
WEBINAR
Is IT Cryptography the Right Tool for Your OT Network?
DRAGOS
SEL
SCHWEITZER
ENGINEERING
LABORATORIES
DUKE
ENERGY

Before we get started…

- The webinar is being recorded
- The recording will be sent out in a few days
- Please submit questions using the Q&A feature
- All attendee phones are muted
- Let’s get started!

AGENDA

INTRODUCTIONS

Speakers

CRYPTO PERSPECTIVES (USER)

Theory **vs** Lessons from the Real World

CRYPTO PERSPECTIVES (OEM)

Benefits, Challenges, and Guidelines

CRYPTO PERSPECTIVES (VENDOR)

Impacts and Considerations for Monitoring

SUMMARY

Close-out with Q&A

Casey Roberts
Senior Cybersecurity Architect – OT

Colin Gordon
Lead Application Engineer

Dan Gunter
Director of Research and Development

Casey Roberts

CSF Framework

Fundamental building block

Effective Crypto cannot function properly unless a thorough asset inventory is complete

Strong, Layered Defenses

Best Practice but dependent on good asset identification

Restoration and Process Improvement

When the incident is over and we're all looking at the remnants, how do we get the system back online

Analysis and Impact Reduction

What is the response to crypto being used against us
Can we regain control and limit the impact to the OT environment

Cyber Situational Awareness

Crypto may adversely effect the IDS / IPS data collection abilities of compromises

Resistant to Change

ICS Architecture slow to change

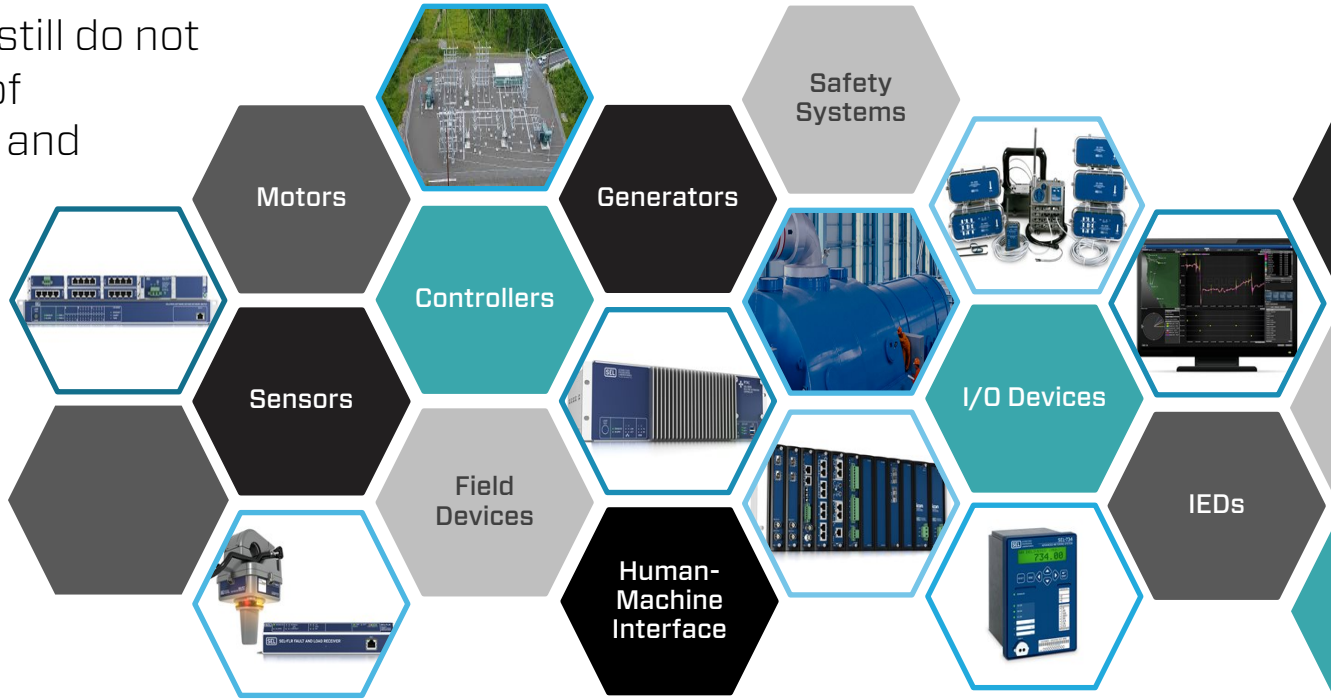
- Requires stability to ensure availability / reliability because of mission critical responsibilities
- Can SCADA reliably have complete control and visibility
- Increased communication errors causes operator distractions
- Unnecessary labor constraints

Let a relay be a relay for crying out loud

- Resistant to change but with good reasoning
- Will the overhead cause a potential issue with protection

Educate – How does this work?

