Popüler 500 Web Sitesinin Sertifika Şefaflığı Uyum Değerlendirmesi

Certificate Transparency Conformity Assessment of Top 500 Websites

Erhan TURAN
WISE Lab.,
Hacettepe University,
Ankara, Turkey
erhan.turan@hacettepe.edu.tr

Tamer ERGUN
e-Signature Technologies, Kamu SM,
BİLGEM, TÜBİTAK,
Ankara, Turkey
tamer.ergun@tubitak.gov.tr

Sevil SEN
WISE Lab.,
Hacettepe University,
Ankara, Turkey
ssen@cs.hacettepe.edu.tr

***Abstract*— Secure Socket Layer (SSL) certificates are electronic files used to encrypt data flow between clients and servers and to verify the identity of websites. SSL certificates are published by Certificate Authorities (CA) that are considered to be completely trustworthy. However, it is necessary to check whether or not a certificate has been accidentally issued by a CA without the user's consent. The Certificate Transparency (CT) Project, developed by Google, aims to satisfy this need within the SSL certificate validation system and offers an open framework to monitor and audit SSL certificates. Chrome requires that all TLS server certificates issued after April 30, 2018 must be compliant with the Chromium CT Policy. In this current study, we investigate whether or not websites and CAs are following this policy. The most popular 500 websites were therefore checked for their CT compliance with the methods that they use.**

Keywords—Certificate Transparency, SSL, Public Key Infrastructure

Özet*— *Güvenli Yuva Katmanı (SSL) sertifikaları, istemciler ve sunucular arasındaki veri akışını şifrelemek ve web sayfalarının kimliğini doğrulamak için kullanılan elektronik dosyalardır. SSL sertifikaları, güvenilir Elektronik Sertifika Hizmet Sağlayıcıları (ESHS) tarafından üretilirler. ESHS'ler ne kadar güvenilir olsalar da, bir sertifikanın ESHS tarafından kullanıcının izni olmaksızın (kazara) üretilip üretilmediğinin de kontrol edilmesi gerekmektedir. Google tarafından geliştirilen Sertifika Şeffaflığı (CT) Projesi, SSL doğrulama mekanizmasında bu ihtiyacı karşılamak ve SSL sertifikalarının takibini/ denetlenebilirliğini sağlamak için açık bir sistem sunmayı amaçlamaktadır. Chrome, 30 Nisan 2018'den sonra yayınlanan tüm SSL/TLS sunucu sertifikalarının Chromium CT Politikası ile uyumlu olmasını zorlamaktadır. Bu çalışmada, web sitelerinin ve ESHS'lerin bu politikaya ne kadar uyduğu araştırılmıştır. Bu doğrultuda, en popüler 500 web sitesinin uyumluluğu, kullandıkları CT yöntemleri de ele alınarak kontrol edilmiştir.

Anahtar Kelimeler—Sertifika Şefaflığı, SSL, Açık Anahtar Altyapısı

I. INTRODUCTION

SSL certificates provide trust-based web security by establishing secure connections between clients and servers. These certificates need to be validated before their use. The steps of the certificate validation system that web browsers use to verify websites' SSL/TLS certificate chain is specified in RFC 5280 [1]. By using this validation system, browsers can detect erroneous certificates such as those that have expired, where they have been signed by a fake authority, or if they have been revoked [2]. There are also problems associated with certification authorities [3]. However, identifying violations of trusted CAs is difficult. In some cases, such fraudulent attempts cannot be detected for weeks or even months.

There have been some faults regarding SSL certifications in recent years. For example, a Dutch certification authority (DigiNotar) was compromised and hackers used the cryptographic system of the certificate authority to generate fake SSL certificates [5]. The Internet sites used for spying in Iran have been presented to users as popular websites such as Gmail and Facebook. Following this event, the certificates issued by DigiNotar were revoked and the certificate authority has since been closed down. In another example, a Malaysian sub-root certificate authority (DigiCert Sdn. Bhd. Sub-root of the Entrust certificate authority) issued certificate revocation information and 22 weak signing certificates without the Extended Key Usage field [6]. Two of these certificates were used to sign malicious software that was employed in phishing attacks against an Asian certification authority. As a result of this, browsers deployed updates and all certificates issued by this CA were removed from their trusted root lists.

