NIST SPECIAL PUBLICATION 1800-37A

Addressing Visibility Challenges with TLS 1.3

Volume A:
Executive Summary

Murugiah Souppaya
Tim Polk*
Computer Security Division
Information Technology Laboratory

William Barker
Dakota Consulting
Silver Spring, Maryland

John Kent
The MITRE Corporation
McLean, Virginia

** Former NIST employee; all work for this publication was done while at NIST.*

May 2023

PRELIMINARY DRAFT

This publication is available free of charge from
https://www.nccoe.nist.gov/addressing-visibility-challenges-tls-13

Executive Summary

The Transport Layer Security (TLS) protocol is an essential building block for enterprise security. TLS is widely deployed to secure both internal corporate traffic and connections across the public Internet. The latest version, TLS 1.3, has been strengthened so that even if a TLS-enabled server is compromised, the contents of its previous TLS communications are still protected—better known as *forward secrecy*. In TLS 1.2 forward secrecy is optional, while in TLS 1.3 it is required. Forward secrecy conflicts with passive decryption techniques that are widely used by enterprises to achieve visibility into their own internal TLS 1.2 traffic. Many enterprises depend on that visibility to implement critical cybersecurity, operational, and regulatory controls (e.g., intrusion detection, malware detection, troubleshooting, fraud monitoring.) This forces enterprises to choose between using the old TLS 1.2 protocol or adopting TLS 1.3 with an alternative method for internal traffic visibility. If an enterprise chooses the old TLS 1.2 protocol, they miss out on the security and performance enhancements in TLS 1.3 and face additional risks in relying on protocol implementations that will be increasingly out of date over time.

This guide summarizes how the National Cybersecurity Center of Excellence (NCCoE) and its collaborators are planning to use commercially available technology to build key management-based solutions for TLS 1.3 visibility. As the project progresses, this preliminary draft will be updated, and additional volumes will also be released for comment. The goal of the completed guide will be to help readers determine whether the solutions are practical for use in their own enterprise environments.

CHALLENGE

Enterprises using the old TLS 1.2 protocol without forward secrecy have tools and architectural solutions that provide visibility into internal traffic. Most of these visibility solutions essentially take advantage of a characteristic in TLS 1.2 that is not present in TLS 1.3. However, TLS 1.2 visibility solutions provide more privilege than is needed to just view the traffic. Visibility solutions must enable an authorized party to decrypt the TLS 1.3 traffic past, present, and future.

To find new solutions for visibility into TLS 1.3 traffic, the NCCoE identified a broad set of options, including:

- endpoint mechanisms that establish visibility, such as enhanced logging;
- network architectures that inherently provide visibility, such as using overlays or incorporating middleboxes (https://doi.org/10.17487/RFC3234);
- key-management mechanisms that defer forward secrecy until all copies of keying material needed to maintain current levels of network visibility are deleted; and
- innovative tools that analyze network traffic without decryption.

This capability demonstration project is examining the practicality and security impacts of the third option, key-management mechanisms in addition to the second option of incorporating middleboxes. Several challenges are associated with these mechanisms. Some of these challenges are shared by TLS 1.2 visibility solutions, while others are unique to TLS 1.3.

- **Secure management of servers' cryptographic keys**. Private and secret keys must be protected throughout the cryptographic lifecycle: creation, distribution, use, retention, and destruction.

Unauthorized disclosure places all past, present, and future traffic encrypted under those keys at risk.

- **Management of recorded traffic**. This demonstration project assumes that recorded traffic is stored in encrypted form, not plaintext. To be useful, the enterprise must be able to identify the corresponding key material. However, recorded traffic remains at risk of compromise until the corresponding key material or the recorded traffic itself is destroyed. Any solution must allow the enterprise to recover plaintext traffic when required but ensure that traffic is not at risk of compromise indefinitely.
- **Managing expectations of privacy**. IT users often have preconceived notions about the privacy of TLS connections, and the security enhancements associated with TLS 1.3 may increase those expectations. Enterprises that rely on visibility for critical controls should ensure that TLS 1.3 connections within that scope are accepted only by informed users.

In addition to the TLS-specific challenges, the NCCoE is also considering the practical challenges of scalability, ease of deployment, and usability of the visibility solutions themselves.

