To Know, Or Not To Know

Learn about the dangers that threaten data security and privacy, and how to manage them with best practices in Transport Layer Security Inspection.

by Greg Maples
Principal Security Architect, CISSP

Basis for this Presentation

NSA: MANAGING RISK FROM TRANSPORT LAYER SECURITY INSPECTION

This presentation is based on the recommendations made in the 'managing risk' document in the title above This document recommends a series of best practices for TLS inspection as a component of a Zero Trust Architecture implementation strategy.

TLS intercept and inspection is a compliance criteria for network visibility in the foundational ZTA documents ZTA Reference Architecture specifically from the “Visibility and Analytics” Pillar as per:

“A ZT enterprise will capture and inspect traffic, looking beyond network telemetry and into the packets themselves to accurately discover traffic on the network and observe threats that are present and orient defenses more intelligently.”

Uninspected Traffic Risk

What percentage of malware is encrypted (2022) using TLS?

- A. 17%
- B. 47%
- C. 55%
- D. 95%

Answer:
95% of all attack traffic
not just malware
is encrypted!

Introduction to Zero Trust and TLS Encryption

1 What is Zero Trust Architecture?

Zero Trust is a security model based on the principle of "never trust, always verify." It assumes that all network traffic, whether inside or outside the organization, is potentially risky and should be authenticated and encrypted.

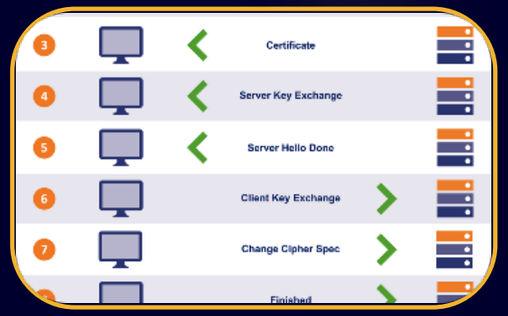
2 Importance of managing TLS encryption

Transport Layer Security (TLS) is the standard protocol used to encrypt data communication between servers and clients. Transport Layer Security Inspection is the process of decrypting and scanning the contents of encrypted traffic, and is essential for protecting against security threats.

3 Need for risk management

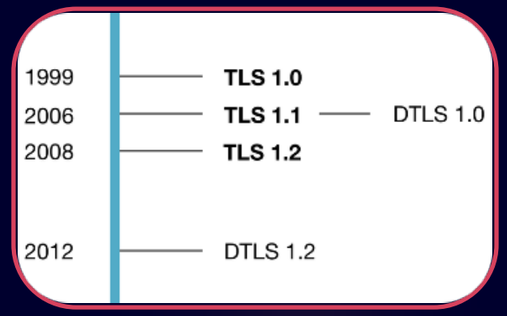
While TLS encryption offers an important layer of protection, it can also introduce risks if not managed properly. In this presentation, we'll examine best practices for managing these risks.

Overview of Transport Layer Security (TLS)



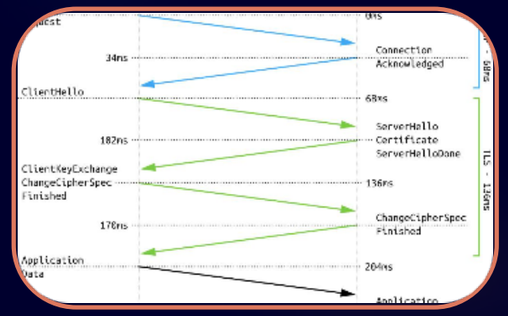
What is Transport Layer Security?

Transport Layer Security (TLS) is a cryptographic protocol used to secure communication over the internet. It establishes a secure connection between a server and a client, encrypting every data packet with unique keys that are negotiated during the TLS handshake.



Background and versions of TLS

TLS is based on the older SSL (Secure Sockets Layer) protocol and has gone through several versions, including TLS 1.0, 1.1, 1.2, and the latest version, TLS 1.3. TLS 1.2 and below are possibly vulnerable to security attacks. Anything below 1.2 has been compromised.