Certificate Transparency (CT) focuses on fraudulent attempts that are hard to detect using the existing certificate validation system; making it possible to detect certificates issued in error or by malicious intent, and to identify the issuing certification authority [4]. It is important for audit purposes to detect incompatibilities and vulnerabilities that can occur on the part of Certification Authorities, which is considered a major deficiency for SSL. Certificate Transparency is an open framework that monitors and inspects SSL/TLS certificates and does not disrupt the existing SSL/TLS certificate validation system that browsers have been using. The system is not an alternative or a substitute to the existing validation system of browsers. Instead, it adds new functions to the validation system and expands the certification chain verification steps in order to provide support for inspection of all SSL/TLS certificates.

Google announced that certificates issued after April 30, 2018 must be compatible with CT. Before the announcement, Nykvist et al. [7] studied the server-side adoption of CT. In their work, they examined the compatibility of websites and characterized the overheads and the potential performance impact of the Signed Certificate Timestamp (SCT) delivery methods. Since there was no obligation before the announcement, it is important to now assess the current process. For this purpose, this current study analyzed the status of the top 500 websites and their certificates issuers [8]. In addition, the compliance of web browsers was also checked.

II. CERTIFICATE TRANSPARENCY COMPONENTS

Certificate Transparency focuses on the problems of the existing SSL system that are difficult to detect. These issues are briefly described as follows.

Malicious certification authorities and Internet sites can take steps to trick users such as issuing fraudulent SSL certificates by certification authorities including the domains of well-known Internet sites, and the deception of users using these certificates on Internet sites within a 'man in the middle' attack.

Even in the absence of malicious intent, it is possible for certification authorities to make a mistake when producing SSL certificates. Many mistakes have been made by certification authorities in the past. These mistakes may not be detected for weeks or even months, with users having been victimized as a result. Certificate Transparency is proposed as a solution to such problems, and has three main objectives:

1. To make it impossible for certificate authorities to issue SSL certificates for a domain without the domain owner's knowledge.
2. To support an open audit and monitoring system that allows domain owners or the certification authority to check whether or not certificates have been produced in error or through malicious intent.
3. It is intended to protect users from certificates produced in error or through malicious intent.

Certificate Transparency aims to achieve these objectives through three main components: certificate logs, monitors, and auditors.

A. Certificate Logs

The most important component of the Certificate Transparency Project is the certificate log servers. A certificate log server is a simple network service that holds and protects hash values of SSL certificates. Certificate log servers have three main features:

- A certificate can only be appended to the log server (append-only) and the certificate record cannot be deleted, modified or retrospectively added.
- In the certificate log servers, a special cryptographic mechanism known as the Merkle Hash Tree is used to prevent subsequent modifications to the records which are cryptographically protected.
- Certificate log servers can be audited explicitly; anyone can query a log server and verify that an SSL certificate has been properly added to the log server.

Certificates are logged to the log servers and maintained securely. Log servers return a Signed Certificate Timestamp which is proof of logging.

B. Monitors

Companies which have websites need to know if any certificates are issued for their websites. Taking into account all of these logs, it is possible to check for the issuance of certificates.

Monitors are servers that periodically connect to the log servers, continuously check for suspicious certificates, and work explicitly. The monitoring function is similar to the credit reporting service, which notifies individuals when a fake credit card is issued on their behalf.

Monitoring tools are progressively developing. Facebook developed a monitoring tool for users and users can check the certificate issuance of their domains [9].

C. Auditors

Auditors are software components that typically perform two functions. It can be used to check whether or not an SSL certificate to be authenticated is in the log server. Auditors can verify that SSL certificates have been correctly added to the log server and are cryptographically consistent.

If SSL certificates to be authenticated are not included in the log server, they are marked as suspicious and subsequently, the TLS client may refuse connection to sites with suspicious certificates.

III. CERTIFICATE TRANSPARENCY LOG AND CONTROL

Certificate Transparency can be achieved via three methods according to the logging and control architecture. These methods are described in the following sections.

