

Analysis of Preventing Tampering HTTPS

— Antiy Labs

In Black Hat DC 09, Moxie Marlinspike, Independent Security Expert, explained how he moved round SSL Security mechanism to get the information of users' credit cards and other account. According to his description, the websites with SSL are not encrypted wholly. The websites only use SSL in some important pages, so an opportunity is given to attackers.

Some banks and Online-pay System are based on SSL certification mechanism, so this vulnerability will threat users' electric trade account. Antiy labs analyzes the above situation, and add a new function in Antiy Ghostbusters v6.5.1.* to prevent HTTPS Tampering. Users can choose this function manually to strengthen the security of electric trade.

1. What is SSL and its how it works

The Secure Socket Layer protocol (SSL) is a protocol based on WEB created by Netscape. SSL appoints a kind of protocol, such as HTTP, Telenet, NMTP or FTP and so on, to provide data security layer mechanism between TCP/IP protocol. It will provide data encryption, server certification, information integrity and closable client certification.

SSL constructs secure channel to transmit data with web servers. SSL runs on TCP/IP layer, but under application layer to provide encrypted data channel. It uses RC4, MD5 and RSA, and other encryption algorithm. It uses a 40-bit key which is suitable for business information encryption. At the same time, Netscape developed HTTPS protocol and built in browser. HTTPS is in fact SSL over HTTP. HTTPS uses default port 443 but not 80 as HTTP to communication with TCP/IP. HTTPS encrypts data in sender with SSL, and then decrypts in receiver. Encryption and decryption should be realized by exchanging public key in sender and receiver. For example, if a user wants to buy a product from some website, user and website should get certification. User provides his name and password to verify him. On the other hand, website should exchange a block of signed data and a valid X.509 certificate to verify it. The browser of user will verify the certificate and verify the signed data with attached public key. Once through verification, the trade will start.

2. What is Man-in-the-Middle Attack (MITM)

Man-in-the-Middle Attack is an attack mode which put virtually a computer controlled by attacker between two communicated computers in network, and this computer is called "Man-in-the-Middle". And then attackers will imitate this computer to one or two original computers to make it connect and get or modify the transmitted information. But the original computer users still consider that the communication is between them. Therefore, it is very difficult to find this attack. MITM is a very old attack mode used by hackers, and it still have huge development potential.

3. What is CA

CA is short for Certificate Authority. It is an organization of granting, managing and repealing certificate. CA acts to check the validity of certificate holder and sign the certificate to prevent faking and tampering so as to manage certificate and key.

Certificate is a record saved in computer, and it is a statement signed by CA to prove the only correspondence between the main part (after getting certificate, applicant will be main part) and public key in certificate. Certificate includes name and relevant information of applicant, public key, digital signature of CA and the validate date of certificate and so on. Certificate acts to reciprocally verify the status of traders to ensure security.

The third-party organization or company will be consigned to issue digital certificate. Certificate is used to create digital signature and public-private keys. CA acts to ensure the person who gets the unique certificate is the grantee. During data security and e-business, CA is a very important component, as it ensures the status of information exchangers.

4. Secure Hypertext Transfer Protocol- HTTPS

HTTPS is developed by Netscape and built in browser to compress and decompress data, and then return the result. HTTPS uses SSL as the sub-layer of HTTP layer. HTTPS uses port 443, but not 80 as HTTP to communicate with TCP/IP. SSL uses 40-bit keyword as RC4 encryption algorithm, and it is very suitable for business information. HTTPS and SSL use X.509 certification. User can check who the sender if necessary.

5. About SSL vulnerability

There are the following kinds of attacks aiming at SSL vulnerability:

1) Attack certificate.

As IIS server provide "Map a Client Certificate" function to map the name who submit certificate in client to user account in NT system. In this situation, we can get the administrator access right. If hacker can't attack server with illegal certificate, they will try violent attack.

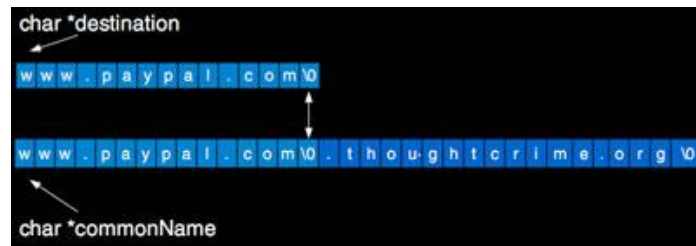
2) Steal certificate.