Role of TLS in securing data communication

Transport Layer Security is crucial for securing sensitive data such as passwords, credit card information, and personal details. It establishes a secure, end-to-end encrypted tunnel that ensures data integrity, authenticity, and confidentiality.

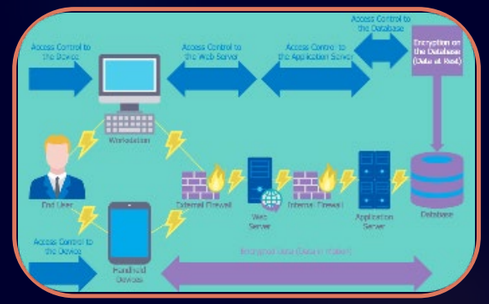
Case Studies

Data Exfiltration

•**Example:** In 2017, a former NSA contractor, Harold T. Martin III, was caught with a massive amount of classified data. This case highlighted the risk of insiders using encrypted channels to exfiltrate sensitive information.
•**Mechanism:** Insiders may use encrypted channels like HTTPS or VPNs to send confidential data outside the organization, bypassing detection mechanisms that cannot decrypt the traffic.

Encrypted Channels

•**Example:** In the Anthem data breach (2015), attackers used encrypted channels to communicate with malware installed within the network, allowing them to stealthily extract sensitive data.
•**Mechanism:** Insiders, intentionally or through compromised accounts, can use encrypted traffic to communicate with external command and control servers.



Encrypted C&C

•**Example:** The Dyre banking Trojan, which emerged around 2014, used SSL encryption to communicate with control servers, making its detection harder for traditional security systems.
•**Mechanism:** Attackers distribute malware via encrypted channels, such as HTTPS, to evade network-based antivirus and intrusion detection systems.

Limits of Metadata Inspection for Encrypted Traffic

While metadata analysis can provide some insights into encrypted traffic, it has limitations. It cannot reveal the actual content of the data, making it challenging to detect certain threats or malicious activities. Additionally, relying solely on metadata for inspection poses risks of false positives and false negatives, potentially leading to security gaps.

What is TLSi – TLS Inspection?

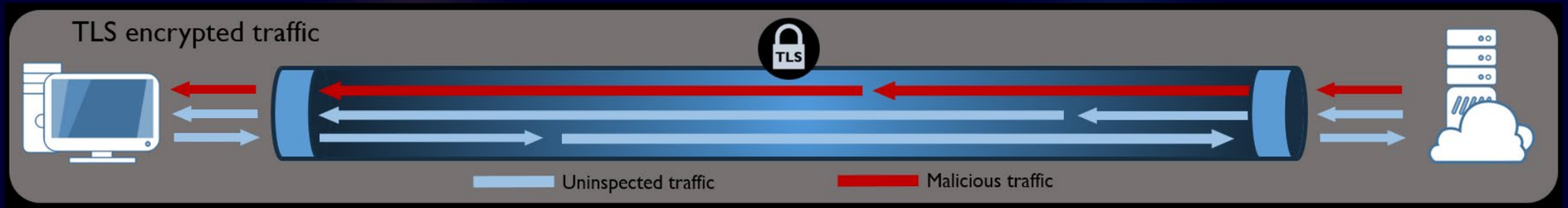


Figure 1a: Encrypted Traffic

Fully encrypted transport tunnel – Contents cannot be examined. The only parties to the contents are the server and the client. Packets intercepted in the middle cannot be understood, and only metadata can be generated for such things as application, port, machines, destination, packet size, etc.

