



**November 12, 2019**

**CENTER FOR CYBERSECURITY  
POLICY AND LAW**

## Introduction

On September 24<sup>th</sup>, 2019, The Center for Cybersecurity Policy and Law (“Center”) hosted a multi-stakeholder meeting to discuss the implications of evolving protocols on the normal operations of both public and private sector enterprises. Protocols designed to address security concerns across the public Internet are also used in enterprise networks, and these security improvements can negatively impact an organization’s visibility into its network traffic. This loss of visibility reduces the effectiveness of network tools and approaches, such as deep packet inspection, which in turn limits their usefulness as security and troubleshooting tools.

Workshop participants represented a cross-section of companies from multiple sectors, including financial services, healthcare, and telecommunications, as well as government agencies from the United States and the United Kingdom.

Participants also included software vendors and members of civil society who provided insight into some of the concerns that have driven the protocol evolutions.

The goals of the workshop were to arrive at consensus around a problem statement, identify potential near- and longer-term solutions, and discuss next steps to continue the discussion.

# Workshop Details

## Participants

The meeting was held under the Chatham House Rule, so this report will not detail those who promoted certain ideas. However, we did receive permission to publish the names of the following individuals who participated in the workshop:

- John Banghart, Venable LLP
- Tommy C, NCSC
- Joseph Lorenzo Hall, Center for Democracy & Technology
- Russ Housley, Vigil Security LLC
- Parthenia Youngblood, DoD/CIO/CS
- Ron Sulpizio, PKH Enterprises, supporting DoD CIO
- Donna Dodson, NIST
- Murugiah Souppaya, NIST
- Tim Polk, NIST
- Paul Barrett, NETSCOUT
- Ari Schwartz, Venable LLP
- Paul Turner, Venafi
- Andrew Kennedy, BITS-BPI
- Michael Ackerman, Industry Network Technology Council
- Avesta Hojjati, DigiCert
- Darrin Pettis
- Additional participants not listed.

The Center made every effort to ensure representation from as many viewpoints as possible while still keeping the attendance size manageable to hold the discussion. However, we recognize there are additional stakeholders across government, industry, and civil society whose positions may not have been captured, in whole or in part. We look forward to continuing the discussion while ensuring all viewpoints are considered.

## Scope

To ensure that the discussion could remain appropriately focused, the scope was limited to enterprise data centers. In the context of the workshop, the term *data center* was used generically to refer to a physical data center owned and managed by an application or service owner, a co-location facility owned by a third party, or a virtual private cloud hosted by a public cloud provider.

The decision to limit the scope in this way was necessary as the protocols at the heart of the issue are themselves applicable across a wide range of technical implementations and contexts. In particular, the intention was to avoid discussions of the public Internet, where political, social, and economic issues are influenced by different requirements than many of those faced by individual enterprises in their own

environments. This limitation was not intended to suggest that the issues facing the public Internet are not important, only that they were not within our scope.

## Starting Point

Based on the talking points within the privacy and security communities, the Center recognized two primary viewpoints shared in whole or in part by all stakeholders, both inside and outside the workshop. Despite those differences in views, there were a few points on which everyone was able to agree at the outset:

- Data privacy is essential in order to:
  - Address regulatory, contractual, or other forms of compliance
  - Establish and maintain user trust.
- Encryption helps protect sensitive information from unauthorized access.
- Loss of network visibility negatively impacts various types of operational functionality.

One starting viewpoint was that the loss of data center visibility does not, by itself, warrant any alteration of the encryption protocols or deployment models being promoted. Those same participants also suggested that alternative technologies, such as host-based logging and monitoring, were adequate substitutes that could and should be deployed today.

The prevailing starting counterpoint to the above was that the loss of visibility is not just a matter of security and privacy, but also introduces significant limitations to an organization's ability to use network inspection to troubleshoot and maintain the availability of its applications, potentially creating exponential delays in correcting mission-impacting technical problems.

While these two views represented the starting point for the workshop discussion, significant progress was made in aligning the viewpoints of all participants, based largely on improved understanding and an acknowledgment that enhanced and continuing dialogue on both near- and long-term solutions and protocol evolutions is in everyone's best interest.

## Goal Outcomes

### Problem Statement

Arriving at consensus regarding the nature of the problem was one of the primary goals of the workshop, and considerable time was spent capturing everyone's views and concerns.