Hacker may steal valid certificate and relevant private key.

3) Security scotoma.

If there is no network detection system and vulnerability checking, the most important servers will be the ones with least protection.

SSp (SSL Strip) can tamper responds without encryption of website; hijack HTTPS links, and give a feint that original website is encrypted. For users, SSp uses several kinds of method to cheat users. Firstly, by using local proxy with legal SSL certificate to make browser to report the page is encrypted (but the certificate provider is different). Secondly, SSp can also use homographic to create an over-length with a false diagonal, and it can prevent browser converting link character to PunyCode*.



Attack Process of Moxie Marlinspike



The attack depends on users enter URL in browser but not activate SSL session directly, and most of the users activate it by clicking on the displayed button. These buttons typically appear in unencrypted HTTP pages, once the users click on them they will enter the encrypted log HTTPS pages.

“It provides a variety of ways for intercepting information”, Moxie Marlinspike said at the Black Hat conference, he also claimed that he had been intercepted 117

email accounts, 7 Paypal registration information, 16 credit card numbers details within 24 hours.

SSp works by monitoring the HTTP traffic, it acts as a proxy when the user attempts to access the encrypted HTTPS session. When the user considers that the safe session has started, SSp also connects to a secure server through HTTPS, all of the connections from users to SSp are HTTP, which means that the "destructive warning" of the browser has been blocked, the browser looks work well when all of the registration information can be easily intercepted.

Marlinspike said that the HTTPS security lock logo can be displayed in the browser address bar, making users even more believe the access security.



SSL has been generally considered secure enough, but some security researchers have claimed that SSL communications can be intercepted. In August last year, a researcher Mike Perry said he was discussing with Google on an upcoming attack vulnerability, the vulnerability would allow hackers intercept users traffic of the secure site through WiFi network.

Hazard

Marlinspike has been successfully cheated the FF and Safari users using SSp, although he has not tested on IE, he estimated that the same strategy will be effective for IE.

Example

- 1) First, the user enters the banking home site <http://www.usbank.com> in the browser

- 2) Enter the user name, click on Enter
- 3) SSL strip gets the bank site URL and user name
- 4) SSL strip connects to the bank web server, submits the user name
- 5) Then SSL strip transfers the returning bank Web server new page to the browser
- 6) The user enter password in the new page
- 7) SSL strip gets the user password, and submits it to the bank web server. Bank web server then considers that the user has logged on.
- 8) SSL strip submits the returning bank Web site new page to the browser again, in my opinion; I have logged in normally and can be the next operation.

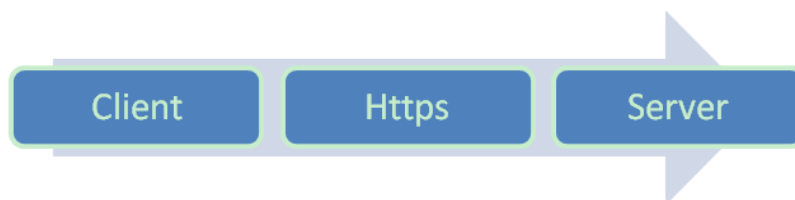
You may ask that why there is no "s" behind HTTP, bank websites aren't all HTTPS form. In this example there is no "s", because the SSL connection is established between the attacked computers and bank site servers. The user just sends all the valid pages back to the browser through SSL strip, but there is not secure tunnel in the process. So it is easy to know who gets the user's password.

Some vigilant and circumspective users may find this trick, but for most users it is hard to notice.

6、Antiy Lab' s analysis for the recent SSL vulnerability

- 1) Https attack:

client->https->server



client->https->we->https->server



Existing problem, certificates issued by https appears untreated prompting.
x->object site

x is not CA's, so verification fails.

2) Solution

client→http→we→https→server



Tamper with web content by arp deception, dns hijack, proxy method and so on, change https link for http, because https link access jumps through hyperlink or 302, so that general user couldn't notice it has been replaced http. Further pretence could tamper with favicon for lock head. so that it looks like .