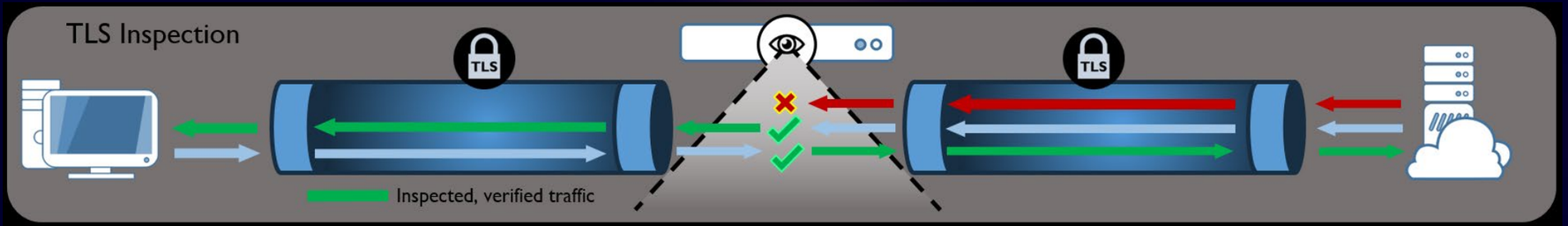


Figure 1b: TLS Inspection

a.) A TLS channel is negotiated between the client and the server. All of the data that passes through the channel is encrypted and therefore not subject to inspection.
b.) The device conducting TLSI replaces the TLS channel with a TLS chain, breaking the encryption on the data, inspecting it, and blocking it, if it is malicious.

Intercepted Transport – If a certificate can be presented and accepted between the client and the server, the tunnel can be decrypted. This is done by creating two secure sessions instead of one. In between the two sessions, security tooling can inspect the traffic before re-encryption.

Many organizations basically ‘give up’ on the challenges and take the following stances which can lead to significant issues:

Concern	Common Compromise	Issues
Lack of Budget	Don’t Inspect	Threats Missed
Traffic Volume	Don’t Inspect East/West	Threat migration is Undetected
Perceived Complexity	Inspect ‘High Risk’ Only	Attackers come through back doors
Certificate Management	Use small number of multi-domain wildcard certs	Certificate failures become catastrophic
Key Management	Ad-Hoc Scripts and Processes	Key disclosure become catastrophic and keys are often handled without a chain of trust
Tool Chain Complexity	Random distribution of tools based on what group bought it and when	Budget often spent unnecessarily and tool distribution is needlessly complex

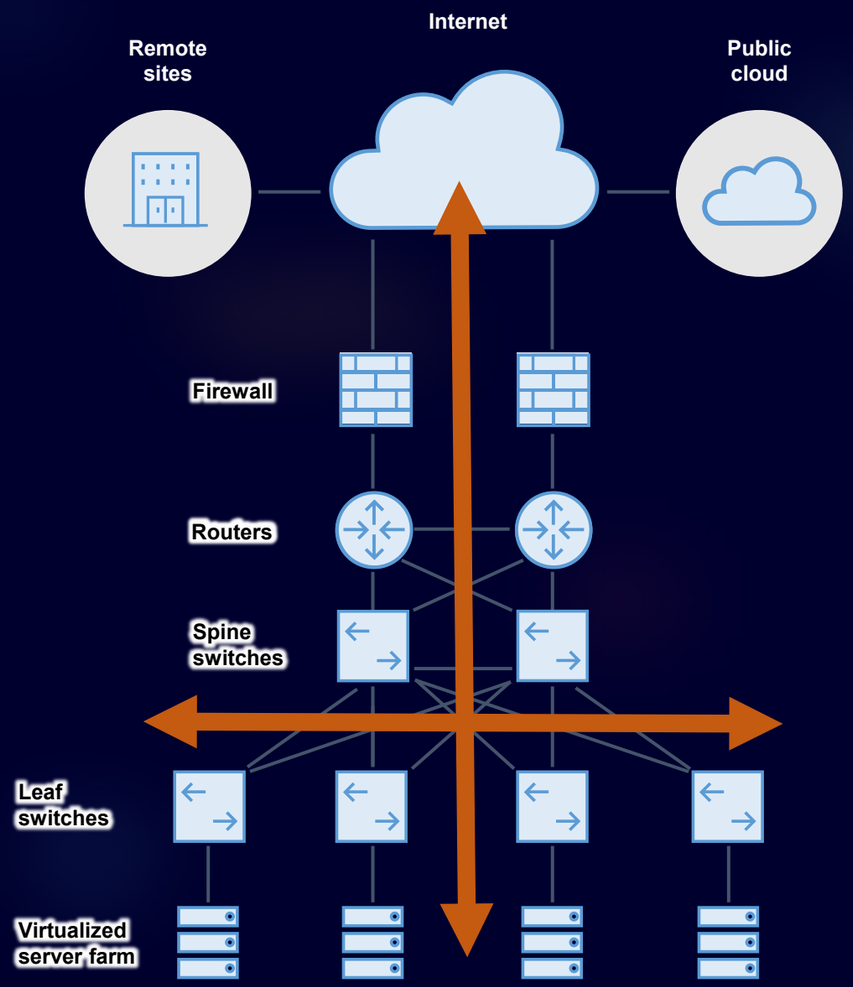
Difference between 'North/South' and East-West Traffic