- Many ICS professionals still do not understand the benefit of Confidentiality, Integrity, and Availability (CIA)
- New tools to implement new practices
- Need training to understand new techniques and how to configure them



Colin Gordon

Cryptography (Crypto) Can Benefit ICS Mission

Safe, Reliable, Available Critical Services

Risks to ICS infrastructure

- Human error
- Cyber threats
- Flora and fauna
- Adverse weather
- Single-event upsets

Subset of mitigations

Crypto for data in motion

- Confidentiality
- Integrity
- Authenticity

Cryptography Can Detract From Mission

- Susceptibility to standards changes
- Long-term key management
- Development complexity and patching susceptibility
- Complex and error-prone for users
- Interoperability with Network Monitoring Tools
- Computational and silicon-level requirements
- Latency effects
- Quantum apocalypse

Most protective relays are in service for **15–25 years**

Separate Dynamic and Static Elements

Dynamic

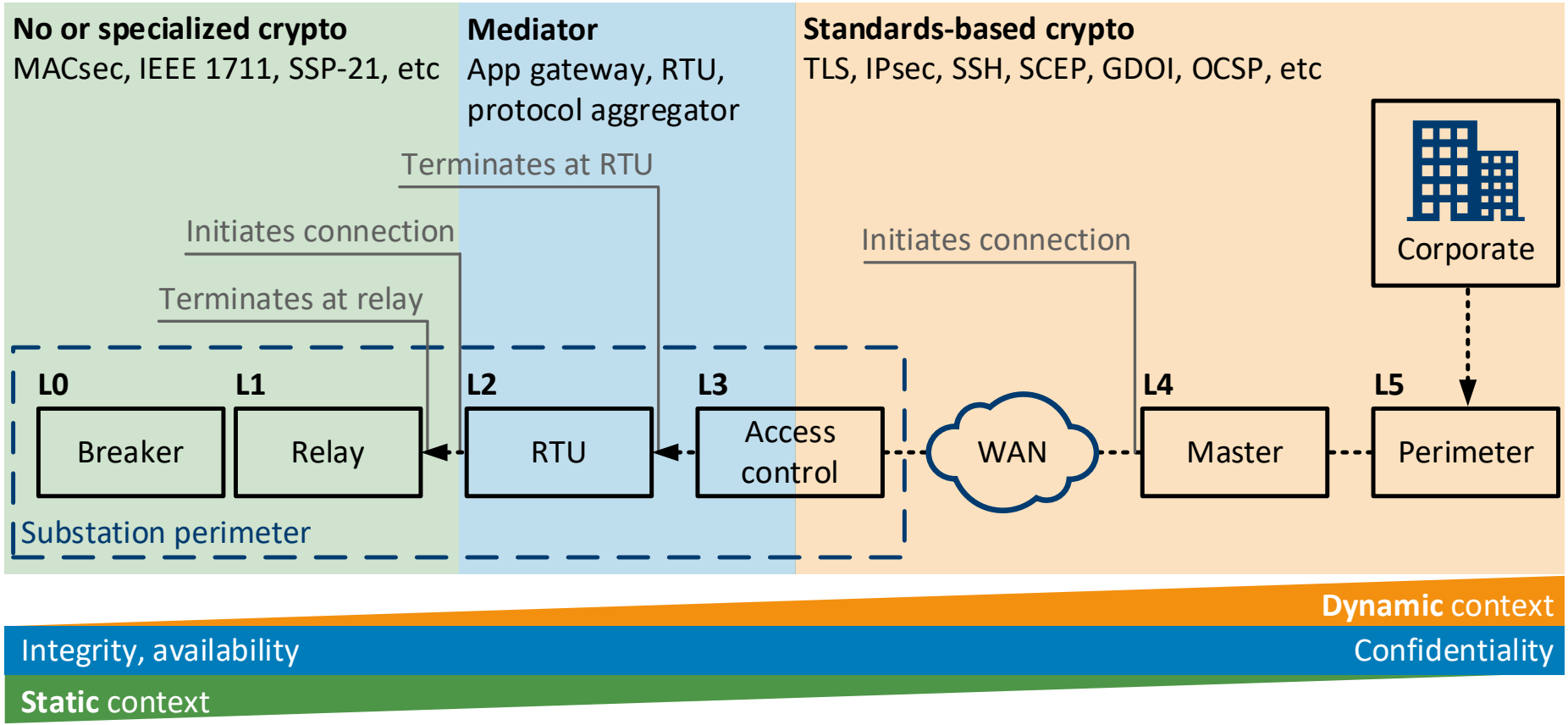
Human-centric, plug-and-play devices and applications

