“Three misunderstandings of SSL certificate” continuance

The author published an article "Three Misunderstandings of SSL Certificate" in the "China Computer World" on January 31, 2005. This is an article from 18 years ago, and it still feels good to read now, although the text is a bit promoting the GeoTrust certificate, because it just started selling GeoTrust SSL certificates at that time, this article may be the first article about SSL certificates in an authoritative newspaper in China. Eighteen years have passed by, today, the author rewrites this topic on the CEO blog, which will bring some new ideas to readers.

Eighteen years ago, only a few online banking websites deployed SSL certificates, but now almost all online banking websites have deployed SSL certificates. All ecommerce websites have implemented https encryption, and some government websites have also deployed SSL certificates on their login pages. In other words, there is still progress, but the author, as one of the promoters and leaders of SSL certificates in China, still feels that the pace can be faster. Especially in the current new and uncertain international situation, it is particularly important and urgent to vigorously promote and correctly deploy the SM2 SSL certificate.

Part I Three Misunderstandings of SSL Certificates

Misunderstanding 1: Thinking that SSL certificates are only used for websites, in fact, SSL certificates are needed in many places.

Websites need SSL certificates. There is no doubt that through the efforts of major browsers, websites that do not deploy SSL certificates display "Not secure" in the browser address bar, because the confidential information entered by users on the website is not encrypted by https. If the transmission is in cleartext during the transmission process, it is very easy to be illegally stolen and used illegally. This is very worthy of the e-government website's great attention because all information entered by the users on the e-government website is confidential information.

However, deploying an SSL certificate on a website is not enough. Since mobile apps have almost become the most way to obtain information, browsers have relegated to the second place. At present, many mobile apps do not use HTTPS to implement encrypted communication when communicating with the server. This problem does not have obvious "not secure" prompts like browsers, which makes this security problem very serious. However, due to the lack of effective supervision, it makes mobile app developers intentionally or unintentionally ignore the problem of deploying SSL certificates for servers that the app communicates with, resulting in frequent app leaks.

In addition, the mail server not only needs to deploy SSL certificates for web pages, but also SMTP and IMAP/POP3 servers must deploy SSL certificates to ensure email account password security and email content transmission security. What is more urgent is that various IoT devices (including the Internet of Vehicles and the Industrial Internet) currently use http cleartext to collect data and communicate with the cloud in cleartext, which is very vulnerable to malicious attacks. This is why there have been several recent large-scale DDOS attacks from IoT devices.

All applications that transmit data from the client to the cloud need to deploy an SSL certificate on the server to implement https encrypted transmission. This is the only reliable and necessary technology that can ensure the security of data transmission, not just a browser as a client.

Misunderstanding 2: Thinking that if the website installed an SSL certificate, everything will be fine, but the correct deployment of SSL certificate may be more important than the installed certificate.

It is necessary to install an SSL certificate for the website, but it is more important to deploy it correctly. Let’s draw an analogy for website as house, not deploying an SSL certificate means that only one door (port 80) is opened to the outside world, while deploying an SSL certificate must open another door (port 443). If the SSL certificate cannot be deployed correctly, it means another risk. The usual certificate deployment problems are not closing insecure SSL 2.0/3.0 and TLS 1.0/1.1 protocols, not deactivating insecure cipher suites, not supporting secure renegotiation, and so on. The most important thing is that since the SSL certificate is deployed, you should close the unencrypted door (port 80), use only the encrypted door (port 443), and use a third-party SSL deployment security test service to check

SSL deployment after the SSL certificate is deployed, the test result must be scored as A or above.

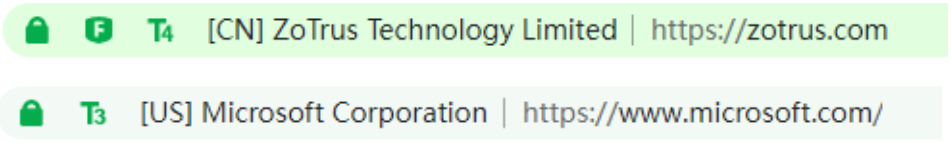
At the same time, the SSL certificate cannot be deployed only in the website login authentication system, and the full site https encryption must be implemented, because the page after the user logs in contains a lot of user confidential information, which is as important as protecting the user's login password, and the site-wide https encryption can effectively prevent SSL man-in-the-middle attack.