For this discussion we will refer to two traffic types:
'North/South' (inbound/outbound) traffic and east-west traffic.

'North/South' traffic refers to the communication that occurs between external sources (outside the organization) and internal resources (within the organization). It encompasses the traffic flowing in and out of the network perimeter, such as data accessed through the internet or connections to external partners.

On the other hand, east-west traffic refers to the communication that takes place within the organization's internal network. It involves the interaction between different devices, servers, and resources within the same network or data center. This includes data transfers between servers, interdepartmental communication, and interactions between various components of an application.

Understanding the distinction between these two types of traffic is essential for effective network security and monitoring. While 'North/South' traffic focuses on securing external connections and protecting against threats from outside the organization, east-west traffic requires robust internal security measures to prevent lateral movement and unauthorized access within the network.



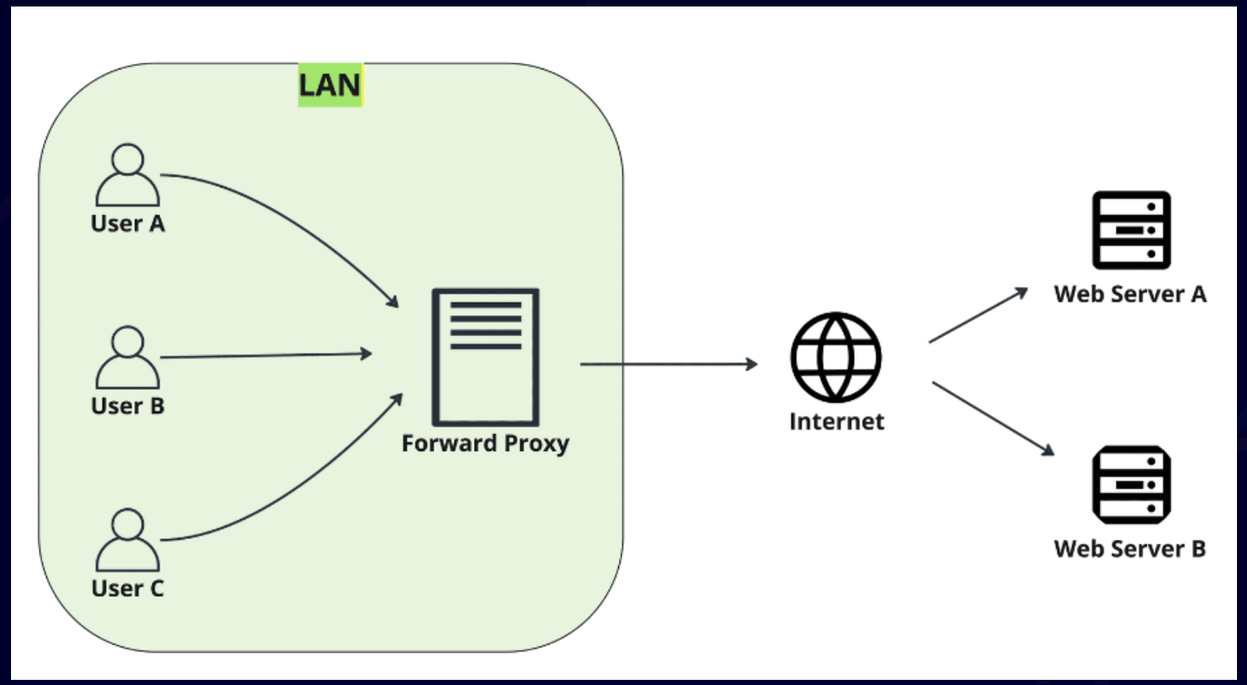
Understanding A Forward Proxy

A forward proxy acts as an intermediary between clients and servers, intercepting and forwarding requests on behalf of the clients. It enhances security by filtering and inspecting traffic, providing an additional layer of protection. Additionally, forward proxies can improve performance by caching and compressing data.

