PROJECT DESCRIPTION

ADDRESSING VISIBILITY CHALLENGES WITH TLS 1.3

Tim Polk
Murugiah Souppaya
National Institute of Standards and Technology

William Barker
Dakota Consulting

May 2021

applied-crypto-visibility@nist.gov

This revision incorporates comments from the public.

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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, adaptable example cybersecurity solutions demonstrating how to apply standards and best practices by using commercially available technology. To learn more about the NCCoE, visit https://nccoe.nist.gov. To learn more about NIST, visit https://www.nist.gov/.

This document describes enterprise challenges associated with compliance, operations, and security when employing encrypted protocols, in particular Transport Layer Security (TLS) 1.3, in their data centers, and proposes an environment for demonstrating approaches and proposed solutions built in collaboration with a Community of Interest, cryptographic product vendors, product testing organizations, and product validation staff.

ABSTRACT

Enterprises use encryption—a cryptographic technique—to protect data transmission and storage. While encryption in transit protects data confidentiality and integrity, it also reduces the organization's visibility into the data flowing through their systems. The NCCoE initiated a project to address enterprise challenges to compliance, operations, and security when deploying modern encrypted protocols, and TLS 1.3 in particular. This effort is an element of the NCCoE's cryptographic applications program and follows successful completion of an earlier TLS certificate management project. This project description documents the project background, scenarios demonstrating efficacy of solutions, a high-level demonstration platform architecture that includes a list of desired components and security characteristics and properties, standards and guidance to be followed in project development and execution, and mappings to security requirements that the demonstration platform is to satisfy.

ACKNOWLEDGMENT

This project description was developed from the presentations and discussions that occurred at the NCCoE-hosted workshop Virtual Workshop on Challenges with Compliance, Operations, and Security with Encrypted Protocols, in particular TLS 1.3. NCCoE thanks John Banghart, Paul Barrett, Russ Housley, Andy Regenscheid, and Paul Turner for contributing to the development of this project description.

KEYWORDS

algorithm; application; compliance; cryptography; encryption; forensics; perfect forward security; protocol; transport layer; troubleshooting; visibility

TABLE OF CONTENTS

1 Executive Summary

Purpose

The National Institute of Standards and Technology (NIST) is planning a project to address compliance, operations, and security challenges associated with adoption of modern encrypted protocols. Deployment of new protocols for exchanging encrypted information, in particular the latest version of the Transport Layer Security (TLS) protocol, TLS 1.3 [1], can impact the ability of some organizations to meet their regulatory, security, and operational requirements due to loss of visibility into the content of communication within their environments. The project will demonstrate practical and implementable approaches to help those organizations adopt TLS 1.3 in their private data centers and in hybrid cloud environments while maintaining regulatory compliance, security, and operations.

Scope

The project will demonstrate various approaches and practices to meet common compliance, operations, and security requirements while gaining the security and performance benefits of TLS 1.3 deployment. The project will focus on enterprise data center environments which include on-premises data center and hybrid cloud deployment hosted by a third-party data center or a public cloud provider. This project will demonstrate real-world visibility approaches utilizing current or emerging components. Solutions may utilize proprietary vendor products as well as commercially viable open source solutions.

The project focuses on the security implications of TLS 1.3 protocol implementations that provide system and application administrators and users the necessary visibility into the content of information being exchanged. Approaches that restore visibility into encrypted data in transit, such as alternative key establishment and management approaches or approaches involving tunneling visibility-supporting protocol versions through TLS 1.3, are of initial interest. Other approaches, such as analysis of encrypted data, enhanced auditing, and novel network architectures, will also be considered. The project will leverage current and ongoing NIST and industry standards, as well as National Cybersecurity Center of Excellence (NCCoE) application projects. Section 4 provides examples of relevant standards and guidance.

Information transmitted over the public Internet (e.g., connections between an enterprise and its customers) is out of scope and must not be impacted by proposed solutions. Also out of scope are emerging deployment models leveraging encrypted transport to protect protocols that were previously in the clear, such as DoT (Domain Name System [DNS] over TLS) and DoH (DNS over Hypertext Transfer Protocol Secure [HTTPS]). DoT and DoH may be the subject of future NCCoE work.

