# SSL/TLS Security Exploration Through X.509 Certificate's Life Cycle Measurement

Peipei Fu, Zhen Li, Gang Xiong, Zigang Cao, and Cuicui Kang
Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China
lizhen@iie.ac.cn

***Abstract*—With the popular use of SSL/TLS, more and more web applications, such as online banking, e-mail, and e-commerce, turn to secured channels for communication, which rely on X.509 certificate for authentication. Generally, every certificate has a theoretical validity period when it is issued. However, the used period in practice is often different from the theoretical validity, namely, before or after the validity, for a long or short time. If a certificate is expired, it is easily to be exploited by cyber-attackers, leading to web users' personal information at risk. To explore the security flaws of the SSL/TLS certificate, we conduct a large-scale measurement study of X.509 certificate life cycle from the view of leaf certificates. Based on a passive data set collected over one year, we investigate the certificate validity period in a fine-grained manner, and uncover that the actual usage of the certificates are not satisfactory. Meanwhile, we discover several security-related issues that may leave the web communication at risk. The recommendations are summarized to ensure the long-term security for certificate use in practice. We believe that the work will be beneficial to web security and improve the certificate utilization in the future.**

***Index Terms*—X.509 certificate, measurement, life cycle, validity period, SSL/TLS security**

## I. Introduction

X.509 certificate[1], known as the public key certificate, is the most significant tool that websites rely on to establish trust with their users. It is the entity that SSL/TLS[2] protocols use for authentication. However, many factors can rise up serious problems of security, such as the spring up of self-signed certificates, the improper deployment, and the abuse of compromised certificates. Especially to the self-signed certificates, they are often used by malicious software and services. Some malicious server in APT1[5] have used self-signed certificates and most of the certificates listed in SSL Blacklist[6] are self-signed.

Each X.509 certificate is associated with a validity period, and the actual use time of it should be within that scope. While most servers renew their certificates before they expire, it also finds some expired certificates are still used in practice[11]. Some web security experts have noted that an expired SSL certificate can lead to phishing scams and the use of it will bring trust withdrawal [7]. Therefore, our work focuses on fine-grained study of the certificate and attempt to reveal the potential security risks of the validity period.

In this paper, we exploit the security of SSL/TLS security from the life cycle measurement of X.509 certificate. The life cycle of the certificate refers to the use time of the certificate. To the best of our knowledge, this is the first attempt. In our measurement, we collect X.509 certificates on two large research networks in China for more than one year from March 2016 to April 2017. Finally, we accumulate millions of leaf certificates, and continue to update their use time. With this dataset, the life cycle and security-relevant properties are investigated comprehensively.

In summary, we make the following contributions:

First, using passive measurement from two ISP level networks over one year, we investigate the certificate life cycle in theory and practice, and discuss anomalies we noticed during our measurement.

Second, by analyzing the validity period in theory, we present the validity period distribution of the certificates. The self-signed certificates that may lead to security problems are investigated. In our measurement, about 70% of the self-signed certificates' validity period are more than 3 years.

Third, by the actual use time analysis in practice, we reveal that the actual usage of the certificate are not satisfactory. Meanwhile, we deeply analyze the certificates only used for one day and the expired ones, and discuss their impact on the security of the certificate.

Finally, based on the measurement, we find the real usage of certificates is not optimistic and highlight the importance of the measurement to the web security. We also make recommendations to enhance the security and utilization of the certificate.

The rest of the paper is organized as follows. The related work is presented in section II. Then, section III presents our data sets that we used in our analysis. The investigation of the X.509 certificates is presented in Section IV and the related security issues is also analyzed deeply. Finally, Section V concludes the paper.