A. X509V3 Extension Method

X.509 is a standard that defines the format of certificates [1]. SSL Certificates have numerous fields conforming to the Certificate Authority/Browser (CA/B) Baseline Requirements [10]. In the X509v3 Extension method, as shown in Fig. 1, firstly a pre-certificate is created by the CA. A pre-certificate has a "poison extension" and thereby cannot be used as an actual SSL Certificate. Secondly, the pre-certificate is logged to the log server and gathers a log response which is known as a Signed Certificate Timestamp (SCT). The SCT is placed as an extension to the certificate and then the certificate is signed. The SCT is shared in the process of the SSL/TLS handshake within the certificate.

B. TLS Extension Method

In the SSL/TLS Extension method, as shown in Fig. 2, the certificate is logged by the domain owner to the log servers and the SCT is serviced by the web server in the process of the SSL handshake. With this method, the website admin needs to log the certificate and deploy the SCT to the server.

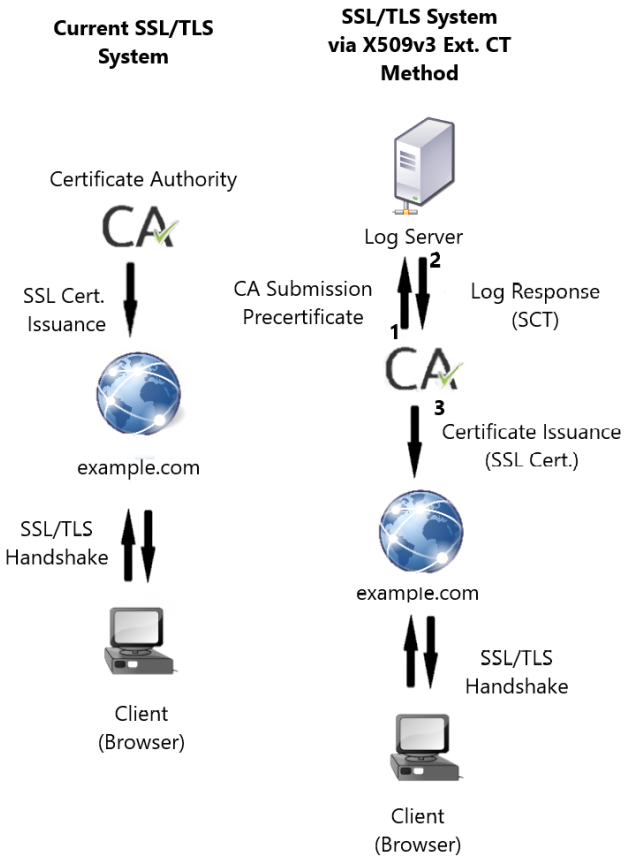

Fig. 1. X509v3 Extension Method

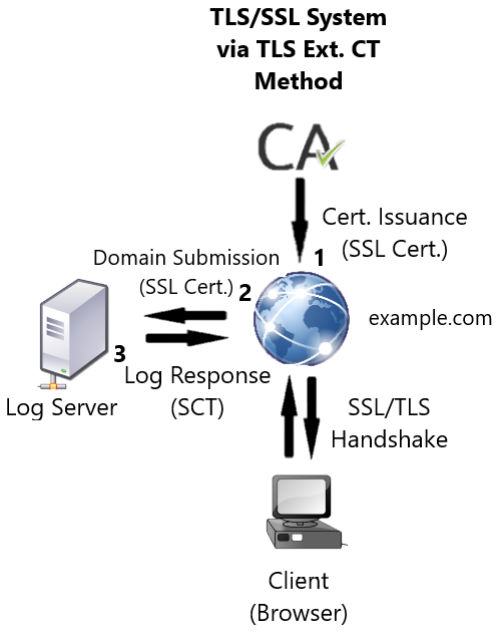

Fig. 2. SSL/TLS Extension Method

C. OCSP Stapling Method

Online Certificate Status Protocol (OCSP) is a protocol used for establishing the revocation status of a certificate [11]. In OCSP, a client sends an OCSP request to the OCSP server and the server creates and signs the OCSP response for the related request. OCSP stapling is a method for boosting the efficiency of the OCSP request and response process. In the OCSP stapling method, the server of the website sends a request for itself and gathers a response and serves this response to its clients. In the OCSP stapling method, as shown in Fig. 3, the certificate is logged to the log servers by the CA, and then the CA gathers the SCT from the log server and service inside of the OCSP response. Website servers obtain the OCSP response and serve it with its clients through OCSP Stapling.

