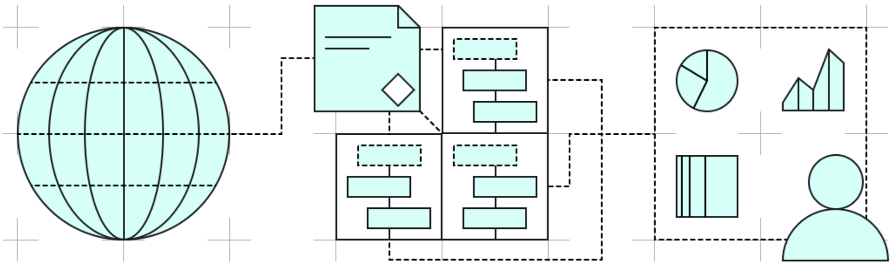
Who is securing the world's 7.3 billion SSL certificates?

We all know that website security is inseparable from an SSL certificate. To achieve https encryption, an SSL certificate is required. So, who is protecting the security of the SSL certificate itself? Some people may say that of course it is the CA operator that issues the SSL certificate. The CA operator must ensure the security of the CA system, this is true. However, what if the CA system is hacked and an SSL certificate that should not be issued is maliciously issued, or if the CA operator makes a mistake and mistakenly issues an SSL certificate that should not be issued? How can we spot malicious or mistakenly issued SSL certificates in real time? These are the questions to be answered in this article.

The author has released three issues of "China SSL Certificate Market Development Trend Analysis Report" in Chinese in CEO Blog. The data source in the report is "According to the data of the Google Certificate Transparency Log System", some readers asked me privately: What is Certificate Transparency? What is Google Certificate Transparency Log System? I just briefly replied "Baidu it", sorry, now I Baidued by myself, and I did not find an article that explained this question clearly.

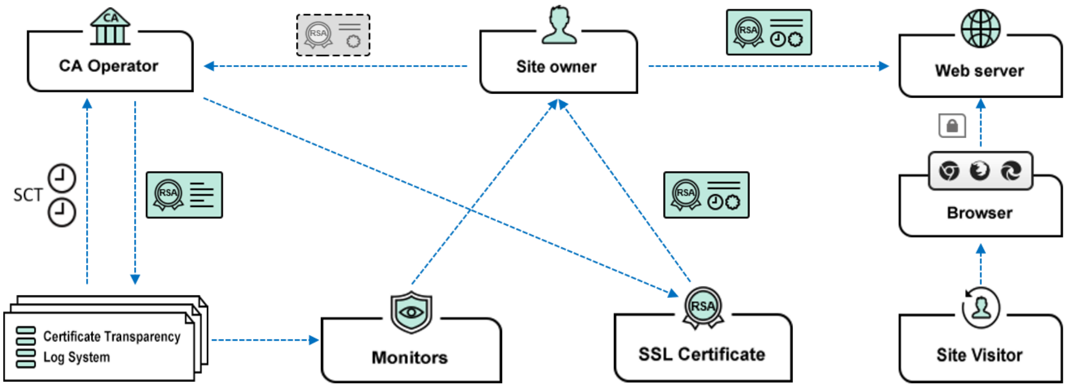
Please don't think that the above two paragraphs are unrelated. Why did you just talk about how to find the wrongly issued SSL certificate, and then suddenly talk about the SSL certificate market report? Don't worry, the above two questions are the same question. The solution to the question proposed in the first paragraph is certificate transparency. This article will explain certificate transparency thoroughly to let readers not only can understand how to detect wrongly issued SSL certificates in time, but also It is clear why the data in the Report released by the author is authoritative and trusted data. Two paragraphs described one question that only need one answer – certificate transparency. The certificate issuance behavior is transparently publicized, and the publicized data is the real data, which can be used for analysis, which is an important application of certificate transparency.

The author believes that everyone is no stranger to the word "transparency", such as: "Improving the transparency of equity transactions", "improving the transparency of the internal management of the enterprise" and so on. So, what is the certificate transparency? As the name implies, it is the transparency and disclosure of the behavior of issuing certificate, the SSL certificate for the website HTTPS encryption. This is an RFC 6962 standard initiated by Google. It is a transparency management system that can timely detect malicious or wrongly issued SSL certificates that are not voluntarily applied by users.



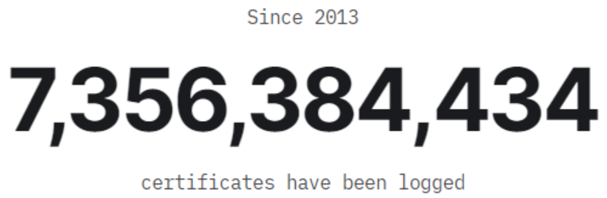
Readers who have applied for an SSL certificate must know that the key step of issuing the SSL certificate is the domain name control validation. You can prove the domain control in three ways. One is CA system sending the verification code to 5 special email address including: admin@domain, administrator@, postmaster@, webmaster@, hostmaster@, the second is to use the verification code as a CNAME domain name resolution, and the third is to place the verification code in a specific file in a specific directory on the web server. These control measures can effectively guarantee that only people control the domain name can apply for SSL certificate for this domain name. However, what should we do if the CA operator does not operate in accordance with this requirement to issue an SSL certificate? Or If the CA system is hacked and bypassed this validation mechanism? Before the certificate transparency system came out, there was really no way to know the behavior of these problems.