Assumptions & Challenges

Recent enhancements to cryptographic security protocols, such as TLS 1.3 and Quick UDP Internet Connections (QUIC), disrupt current approaches to achieving visibility into internal network communications within enterprise data centers. While these protocol enhancements increase performance and address security concerns within the enterprise and on the public Internet, they also reduce enterprise visibility into internal traffic flows. These enhanced security protocols and new deployment models were not designed to accommodate decryption of internal network traffic by passive monitoring devices, creating potential compliance, security, and operational impacts in enterprises that currently rely on such devices.

Consequently, enterprises have raised questions about how to meet enterprise security, operational, and regulatory requirements for critical services while using the enhanced security protocols and leveraging new deployment models. Such enterprises may need to consider applying new architectures and novel techniques to augment or replace conventional monitoring devices while satisfying their business, regulatory, security, and network operations requirements.

Many enterprises choose to rely on the same standard transport security protocols to exchange information over the public Internet and within internal enterprise network environments. For these enterprises, the ability to naturally migrate to the most current versions offers continuity and simplifies network evolution. As a result, this project assumes that enterprises cannot rely on older protocol versions as a long-term solution.

It is expected that the majority of the components of the new demonstration environment that are part of the on-premises data center will be located in a lab at the NCCoE facility in Rockville, Maryland. This will ease the integration of the components and provide an open and transparent environment for the participants to collaborate on building and testing the proposed approaches.

Background

Enterprises have typically depended upon visibility into data in transit within their networks to implement critical cybersecurity, operational, and regulatory controls (e.g., intrusion detection, malware detection, troubleshooting, fraud monitoring). The deployment of network security protocols within enterprise data centers to protect integrity and confidentiality has posed challenges to network visibility required by these controls. To maintain visibility, enterprise architectures facilitate comprehensive inspection, collection, and analysis of internal network traffic (i.e., both enterprise and personal data) through a small number of passive or active monitoring devices. To facilitate decryption of network traffic, passive decryption devices are provided copies of the servers' long-term cryptographic keys. In these cases, these long-term cryptographic keys allow decryption of past, current, and future network traffic for the lifetime of a key, as well as the ability to impersonate the server that uses that key.

To improve the security of communications on the public internet, modern protocol designers have made changes to protocols to implement stronger security properties that protect the secrecy of historical traffic even if the servers' long-term secret keys are compromised, a property referred to as *forward secrecy*. This property, however, has correspondingly created significant challenges for the network visibility strategies used by enterprises.

Potential Solution Space

The NCCoE has, in collaboration with industry providers and enterprise customers, been researching options for maintaining visibility within an enterprise given these challenges. In particular, the NCCoE hosted an industry roundtable in 2018 to assess the scope of the visibility challenges faced by enterprises, participated in an industry-led workshop in fall 2019 [2], and hosted a virtual workshop focused specifically on TLS 1.3 in October 2020 [3].

Through this research the NCCoE has identified a broad set of options for maintaining visibility, including:

1. endpoint mechanisms that establish visibility, such as enhanced logging;

2. network architectures that inherently provide visibility, such as use of overlays, or through incorporation of middleboxes [4];
3. key management mechanisms that forgo forward secrecy to maintain current levels of network visibility;
4. innovative tools that analyze network traffic without decryption; and
5. deployment of alternative standards-based network security protocols where forward secrecy is optional or not supported.

This project intends to demonstrate a range of approaches for enabling intra-enterprise access to unencrypted/decrypted information necessary for satisfying enterprise auditing, forensic analysis, and communications/access management troubleshooting imperatives. The NCCoE is primarily interested in approaches that can be deployed in existing operational environments that rely upon TLS 1.3 for network security, but alternative network protocols may also be considered.

2 Demonstration Scenarios

The TLS 1.3 visibility project will encompass several application scenarios that impact enterprise compliance, security, and operational challenges. All scenarios will address enterprise data center environments which include on-premises data center and hybrid cloud deployments hosted by a third-party data center or a public cloud provider.