## II. Related Work

As SSL/TLS has been widely used, the research on SSL/TLS has always been active in the field of network security and measurement during the past decade. Some previous works focus on the weakness of the SSL/TLS protocol itself. Specifically, the security flaws in SSL/TLS implementations are discussed by Brubaker et al. in [11], the study of common TLS warnings and connections is presented in [4], [10], and Olivier et al. [3] analyze the SSL host security from cipher suites, certificate chain and so on. In our work, we are only

978-1-5386-6950-1/18/$31.00 ©2018 IEEE

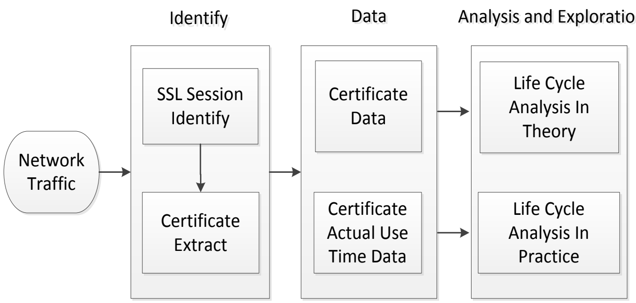


Fig. 1. The framework of our work.

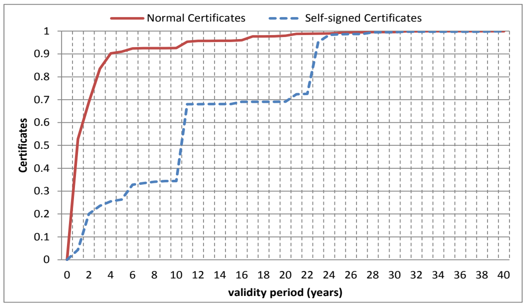


Fig. 2. The CDF of validity period.

concerned with the exploration of the certificate life cycle to uncover the potential risk.

Since SSL/TLS relies on X.509 certificate for authentication, it is a general approach to investigate SSL/TLS security through the measurement and analysis of the certificates. Holz et al. [8] present a comprehensive analysis of X.509 certificates from active and passive measurements. Durumeric et al. [9] report the results of a large-scale measurement study of the HTTPS certificate ecosystem in the field of active measurement using Zmap to complete scan.

However, although SSL/TLS related research has gradually matured, but the measuring work of our paper compared with the existing measurements, there is a big difference in emphasis. For the works in [8], [9], have some analysis about the validity period, but they focus on the overall ecosystem rather than fine-grained points. And, their work are performed using the active measurement, which is different from our pure passive measurement.

## III. Data Set

Each X.509 digital certificate includes the following information: version, serial number, signature, issuer, validity, subject, information on the public key of the subject. At the same time, subject and issuer fields also include common name(CN), country name, organization name and so on. Common name and validity in certificate present the information related to the application and the certificate validity period respectively. In this paper, we focus only on the leaf certificate as it can indicate which kind of application or service the user uses.

We adopt a high-performance network traffic process system to identify SSL/TLS session on two large research networks, draw certificate information and conduct detailed investigations (see Fig. 1). We extract certificates appearing in the SSL/TLS sessions at both gateways. All SSL/TLS traffic is identified no matter which port the SSL/TLS service is running at. Finally, we complete the collection of two kinds of data sets:

1. The certificate data set: it describes the detailed information of the certificates, including validity period, issuer CN, subject CN, public key length.
2. The actual use time data set: it describes the actual use time of the certificates, including the first and recent use time.

From March 2016 to April 2017, we have completed the collection of X.509 certificates, over a time span of one year. We accumulate the certificate regularly and update the use time of a certificate every day. We have collected **13,092,365** unique certificates totally, including 3,665,030 self-signed certificates and 9,427,335 normal certificates. Here, the self-signed certificate is a special kind of certificate issued by itself, i.e., issuer and subject are the same. The normal certificates here refer to those certificates excluding the self-signed certificates.

## IV. Measurement and Investigation

This section aims to describe the overall results of our analysis and measurement.

