Journal of Technological Innovations

Est. 2020

Handling SSL Certificate Challenges & Solutions Properly for Improved Network Security

Prashanth Kodurupati

Information Technology, Managed File Transfer Engineer, Minisoft Technology LLC

Alpharetta, United States of America

Prashanth.bachi21@gmail.com

Abstract:

Cyberattack cases rise along with the growth of the internet across the globe. Therefore, the corresponding need for a cybersecurity protocol becomes the most needful as well. SSL is usually a known as an encryption protocol that was designed to provide security as well as authentication when there is an interaction between two or more people across the network setting. However, there are several SSL-related challenges, as well, such as certificate expiration, mismatching serial number, and length and size of the certificate. This paper will discuss automated reminders as a key solution that network providers and users can implement to ensure the certificate remains up to date, is fully supported, and compatible with the network's requirements.

Keywords: SSL certificate, secure socket layer, network security, cryptography, communications, authentication

1. Introduction

The Information Age has brought forth a new era of communications and network reliance for the entire globe. Whether it is a simple chat between friends, banking system or a regular security check where PII (personally identifiable information) is needed, the need for a constant flow of information in a online setting, based on every byte of data shared is huge since the data is confidential. Nevertheless, the year of 2022 records the quickest acceleration in both the number of attacks and the amount of attack volume[1].

Nowadays the cybersecurity has vastly changed, and forecasting possible impact of criminals, when the new year on the other hand is on the way, is getting to be extremely challenging. Furthermore, an individual's privacy has also become a major concern. In such a world, the need for robust and strong security measures in network setting is key to protect sensitive data from unauthorized access is at an all-time high. One such security measure is the Secure Socket Layer (SSL)[2]. It is a cryptographic protocol designed to be implemented on networks to ensure secure communications over websites, applications, and more on a computer network.

SSL Certificates have become a staple for network security recently. They provide a secure channel between machines operating over the internet, be it an external or internal network. As a result, they have now become the first line of defense, encrypting data to keep it safe from attackers.

However, the effectiveness of SSL certificates is subject to a large number of issues, such as user error, implementation issues, certificate expiration, mismatching serial numbers, and inappropriate length and size of the certificate being implemented.

Naturally, poor implementation or a lack of maintenance therein can lead to a number of issues, not only for the direct user, but all others on the same network as well. There are several ways to test the integrity of and SSL certificate, called challenges. These include the HTML-01, DNS-01, TLS-SNI-01, TLS-ALPN-01, and more [3][4].

This paper will look into these challenges and explore the solutions therein, focusing particularly on the use of automated reminders to maintain certificates' expiration. Furthermore, these reminders aim to ensure compatibility of the certificates with network requirements. Ensuring that the primary issues with SSL Certificate maintenance are catered to will help users improve their network security and in turn, maintain a safe operating environment.

2. Literature Review

The literature surrounding SSL/TLS certificates and network security highlights several key challenges and proposed solutions.

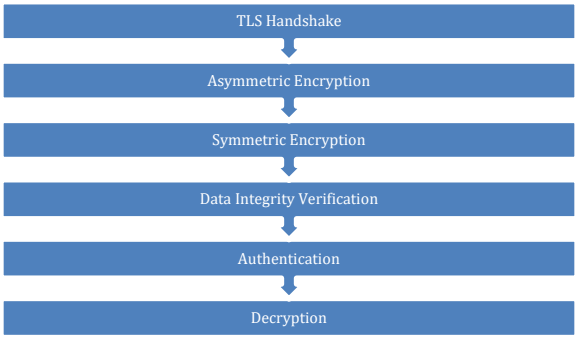
Mohammed et al. conducted a literature review on financial losses statistics for cybersecurity and future trends, shedding light on the economic impacts of cyber threats. Similarly, Thomasprovided foundational knowledge in SSL/TLS essentials, offering insights into the core principles and functionalities of secure socket layer protocols.