As shown in Figure 1, there are a variety of potential communications scenarios where visibility into communications for compliance, security, and operations are required. These include outbound traffic, connections across the internet to the enterprise network boundary, and communications within the enterprise network between internal systems. This project specifically focuses on communications within the enterprise network and does not include outbound connections or communications across the public internet.

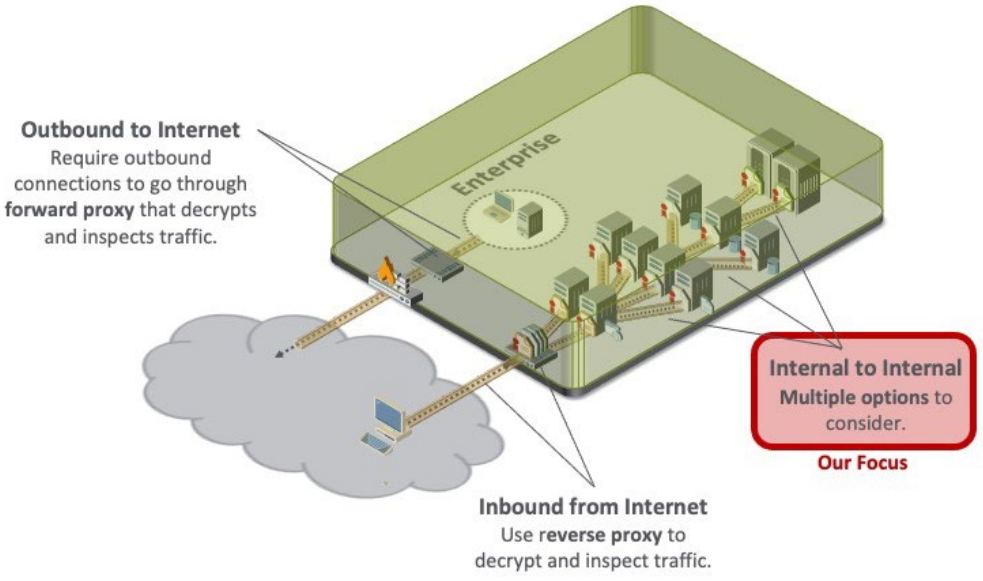

Figure 1: Demonstration Environment

Scenario 1: Operations Troubleshooting

Enterprises providing services to customers, partners, and employees must have the ability to rapidly troubleshoot and fix issues when availability and operational issues occur. The operations troubleshooting scenario shown in Figure 2 demonstrates the enterprise need to trace transactions through all tiers of an application, including collection of detailed information such as transaction identifiers, data payload, and the results of operations performed by each application tier. Because operational issues can be intermittent and difficult to replicate, the scenario includes the ability to proactively collect and view detailed historical data that may or may not be available in logs. Examples of troubleshooting situations include application unavailability and intermittent system failures. Visibility may be required into communications for network-attached storage (NAS), identity management systems, databases, routers and switches, application servers, web servers, load balancers, and firewalls in order to build a complete picture of the end-to-end session across the enterprise.