For the https support of mobile apps, it is not only necessary to enable https encryption. The app should also determine whether the domain name of the server it communicates with is the same as the domain name bound to the SSL certificate, whether the SSL certificate is revoked, and whether it is an SSL certificate trusted by the app. The default mode of Android system does not make these judgments. App developers need to program themselves to increase these security judgments. This is also a relatively common app security problem that the author has found, and it is worthy of great attention by app developers, especially online banking apps. The author will write a separate blog post to guide users how to solve this app security problem.

Misunderstanding 3: Thinking that the website installed an SSL certificate is enough, but it is not enough that you should deploy an SSL certificate that have validated the identity of the website.

The encryption attribute of the SSL certificate is more important, or the identity authentication attribute is more important. This is a topic that has been debated many times in the CA/Browser Forum. Browsers do not recognize the importance of website identity, and they removed the green address bar for websites that have deployed EV SSL certificates, so that websites that deploy a DV SSL certificate that only validates domain name ownership are displayed padlock same as those that deploy an EV SSL certificate that strictly validates the identity of the website, these browsers think that as long as it is encrypted, it is secure, and they do not realize the importance of website identity validation. In fact, the trust identity of the website is as important as encryption. A fake bank website also deploys an SSL certificate, and the browser will also display the padlock, which is more hidden and more harmful than a fake bank website that does not deploy an SSL certificate.

Therefore, ZT Browser not only insists on displaying the EV SSL certificate as a green address bar, but also innovatively displays the identity information of the website where the OV SSL certificate is deployed, to reflect the value of the validated identity of the website.



Please remember a famous saying: cheap is not good, good is not cheap. Free SSL certificates or cheap DV SSL certificates are SSL certificates that do not verify the identity of the website, which cannot convince visitors of the identity of the website and cannot truly guarantee the security of the website. Therefore, don't think that everything will be fine if you deploy a free or cheap DV SSL certificate that does not validate the identity of the website. You should deploy an OV SSL certificate that validates the identity of the website and an EV SSL certificate that strictly validates the identity of the website, ZT Browser displays the EV SSL websites as green address bar to let the site visitor know the identity of the website at a glance, enhance online trust, and win more online orders.

Part II Three Misunderstandings of SM2 SSL Certificates

In the current very uncertain international situation and the reality that many SSL certificates have been revoked and supply break after the Russian-Ukrainian conflict, China websites must not only deploy SSL certificates correctly, but also must deploy SM2 SSL certificates as soon as possible to prevent similar threat of SSL certificate revocation and supply break. For SM2 SSL certificate, there are also three misunderstandings. These misunderstandings must be corrected intime to ensure the healthy development of the SM2 SSL certificate, to truly protect the security of China website system.

SM2 SSL Misunderstanding 1: It is believed that there is no need to deploy an SM2 SSL certificate, but an RSA SSL certificate is deployed.

In peacetime, it is okay to deploy RSA/ECC SSL certificates with RSA/ECC algorithms, but after the Russian-Ukrainian conflict on February 24, the top three CAs that have more than 99% of the China market share revoked more than 3000 SSL certificates within 10 days, those certificates are for Russian government websites and bank websites, which makes these websites unable to access normally. Not

only that, but these CAs cut off issuing SSL certificates for these websites on the 7th day after the conflict. Aren't these lessons worthy of our vigilance? Are we still naive to believe that this cannot happen in China in someday?

Just deploying an RSA SSL certificate can no longer protect the security of China website! China must plan ahead, take precautionary measures, popularize and deploy the SM2 SSL certificate as soon as possible! Only in this way can we truly protect the security of China websites and systems.

SM2 SSL Misunderstanding 2: It is believed that the technical conditions for deploying SM2 SSL certificate are not mature, but in fact it is relatively mature.

This is also a relatively common misunderstanding. It is believed that Google Chrome does not support the SM2 algorithm, then the conditions for popularizing and deploying the SM2 SSL certificate are not mature. This is an ecological problem that cannot be solved in the short term. Yes, it is an ecosystem, if we want to use SM2 SSL certificate to implement https encryption, we must have at least three products that must support SM2 algorithm: Browser, SSL certificate and Web server. But now there are already many products on the market that support SM2 algorithm provided by many companies, these products can fully meet the compliance requirements of deploying SM2 SSL certificate to realize the SM2 https encryption.

