TLS for PVA?

Michael Davidsaver
George McIntyre

EPICS
Osprey DCS

… what is best in life?

- Maximize control system uptime
- Minimize time to repair
- Get a good night’s sleep

EPICS Osprey DCS

Why talk about “Security”?

https://arstechnica.com/information-technology/2018/01/the-internet-of-omg-vulnerable-factory-and-power-grid-controls-on-internet/

… Part of the issue is that many of these systems are outside of the usual domain of IT departments and run by separate organizations with a much different sort of security ethos. ...

This is us!

EPICS Osprey DCS

Why talk about “Security”?

https://arstechnica.com/information-technology/2018/01/the-internet-of-omg-vulnerable-factory-and-power-grid-controls-on-internet/

> *… Part of the issue is that many of these systems are outside of the usual domain of IT departments and run by separate organizations with a much different sort of security ethos. ...*

- Implications...
  - Outside of this room our concern for operational efficiency can be an **issue**!
  - IT will take blame if we get hacked regardless of prior involvement
  - IT folks are not (always) incentived to maximize uptime, etc.

EPICS Osprey DCS

Why am I talking to you?

- Opportunity
  - … to be proactive and add strong security EPICS toolbox.
- Fear
  - Reaction to a ~high profile hack of a science facility will force control systems to ~entirely disconnect from the internet.

EPICS Osprey DCS

Why talk about “Security”?

- Zero-ish trust
  - Trust is the hardest part of securing anything
  - … because you have to trust someone(s)
- Air-ish gap
  - imo. an “aspirational” more than a practical reality
  - Still has the potential to be massively inconvenient

EPICS Osprey DCS

Why not air gap?

- Notifications
- Remote troubleshooting / repair
- Continuous improvement
  - SNS added 2x PVs *since end of commissioning*
- User facilities have users
  - … who are remote
  - … who can go elsewhere!

EPICS Osprey DCS

HTTP vs. PVA/CA

- Multiplicity
  - HTTP has few “big” Servers, and many “small” Clients
  - PVA/CA has few “big” Clients, and many “small” Servers
- Time scales
  - HTTP connections mostly short lived
  - PVA/CA connections live longer
- Administration
  - HTTP installations span the planet
  - PVA/CA mostly within an organizational unit
- Names
  - HTTP can leverage the distributed DNS name database
  - PVA/CA use (mostly) broadcast name lookup

NSLS2 circa 2015 had ~800 servers on ~100 hosts.

PVA/CA w/ broadcast/multicast search has special vulnerability to MitM by “adjacent” attacker

EPICS Osprey DCS

What has been done?

- CA style "voluntary" authentication (host+user names)
  - "threat model" is stray mouse click
  - PVA does the same
- Access "Security" (aka. EPICS ACL)
- Server weakly authenticates client
- client does **not** authenticate server
- `var asCheckClientIP 1`
  - CA/PVA client host name can't spoof host name
  - Base 7.0.3.1

Partial mitigation

EPICS Osprey DCS

What **needs** protection?

Yes

- Unauthorized PUT
- Tampering with GET/MONITOR

  Trick authorized user into Making incorrect PUT

No

- Secrecy

  May come incidentally, just not required

EPICS Osprey DCS

Threat model

- Actors
  - Passive attacker on adjacent host
  - Active attacker on adjacent host
  - Attacker on client host
  - Attacker on server host
  - Compromised client
  - Compromised server

Same subnet

Same host

Same process

EPICS Osprey DCS

Threat Vectors (1)

	Reasonable © Mitigation?	
• Passive traffic inspection (TCP/UDP)	Yes/No	*Doesn't matter*
• Denial of service by search spam	Partial	
• Search hijacking	Yes	
• Server impersonation	Yes	
• Server credential theft	Partial	

EPICS Osprey DCS

Threat Vectors (2)

	Reasonable © Mitigation?	
• Passive traffic inspection (TCP/UDP)	TLS/???	*Doesn't matter*
• Denial of service by search spam	NameServer	
• Search hijacking	NS	
• Server impersonation	TLS	
• Server credential theft	NS + cert. pinning	

EPICS Osprey DCS

TLS for PVA

System Considerations

- Distributing CA certs.
  - Straight forward copying of (mostly) static files
- Issuing Server (and Client) certs.
  - Tedious ~manual process
  - What Common Name?
- Cert. validity
  - Expiration date?
  - Certificate Revocation List?
  - **Periodic online check** (Open Certificate Status Protocol)?

EPICS Osprey DCS

Certificate Validity

- Time based
  - Valid between X and Y
  - Encoded in certificate

Trust in NTP becomes critical

- CRL
  - Periodically published list of revoked (bad) certs.
- Open Certificate Status Protocol
  - Access to database of signatures on valid certificates (w/ time)
  - Like an expiration date
  - Can be updated **w/o reissuing** cert.
  - Requires client connection to OCSP server(s)

“stapling” helps

EPICS

Osprey DCS

“secure” EPICS?

- Distributed name server
  - Bridge to site user auth. systems
  - Cert. management
- IOCs
  - TLS Cert.
  - Key is unique ID

EPICS Osprey DCS

What to do now?

- Strong_{er} authentication
  - in both directions
- *Distributed* Name server
  - prevent trivial MitM
  - “pinning” prevents (some) impersonation
- Secure transport (TLS)

Zoo of user auth. mechanisms (kerberos, ldap, ...)

Client authenticates server!

EPICS Osprey DCS

What to do now?

Can sites collect operations stats on how remote access affects MTtR?
- *How many trouble calls involving remote triage?*
- *How many trouble calls involving remote repair?*

I can help to aggregate

EPICS Osprey DCS