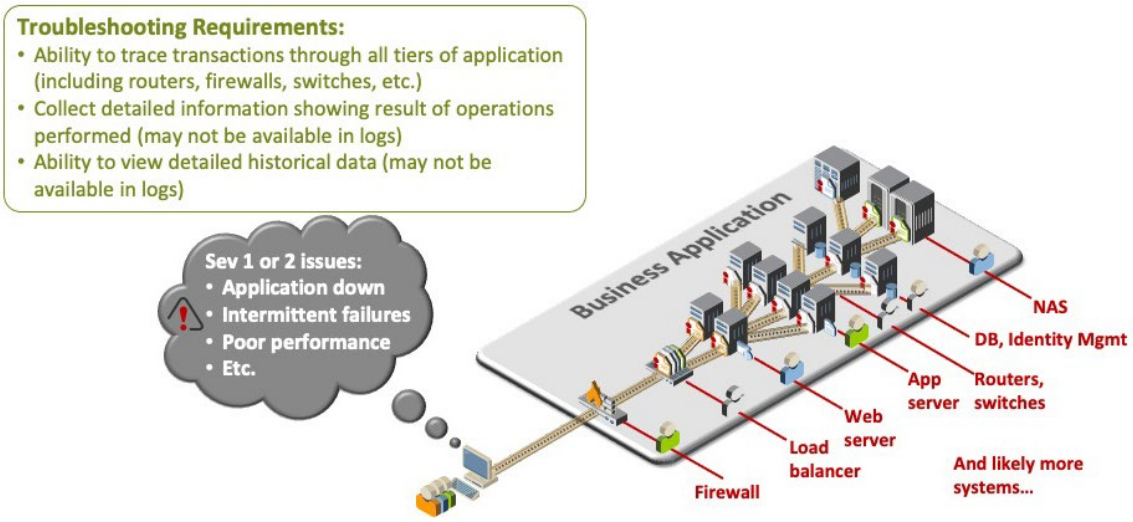

Figure 2: Troubleshooting Scenario

Scenario 2: Performance Monitoring

Application performance and response times are critical to customer service and time-sensitive mission-critical applications. Enterprises must be able to proactively detect and isolate performance issues for multi-tier applications. The performance monitoring scenario (Figure 3) involves rapidly and accurately detecting user performance issues, predicting and resolving customer performance issues based on upstream degradation, maintaining the ability to rapidly identify sources of performance issues, monitoring across all mission-critical applications and platforms, and minimizing performance loads on applications and platforms.

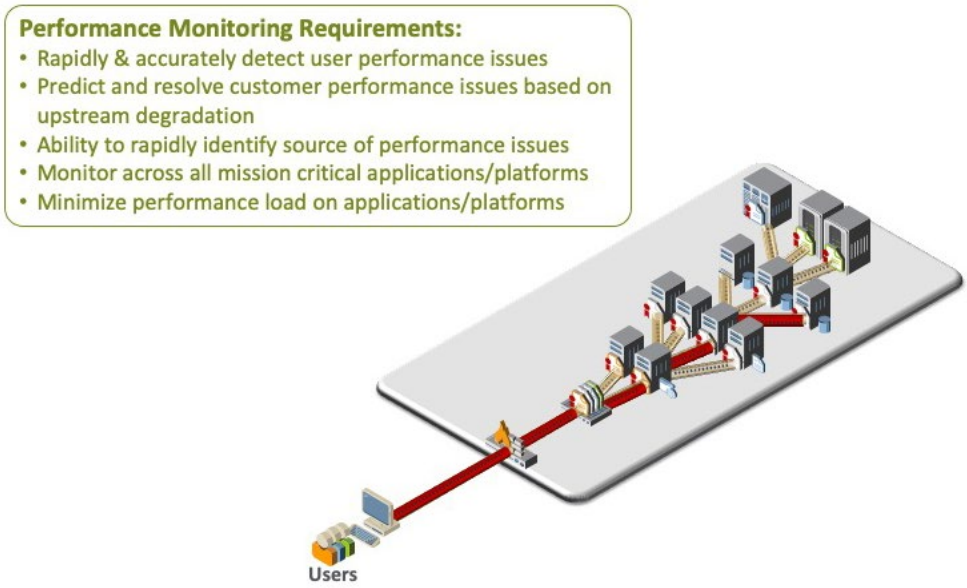

Figure 3: Performance Monitoring Scenario

Scenario 3: Cybersecurity Threat Triage

With the widespread threat of cyber attacks, enterprises must be able to rapidly triage indicators of compromise (IOCs), quickly distinguishing false positives from real attacks. The threat triage scenario (Figure 4) includes triage, identification, and response to IOCs. IOCs may arise in network-attached storage, identity management systems, databases, routers and switches, application servers, web servers, load balancers, and firewalls. They may be found in processes, open ports, and logs. Performing threat triage may require visibility into current and historical inbound and outbound communications. Effective performance of threat triage requires rapidly obtaining a clear picture of system state, reducing triage time with an accurate and detailed picture of current and historical communications, minimizing reliance on data sources that can be manipulated by attackers, and using independent data sources for verification.