The first is the browser. ZT Browser, Red Lotus Browser, Qianxin Browser and 360 Browser all already support SM2 algorithm and SM2 SSL certificate. And ZT Browser is a completely free SM2 browser.

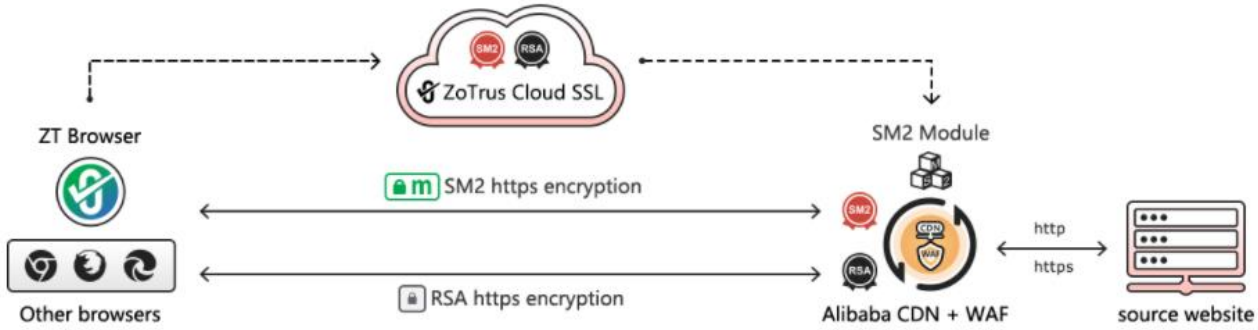
The second is the SSL certificate. There are more than a dozen domestic CA operators that can issue the SM2 SSL certificate and have the ability to provide enough SM2 SSL certificates to ensure the market supply. The author recommends that the website deploy dual SSL certificate (SM2/RSA) to implement adaptive algorithm encryption to ensure that site visitors can normally achieve https encryption using both SM2 browsers and non-SM2 browsers. CerSign Technology plans to provide a 90-day free SM2 SSL certificate, together with the provided 90-day free RSA SSL certificate, can realize dual SSL certificate deployment for free.

The third is the Web server. The most common solution is to recompile Nginx to support the SM2 algorithm. At present, there are several Nginx SM2 support modules on the market, ZoTrus Technology plans to provide for free. If the user is using another web server, Nginx can be used as a proxy to support the SM2 algorithm to realize SM2 https encryption.

SM2 SSL Misunderstanding 3: It is thought that all system must be transformed in order to realize SM2 https encryption. In fact, SM2 https encryption can be done without any transformation.

Readers can see from the second misunderstanding that in order to realize the SM2 https encryption, the Web server must be transformed, and the browser that is usually used must be replaced with SM2 supported browser. And dual SSL certificates must be deployed to meet the access needs of users' different browsers. This is indeed a bit more complicated than deploying an RSA SSL certificate.

ZoTrus Technology is also well aware of this pain point and has solved this problem. This is ZoTrus Website Security Cloud Service, which is based on Alibaba Cloud CDN and WAF cloud service and realizes automatic configuration of SM2 SSL certificate and ECC SSL certificate for website, fully automatic implementation of adaptive algorithm https encryption. Users only need to do 3 domain name resolution, zero transformation to achieve SM2 https encryption.



Zero transformation will definitely become the common method of SM2 https encryption, because users need SM2 https encryption, not SM2 SSL certificate. And website security not only requires https encryption, but also requires multi-faceted website security protection including WAF protection, CDN distribution and website trusted identity validation.

In summary, full deployment of SSL certificates on all websites and various information systems is inevitable, especially the implementation of the "Cryptography Law", "Cyber Security Law", "Data Security Law" and "Personal Information Protection Law", making SSL certificates all-round, extensive, and correct deployment is a must, and China websites must deploy the SM2 SSL certificate to truly ensure the security of the websites and systems.

Richard Wang

Sept. 21, 2022
In Shenzhen, China

Photo: Newspaper "China Computer World" January 31, 2005, B27 edition article "Three Misunderstandings of SSL Certificate".

