NIST SPECIAL PUBLICATION 1800-16A

Securing Web Transactions

TLS Server Certificate Management

Volume A:
Executive Summary

Murugiah Souppaya
Computer Security Division
Information Technology Laboratory

William Haag
Applied Cybersecurity Division
Information Technology Laboratory

Paul Turner
Venafi
Salt Lake City, UT

William C. Barker
Dakota Consulting
Silver Spring, MD

November 2018

DRAFT

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

Executive Summary

- Organizations that improperly manage their Transport Layer Security (TLS) server certificates risk system outages and security breaches, which can result in revenue loss, harm to reputation, and exposure of confidential data to attackers.
- TLS is the most widely used protocol for securing web transactions and other communications on internal networks and the internet. TLS certificates are central to the operation and security of internet-facing and private web services.
- Some organizations have tens of thousands of TLS certificates and keys requiring ongoing maintenance and management.
- The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) built a laboratory environment to explore how large and medium enterprises can better manage TLS server certificates in the following ways:
  - defining operational and security policies, and identifying roles and responsibilities
  - establishing comprehensive certificate inventories and ownership tracking
  - conducting continuous monitoring of the certificate 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 cryptographic mechanisms are found to be weak, compromised, or vulnerable
- The NCCoE strongly recommends that all enterprises establish and implement a formal TLS server certificate management program with executive leadership, guidance, and support for the following purposes:
  - recognize the harm that improper management of TLS server certificates can cause to business operations
  - 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 to track progress

CHALLENGE

The security of web transactions and many other communications relies on the TLS protocol. TLS enables clients to confirm that they are talking to the right server—so that a user does not enter a password into an attacker's website that is masquerading as a legitimate server, for example. To accomplish this authentication, each TLS server is uniquely identified by its TLS server certificate, which contains the server's domain name and other information. TLS also provides a protected communication channel for connections between clients and servers so that exchanged data cannot be read or altered while in transit on the network. The proper deployment and use of TLS are required to comply with many industry standards and regulations that require security and privacy.

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 the following risks:

- application outages caused by expired TLS server certificates
- security risks 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 certificate authority compromise or to discovery of vulnerabilities in cryptographic algorithms or libraries

Managing TLS server certificates is challenging due to the broad distribution of certificates across enterprise environments and groups, the complex processes needed to manage certificates, and the multiple roles involved in certificate management and issuance. TLS server certificates are typically issued by a central certificate services team. However, the certificates are commonly installed and managed by the groups (lines of business) and local system administrators responsible for individual web servers, application servers, network appliances, and other network components for which certificates are used.

Typically, business units and system administrators are not knowledgeable about the risks associated with certificates or the best practices for effectively managing certificates. Certificate services teams have certificate expertise but do not have the necessary access to the systems where these certificates are deployed.

Despite the mission-critical nature of TLS server certificates, many organizations do not have clear policies, processes, roles, and responsibilities defined to ensure effective certificate management. Moreover, many organizations do not leverage available technology and automation to effectively manage the large and growing number of TLS server certificates. As a result, many organizations continue to experience significant incidents related to TLS server certificates.

SOLUTION

Organizations must recognize the critical role that TLS server certificates play in securing their operations, and must establish formal TLS server certificate management programs. Executive engagement is critical because certificates are broadly deployed across multiple groups. Once the decision is made to establish a formal TLS server certificate management program, specific milestones should be set. Some examples of these milestones are provided below:

- **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 the near-term risks, and establish formal management processes that leverage automation to address the broader scope of risk and to minimize ongoing risks

The NCCoE, in collaboration with industry partners, is developing this draft practice guide. Volume A (Executive Summary) and Volume B (Security Risks and Recommended Best Practices) are being released concurrently for public comment. In early 2019, we plan to release volumes C and D:

- **Volume C:** a description of an example automated TLS server certificate management solution for preventing, detecting, and recovering from certificate-related incidents, and a mapping of the example solution's capabilities to the recommended best practices and to NIST security guidelines and frameworks
- **Volume D:** a description of how to build this example solution

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