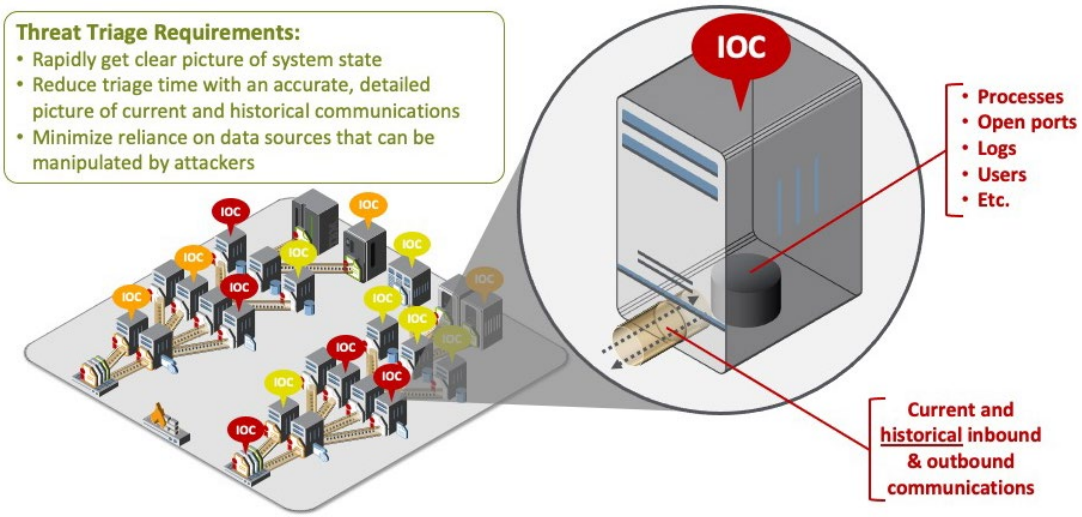

Figure 4: Threat Triage Scenario

Scenario 4: Cybersecurity Forensics

Following a major compromise, enterprises must be able to establish a clear picture of how the attack occurred, including each system that was compromised, vulnerabilities that were exploited, attack methods that were used, and data that was exfiltrated. To be effective, accurate information must be obtained about all operations performed by attackers (even if logs were manipulated) from independent data sources. The security forensics scenario (see Figure 5) includes the ability to trace paths of attacks as they pivot laterally across the internal network of compromised systems. Affected systems may involve network-attached storage, identity management systems, databases, routers and switches, application servers, web servers, load balancers, and firewalls.

