Transport vs Application Intercept

MAMI Management & Measurement Summit

David Wells
Roelof du Toit
Noah Robbin

Agenda

1 Definition of Intercept types

2 Comparison of Intercept types

3 Generic Issues affecting Intercept

4 Details of specific issues

5 Discussion

Symantec™

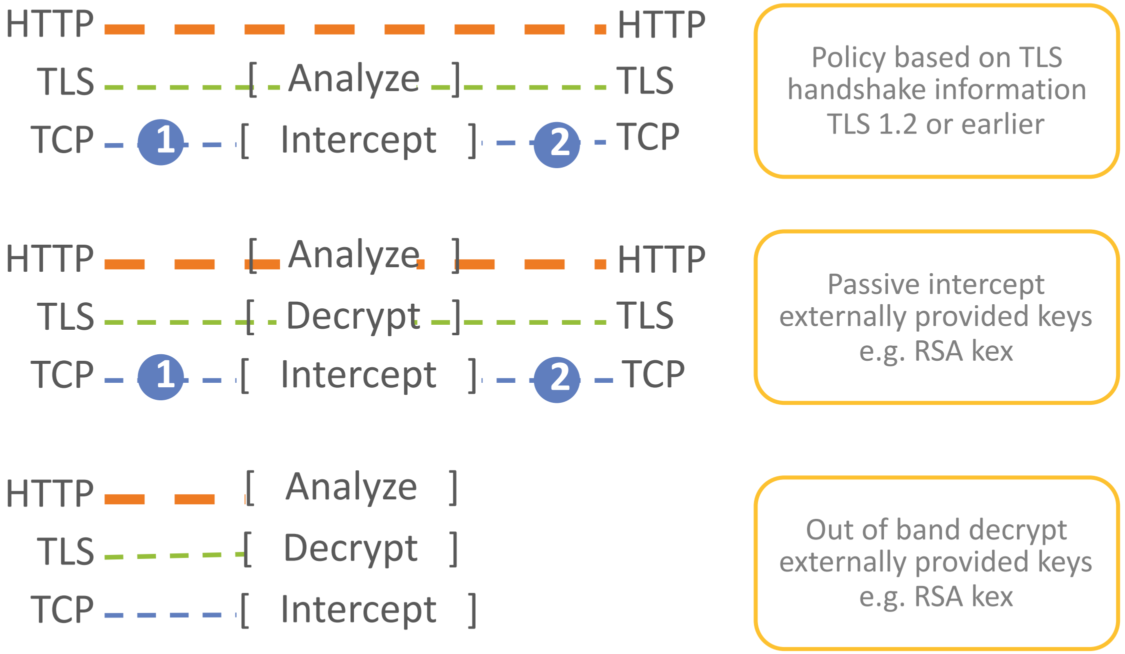
Intercept Types

Definitions

- Passive
  - No modification – implies terminate is optional
- Active
  - Terminate and modify
- Need to consider three layers
  - Transport – TCP/IP for example
  - Security – TLS for example
  - Application – HTTP for example
- Intercept type may be different for the different layers

Transport Layer – Passive Intercept

- Passive on Application and Security layer, optionally Active on Transport layer
- Examples:



Policy based on TLS handshake information TLS 1.2 or earlier

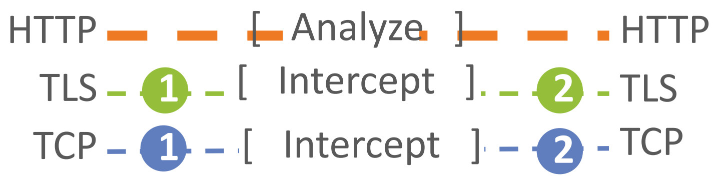
Passive intercept externally provided keys e.g. RSA kex

Out of band decrypt externally provided keys e.g. RSA kex

Intercept Types

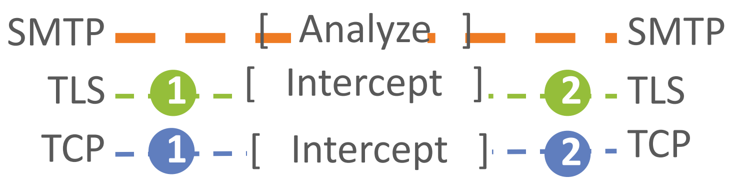
Transport Layer Active Intercept

- Passive on Application layer. Active on Transport and Security layer



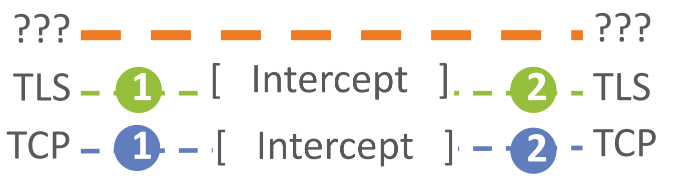
HTTP [Analyze] HTTP
TLS 1 [Intercept] 2 TLS
TCP 1 [Intercept] 2 TCP