3. Problem Statement –Certificate Expiration in SSL/TSL Settings

Secure Socket Layer (SSL), also known as Transport Layer Security (TLS), starts off with a TLS handshake[5], where the two communicating systems establish a secure connection with each other by sharing a public key with each other. This "handshake" allows the client and server to use dedicated keys to exchange randomly generated data that is used to create new keys. This is known as a session key. The performance of this handshake can be improved via data batching, if needed. [6]

Next, the TLS handshake utilizes asymmetric encryption, i.e., two different keys are used at both ends of the conversation. This is done via public key cryptography. Here, one key is made publicly available while the other remains a secret. This secret key is only for the server side. There is also the option of symmetric encryption, which uses the same key on both sides. The most common type of symmetric algorithms used are AES-192 and AES-256. While communicating, SSL digitally signs the data to ensure data integrity. This signature ensures that the data has not been tampered with before being transferred or decrypted at the other end.

Once the data is received at the client side, the SSL certificate verifies it using the encryption key(s) used in the first step. This is called authentication. Once verified and the certificate ensures that both sides of the communication are for and by the intended parties, the data is then decrypted.



Throughout this process, ensuring that the data is securely encrypted and verified, and decrypted ultimately falls on the SSL/TSL certificate.

The Issue of Certificate Expiration

SSL/TLS certificates is different from each other and none of them is valid always. They all have an expiration time and it is necessary to notice their expiration and replace outdated with new. The Certificate Authority/Browser Forum - a de facto self-regulating organization of the SSL/TLS industry, decreed that the Certificates (or SSL certificates) shall contain validity period and no more than 27 months.This means that every website needs to renew or replace its SSL certificate at least once every two years.

When an SSL certificate expires but remains on a website's server, all web and mobile browsers will show the site as "Not secure". This red security warning can overshadow all the hard work put into the website, and if not addressed quickly, the website's traffic can suffer as well. Furthermore, even if traffic does enter the website, their security may be compromised. This is particularly the case for internal networks, where a single vulnerability is all it takes for a potential attack.

IPv4 studies have shown that on average, more than 65% of all SSL certificates are invalid, either due to expiry, size issues, length limitations, or poor implementation of the algorithm[7][2].

Consequences of Certificate Expiration

There are several dire circumstances that may arise due to an expired SSL certificate, ranging from poor performance and security risks to revenue and trust losses – for the website owner as well as the end user.

Security Risks

Once an SSL certificate expires, other clients (users with browsers) cannot verify your website's authenticity. In addition, it may not comply with the latest security standards, leading to vulnerabilities in encryption mechanisms.

Ultimately SSL certificates that have expired will be the loopholes for cyber criminals to exploit the networks and transmitted data via interception without authentication. The network will be vulnerable to unauthorized entry, which causes unapproved information transmission and database manipulation after the fingerprint absence in certificates which provide cryptographic safeguards.

Loss of Trust

Expiring SSL certificates undermine user confidence in the reliability and authenticity of the network's security infrastructure. Users are confronted with messages and errors associated with certificates expiry may, in turn, make them unsure whether the platform they use is safe and thus discourage their further involvement.

Service Disruption

Some Web browsers or client-sided applications may form behind the times servers which have this type of expired certificates thus leading to service disruptions as well as user inconveniences. Service disruption badly breaks through user experience that makes it inefficient and may cause business a bit of money or assets.

Regulatory Non-Compliance

Agreeing to imperatives set forth by authorities and having industry standard norms implies keeping valid SSL certificates to protect sensitive data and privacy rules, at the same time.

Reputational Implications

Since expired SSL certificates represent a poor cybersecurity and an operational compliance issues, this is a reason why these certificates should not be present in an organization.