This preliminary practice guide can help your organization:

- understand what types of key management-based solutions could be used for achieving TLS 1.3 visibility
- determine whether key management-based solutions for TLS 1.3 visibility are practical for your enterprise environment

SOLUTION

NCCoE is currently collaborating with technology providers on finalizing the demonstration architecture for TLS 1.3 visibility. The demonstration architecture will include two key management-based solutions and a third that combines network architecture and key-management techniques.

Once implemented, the solutions are expected to provide controlled enterprise visibility into encrypted TLS 1.3 traffic to support four specific scenarios identified by the NCCoE: operational troubleshooting, performance monitoring, threat triage, and cybersecurity forensics. Data requirements for performance monitoring and threat triage are largely real-time, while operational troubleshooting and cybersecurity forensics require access to historical data stored in encrypted form.

To achieve visibility through key management, the enterprise might apply one of two technical mechanisms for each server whose traffic is of interest to the enterprise. In the first option, the enterprise would provision bounded-lifetime Diffie-Hellman key pairs for TLS 1.3 servers as a substitute for the standard ephemeral key pairs. In the second case, the server would use ephemeral Diffie-Hellman key pairs as specified in TLS 1.3 and the enterprise would retain the symmetric key used to encrypt the connection.

The managed Diffie-Hellman keys and symmetric traffic keys would be retained by a key distribution function until all corresponding encrypted traffic has been decrypted or is destroyed or otherwise no longer available. Systems that are authorized to examine traffic would obtain the appropriate keys from the key distribution function. The solution would also incorporate components to retain traffic for retrospective applications, like troubleshooting and cybersecurity forensics. The stored traffic would be

retained in encrypted form until policy conditions (e.g., retention time) are met, then data would be deleted by the storage function.

Since TLS 1.3 is designed to achieve forward secrecy as soon as the connection closes, the solution also assumes out-of-band notification of the visibility policy.

Some aspects of analytic functions that need enterprise operational visibility into encrypted traffic may require combining the network architecture and key-management techniques. The scope of the project also includes demonstration of an architecture that achieves visibility inside the data center through tools that break and inspect traffic. These middleboxes are commonly used at the enterprise edge to achieve real-time visibility; in this demonstration project, we expand the scope to examine deployment within the enterprise and address access to historical data by leveraging key-management-based solutions.

Collaborators		
AppViewX	Mira Security, Inc.	Nubeva
DigiCert	NETSCOUT	Thales Trusted Cyber Technologies
JPMorgan Chase	Not For Radio, LLC	U.S. Bank

While the NCCoE will use a suite of commercial products to address this challenge, this guide does not endorse 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 their entirety, or you can use this guide as a starting point for tailoring and implementing parts of a solution.

HOW TO USE THIS GUIDE

Depending on your role in your organization, you might use this guide in different ways:

Business decision makers, including chief information security and technology officers can use this part of the guide, *NIST SP 1800-37A: Executive Summary*, to understand the drivers for the guide, the cybersecurity challenge we address, our approach to solving this challenge, and how the solution could benefit your organization.

Technology, security, and privacy program managers who are concerned with how to identify, understand, assess, and mitigate risk can use *NIST SP 1800-37B: Approach, Architecture, and Security Characteristics* once it is available. It will describe what we built and why, including the risk analysis performed and the security/privacy control mappings.

IT professionals who want to implement an approach like this can make use of *NIST SP 1800-37C: How-To Guides* once it is available. It will provide specific product installation, configuration, and integration instructions for building this project's example implementations, allowing you to replicate all or parts of this project.

SHARE YOUR FEEDBACK

You can view or download the preliminary draft guide at the NCCoE TLS 1.3 Visibility project page. NIST is adopting an agile process to publish this content. Each volume is being made available as soon as possible rather than delaying release until all volumes are completed. Work continues on designing and implementing the example solution and developing other parts of the content. As a preliminary draft, this volume will have at least one additional draft released for public comment before it is finalized.

Help the NCCoE make this guide better by sharing your thoughts with us as you read the guide. Once the example implementation is developed, you can adopt this solution for your own organization. If you do, 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 recommended practices for transforming the processes associated with implementing this guide.

To provide comments or join the TLS 1.3 Visibility community of interest, contact the NCCoE at applied-crypto-visibility@nist.gov.

COLLABORATORS

Collaborators 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). Those respondents with relevant capabilities or product components 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.