TLS decryption feeding security tool such as IPS



SMTP [Analyze] SMTP
TLS 1 [Intercept] 2 TLS
TCP 1 [Intercept] 2 TCP

TLS decryption feeding security tool such as AV

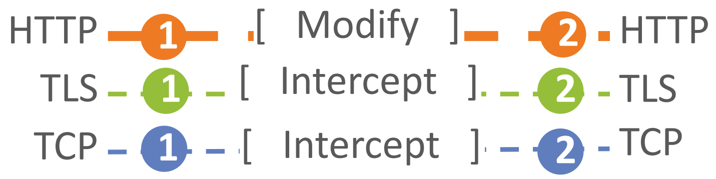


??? ???
TLS 1 [Intercept] 2 TLS
TCP 1 [Intercept] 2 TCP

Protocol agnostic TLS decryption tool

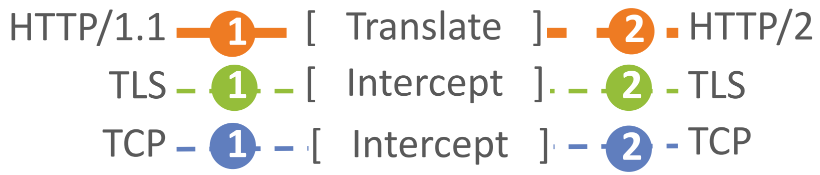
Application Layer Intercept

- Active on Transport, Security and Application layer



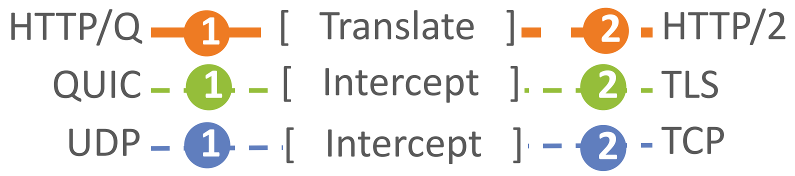
HTTP 1 [Modify] 2 HTTP
TLS 1 [Intercept] 2 TLS
TCP 1 [Intercept] 2 TCP

Forward proxy handling encrypted HTTP



HTTP/1.1 1 [Translate] 2 HTTP/2
TLS 1 [Intercept] 2 TLS
TCP 1 [Intercept] 2 TCP

Forward proxy translating HTTP to HTTP/2



HTTP/Q 1 [Translate] 2 HTTP/2
QUIC 1 [Intercept] 2 TLS
UDP 1 [Intercept] 2 TCP

Forward proxy translating QUIC to HTTP/2

Comparison of Intercept Types

Transport Layer Intercept

- Protocol Agnostic (optional)
- Protocol Detection not required
- Security and performance monitoring
- Analyze application content (optional)
- Typical devices
  - IPS
  - NGFW
  - TLS decryptor

Application Layer Intercept

- Supported protocols only
- Protocol Detection and / or protocol configuration
- Security and Performance optimization
- Modify application content and / or protocol translation
- Typical devices
  - Forward Proxy
  - Reverse Proxy
  - Anti-Virus

General Issues Affecting Intercept

- Trend is to remove separation between Security layer and Application layer
  - Endpoint applications moving to use Security layer functions at the Application layer
  - Problematic for Transport Layer intercept devices that by choice or due to legal reasons do not modify Application layer protocols or data
- Transport layer intercept devices are likely to affect, or even break, proposed integrations between the Application layer and the Security layer
- Some endpoint applications assume end to end security (vs. hop by hop security), disregarding the impact of middleboxes
- Other endpoint applications actively attempt to work around middleboxes
- Reference: Requirements for CoAP End-To-End Security – IETF CoRE Working Group https://tools.ietf.org/html/draft-hartke-core-e2e-security-reqs-03

Specific Issues

TLS 1.3 handshake message confidentiality

- TLS 1.3 complicates Transport layer active intercept and, for the most part, prevents Transport level passive intercept
- TLS 1.3 prevents Transport layer passive intercept devices from validating the SNI for security policy purposes
  - SNI in ClientHello TLS message must match a Subject Alternate Name (SAN) in the server certificate
- Transport layer active intercept devices may use policy based on the SNI to determine whether to intercept or not
  - The SNI can be validated if the policy decision is to intercept the session but not if the policy decision is to leave the session alone