The following is the proposed problem statement, in three parts, as agreed upon by the participants:

- A) Maintaining the confidentiality, integrity, and availability of information and services in the enterprise data center environment is essential to mission success.**
- B) Evolving protocols can negatively impact an organization's ability to maintain visibility in the enterprise data center environment, including threat detection and mitigation, troubleshooting, and service resiliency.**

**C) These impacts can impede an organization's ability to respond to regulatory, contractual, or other requirements.**

The statement is broken into parts as shown above in order to highlight the three key points that the group wished to communicate. *Note: Some minor changes were made in preparation for this report to improve clarity without impacting meaning or intent.*

## Other Outcomes

### Data Center vs. Public Internet

While the scope of the workshop was limited to data centers, discussion of how that environment contrasts with the public Internet did come up at various points. Further refining of that contrast proved useful in establishing the following point, agreed to notionally by all participants:

**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.**

The above statement was not crafted by the participants but is intended to capture the spirit of the conversation and conclusion.

Prior to the discussion, this distinction seemed unclear, with some participants operating under the assumption that the loss of visibility due to evolving protocols was considered by some stakeholders to be universally applicable and acceptable regardless of deployment context.

### Approaches to Visibility

There was acknowledgment within the group that deep packet inspection (DPI) is used in data centers as a critical form of visibility to protect against breaches and to perform application troubleshooting, and that DPI is one the main forms of visibility addressed by the problem statement. Several examples of how DPI is used were provided by both enterprises and a government agency. One observation was that packet data may need to be kept for up to two months to satisfy compliance requirements.

While the participants agreed that host-based logging is also a valuable tool, the unstructured nature of many log messages, and the likelihood of logs being disabled to save resources or to disguise the actions of an attacker, makes their efficient and effective use as a sole method impossible as a practical matter. Comments were also made relating to the high cost of storing log information.

In many cases, in-line decryption can be used for DPI, but there are also many situations where passive decryption is required, for example, retrospective decryption of packet traces during forensic investigations of east-west traffic where in-line decryption is not economical.

End-point agents are also often cited as an alternative to DPI. However, it was observed that end-point monitoring agents have increasingly limited privilege as a) more activity is locked down in applications; b) the agent itself may be compromised; c) BYOD devices in an enterprise environment may not have any end-point monitoring solution at all; and d) constrained devices may not support a rich-enough agent. Additionally, end-points represent only one part of the overall organizational infrastructure, and some devices may not have end-point agents available at all.

Finally, technology is available that can identify certain classes of threat or risk based on analysis of encrypted traffic. However, it was acknowledged that DPI is still required in many cases as this type of analysis is largely heuristic based, which may not detect unknown attack vectors. Nor does this approach address the troubleshooting use case.

## Risk Context

At various points in the discussion, it was clear that all participants agreed that deployment of any protocol should not happen without properly understanding the risk that the organization is attempting to manage. The nature of that context needs to incorporate security, privacy, and troubleshooting requirements in a way that strikes a reasonable balance.

# Proposed Solutions

## Principles

The following principles were discussed and agreed upon as useful to ensuring that any proposed current or future solution could meet baseline criteria for acceptability:

- 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.
- Must be widely available and supported in mainstream commercial products and services.

## Solutions

The following were identified as potential solutions.<sup>1</sup> This list of solutions reflects different levels of abstraction; some address visibility broadly while others are specific to the deployment of TLS 1.3. This should not be considered a definitive list, and an evaluation of the solutions' respective pros and cons requires further work. In particular, proposed solutions were not assessed for adherence to the principles stated above.

### Overlays/microservice mesh

Service Mesh architectures such as ISTIO help to control how different applications and services are allowed to communicate in container and other environments. For example, in Kubernetes, traffic to and from a specific pod is routed via a module called a sidecar, which provides a potential location to perform TLS offload and/or to deploy a man-in-the-middle proxy.

### Key Retention

---

<sup>1</sup> The description of each solution is provided for clarity and may not have been explicitly discussed during the workshop.

Key retention systems allow the key material generated in forward secrecy schemes such as Ephemeral Diffie-Hellman (DHE) to be stored. The key retention system can retain the session key material for a short time, e.g., to support real-time decryption, or for a longer period to allow post-capture decryption at a later date. True forward secrecy is achieved for a given time interval once the corresponding key material is permanently deleted. There were some concerns raised about the ability to get the key sent quickly enough, which could impact scalability.

### **Static Diffie-Hellman (DH) with frequent key rotation**

Rotation of static keys does not achieve per-session forward secrecy in the way that DHE does, but it can still provide forward secrecy after a given time interval. By increasing the frequency of key rotation, forward secrecy can be achieved after shorter time intervals. As with key retention, true forward secrecy is only achieved once the private keys used by both parties and the session keys are permanently deleted.