The certificate transparency log system can be simply understood that each certificate issued must be publicly disclosed in this system. In layman's terms, it must be publicized and applied for a "birth certificate" before the SSL certificate is born. The CA system submits the precertificate to the certificate transparency log system before issuing the certificate. Once the CA system get the certificate transparency signature data (SCT), which is equivalent to obtaining the "birth certificate". The CA system must embed the SCT data as an extension filed of the SSL certificate to the officially issued SSL certificate (carry the birth certificate with for checking), then the SSL certificate can be officially born, it can be deployed and used by users, and the browser will trust this certificate, because this certificate has been publicly disclosed in the certificate transparency log system. The reason why the "birth certificate" data should be embedded in the certificate is, of course, for the browser can verify it in real time whether it has been publicly disclosed, whether it has been publicly disclosed in the designated CT log system, and when it is logged. And the third-party monitoring system can monitor each issued SSL certificate in real time by searching and analyzing the CT database and can notify the user in real time once an illegally issued certificate is found. This is zero trust to CA system and CA operator, and it is a zero trust security measure that can effectively protect the security of SSL certificates.



The certificate transparency mechanism can also be compared to China ICP filing mechanism. Before a website domain name is activated, it must be filed first. To issue an SSL certificate, CA operator must file the precertificate to CT log system first. The difference is the CT filing procedures is simpler, just need to get a digital signature of the CT log system. But the mechanism is the same, improving transparency, reducing risk and strengthen supervision. In other words, it is the certificate transparency mechanism that protecting the security of each SSL certificate.

Let's look at the statistics of the certificate transparency log system. Since 2013, 7.3 billion SSL certificates have been logged. Google Chrome has been forcibly required every CA to issue every SSL certificate must be submitted to the designated certificate transparency log before being trusted by Google Chrome since May 2018. These log data are reliable data sources that the author released the SSL market analysis report quarterly, so the author explained in the report that the source of the data is "according to the Google Certificate Transparency log system", because this log data will not miss one SSL certificate, this is an absolutely reliable and trusted data.

