2022 ODVA

INDUSTRY CONFERENCE
AND 21ST ANNUAL MEETING

# Threat Modeling CIP Security

# Threat Modeling – Introduction

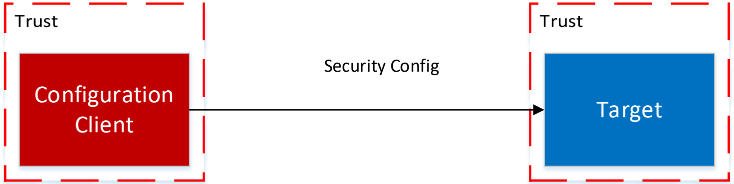
- Threat models are how we make sense of threats and mitigations on a given system
- They can take many forms but are pretty standard for cybersecurity
- Identify:
  - Critical resources: what’s important in the system
  - Trust boundaries: where are the places where if data crosses over it might need some additional assurance (e.g. encryption)
    - Generally, the network is considered untrusted
  - Threats: what are the bad things that someone/something might do
  - Mitigations: what can be done? This might be a protection, or an acceptance that the threat is sufficiently low for the system

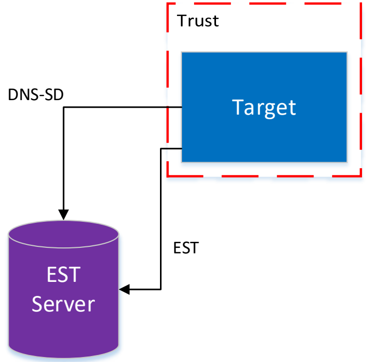
# Threat Modeling CIP Security

- Within Volume 8 of the spec a threat model was developed
  - To be published in 2022
- The threat model is general and includes many simplifying assumptions
  - Users/Vendors can use this as a starting point but will need to apply independent analysis to their products and systems
- Many things out of scope
  - Non-EtherNet/IP communication
  - Security of non CIP endpoints (e.g. time servers, certificate authorities, etc.)
  - Network based denial of service (e.g. data storms/dropped packets)
- This presentation includes a sampling of threats/mitigations, but refer to Volume 8 for more complete information

# Threats against provisioning (EIP Confidentiality Profile)

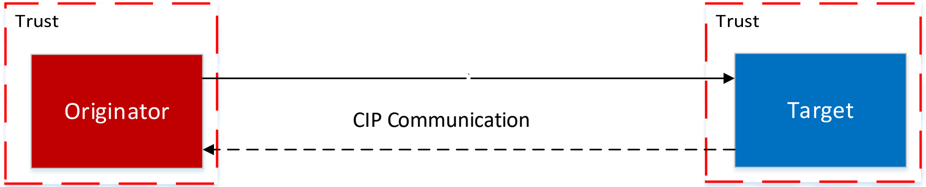
- CIP Security endpoints are generally TOFU (Trust On First Use)
  - In some circumstances this leaves them open to a bad actor configuring security before the legitimate user, that is, the config client or EST server could be spoofed
  - Both Pull and Push model
- Response: device authenticity can be validated by the vendor-signed certificate, but the device is TOFU based on market requirements
  - A mitigating technology like 802.1X can be used to further reduce this risk
  - This is an example of accepting a risk with an option to reduce it further through a mitigating technology





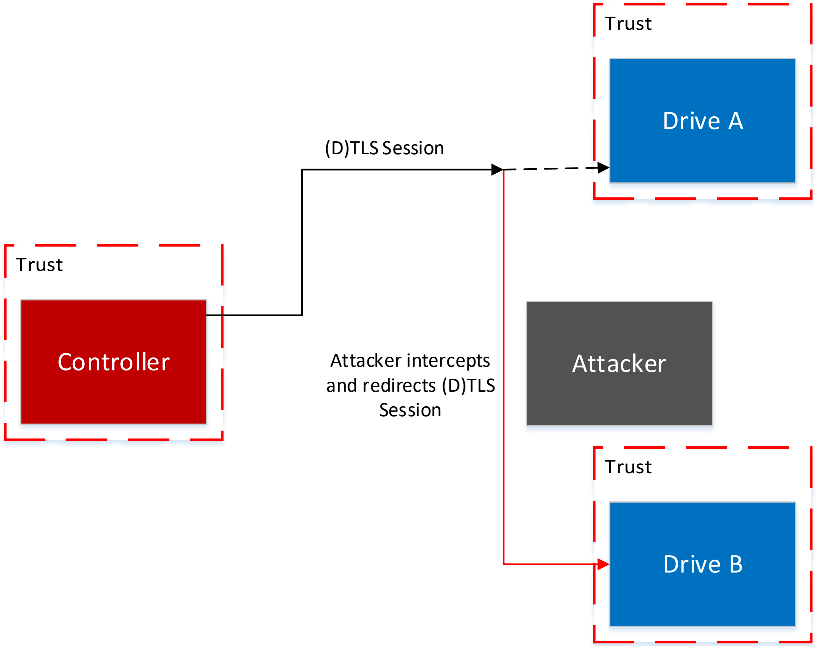
# Threats against data in transit (EIP Confidentiality Profile)