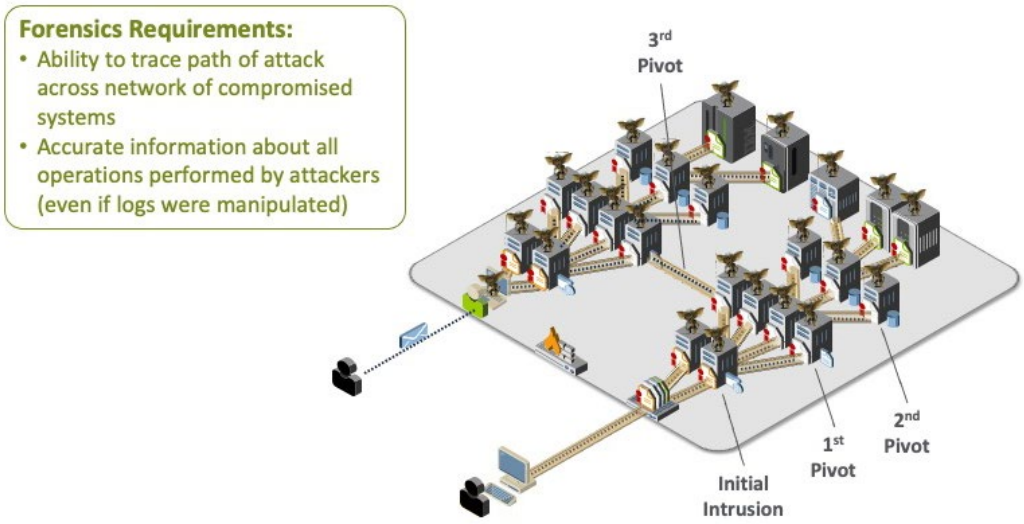

Figure 5: Cybersecurity Forensics Scenario

3 High-Level Architecture

The architecture for the demonstration environment will support the simulation of each of the enterprise scenarios included in Section 2. Enterprise applications typically include multiple tiers and different types of components, including load balancers, web servers, application servers, databases, identity management systems, routers, firewalls, etc.

The demonstration environment will include a combination of physically hosted and cloud-based services serving a single enterprise. Connections between (a) physically hosted systems, (b) physically hosted systems and a cloud-based service, or (c) two cloud-based services are all considered within the enterprise data center. To facilitate ease of deployment in existing environments and use of commercial tools, we expect that data transfers between systems in the demonstration environment will be protected by TLS 1.3. However, other modern, standardized network security protocols may be used to protect data transfers in special cases where the alternative protocol is an essential component of the visibility solution and can be satisfactorily integrated with the demonstration environment.

Connections between systems on the public internet and the enterprise network are explicitly out of scope and must not be impacted by the proposed solutions.

Proposed Component List

- Network infrastructure
  - Firewalls
  - Routers and switches
  - Load balancers
- Physically hosted and cloud-based servers
  - Applications servers
  - Web servers
  - Network-attached storage
  - Databases
  - Identity management systems

Proposed solutions will identify additional components required to achieve visibility (e.g., traffic collection or sensors).

Desired Properties and Security Characteristics

Proposed solutions must address security, operational, or compliance requirements where traffic is encrypted between one or more sets of components in the demonstration architecture. For example, a solution might focus on achieving visibility into information exchanges between cloud-hosted application servers to support troubleshooting. Alternatively, a solution might analyze information exchanges between physically hosted web servers with HSMs and cloud-based services relying on software cryptographic modules to monitor for fraudulent transactions. Solutions are not required to address all challenges or all components in the architecture, although comprehensive solutions are strongly encouraged.

As noted in the industry-led 2019 workshop, "The use of visibility technologies within the enterprise data center environment is generally acceptable in ways that visibility technologies on the public Internet may not be." [2] Solutions that forgo forward secrecy within the enterprise must be deployable in a manner that preserves forward secrecy for information exchanges over the Internet.

While visibility challenges are not limited to a single protocol, the focus for this project is TLS 1.3. Solutions must be compatible with TLS 1.3, excepting those solutions relying upon an alternative network security protocol as a replacement for TLS. That is, solutions that modify TLS 1.3 or restrict enterprises to earlier version of TLS are not of interest.

The Center for Cybersecurity Policy's 2019 workshop on enterprise visibility identified a set of baseline criteria for acceptability of solutions for visibility challenges. The NCCoE will adopt them as the baseline criteria for a generally effective solution. The criteria are repeated here without change:

- Must be scalable.
- Must be relatively easy to implement/deploy.
- Must be protocol agnostic.
- Must be usable in real time and post-packet capture.

- Must be effective for both security and troubleshooting purposes. [Note: This paper adopts the four scenarios presented in Section 2 as a proxy for "security and troubleshooting purposes".]
- Must be widely available and supported in mainstream commercial products and services.

The baseline criteria apply across the range of solutions, but different aspects are considered more interesting for different categories of solutions. The NCCoE has identified specific areas of interest to explore in demonstration projects for different classes of solutions:

- For solutions that achieve visibility through endpoint mechanisms (e.g., logging) or network architectures (middleboxes, overlays, or mesh service architectures), the NCCoE is interested in demonstrating scalability, ease of deployment, and reliable and timely access to information. For example, scalability and reliable access to historical information would be an area of interest for centralized logging solutions.

