NIST SPECIAL PUBLICATION 1800-16A

Securing Web Transactions

TLS Server Certificate Management

Volume A:
Executive Summary

William Haag
Murugiah Souppaya
NIST

Paul Turner
Venafi

William C. Barker
Dakota Consulting

Mary Raguso
Susan Symington
The MITRE Corporation

July 2019

DRAFT

This publication is available free of charge from:
https://www.nccoe.nist.gov/projects/building-blocks/tls-server-certificate-management

Executive Summary

The internet has enabled rapid, seamless commerce across the globe. Billions of dollars' worth of transactions are performed across the internet every day. This is possible only because connections across the internet are trusted to be secure. Transport Layer Security (TLS), a cryptographic protocol, is fundamental to this trust.

Organizations leverage TLS to provide the connection security that has enabled today's unprecedented levels of commerce across the internet. TLS, in turn, depends on TLS certificates. Organizations must deploy TLS certificates and corresponding private keys to their systems to provide them with unique identities that can be reliably authenticated. The TLS certificate enables anybody connecting to a system to know that they are sending their data to the right place. In addition, it also enables establishment of secure connections so that no one in the middle can eavesdrop on communications.

Many organizations might be surprised to discover how many TLS certificates they have. A large- or medium-scale enterprise may have thousands or even tens of thousands, each identifying a specific server in their environment. This is because organizations use TLS not only to secure external connections between themselves and their customers over the internet but also to establish trust between different machines inside their own organization and thereby secure internal communications.

Even though TLS certificates are critical to the security of both internet-facing and private web services, many organizations do not have the ability to centrally monitor and manage their certificates. Instead, certificate management tends to be spread across each of the different groups responsible for the various servers and systems in an organization. Central security teams struggle to make sure that certificates are being properly managed by each of these disparate groups. This lack of a central certificate management service puts the organization at risk because once certificates are deployed, they require regular monitoring and maintenance. Organizations that improperly manage their certificates risk system outages and security breaches, which can result in revenue loss, harm to reputation, and exposure of confidential data to attackers.

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory environment to explore and develop guidelines to help large and medium enterprises better manage TLS server certificates by:

- defining operational and security policies and identifying roles and responsibilities
- establishing comprehensive certificate inventories and ownership tracking
- conducting continuous monitoring of certificates' operational and security status
- automating certificate management to minimize human error and maximize efficiency on a large scale
- enabling rapid migration to new certificates and keys when certificate authorities or cryptographic mechanisms are found to be weak, compromised, or vulnerable

The NCCoE has identified as a best practice that all enterprises establish a formal TLS server certificate management program that is consistent with overall organizational security policies and that has executive responsibility, guidance, and support for the following purposes:

- Recognize the harm that improper management of TLS server certificates can cause to business operations, and provide guidance to mitigate risks related to TLS certificates.
- Ensure that the central certificate services team and the local application owners and system administrators understand the risks to the enterprise and are accountable for their roles in managing TLS server certificates.
- Establish an action plan to implement these recommendations and track progress.

CHALLENGE

As the use of web transactions has grown, the number of TLS server certificates has increased to many thousands in some enterprises. Many of these enterprises struggle to effectively manage their certificates and, as a result, face significant risks to their core operations, including:

- application outages caused by expired TLS server certificates
- hidden intrusion, exfiltration, disclosure of sensitive data, or other attacks resulting from encrypted threats or server impersonation
- disaster-recovery risk that requires the rapid replacement of large numbers of certificates and private keys in response to either certificate authority compromise or discovery of vulnerabilities in cryptographic algorithms or libraries

Challenges to TLS server certificate management include the broad distribution of certificates across enterprises, the complexity of certificate management processes, and the multiple roles involved in certificate management and issuance. TLS server certificates are typically issued by a central certificate services team, but the certificates are often installed and managed by the groups (lines of business) and local system administrators responsible for individual web servers, application servers, network devices, and other network components for which certificates are used. Some of these managers and administrators lack awareness of the risks and best practices associated with certificate management. Certificate services teams having this awareness often lack access to systems holding the certificates.

Despite the mission-critical nature of TLS server certificates, many organizations have not defined clear policies, processes, roles, and responsibilities needed for effective certificate management. Moreover, many organizations do not leverage available technology and automation to effectively manage the growing numbers of certificates. The consequence is continuing incidents due to TLS certificate issues.

SOLUTION

Executive leadership should establish formal TLS server certificate management programs across their enterprises and set organization-specific implementation milestones. For example:

- Within 30 days, define the TLS server certificate policies, and communicate the responsibilities.
- Within 90 days, establish the inventory of TLS server certificates, and identify the risks.
- Beyond 90 days, address near-term risks, and establish automated implementation processes.

The NCCoE, in collaboration with industry partners, has developed this practice guide, *Securing Web Transactions: TLS Server Certificate Management*, to help large- and medium-size organizations better manage TLS server certificates. It provides recommended best practices for large-scale TLS server certificate management and describes the automated TLS certificate management example solution that was built to demonstrate how to prevent, detect, and recover from certificate-related incidents.

While the NCCoE used a suite of commercial products to address this challenge, this guide does not endorse these particular products, nor does it guarantee compliance with any regulatory initiatives. Your organization's information security experts should identify the products that will best integrate with your existing tools and IT system infrastructure. Your organization can adopt this solution or one that adheres to these guidelines in whole, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

SHARE YOUR FEEDBACK

You can view or download the guide at https://nccoe.nist.gov/projects/building-blocks/tls-server-certificate-management. Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. If you adopt this solution for your own organization, please share your experience and advice with us. We recognize that technical solutions alone will not fully enable the benefits of our solution, so we encourage organizations to share lessons learned and best practices for transforming the processes associated with implementing this guide.

To provide comments or to learn more by arranging a demonstration of this example implementation, contact the NCCoE at tls-cert-mgmt-nccoe@nist.gov.

TECHNOLOGY PARTNERS/COLLABORATORS

Organizations participating in this project submitted their capabilities in response to an open call in the Federal Register for all sources of relevant security capabilities from academia and industry (vendors and integrators). The following respondents with relevant capabilities or product components (identified as "Technology Partners/Collaborators" herein) signed a Cooperative Research and Development Agreement (CRADA) to collaborate with NIST in a consortium to build this example solution.

Certain commercial entities, equipment, products, or materials may be identified by name or company logo or other insignia in order to acknowledge their participation in this collaboration or to describe an experimental procedure or concept adequately. Such identification is not intended to imply special status or relationship with NIST or recommendation or endorsement by NIST or NCCoE; neither is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE

Visit https://www.nccoe.nist.gov
nccoe@nist.gov
301-975-0200