Forward proxies are commonly used in corporate networks to control and monitor internet access. They can enforce policies, such as blocking certain websites or restricting access to specific resources. This helps organizations maintain security and control over their network traffic.

By intercepting requests from clients, forward proxies can also perform content filtering, preventing users from accessing malicious or inappropriate content. They can analyze and scan incoming traffic for viruses, malware, or other threats, protecting the internal network from potential risks.

Furthermore, forward proxies can enhance performance by caching frequently accessed content. When a client requests a resource, the forward proxy can check if it already has a cached copy. If so, it can deliver the content directly to the client, reducing the load on the backend servers and improving response times.



The Role of Reverse Proxy in Web Applications

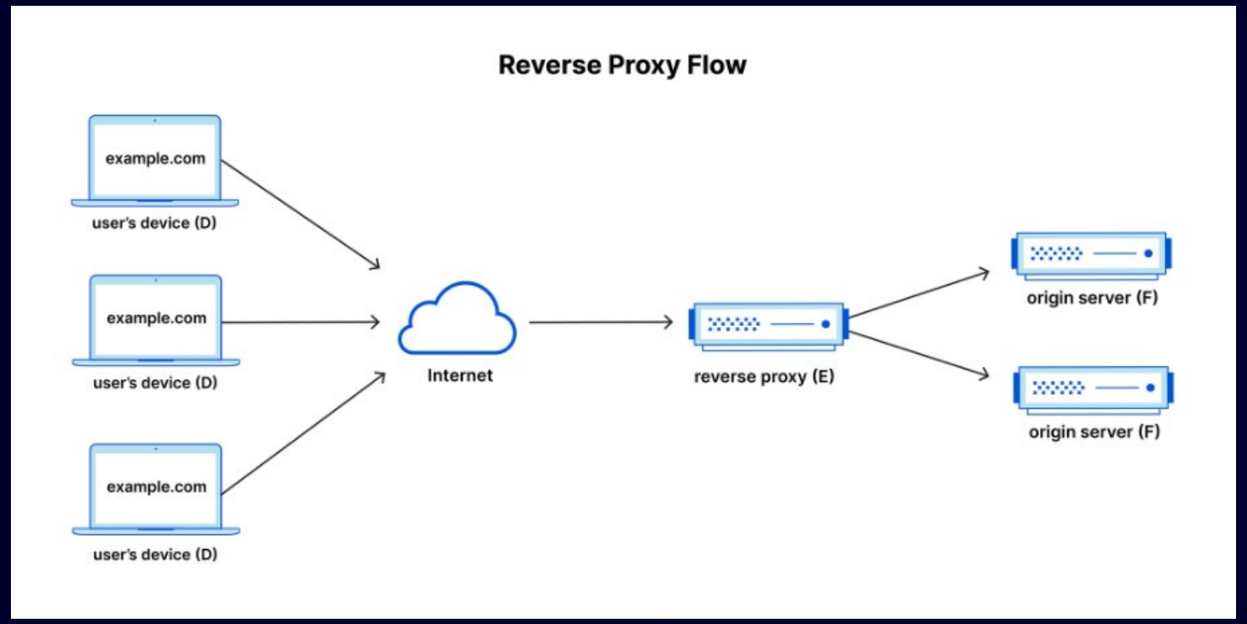
A reverse proxy plays a critical role in web applications, providing an extra layer of security by shielding servers from direct exposure to the internet. It acts as an intermediary between clients and backend servers, handling incoming requests and forwarding them to the appropriate destination.