### A. The Life Cycle Measurement in Theory

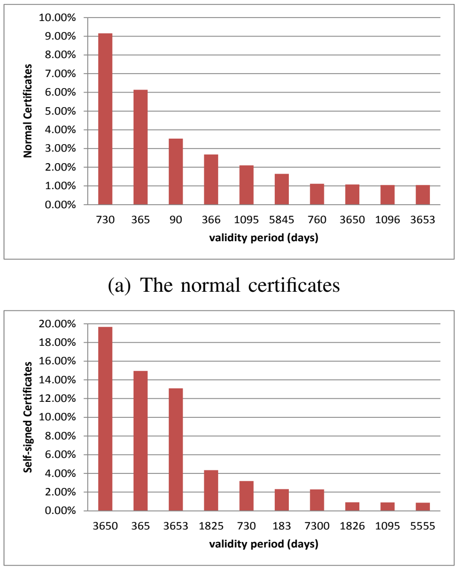
The theoretical life cycle of a certificate refers to the available time of the certificate in theory, namely the validity period. We measure the validity period of certificates from two kinds of certificates, the self-signed certificates and the normal ones. Fig. 2 shows the CDF of the validity period. We find 90% of normal certificates are issued within 4 years. However, to the self-signed certificates, there are big fluctuations in two time periods: 10-11 and 22-23 years, respectively. It indicates that validity period of most self-signed certificates are set in these two time periods. In addition, until 23 years, the CDF of the self-signed certificate reach to 95%, and these certificates with long validity are far beyond the predicted security of the keys they contain.

Although two kinds of certificates are both used to encrypt and ensure data integrity, according to the measurement results, we find there is a big difference between the normal certificates and the self-signed ones in validity period distribution. The main reason for the result is that the self-signed certificates are signed by themselves rather than by a trusted certificate authority. They can set the validity period randomly without any other restrictions.

*1) The analysis of the self-signed certificate:* By comparing the two kinds of certificate validity periods, we observe that the validity period of self-signed certificate is much longer than the normal certificate. The top 10 validity period distributions are shown in Fig.3 respectively.

From the result, we can get that the validity period distribution of a normal certificate is in a relatively short time,

978-1-5386-6950-1/18/$31.00 ©2018 IEEE



(a) The normal certificates

(b) The self-signed certificates

Fig. 3. The top 10 validity period distributions.

the validity period within three years counts to **86%**. 730 days (namely two years) period is the highest and reaches to around 9%, then 365 days period and 90 days period. However, a great amount of the validity period of self-signed certificate are in a relatively long time, such as the rate of 3650 days (namely 10 years) period is nearly 20%. And the validity period of the certificate more than three years counts for **70%**.

Shortening the validity period will greatly improve web security by requiring administrators to update and verify their certificates more often. Therefore, a certificate should be issued with shorter length of the validity period to ensure its security. So the self-signed certificates are more difficult to guarantee their security because of their long validity period.

*2) Some abnormal observations:* We also observe a variety of unexpected phenomena during our analysis of the validity period of the certificates.

The actual use time before the date on which the certificate validity period begins. This kind of phenomenon actually should not appear. It is impossible for a certificate used by others before issuing. But in our measurement, we find 2,247 certificates are used before issuing time. The existence of this phenomenon may present that the validity of a certificate is misconfigured or it is a kind of malicious behaviors.

The date on which the certificate validity period begins less than the year of 1950. According to the regulations of the PKI birth time and the RFC[1], the date on which the certificate validity period begins are not as early as 1950. However, we find a few certificates of which the initial time of the validity period is earlier than 1950. Based on the passive measurement we implemented, we discover that, the earliest taking effect time could be traced back to 1910 in the self-signed certificate. And for the normal certificates, the value is changed to 1900. All these kinds of certificates are generally identified as fake certificates.

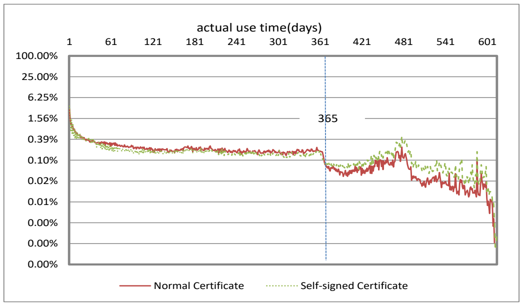


Fig. 4. Validity period is 365 days.