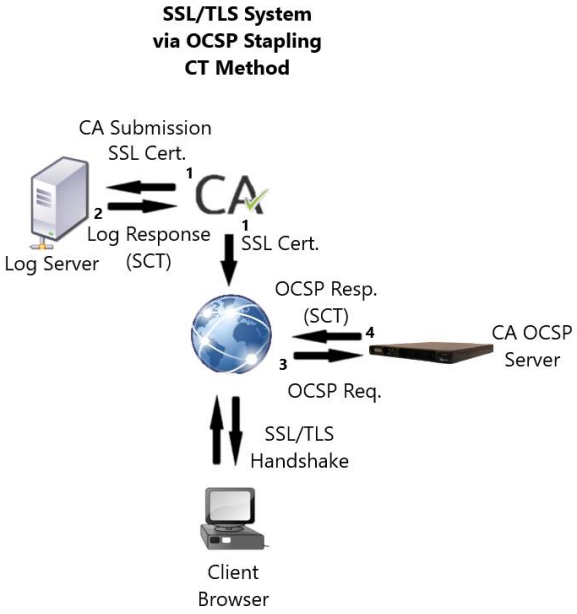

Fig. 3. OCSP Stapling Method

IV. The Process of Compliance With Certificate Transparency

The main components of Certificate Transparency (CT) in the light of Google's notifications are log servers and monitors, which can be operated by Google, certification authorities or third parties. Log servers are run by certification authorities such as DigiCert, WoSign, and StartCom. Auditors can also be run by browsers and clients who implement TLS.

Firstly, we examined browsers for their CT compliance as presented in Table I.

Google Chrome supports CT in versions released after January 2015.

Mozilla Firefox supports CT, and published its time schedule for CT on June 9, 2015 [12]. It is enabled within "about:config" security.pki.certificate_transparency.mode value=1 setting.

Safari announced that certificates issued after October 15, 2018, must meet their CT policy in order to be evaluated as trusted on Apple platforms [13]. However, the current version of Safari (v11) does not show any notification with regards to CT.

Yandex does not support CT. There is no information about CT on their website.

Internet Explorer does not support CT, but Microsoft developed a new extension to the Active Directory Certificate Services to support CT [14].

TABLE I. CT COMPLIANCE OF BROWSERS

	CT Compatibility of Browsers				
	Google Chrome v67.0	***Firefox v61.0.1***	***Safari v11***	***Yandex v18.6.1***	***Internet Explorer v11.165***
Compliance	✓	✓	✗	✗	✗

V. CERTIFICATE TRANSPARENCY CONFORMITY ASSESSMENT OF TOP 500 WEBSITES

Google announced that Chrome required all TLS server certificates issued after April 30, 2018 must be compliant with the Chromium CT Policy. After this date, when Chrome connects to a website serving a trusted certificate that is non-compliant to the Chromium CT Policy, Chrome will show a full-page warning that the connection is non-CT-compliant. CAs are strongly encouraged to work with their clients in order to ensure that their TLS certificates are compliant with the Chromium CT Policy through at least one of three methods mentioned in Section 3 before the end of March 2018 so as to ensure that any issues with deploying CT support are resolved in advance of the enforcement deadline. These changes were first rolled out to Desktop platforms, including macOS, Windows, Linux, and Chrome OS [15].

Experiments were conducted in this study in order to check the status of certificates for popular websites and CAs after Google's CT announcement. First, the names of the top 500 websites were obtained from the MoZ Top 500 on May 25, 2018. Then, a Certificate Transparency Control program was implemented in order to achieve the design needs. The program was developed on the Java platform using the Google Certificate Transparency API for handling SCT [16,17]. Where a certificate has a SCT extension, the browser can use it for checking. Windows OS shows a certificate transparency extension on their certificate viewer as shown in Fig. 4. OpenSSL is used for triple handshake packet capture in the SSL/TLS method.