Because it would be obvious that latest browser prompt for https site, so above method is still easy to be found in some user's eyes.

3) So research verification mechanism of CA certificate, and then find that there are vulnerabilities in some browser.

client→https→we→https→server



For achieving perfect spoofing, further method is that alter https certificate into trusted certificate.

We describe this vulnerability as follow:

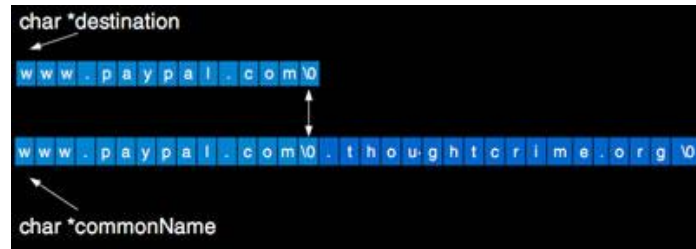
Some SSL's implement don't verify CA field in certificate whether FALSE or not. So that even if leaf node (whichever site obtaining valid CA certificate) could act as middleman (Issue valid certificate). Certificate of not CA issue would be verified as a valid site when verify certificate.

CAROOT→middleman→middleman→...→X→object site, it is legal.



Optimize this method further. By inserting \0 in Common name to tamper certificate to show perfect certificate information. There are more valid optimization methods

to realize regular code vulnerability by making use of SSL and even construct ones dispense with signature verification.

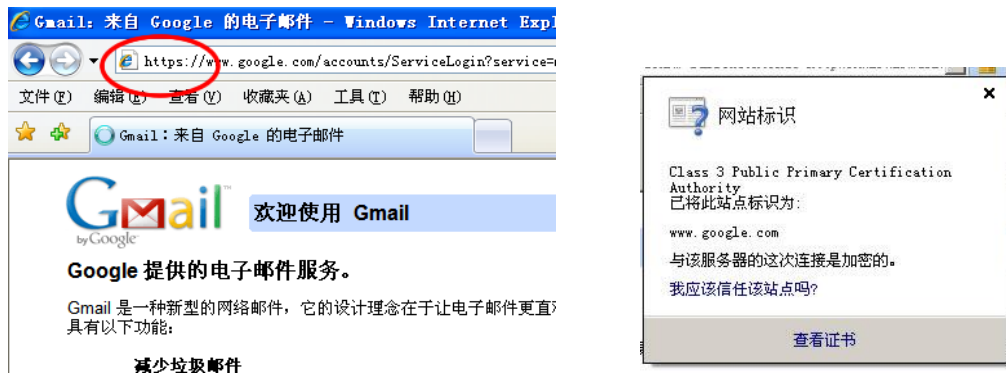


www.paypal.com\0.thoughtcrime.org

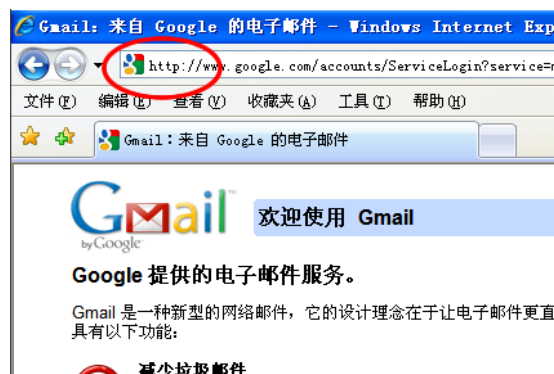
The certificate of www.paypal.com.thoughtcrime.org is shown as the certificate of www.paypal.com.

Antiy Ghostbusters preventing tampering function:

- 1) Google will use HTTPS Certification mechanism to ensure security.



- 2) After exploiting SSL vulnerability of website, HTTPS link is tampered as HTTP link.



- 3) Enable the function of preventing tampering in Antiy Ghostbusters. This function will prompt and block the website which try to exploit SSL vulnerability. The Screenshot of Antiy Ghostbusters:



The mechanism of preventing tampering HTTPS:

Connect by http if there is no prevention. After enable the function in Antiy Ghostbusters, it will monitor the SSL vulnerability in websites.