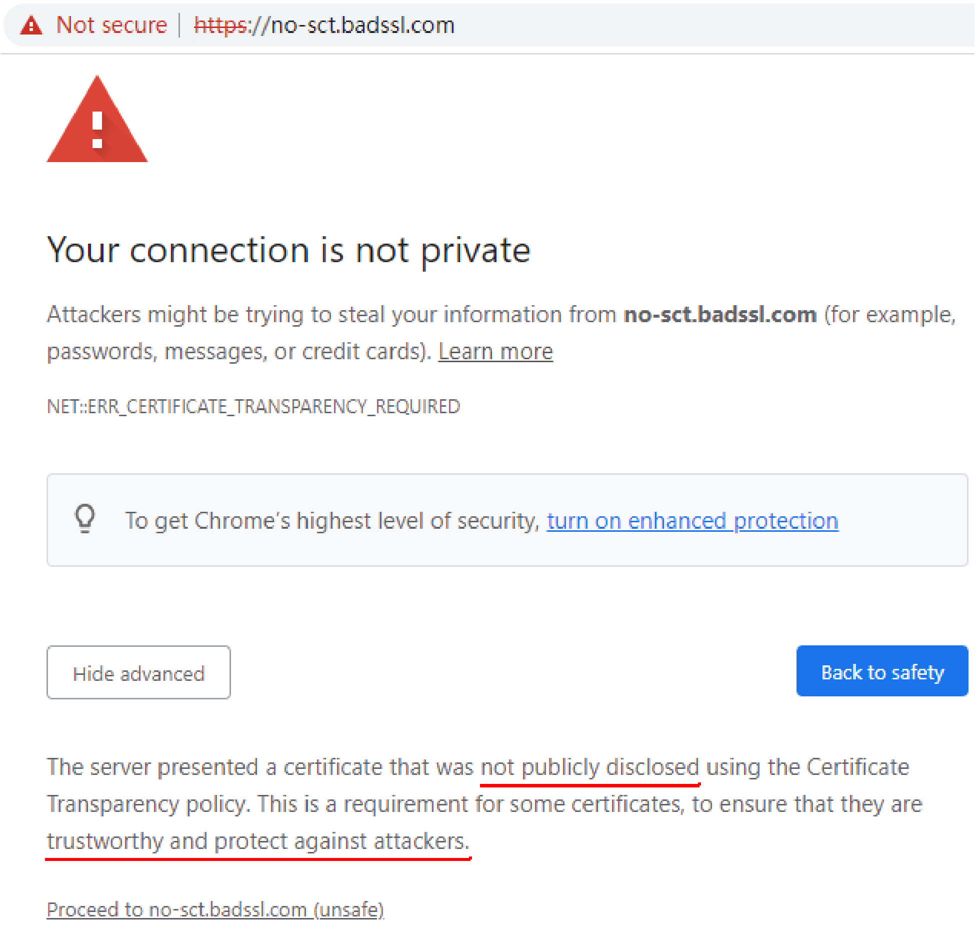


Since 2013

7,356,384,434

certificates have been logged

What happens if an SSL certificate is not logged in the certificate transparency log system? Google Chrome will not trust this SSL certificate, as shown in the figure below, the address bar displays “Not secure”, and "ERR_CERTIFICATE_TRANSPARENCY_REQUIRED". Clicking "Advanced", it says "The server presented a certificate that was not publicly disclosed using the Certificate Transparency policy. This is a requirement for some certificates, to ensure that they are trustworthy and protect against attackers." This is to say, this SSL certificate without the CT log data is not trustworthy due to the lack of public disclosure of the issuance behavior, which makes people suspect that it may be an SSL certificate used for malicious attacks.



Your connection is not private

Attackers might be trying to steal your information from **no-sct.badssl.com** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERTIFICATE_TRANSPARENCY_REQUIRED

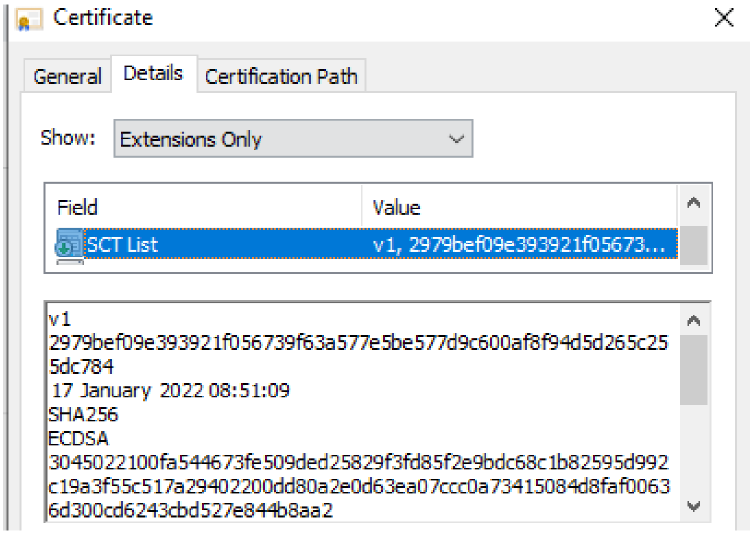
To get Chrome’s highest level of security, turn on enhanced protection

The server presented a certificate that was not publicly disclosed using the Certificate Transparency policy. This is a requirement for some certificates, to ensure that they are trustworthy and protect against attackers.

Proceed to no-sct.badssl.com (unsafe)

So, how do you know that the SSL certificate you got has been CT-logged? Or how to verify that the SSL certificate issued by the CA operator has been publicly disclosed to ensure that Google Chrome will not prompt "Not secure"? It is recommended that all users click to view the certificate details after getting the SSL certificate and see if there is a "SCT list" field in the certificate, as shown in the figure below, if there is, it means that this is a qualified certificate. You can look at several pieces of SCT data. Generally, there are two or three SCT data shown in the figure below. The first line of each SCT data is the version number of CT. Currently, all CAs are using V1 version, and certificate transparency

V2 version of RFC 9162 is still experimental. The second line is CT log server ID, the third line is the signature timestamp, the fourth line is the signature algorithm (SHA256/ECDSA), and the fifth line is the SCT signature data. The browser verifies these data to check whether the SSL certificate was logged and when it is logged, whether the certificate transparency log system is trusted by the browser, etc. Only after passing verification, the browser will display the padlock normally.



Show: Extensions Only

Field	Value
SCT List	v1, 2979bef09e393921f05673...

```
v1
2979bef09e393921f056739f63a577e5be577d9c600af8f94d5d265c25
5dc784
 17 January 2022 08:51:09
SHA256
ECDSA
3045022100fa544673fe509ded25829f3fd85f2e9bdc68c1b82595d992
c19a3f55c517a29402200dd80a2e0d63ea07ccc0a73415084d8faf0063
6d300cd6243cbd527e844b8aa2
```

The author believes that readers can already see that the certificate transparency mechanism is actually an ecosystem, it not only need a certificate transparency log system, but also need the joint participation of browsers, CA operators, monitors and other related product and service providers. Therefore, to be precise, it is the certificate transparency ecosystem that protects the security of the global trusted 7.3 billion SSL certificates, thus effectively ensuring https encryption security and global Internet security.

Richard Wang

Sept. 13, 2022
In Shenzhen, China