Incorrect SSL Certificate Size and Length

The length and scale of an SSL certificate also possess a crucial area of influence whether it will be effective or not. SSL certificates signed with RSA keys less than 2048 bits constitute weak ones as due to the laps in computing power they will force the certificates to be broken in quite short time.[8]

A successful attack of this nature would provide an attacker with clear text access to encrypted data as it's in transit between client and server.

Longer keys require more computation time on both the server and the client. For example, 4096-bit RSA key verification is approximately 10 times slower to process than 2048-bit RSA key verification.

Challenges in Managing SSL Key Expiration

Certificate authority must have the SSL keys for expired certificates to maintain proper SSL/TLS certificate management. Though key revoke is often perceived as the main key to the stability of the system, there are several reasons why more than 65% of companies fail at it.

Complexity of Timely Key Rotation

One of the primary challenges in managing SSL key expiration is ensuring timely key rotation. This involves generating and distributing new keys before the old ones expire[7]. A delay in this process can lead to the system downtime, which can be enormous for the system of the law enforcement or others.

The more frequent expiration of the certificates will enable implementing security and cryptographic algorithms updates more quickly, as well as replacing a certain portion of certificates and private keys significantly faster during emergency situations like malicious cyberattacks.

Synchronization and Backward Compatibility

Maintaining synchronization across all systems is another challenge. All systems using a particular key need to switch to the new key simultaneously when the old key expires. Failure to do so can result in communication failures and data loss.

Security Risks

Securely storing expired keys is another issue. Expired keys, if fallen into the wrong hands, can still be used to decrypt old data. Therefore, expired keys must be stored securely if they are not immediately destroyed. Once an SSL certificate expires, other clients (users with browsers) cannot verify your website authenticity.

Lack of Centralized Visibility and Control

Inadequate visibility and control over SSL key lifecycle events impede organizations' ability to proactively monitor key expiration and renewal activities.

Without centralized oversight mechanisms and real-time monitoring capabilities, organizations may overlook critical key expiration events, leading to security vulnerabilities, service disruptions, and compliance violations.

4. Academic Review of Key Challenges and Proposed Solutions

Research	Challenge	Solution
Mohammed et al. [1]	Financial Losses Statistics for Cybersecurity	Future Trends Analysis
Thomas [2]	Understanding SSL/TLS Essentials	Foundational Knowledge
Clark and Oorschot [3]	SSL and HTTPS Challenges	Certificate Trust Model Enhancements
Sippo [4]	Time-based SSL/TLS Expiration	Timely Renewal Importance
Cai et al. [5], Boneh [6]	SSL Handshake Performance	Protocol Optimization
Chung et al. [7]	Invalid SSL Certificates	Certificate Validity Analysis
Ikbal [8]	Weaknesses in SSL/TLS Certificates	Security Recommendations

5. Proposed Solution: Automated Notifications for Certificate Expiration

Addressing the common obstacles that everyone encounters upon the expiration of the existing SSL/TLS certificates, the implementation of notification system becomes an essential way to combat the problem promptly and efficiently.

The proposed solution is to put an automated system in place that would track the expiry date of the SSL certificates and send out notifications to inform your organization when these certificates are almost to expiring the date.

This infrastructure can be plugged into any existing certificate management system and set off alert messages to the authorized site owners like system administrators or IT managers. With that, the organization will be able to maintain a consistent safety plan, as well as boost the operational efficiency and compliance issues to the regulations that will be provided.

Implementation of the process typically involves four steps:

1. Monitoring Setup: Parameterizing the monitoring system to observe the life cycles of the SSL/TLS certificates' validity.

2. Threshold Setting: Setting a threshold (e.g., 30 days before expiration) at which the system will trigger a notification.

3. Notification Configuration: Configuring the system to send notifications to the appropriate recipients.

4. Testing: Testing the system to ensure that it correctly identifies certificates nearing expiration and sends notifications as expected.

This automated notification system can be integrated with existing certificate management systems quite easily as well. This integration allows for a seamless flow of information and ensures that all certificates, regardless of where they are managed, are monitored for expiration.