- For solutions that achieve visibility through key management mechanisms that share keys to facilitate TLS decryption, the NCCoE is interested in demonstrating that keys and data are protected against misuse or compromise, and that recorded traffic is not at risk of compromise indefinitely. Specifically, projects would focus on (1) the systems and procedures used to transmit, store, provide access to, and use the keys, and (2) mechanisms that perform comprehensive deletion of decryption keys when established temporal or data protection limits are met.

- For solutions that achieve visibility through analysis of encrypted data, projects would focus on demonstrating the capabilities and limitations of these emerging tools with respect to each of the four scenarios.

- For solutions that rely on alternative standards-based network security protocols, projects would focus on scalability, usability, and ease of deployment. If the solution includes key management mechanisms to share keys for decryption, the project would also demonstrate the properties identified above for solutions that facilitate TLS decryption.

- For all solutions, management, operational, and technical security controls are in place to compensate and mitigate any potential new risks that may be introduced into the environment.

Note that the suitability of solutions with respect to specific criteria may depend upon the scenario. Timely access to information is one such criteria. While some scenarios (e.g., troubleshooting) could be amenable to selective access during post-mortem analysis, others (e.g., threat triage) will likely demand real-time access.

The preceding list highlights specific properties of interest based on the class of solution. These properties must necessarily be complemented by appropriate security controls (e.g., host security mechanisms or trusted execution environments) to ensure the reliability of the solution. The NCCoE will informally review solutions to ensure that appropriate security controls are in place based on current NIST guidance.

The demonstration environment will utilize commercially available hardware and software technologies, which will include typical IT components to support the underlying functionality.

The commercially available hardware and software may be supplemented by open source tools and emerging commercial components.

4 Relevant Standards and Guidance

Here is a list of existing relevant standards and guidance documents.

- Federal Information Processing Standard (FIPS) 140-3, *Security Requirements for Cryptographic Modules*
  https://doi.org/10.6028/NIST.FIPS.140-3
- Internet Engineering Task Force (IETF) Request for Comments (RFC) 8446, *The Transport Layer Security (TLS) Protocol Version 1.3*
  https://tools.ietf.org/html/rfc8446
- IETF RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2*
  https://tools.ietf.org/html/rfc5246
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-52 Revision 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*
  https://doi.org/10.6028/NIST.SP.800-52r2
- NIST SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*
  https://doi.org/10.6028/NIST.SP.800-53r5
- NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
  https://doi.org/10.6028/NIST.SP.800-53r4
- NIST SP 1800-16, *Securing Web Transactions: TLS Server Certificate Management*
  https://doi.org/10.6028/NIST.SP.1800-16
- NIST SP 1800-19, *Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments*
  https://csrc.nist.gov/publications/detail/sp/1800-19/draft

APPENDIX A REFERENCES

[1] E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3*, Internet Engineering Task Force (IETF) Request for Comments (RFC) 8446, August 2018. Available: https://tools.ietf.org/html/rfc8446

[2] Center for Cybersecurity Policy and Law, *Enterprise Data Center Transparency and Security Workshop Report*, November 2019. Available: https://centerforcybersecuritypolicy.org/enterprise-data-center-transparency-and-security-initiative

[3] National Institute of Standards and Technology (NIST), *Virtual Workshop on Challenges with Compliance, Operations, and Security with TLS 1.3*, September 2020. Available: https://www.nccoe.nist.gov/events/virtual-workshop-challenges-compliance-operations-and-security-tls-13

[4] B. Carpenter and S. Brim, *Middleboxes: Taxonomy and Issues*, IETF RFC 3234, February 2002. Available: https://tools.ietf.org/html/rfc3234

APPENDIX B ACRONYMS AND ABBREVIATIONS

DNS	Domain Name System
DoH	DNS Over HTTPS
DoT	DNS Over TLS
FIPS	Federal Information Processing Standard
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IETF	Internet Engineering Task Force
IOC	Indicator of Compromise
NAS	Network-Attached Storage
NCCoE	National Cybersecurity Center of Excellence
NIST	National Institute of Standards and Technology
QUIC	Quick UDP Internet Connections
RFC	Request for Comments
SP	Special Publication
TLS	Transport Layer Security
UDP	User Datagram Protocol