One of the main benefits of a reverse proxy is its ability to distribute incoming traffic among multiple backend servers. This process, known as load balancing, ensures that no single server becomes overwhelmed with requests, leading to improved performance and scalability.

Reverse proxies also offer additional security measures by implementing features such as TLS termination. By terminating SSL/TLS connections at the reverse proxy, it offloads the encryption and decryption workload from the backend servers, reducing their processing overhead.

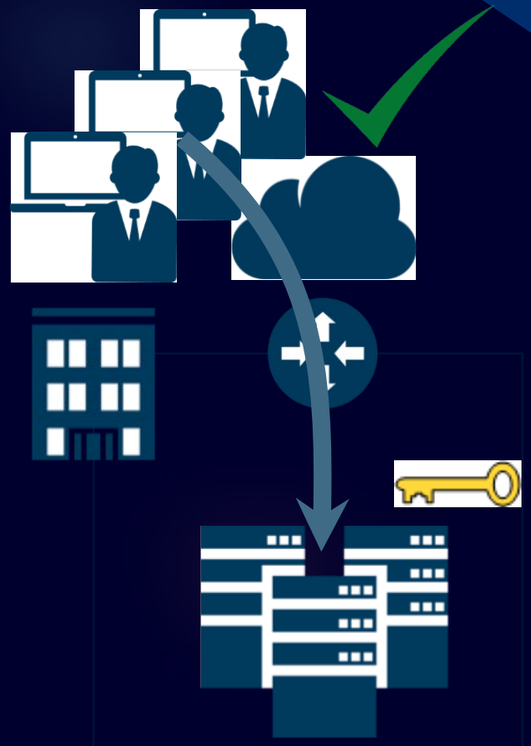
Furthermore, reverse proxies can perform various security checks, such as filtering and inspecting incoming traffic for potential threats. They can block malicious requests, prevent DDoS attacks, and provide protection against common web vulnerabilities.

Here is a visual representation of how a reverse proxy works:



Certificate challenges

“Inbound” deployment



- Local server keys available to inline SSL decryption
- Inline SSL decryption spoofs the local server
- External clients believe they are connected to the local server

“Outbound” deployment

- Internet server keys unavailable
- Local clients receive a new trusted CA
- Inline SSL decryption acts as man-in-the-middle

Risks in 'North/South' Inspection vs East-West Traffic

When it comes to security risks, 'North/South' inspection focuses on threats like unauthorized access and data breaches. In contrast, east-west traffic poses risks of lateral movement, insider threats, and internal attacks. Implementing appropriate security measures for both is crucial for comprehensive network protection.

Risks Associated with Encrypted Insider Threats

Encrypted insider threats present unique challenges for network security. As insiders with legitimate access to sensitive information, these individuals can exploit encrypted channels to carry out malicious activities without detection. Here are two examples of risks associated with encrypted insider threats:

1. Data Exfiltration: An insider can leverage encrypted communication channels to exfiltrate sensitive data from the organization without being detected. By encrypting the data being transferred, they can bypass traditional security controls, making it challenging to detect and prevent the unauthorized transfer of sensitive information.
2. Malware Distribution: An attacker with access to encrypted channels can use them to distribute malware within the organization's network. They can encrypt the malware payload, making it impossible for security systems to identify and block the malicious content. This enables the attacker to propagate the malware across different systems and potentially cause significant damage.

Cost Comparison of 'North/South' vs East-West Traffic Inspection

When it comes to inspecting network traffic, there are different approaches for different types of traffic. 'North/South' inspection focuses on traffic that flows in and out of the network perimeter, while east-west traffic is internal network traffic between different systems. The Department of Defense (DOD) and National Security Agency (NSA) recommend inspecting all traffic, regardless of direction, to ensure comprehensive security.

However, the costs associated with inspecting north-south traffic versus east-west traffic can vary. North-south inspection typically involves inspecting a smaller volume of traffic, but requires more powerful inspection devices due to the higher throughput requirements. In contrast, east-west traffic inspection requires more granular visibility and a higher number of inspection points, which can increase the overall cost of inspection dramatically.