- Active Transport Layer intercept devices need to implement efficient intercept mechanisms and provide the required level of security
- References
  - The Transport Layer Security (TLS) Protocol Version 1.3 https://tools.ietf.org/html/draft-ietf-tls-tls13-26
  - Why Enterprises Need Out-of-Band TLS Decryption https://tools.ietf.org/html/draft-fenter-tls-decryption-00
  - TLS 1.3 Impact on Network-Based Security https://tools.ietf.org/html/draft-camwinget-tls-use-cases-00

Specific Issues

Exported authenticators used for post handshake application layer authentication

- Goal is out of band post TLS handshake proof of ownership of a X.509 certificate
- Authenticator is exported from an existing TLS session then sent on the Application layer
- Capability is not negotiated, **RFC5705** is used. TLS 1.2 extended_master_secret is required but a reliable intercept device will never strip this extension. So, a Transport layer active intercept device has no control
- Keying Material Exporters for Transport Layer Security (TLS) https://tools.ietf.org/html/rfc5705
- Example: HTTPS server enforcing access to sensitive resource. Client connects, exports an authenticator from the TLS session and then includes it with a subsequent HTTP request
- Authenticators exported from an intercepted TLS session will fail if sent without modification at the Application layer
- Only an Application layer intercept device could intercept and modify the authenticator so it would work
- Exported Authenticators in TLS https://tools.ietf.org/html/draft-ietf-tls-exported-authenticator-06

Specific Issues

Server Name (SNI) and Application Protocol (ALPN) encryption

- Goal. A fronting server hides the identity of a hidden server and the application protocol used by the hidden server
- Draft describes two mechanisms https://tools.ietf.org/html/draft-ietf-tls-sni-encryption-02
- Neither mechanism is effective if an active Transport or Application intercept device is being used
- Both mechanisms do hide the true SNI and APLN from a passive Transport layer intercept device
- The proposed mechanisms go to great lengths to hide its use. This creates a risk that an active Security layer intercept could break the session if it does not implement the protocol changes required by the mechanism

Specific Issues

Active Transport Layer Intercept stripping unsupported/unknown elements of the security layer

- Example: The endpoint application relies on the TLS ALPN mechanism to negotiate the application layer protocol. An active intercept device strips out ALPN values it does not support from the ClientHello. So, even though the client indicated SMTP in the ALPN this is not seen by the server
- The intercept device is actually behaving properly according to the security protocol specification. See Section 9.3 https://tools.ietf.org/html/draft-ietf-tls-tls13-26

- Application layer is at fault for assuming all devices on the path understand the required extensions and values
- Stripping or modifying the APLN can be used by an active intercept device to ensure that application protocols it understands are used. For example a security device that can detect threats in HTTP but not in SPDY can ensure that only HTTP is used

Specific Issues

Token Binding

- Goal: Cryptographically bind application security tokens to the TLS session
- Binding involves a user generating a private-public key pair, providing the public key to the server, and proving possession of the corresponding private key, on every TLS connection to the server. Proof of possession involves signing the exported keying material (EKM) **RFC5705** from the TLS connection with the private key
- The Token Binding Protocol Version 1.0 https://tools.ietf.org/html/draft-ietf-tokbind-protocol-16

- Use is negotiated during the TLS handshake but the token is sent at the Application layer
  - Transport layer intercept devices are passive at the application layer so they cannot intercept TLS sessions when the server relies on the presence of a token binding
  - Application layer intercept devices could participate in Token binding allowing interception of a TLS session when the server relies on the presence of a token binding
  - If the Application layer intercept device stops intercepting then the Token binding will become invalid as the EKM will be different
- Transport Layer Security (TLS) Extension for Token Binding Protocol Negotiation https://tools.ietf.org/html/draft-ietf-tokbind-negotiation-10

Specific Issues

Application Layer TLS (ATLS)

- Goal: End to end encrypted transport, even in a Transport layer active intercept environment
- Two architectures
  - Application layer TLS session encrypts application data as TLS records
  - Application layer TLS handshake derives encryption keys from EKM **RFC5705**
- Encrypted application layer content is in identifiable ATLS packets. Meaning it is identifiable at the Application layer

- Transport layer intercept devices are supposed to recognize ATLS packets as end to end protected
  - ATLS packets will be more visible to an Application layer intercept device
- The Application layer TLS session is independent of the transport layer TLS session, indeed there need not be a transport layer TLS session
- Application-Layer TLS (ATLS) https://tools.ietf.org/html/draft-friel-tls-atls-00

Symantec™

Thank You!

David_Wells@symantec.com