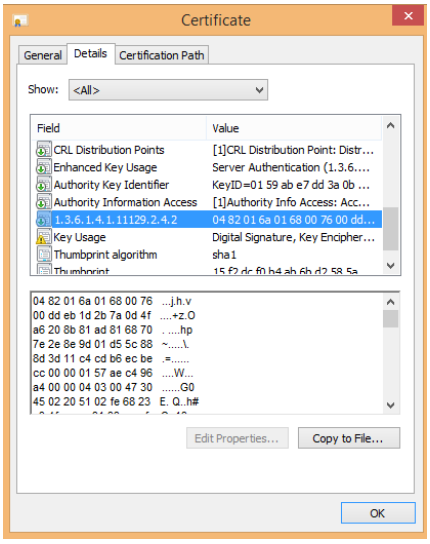

Fig. 4. Certificate with SCT Windows View

In our approach, we first fetch the certificate from the server and then parse the certificate in order to examine the SCT extension. If an SCT extension is found, other methods, OCSP Stapling and SSL/TLS handshake, are then checked. For the second method, OCSP stapling, a module was developed for checking the presence of the SCT in the OCSP responses. For the third method, TLS extension, OpenSSL is employed. The TLS responses are intervened and parsed in order to check the existence of SCT.

VI. RESULTS

The top 500 websites were analyzed. Details of the top 10 websites are given in Table II. It was determined that the dominant method (80%) used in the top 10 websites is the X509v3 extension method. The overall analysis of the top 500 websites is shown in Fig. 5. As shown in Fig. 5., while only half of the websites (54%) are CT-enabled, 16% of the websites do not even use SSL directly on their pages. As shown in Table III, the X509v3 extension method is widely used. Since the whole process could be achieved by only CAs without contribution from the domain owner with this method, it is therefore deemed easier to deploy. The OCSP stapling extension method was not used by the top 10 websites. The reason why it might not be the preferred method by CAs is that the OCSP stapling case domain owner has some responsibilities to perform. It can be hard to deal with domain-based problems during integration. The TLS extension method was found to be rarely used (15% of CT methods). We believe that the TLS extension method is only applied by domain owners who are CT-aware, and whose certificates do not include SCT. We found that 43 CA chains support CT methods and 17 CAs do not support any methods, as shown in Fig. 6. We found that some popular CAs are incompatible with CT. Microsoft and Yandex do not support CT as a CA (Microsoft IT TLS CA v5, Microsoft IT TLS CA v2, Yandex CA).

TABLE II. REPORT OF TOP 10 WEBSITES

	Top 10 Websites				
ID	***Site URL***	***X509v3 Ext. Method***	***OCSP S. Ext. Method***	***TLS Ext.***	***Stat***
1	https://facebook.com	✓	✗	✗	✓
2	https://twitter.com	✓	✗	✗	✓
3	https://google.com	✗	✗	✓	✓
4	https://youtube.com	✗	✗	✓	✓
5	https://instagram.com	✓	✗	✗	✓
6	https://linkedin.com	✓	✗	✗	✓
7	https://wordpress.org	✗	✗	✗	✗
8	https://pinterest.com	✓	✗	✗	✓
9	https://wikipedia.org	✓	✗	✗	✓
10	https://wordpress.com	✓	✗	✗	✓

These results show that Certificate Transparency is not implemented completely and that CAs commonly use the X509V3 method.