Server Certificates in a Reverse Proxy

When a client connects to the reverse proxy, it presents the server certificate. The client then verifies the certificate's validity and checks if it is issued by a trusted certificate authority (CA). This process authenticates the server's identity and creates a secure, encrypted connection between the client and the reverse proxy.

Once the secure connection is established, the reverse proxy acts as an intermediary between the client and the destination server. It receives requests from the client, decrypts the encrypted traffic, and forwards the requests to the appropriate server. The server's response is then encrypted by the reverse proxy and sent back to the client, ensuring end-to-end security.

This is easy because the organization owns and manages the certificates involved. However, on larger sites hundreds of certs may be needed, presenting management challenges.

A certificate management system is often needed.

Understanding Certificate Re-Signing in a Forward Proxy

- In a forward proxy the organization does not own the remote certificate!
  XYZ Corp cannot provide a valid certificate for `https://www.apple.com` (for example)

- So, how do you intercept and decrypt the TLS tunnel without access to the certificate?

- Certificate resigning in forward proxies involves the reissuing of certificates using an intermediate root certificate, allowing for inspection and monitoring of encrypted traffic.

- The forward proxy software must generate a certificate ‘on the fly’, acting as a local Certificate Authority (CA). When the ‘apple.com’ certificate is examined, it can be seen that the signing authority is XYZ Corp.

Detecting TLS on non-443

So-called ‘clever’ attack methods often move TLS traffic to obscure ports in an attempt to evade detection.

To detect TLS on non-443 ports, you can use the following hex sequence:
16 03 (TLS version) followed by 01 or 02 or 03 (TLS record type).

In the record following (indicated by 00 xx), where xx is the byte count, you can find the client hello. You can do this with an eBPF or on any wireshark like interface.

Risks associated with Transport Layer Security Inspection

Vulnerabilities and attacks

Transport Layer Security Inspection can introduce risks such as unauthorized access, data leakage, and man-in-the-middle attacks. Hackers can exploit vulnerabilities in the process to steal sensitive data or perform phishing attempts.

Stored certificates can be stolen!

Implications for data privacy and security

Transport Layer Security Inspection can also raise concerns about data privacy. Encrypting traffic is a key element of anonymity, but decrypting traffic means potentially exposing user activity and data.

Best Practices for Managing Risk from Transport Layer Security Inspection

1

Encryption and authentication strategies

One of the most effective ways to manage risk from Transport Layer Security Inspection is to use strong encryption and authentication protocols. This includes configuring servers to use the latest TLS standards, avoiding weak ciphers, and implementing certificate pinning to verify the identity of servers.

2

Monitoring and analysis techniques

Organizations can use monitoring and analysis techniques to detect and prevent attacks. This includes analyzing SSL/TLS certificates, setting up intrusion detection systems, and using advanced threat intelligence tools.

3

Network segmentation and access control

Organizations can also segment their network traffic and implement access control policies to limit the number of people who can access sensitive data. This includes using firewalls, VPNs, and role-based access control.

Recap of Key Points

1

Transport Layer Security (TLS)

is a cryptographic protocol used to secure communication over the internet. It establishes a secure connection between a server and a client, encrypting every data packet with unique keys that are negotiated during the TLS handshake.

2

Transport Layer Security Inspection

is the process of decrypting and scanning the contents of encrypted traffic to identify potential security threats. It can introduce risks such as unauthorized access, data leakage, and man-in-the-middle attacks.

3

Best Practices for managing inspection risk

include using strong encryption and authentication protocols, implementing network segmentation, access control policies, and monitoring and analysis techniques. Ongoing risk management is crucial for ensuring secure communication and protecting sensitive data.

Closing Question:

Is it worth the risk to inspect traffic?

A. No, I really want to have my organization get hacked!

B. Someday, maybe. I'll delay because I really want to have my organization get hacked!

C. It seems complicated! I'd prefer to get hacked!

D. It's Expensive! I'd prefer to get hacked!

E. The only possible way to know threats in my environment is to intercept traffic. I get it!

Thank You For Your Time!

Greg Maples, CISSP
linkedin.com/in/gregmaples/