DNS TAPIR Security

2024-11-26

Trust

- As DNS TAPIR deals with information pseudonymised at the edge, transferred data is non-confidential and may be inspected.
- Data integrity on the other hand is critical for trusting any submitted data, and for accepting configuration and intelligence.

We use transport encryption, interceptable if required, and also sign all data independently.

X.509 PKI for TLS connections

Each DNS TAPIR node has a classic X.509 certificate for TLS client authentication (mTLS).

- Internal PKI
- Currently NIST P-256

Keys for signing data

DNS TAPIR nodes (and core) has key pairs for signing data:

- No certificates– only keys
- All JWS algorithms supported (e.g., P-256/SHA-256, Ed25519, Ed448)

Used for signing MQTT message and some HTTP transactions.

Aggregates

- Submitted aggregates are signed using HTTP Message Signatures[1].
    - The HTTP message is signed (in cleartext) independently of transport security (TLS).
    - Allows for traffic inspection while maintaining data integrity.
- Original signatures are stored in the database and can be used to verify stored aggregates at a later time if needed.

All connections to the aggregate receiver is protected by TLS and authenticated using mTLS.

[1] HTTP Message Signatures are described in RFC 9421

MQTT Messages

- MQTT messages from/to edge nodes are signed using JSON Web Signatures (JWS)
    - Allows for traffic inspection while maintaining data integrity.

All connections to the MQTT broker is protected by TLS and authenticated using mTLS. Allowed topics are configured per peer (based on client certificate).

Traffic Inspection FTW

- You may, at your own discretion, intercept and inspect any traffic without altering the security model:
  - MQTT messages sent or received
  - HTTP message sent or received
- Inspected traffic must be forwarding using the correct mTLS certificate (or upstream MQTT messages will not be accepted)

Automatic Edge Node Enrollment

Implementation in progress

1. When enrolling a new node, the administrator will receive a node name and a shared secret
2. The node generates keys and submits CSR & public data signing key to Core
3. Core responds with bootstrap information:
    - A certificate for mTLS
    - Set of trusted data signature keys (JWKS) and root CA certificates
    - MQTT broker URL and configuration topic
4. The TAPIR edge node is ready to rumble!

The certificate for mTLS needs to renewed periodically, just like all other certificates, but the data signing key is valid until removed.

Summary

- All information transmitted encrypted (TLS)
- All information signed by creator independently of transport encryption
- Signatures kept for later verification
- Internal X.509 PKI
- Internal plain keys for signing data
- Semi-automatic enrollment (planned)