- EtherNet/IP is sent over TCP/IP routes, just like other standard IT and Internet traffic
  - Therefore it's subject to similar attacks like person-in-the-middle
  - This can result in spoofed data or tampered data
- TLS and DTLS provide HMACs on data to mitigate against packet tampering and the handshake authenticates both parties via certificate and challenge or PSK
  - This is an example of a threat to which CIP Security provides a strong mitigation



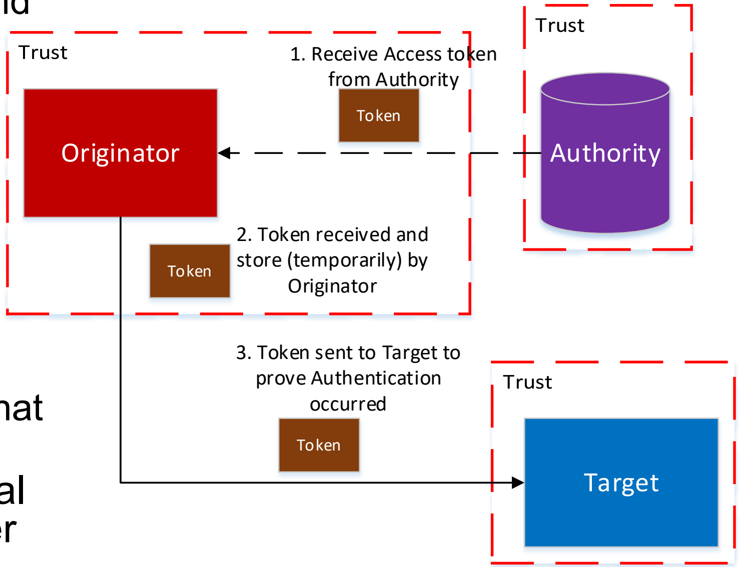
# Threats against comm. redirection (EIP Confidentiality Profile)

- TCP/IP-based attacks can result in re-direction of communication from the intended recipient to a different recipient in the system
  - Although no tampering of the data occurs, this could still result in tampering of the new recipients protected resources, and is a spoofing threat as the originator is being spoofed
- A mitigation is to check identifying information in the Target's certificate, such as the SAN
  - This represents a class of threat that is not entirely obvious, but still important to consider via threat modeling



# Threats Against Proof of Authentication (User Auth Profile)

- In the User Authentication Profile, the Token is the main proof of authentication
  - Issued by the Authority to the Originator, and then presented to the Target as proof
  - Spoofing threats exist against the various endpoints and the token itself
  - Tampering of the token could allow for an elevation of privilege
  - Information disclosure of the token would allow an attacker to impersonate the proper owner of the token
- Mitigations
  - Token is signed by the authority which can mitigate tampering of the token or spoofing of the token
  - TLS/DTLS session protects confidentiality and authenticity of the token while in transit, and ensures that an endpoint is not spoofed to obtain the token
- This is an example of a complex data flow where several mitigations work together to protect the identity of a user