计算机世界 CHINA COMPUTERWORLD 责任编辑：胡英 E-mail:hu_ying@ccw.com.cn

CSO&信息安全

第5期 2005年1月31日 B27

网站欺诈（Phishing）目前日益猖獗，而很多安全厂商对此却束手无策，在目前条件下，这类攻击不是靠技术能解决的，需要靠人们擦亮眼睛。此外，网站作为受害方之一，也可以采取一定的措施自我保护。SSL认证曾经被认为是好方法，但目前存在认识误区。那么，还有什么好方法呢？

SSL的三大误区

王高华

误区一：对SSL数字证书功能的误解。

许多网站开发者认为只要部署了SSL数字证书就万事大吉了，错误地夸大了数字证书的功能。实际上部署了SSL数字证书，只能证明如下三点：

(1) 从用户的浏览器到正在访问的Web服务器之间所传输的数据是通过加密传输的，是不可被篡改、窃取和破译的，保证了用户输入的机密信息(如银行卡信息)在网络传输过程中是安全的。

(2) 浏览器右方有锁标志说明了此数字证书是由信任的机构颁发，并且与用户正在使用的浏览器兼容。

(3) 说明用户正在访问的Web服务器已经申请了SSL数字证书，并且正在访问的网站的域名的所有者与SSL数字证书申请时填写的域名所有者是一致的。

有锁标志只能说明机密数据在传输过程是安全的，但是网上用户首先应该搞清楚的是您正在与谁交易，正在付钱给谁，一个假冒在线购物的网站也可以申请一个SSL数字证书来麻痹用户，用户应该检查正在访问的网站是否就是要访问的购物网站，域名是否正确。点击锁标志，检查此证书是颁发给哪个网站的?此证书的网址是否就是您要访问的网址?再点击“详细信息”的“主题”项、VeriSign的数字证书一般在“O”或“OU”字段会列出此证书的网站的所有者，即会清楚地告诉您此网站是否是您计划与之交易的公司的网站。而GeoTrust的数字证书一般在“OU”字段有一个ChoicePoint CUI查验网址，可以在线查验该网站的所有者资料。而一个假冒的网站即使也有SSL数字证书，如果检查证书的详细信息就会发现问题。如招商银行信用卡网站的安全链接网址为：https://creditcard.cmbchina.com，访问后会发现浏览器下面有锁标志，点击锁标志后会显示此证书是颁发给creditcard.cmbchina.com，而再点击“详细信息”的“主题”项后会显示：CN = creditcard.cmbchina.com (Web服务器公用名称)，OU = head office (申请机构的部门信息)，O = China Merchants Bank (申请机构信息)，L = Shenzhen (机构所在城市)，S = Guangdong (机构所在州/省)，C = CN (机构国家)。

误区二：以为在屏幕右下角有“显示锁标志”就可以放心地在线填写信用卡等机密信息了。

但是，用户一定要明白，SSL数字证书仅仅是为了保证数据传输的安全，它并不等于身份验证。要搞清楚的是用户正在访问的网站是否就是用户希望与之发生交易的公司的网站，这是最重要的。所以，要保证网上安全交易，还需要对网站的身份进行验证，验证此网站是否就是交易方的正宗网站。假如有一个假冒招商银行信用卡网站的安全链接网址为：https://creditcard.cmb-china.com，该假冒者在注册域名时也是填写域名注册者为China Merchants Bank，申请SSL数字证书时也都是填写与域名cmbchina.com一样的信息，该假冒者当然也可以申请到SSL数字证书，只要申请证书时的信息与注册域名的信息一样。所以，此假冒网站也会显示锁标志，按以上方法验证证书，都可以是同样的正确信息。但是此网站是假冒网站，而用户只能以网站的网址做判断了。所以作者认为：最重要的是网站身份认证，目前全球惟一的网站身份认证服务提供商是美国GeoTrust公司，该公司提供的True Site认证和Ture Site认证标志能确保网站不可能被全部假冒，假冒网站不可能有Ture Site认证标志，因为此标志是动态实时生成的，是不可能被假冒和抄袭的。

误区三：选择SSL数字证书颁发机构的误区

目前国内各种数字证书颁发机构有近百家，网站应该根据自己的业务需要正确选择数字证书颁发机构。对于面向国际市场和希望有国际合作的网站(希望国外用户也能正确浏览安全页面的网站)，推荐申请支持所有浏览器的全球Web服务器数字证书(如：GeoTrust或VeriSign)，此类证书无需要求客户端浏览器下载和安装根证书，使用非常方便。