TABLE III. CT METHODS USAGE RATES

	CT Methods Usage Numbers		
ID	***X509v3 Ext. Method***	***OCSP Stapling Method***	***TLS Extension Method***
1	224	0	41

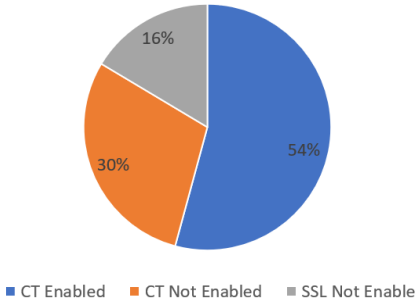

Fig. 5. CT Compliance of websites

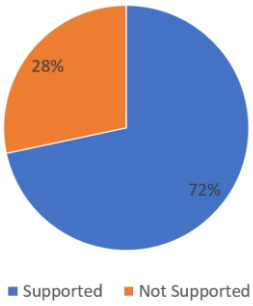

Fig. 6. CT Compliance of CAs

VII. CONCLUSION

In this study, the Certificate Transparency conformity assessment of top 500 websites and their certificate issuers were analyzed. It was observed that CT usage is not sufficiently widespread and that there are many CAs and websites which do not use CT or even SSL. The usage rates of CT methods were also explored. Although all three methods are deemed to be usable, user-friendly methods are preferred due to their ease of use for website admins. The OCSP stapling method is not used by the top websites. In this method, both the CA and the domain must work together for integration. It is believed that the CA chooses to implement the X509v3 extension method rather than the OCSP stapling method since logging and SCT deployment processes are challenging for website admins. This study is considered the first analysis of websites and browsers after Google's announcement on CT usage. There have already been some improvements seen on CT [18] and it is believed that studies in this area will increase in the near future. Hence, this current study makes a contribution to the literature by presenting the current status of websites and browsers.

VIII. REFERENCES

[1] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, "IETF, RFC5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", May 2008.

[2] D. Akhawe, B. Amann, M. Valentin, and R. Sommer, "Here's my cert, so trust me, maybe? Understanding TLS errors on the web", In Proceedings of the 22nd international conference on World Wide Web, pp. 59-70, May 2013.

[3] Z. Durumeric, J. Kasten, M. Bailey, J. A. Halderman, "Analysis of the HTTPS Certificate Ecosystem", IMC'13, pp. 23–25, October 2013,

[4] B. Laurie, A. Langley, E. Kasper, "IETF, RFC6962 – Certificate Transparency", June 2013.

[5] A. Johanna, G. Oliver, S. Quirin, B. Lexi, G. Carle, R. Holz, "Mission Accomplished? HTTPS Security after DigiNotar", Proceedings Of The 2017 Internet Measurement Conference IMC '17 pp. 325-340, November 2017.

[6] Mozilla Announcement for Digicert Revocation Process, https://blog.mozilla.org/security/2011/11/03/revoking-trust-in-digicert-sdn-bhd-intermediate-certificate-authority/".

[7] C. Nykvist, L. Sjöström, J. Gustafsson, N. Carlsson, "Server Side Adoption of Certificate Transparency", PAM 2018: Passive and Active Measurement, pp. 186-199, March 2018.

[8] Moz Top 500 Websites, https://moz.com/top500

[9] Facebook Certificate Transparency Monitor Tool, https://www.facebook.com/notes/protect-the-graph/introducing-our-certificate-transparency-monitoring-tool/1811919779048165/

[10] CA/Browser Forum. Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.5.9, June. 2018. https://cabforum.org/wp-content/uploads/CA-Browser-Forum-BR-1.5.9.pdf

[11] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, "IETF, RFC2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP", June 1999.

[12] Mozilla Time Schedule about Certificate Transparency, https://wiki.mozilla.org/SecurityEngineering/Certificate_Transpareny

[13] Apple Announcement about CT compliance and obligations, https://support.apple.com/en-us/HT205280

[14] Microsoft Announcement about CT compliance for ACCS https://support.microsoft.com/en-us/help/4093260/introduction-of-ad-cs-certificate-transparency

[15] CT Certificate Transparency Enforcement in Google Chrome Announcement, https://groups.google.com/a/chromium.org/forum/#!topic/ct-policy/wHILiYf31DE

[16] Google's Certificate Transparency Code Archive and Wiki, https://code.google.com/p/certificate-transparency/

[17] Google's Certificate Transparency Java API and Sample Codes, https://github.com/google/certificate-transparency

[18] R. Ellgren, T. Löfgren, "Distributed Client Driven Certificate Transparency Log", Linköping University, Department of Computer and Information Science Bachelor thesis, 2018