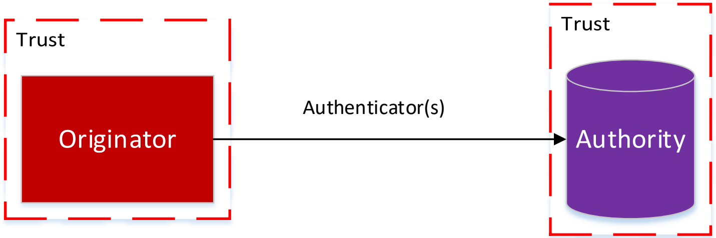
1. Receive Access token from Authority

2. Token received and store (temporarily) by Originator

3. Token sent to Target to prove Authentication occurred

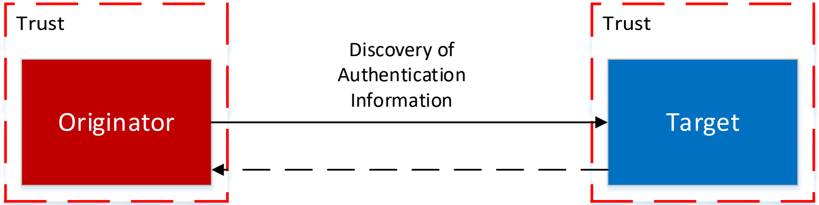
# Threats against user to authority authentication (User Auth Profile)

- A user may send authenticators (e.g. passwords) to a CIP endpoint acting as an authority to authenticate
  - Information disclosure of the authenticators is a risk as someone capturing authenticators like passwords could impersonate that user
- Mitigation is to send these authenticators over a TLS/DTLS session that is using confidentiality
  - Mitigates against packet sniffing to capture the authenticator and against sending the authenticator to the wrong endpoint via the TLS/DTLS handshake authentication
- This is an example of a threat where a technology from a different profile (EIP Confidentiality Profile) provides a strong mitigation



# Threats against discovery (User Auth Profile)

- An Originator can query the Target to find out where to authenticate (where is the Target's authority)
- Threats exist against this:
  - Spoofing: an attacker could spoof the target to redirect the user to a rogue authority
  - Tampering: an attacker could tamper with the data to redirect the user to a rogue authority
- Mitigation relies on TLS/DTLS session to provide authentication of the target and data authenticity of the discovery information
- This is another example of a mitigation provided by the EIP Confidentiality Profile, but for the User Auth Profile



# Supporting Technologies – PKI

- Needed for issuing certificates, which are the basis of authentication in TLS and DTLS
- Many commercial options for this
  - EST support helps to directly integrate with an IT-based CA
  - Or options for OT-specific PKI through vendor tools
- Security of the PKI is important!
  - How are certificates issued? How are requests authenticated/authorized
  - Same for revocation

# Supporting Technologies – OpenID Connect Identity Provider

- Provides Authentication services and issues tokens as proof of authentication
- May support many different authentication schemes like multi-factor
- Commercial and open source options (see OpenID Connect Website for a list)
  - Integrates directly with these IT systems
- Security concerns around
  - Communication: securing transport to/from Identity Provider
  - Authentication itself: ensure proper controls exist for authentication
  - Token issuance and handling: expiration, intended audience, etc.

# Supporting Technologies – Network Time Server

- Important for expiration/validity period of certificates and tokens
  - Attacker that controls this can either use old tokens or DoS through changing current time to far in the future or past
- Security options exist
  - NTPv3: MACs for data authenticity, but key management was very difficult
  - NTPv4: autokeying, but had design flaws
  - NTS4NTP: new RFC that provides robust data assurances against the attacks

# Mitigating Technologies – Firewall

- Used to prevent certain type of traffic
  - May be based on source/destination
  - May be based on traffic type
  - Or other more nuanced characteristics
- Wide range of options, from basic to sophisticated
- Generally placed at a network boundary, although what that means is subjective
  - However, generally this means that it doesn’t interfere with CIP Security communication
  - At most might need to add some configuration to allow CIP Security traffic to pass, if that is desired
  - Good compliment to the protection CIP Security offers for defense-in-depth

# Mitigating Technologies – IDS/IPS

- IDS – Intrusion Detection System, detects attacks and sends alerts
  - Can be simple pattern matching or advanced machine-learning analysis
- IPS – Intrusion Prevention System, same as IDS but attempts to actively stop the attack (may use a variety of means)
- These are often a good compliment to CIP Security and add to defense-in-depth
  - However, if they rely on deep packet inspection then encryption of CIP Security traffic will be an issue
  - Given that a lot of IT traffic is encrypted many have ways to work around this (e.g. analysis of things other than the payload)

# Conclusions

- Threat modeling is critical to understanding the risks and mitigations within a system
- CIP Security can provide strong protections, but an individual threat model is needed to understand exactly where these protections fit and what else is needed
  - CIP Security relies on some other technologies which need to also be threat modeled
  - Many other security protections fit well with CIP Security and help defense-in-depth
- Volume 8 provides a threat model as a starting place to help this effort

2022 ODVA

INDUSTRY CONFERENCE
AND 21ST ANNUAL MEETING