### **Enterprise Transport Security (ETS) Standard**

ETS is described in ETSI Technical Specification 103 523-3. It describes a profile for TLS 1.3 that uses static Diffie-Hellman keys. ETS includes requirements to notify the user of the TLS client, through either technical or procedural methods, that a static key is in use.

### **RHRD**

RHRD refers to a proposal made to the IETF during the TLS 1.3 discussions. It proposed a handshake extension that allows the client to opt-in to passive decryption of the session. The proposal can be found here: <https://tools.ietf.org/html/draft-rhrd-tls-tls13-visibility-00>

### **Multi-Party Computation (MPC)**

In classic Diffie-Hellman, only two parties are involved in the key agreement process. MPC allows more parties to be involved and therefore provides a means of sharing key material with an authorized decryption tool. One option would be to use an MPC framework with the pre-shared key (PSK) capability in many encryption protocols, including TLS. It was noted that this approach is largely in the conceptual phase and not a reasonable near-term solution.

### **Hardware Security Module (HSM)**

An HSM can perform the encryption handshake calculations on behalf of a server such that the static keys involved never need to leave the HSM, thus preventing them from being stolen. HSMs alone do not offer a solution to visibility challenges, but they can enhance the security of implementations of many solutions. In particular, the question was raised as to whether HSMs could be used to improve the security of a key escrow or key rotation framework.

## **Next Steps**

### **Research**

Research was identified as a key area where progress could be made, both in terms of the viability of proposed technical solutions, as well as providing additional data points concerning the impact that evolving protocols can have and are having in enterprise data center environments. Specifically, the following were mentioned by several stakeholders:

- Assess the proposed solutions against the principles for visibility solutions established by the participants.
- How many actual data center breaches resulted from people decrypting data they captured over the wire?
- How often, and in what ways, are malicious actors using encrypted channels once they have gained unauthorized access?
- How much information is actually being hidden by encryption? Perhaps take known data and study it in simulated real-world contexts to demonstrate impact.
- How often do network defenders use TLS inspection to troubleshoot applications and detect and mitigate attacks?

Potential options for conducting research include:

- Using existing government and private sector data sets to conduct various types of analysis;
- Defining and establishing a multi-stakeholder program within the National Cybersecurity Center of Excellence (NCCoE) at NIST to demonstrate that one or more of the potential solutions is deployable and scalable in the enterprise data center without “leaking” into the public Internet; and
- Identifying other entities, such as in the academic sector, where longer-term research projects could be established.

No specific follow-ups were identified at the workshop, but multiple participants expressed an interest in pursuing these options further.

## Outreach

While many views were represented in the workshop, there are many other stakeholders across multiple communities whose input would be beneficial. Additionally, socialization of the workshop outcomes will aid in achieving long-term success.

The group agreed to have follow-up conversations to determine the best means of outreach. Ideas included:

- Draft white papers or other publications to increase CIO-level awareness of the trend toward reduced visibility and its implications.
- Additional workshops to further define the challenge with different stakeholders and/or to further explore potential solutions.
- Producing a comprehensive study and associated paper based on the workshop outcomes and additional exploration.
- Increase awareness within protocol standards bodies in general by ensuring more stakeholder voices are present and heard during standards development.
- Increase participation by technical staff (including protocol designers, engineers, and implementers) in the Internet Engineering Task Force through the standards development process to champion enterprise use cases and help shape the evolution of the Internet protocols.

## Deployment Guidance

There was general agreement that additional deployment guidance would be beneficial for enterprises deploying TLS within their data centers. Some thoughts that were shared:

- Developing guidance to help organizations manage TLS-based services as a critical asset and maintain cryptographic agility when migrating to TLS 1.3.
- Developing tools and techniques to audit services for the unexpected deployment of Diffie-Hellman.
- Proactively determining where loss of visibility may impact the ability to troubleshoot problems.
- Ensuring that TLS guidance does not unnecessarily become regulation.

There were no specific next steps identified with this topic, but there was general agreement that stakeholders are willing to assist.

## Additional Observations

Anecdotal feedback received during and subsequent to the workshop strongly suggests that participants found the discussion to be pertinent and substantive, and that it served the purpose of advancing the conversation where other attempts have not. There was expressed interest in having additional workshops as needed, possibly focused on further refining and promulgating proposed solutions.

Additionally, there is interest in holding a related workshop concerning DNS over HTTPS (DoH). While DoH was discussed in passing during the workshop, there was a general sense that as a topic, it has sufficient complexity to warrant its own discussion. The Center will pursue this course of action and notify interested stakeholders.