An analysis of the methodology and issue shows that having an automated certificate update protocol in place is no longer just a “nice-to-have” but has become a “must-have” due to the increased cybersecurity issues.

6. Use Case: Setting up SSL Certificate Expiry Alerts in Google Cloud Platform (GCP)

When working on a GCP project, one key issue to deal with includes handling cloud security. Establishing alert policies for Google-managed certificates to receive notifications is a great way to do that. The automated algorithm must be able to notify relevant parties well in advance of their expiration, typically 5- or 10-days prior.

This can be accomplished by:

1. Heading to Monitoring>Alerting>Create Policy section.

2. Selecting the relevant metric associated with SSL certificate expiration.

3. Setting the threshold value to any value below 90 days, the typical lifespan of a GCP managed certificate.

4. Choosing "Below Threshold" as the threshold position to trigger alerts when the SSL certificate expiration is within the specified time frame.

5. Configuring the notification channel to determine who receives the alerts.

After configuration of alerts, visual representations continue to display the remaining time until certificate expiration as an orange line. On the other hand, the threshold value is visible as a red line,

based on the value set by the developer or manager for triggering alerts.

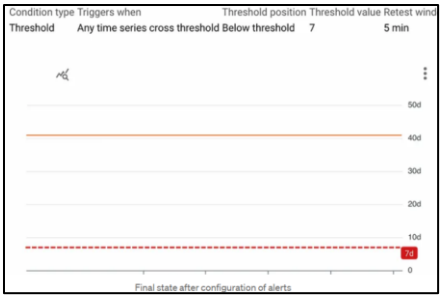


Figure 1: GCP Screenshot for setting SSL Certificate reminder

Alerts will be triggered whenever the orange line falls below the red line, indicating imminent certificate expiration.

7. Conclusion

Establishing alerts for SSL certificate expiration within a Google Cloud Platform (GCP) project reflects a proactive strategy towards maintaining service security and continuity. With the growing reliance on secure data transmission, timely certificate renewal is crucial.

Automated alerts let organizations mitigate risks associated with expired certificates, preventing service disruptions, security vulnerabilities, and erosion of user trust.

IT teams receive timely notifications, allowing them to renew or replace certificates without impacting critical services. This also allows time for research to ensure compatibility in terms of length, size, and nature of the certificate.

8. References

[1] M. H. U. S. *. a. M. A. Mohammed, "A literature review of financial losses statistics for cyber security and future trend," World Journal of Advanced Research and Reviews, 13 05 2022.

[2] S. Thomas, SSL & TLs Essentials, USA, 2000.

[3] J. Clark and P. C. v. Oorschot, "SoK: SSL and HTTPS: Revisiting Past Challenges and Evaluating Certificate Trust Model Enhancements," in IEEE Symposium on Security and Privacy, 2013.

[4] M. Sippo, "Time-based expiration problem of the SSL/TLS certificates," Tietojärjestelmätiede, 2021.

[5] J. Cai, X. Huang, J. Zhang, J. Zhao, Y. Lei, D. Liu and X. Ma, "A Handshake Protocol With Unbalanced Cost for Wireless Updating," IEEE Access, vol. 6, pp. 18570 - 18581, 27 03 2018.

[6] H. S. &. D. Boneh, "Improving SSL Handshake Performance via Batching," Cryptographers' Track at the RSA Conference, vol. 2020, pp. 28-43, 2001.

[7] Y. L. D. C. D. L. B. M. M. A. M. C. W. Taejoong Chung, "Measuring and Applying Invalid SSL Certificates: The Silent Majority," in IMC '16: Proceedings of the 2016 Internet Measurement Conference, November 2016.

[8] A. Ikbal, "Reduce Your Risks: SSL / TLS Certificate Weaknesses," 2017. [Online]. Available: https://perspectiverisk.com/multiple-ssl-tls-certificate-weaknesses.