular session. This is a somewhat simplified version of what really happens though in essence it is accurate.

Here again, it was found that the same Man in the middle attack was possible. The only thing the hacker in the middle would need is a digital certificate of his own. He then establishes a session with the server using the server's digital certificate and establishes another session with the user using his own certificate and continues to pipe the data as before. In fact some of the web traffic analysis applications (like the HTTP Analyzer) are able to work exploiting this vulnerability only.

Protecting against Man-In-The-Middle attacks

Domain Mismatch Warnings

To protect users from this kind of attacks, the browser vendors came up with additional warnings to indicate if the certificate the browser receives does not match the domain it is attempting to connect. Thus, if a user connects to www.hdfcbank.com, and if there is a man in the middle, the user's browser will be getting the man's certificate rather than the hdfcbank.com's certificate. Thus there will be a mismatch between the domain name in the URL and the domain name mentioned in the certificate and the browser will raise an alert asking for the user's input on whether to continue or abort. The browsers could not very well abort on their own without asking the user because, there are a huge number of web sites which continue to use expired certificates and which use certificates issued by not so well known certifying authorities. Denying the users the option to connect to those sites was not feasible for the browser makers. Therefore they had to satisfy themselves with putting up these alerts.

There were two problems with this. The first was user apathy. As mentioned earlier, there were a large number of sites using expired or otherwise unrecognized certificates. There were also others who rebelled against the browser makers' commercial models of including only CAs recognized by them in the browsers, and therefore ran their own CA setups, which were not recognized by the browsers as valid certificates. These caused these alerts to be thrown up too often. The users became immune to these warnings and got into the habit of simply clicking 'OK' to these alerts. This plays right into the hacker's hands.

Secondly, the proliferation of Certifying Authorities and their inclusion in the browsers made it possible for hackers to get legitimate looking certificates from questionable but recognized CAs. Thus, while “citibank.com” would have been certified by Verisign or some such reputed CA, someone like “FNMT Clase 2 CA” may certify “citlbank.com” to a hacker. The hacker then can easily emulate Citibank by using this legitimate looking domain name. Unless the user personally types in the correct domain name each time in the URL bar of the browser, he can be easily misled to the hacker's site when he believes he is in the site belonging to Citibank.

Extended Validation Certificates

The browser industry and the Certifying Authorities together have come up with yet another fix to this problem. This is called the “EV certificate” or 'Extended Validation' certificate. These certificates are the same as regular digital certificates but carry a flag to indicate that it was issued after carrying out some prescribed validation processes by the CA. These certificates are priced much higher than the normal certificates. The browsers, when they come across such a certificate, indicate the higher level of validation by some indication – Firefox in gold color, IE in green or so on.

While this looks like a fix, this is what the Certifying Authorities are meant to have been doing all along. Their present stance looks like “We took your money but did not provide the expected assurance, but now give us more money and we will do a proper job” It is also not clear if these validation procedures would be maintained or relaxed in the face of commercial exigencies. Of course not every organization has opted for a EV certificate and the web will always have a mixed population of sites. This is very likely to lead to another kind of user apathy. For some time they may keep looking for the EV indication and when they find that they do not come on several genuine sites also, the signal will fail to have any significance.

User Vigilance

Therefore, while technically there is a way for the browser users to conclusively identify the site they are connecting to, the only way for it to work is by user vigilance. This means, every time the user connects to a site of some importance to him (meaning a site where he carries out financial transactions) he has to personally verify the digital certificate by double clicking on the 'lock' icon in the browser and checking that the domain name in the certificate is the one he wanted to connect to, and that it has been issued by a Certifying Authority known to him. This is a lot of work for an average user, but there is no other way.

The conclusion runs this way. SSL protocol does provide a way to identify the server but only with some user vigilance.

Odyssey Snorkel Toolbar

Recognizing this problem and to enable users to be automatically vigilant, Odyssey provides a toolbar based solution.

This toolbar enables the browser to 'remember' a few sites and their certificates and give out positive signals (like a green lamp) when the user is in one of those remembered sites. To make it efficient, there is a cap on the number of sites a user can register so that the user does not become immune to the signal. Recognizing that different users will need different sites to be trusted, the toolbar also lets them to individually customize the 'trusted' list. This is more akin to the process done at the server end. The server recognizes only registered users. The same way, now the browsers can recognize only those sites trusted by the users. The power to handle the trust mechanism is effectively moved from some arbitrary CA to the end user.

To learn more about Snorkel Toolbar, visit http://www.odysseytec.com/AntiPhishingToolbar.html

About Odyssey

Odyssey Technologies Limited is a pioneer in PKI technology in the Asia-Pacific region. The company develops products and solutions for transaction security and is recognized by the Controller of Certifications in India as a technology vendor.

By isolating the security components and business logic, Odyssey stays true to its zero-touch philosophy and ensures deployment of solutions quickly and effectively without the need for integration or changes to the existing code-base. The company proudly supports the security needs of major banks and financial institutions in the Asia-Pacific region and has earned their trust as a reliable vendor.

Odyssey Technologies Limited is based in Chennai, India and is listed in the Bombay Stock Exchange.

To learn more about solutions from Odyssey Technologies Limited, visit www.odysseytec.com or e-mail info@odysseytec.com.