In fact, the above phenomenon should not be appeared in practical use of a certificate. Generally, a well-known or trusted CA will not issue these kinds of certificates. The existence of the phenomenon indicates that some certificates on the Internet are not used correctly, or they may be the forged certificates for doing something bad, because most of these certificates are self-signed who can't verify their legitimacy.

## *B. The Life Cycle Measurement in Practice*

We present the measurement results of the actual use of the certificate in this section. From the analysis, we get a thorough distribution of the actual use time.

Based on the validity period distribution in section IV-A, the validity period of a large amount of certificates are set to 365 days. We then analyze the actual use time distribution of certificates whose validity period is 365 days.

According to the Fig. 4, we get that the actual use time distribution of normal and self-signed certificate is very similar. The actual use time of most certificates are very short. For the normal certificate, the percentage of actual time span less than 365 days is 95.78%; and 6.43% certificates are still used when expired, namely, the actual usage time is more than 365 days. And for the self-signed certificate, the percentage is changed to 90.36% and 9.64%. Furthermore, it finds that a vast majority of certificates are appeared only one day and some certificates still used when they expired.

*1) The analysis of the certificate only used for one day:* From the analysis results, we find that the actual use time of most certificates are no more than one day. Therefore, we conduct a deep analysis on our entire data sets. It finds that the actual use time of most certificates are very short or even the first and the last use time is the same day, accounting for 68.7% of the entire data sets. Then, we take a deep inspection of the kind of certificate starting from the certificates' common name and attempt to trace out who used these certificates.

First, from the analysis of the Common Names, we find that there are about 75.7% of certificates whose subject CN and issuer CN consistent with Tor's certificate characteristic which is described in [12], we speculate that these kinds of certificates are used by Tor, and the certificates are generated automatically, and changing their certificates CN constantly.

Second, we inspect those certificates excluding the Tor certificates. It reveals that most of the certificates are belonged to the self-signed ones. Most of the certificate CNs are used for local application(e.g.,192.168.1.1), device application(e.g.,OpenWrt), temporary application(e.g.,ASA Temporary Self Signed Certificate) or proxy application(e.g.,mitmproxy).

Based on the above analysis, we conclude that some special application, like Tor, fast flux their certificates, resulting in the low certificate effective utilization rate. Most of these certificates are only temporarily used, or may be a kind of fast-flux covert service to evade detection. Whatever the reason, the emergence of this phenomenon poses a great challenge to the network management.

*2) The analysis of the expired certificate:* Generally, after the end of the validity period, the certificate is no longer considered an acceptable or usable credential. The browser will pop up a security warning when website use the expired certificate. In our measurement, while most of the actual use time of the certificate is within the validity period, we also find expired certificates are still used in practice. We find that 49.6% certificates are expired in the dataset at the end of observation, and 17.5% of those are still used. From the result, we find that most of the expired certificates, no matter the self-signed or the normal ones, most focus on ”localhost”, ”localhost.localdomain” and virtualization field (like Parallels Panel etc.), which can hide their practical applications and information. According to the malicious SSL certificates listed in the SSL Blacklist[6], we find out 5 SSL certificates' common name are ”localhost.localdomain”, and 221 SSL certificates' common name are ”localhost” in 2465 blacklisted SSL certificates. Therefore, these certificate common names are exploited by malicious application easily. In order to improve the situation and avoid the malicious use of expired certificates, the user of the certificate should improve their safety awareness and audit the effectiveness of the certificate when using it.

Through the analysis and measurement of the life cycle of the leaf certificate, we find that the real situation of the certificate usage is not optimistic. In order to create a more harmonious environment for the use of certificates, we summary some recommendations to ensure the long-term security. For security's sake, the web service or application should use the certificate issued by a trusted CA. Even if self-signed certificates are often chosen by many web services and applications from the perspective of economy and convenience, it should be issued with a shorter validity period to ensure security. Once the certificate has expired, it should be renewed timely in case of malicious use. In addition, it is necessary to avoid unreasonable use of certificates, such as the certificate only used for one day, to improve the utilization of certificates.

Although we only select the validity period of the certificate for analysis, many problems in the use of the certificate are discovered and some findings or anomalies are deeply analyzed. However, some discovered problems still can not be well explained. In our future work, we will combine other method or technology, such as the active scanning and detection, and not just the passive measurement to dig into these problems.

## V. Conclusion

In this paper, we have conducted a detailed inspection of the SSL/TLS certificate security. Using the data sets collected over one year, the validity period and the actual use time of the leaf certificates are investigated. From the aspect of the theoretic analysis, we find a big difference between the self-signed certificates and the normal ones. From the practical aspect, we uncover the non-optimistic usage of certificates in practice, which shows that a large amount of certificates are only used for a short time. Meanwhile, the study provides detailed and fine-grained visibility into the security issues of the SSL/TLS certificates, and gives some recommendations for the practical use of the certificates. In our future work, we should make further research on the security exploration, and complete the secure investigation into the life cycle of the entire certificate chain.

## Acknowledgment

This work is supported by The National Key Research and Development Program of China (No.2016QY05X1000 and No.2016YFB0801200) and The National Natural Science Foundation of China (No.61702501). Research is also supported by the CAS/SAFEA International Partnership Program for Creative Research Teams and IIE, CAS international cooperation project. Zhen Li is the corresponding author.

## References

[1] Cooper,D., et al., ”Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (IETF RFC5280),” http://www.ietf.org/rfc/rfc5280.txt, 2008.

[2] Dierks T., Rescorla E., ”The transport layer security (TLS) protocol version 1.2(RFC 5246),” http://www.ietf.org/rfc/rfc5246.txt ,2008.

[3] Levillain O, et al., ”One year of SSL internet measurement,” In Proceedings of the 28th Annual Computer Security Applications Conference, NY, USA , pp. 11-20, 2012.

[4] Akhawe, D., Amann, B., Vallentin, M., and Sommer, R., ”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, New York, NY, USA , pp. 59-70, 2013.

[5] Mcwhorter, Dan., ”Mandiant Exposes APT1-One of China's Cyber Espionage Units & Releases 3,000 Indicators,” Mandiant, February 18, 2013.

[6] SSL Blacklist, ”https://sslbl.abuse.ch/.”

[7] Hazards of an Expired SSL certificate, ”https://comodosslstore.com/blog/hazards-of-an-expired-ssl-certificate.html.”

[8] Holz R., Braun L., Kammenhuber N., et al, ”The SSL landscape: a thorough analysis of the x. 509 PKI using active and passive measurements,” In Proceedings of the 2011 ACM SIGCOMM Conference on Internet Measurement, Toronto, Ontario, Canada ,pp. 427-444,2011.

[9] Durumeric Z., Kasten J., Bailey M., et al., ”Analysis of the HTTPS certificate ecosystem,” In Proceedings of the 2013 conference on Internet measurement conference, ACM, Barcelona, Spain ,pp. 291-304, 2013.

[10] Lee H. K., Malkin T., and Nahum E., ”Cryptographic strength of SSL/TLS servers: Current and recent practices,” In Proc. 7th ACM SIGCOMM Conference on Internet Measurement, San Diego, CA, USA, pp. 83-92, 2007.

[11] Brubaker C., Jana S., Ray B., Khurshid S., and Shmatikov V., ”Using frankencerts for automated adversarial testing of certificate validation in ssl/tls implementations,” In IEEE Symposium on Security and Privacy, Washington, pp. 114-129. 2014.

[12] Amann J, Sommer R., ”Exploring Tor's Activity Through Long-Term Passive TLS Traffic Measurement,” In International Conference on Passive and Active Network Measurement. Springer International Publishing, pp.3-15, 2016.