Static

Critical elements emphasizing reliability and availability

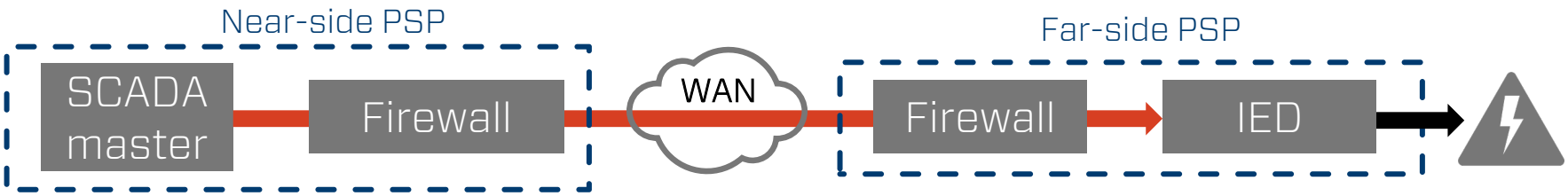
Mediator

Appropriately secured chokepoint that can be both dynamic and static


No or specialized crypto
MACsec, IEEE 1711, SSP-21, etc
Mediator
App gateway, RTU, protocol aggregator
Standards-based crypto
TLS, IPsec, SSH, SCEP, GDOI, OCSP, etc
Terminates at RTU
Initiates connection
Terminates at relay
Initiates connection
Corporate
L0
L1
L2
L3
L4
L5
Breaker
Relay
RTU
Access control
WAN
Master
Perimeter
Substation perimeter
Dynamic context
Integrity, availability
Confidentiality
Static context

Why Not End-to-End?

- Some protocols (TLS 1.3) mandate confidentiality
- Threat vectors originate from dynamic elements (e.g., humans)
  - Compromised near-side endpoints offer little to no protection
  - Attacks over VPNs bypass far-side firewalls
- Attackers can attempt DoS against exposed protocol stacks
- Near-side dynamic elements force far-side static elements into short life cycles

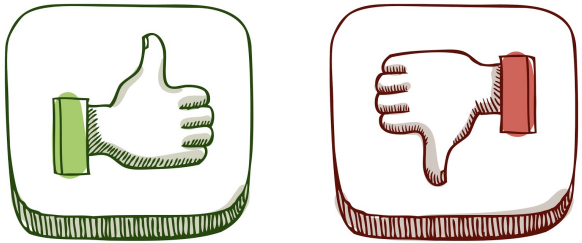


Dan Gunter

How Cryptography Impacts ICS Security Monitoring

Cryptography for Integrity

- Prevents replay and other attacks
- Works with existing security program
- Time, and sometimes life, sensitive



Cryptography for Confidentiality

- Short term benefit that also hides attacker presence and movement
- Shifts collection management framework to host based solutions
- IT crypto defense approaches not appropriate in industrial networks

Cryptography For Integrity

PROs

Prevents replay and other attacks

- Packet or code signing provides authentication factor
- Assumes keys aren't compromised

Works with existing security program

- A network + host security program is less complex than a all host security program

VS

CONs

Time, and sometimes life, sensitive

- Signing algorithms and options need to be appropriately responsive

Cryptography For Confidentiality

Short term benefit that also hides attacker presence and movement

- Encryption leads to loss of network visibility

Shifts collection management framework to host based solutions

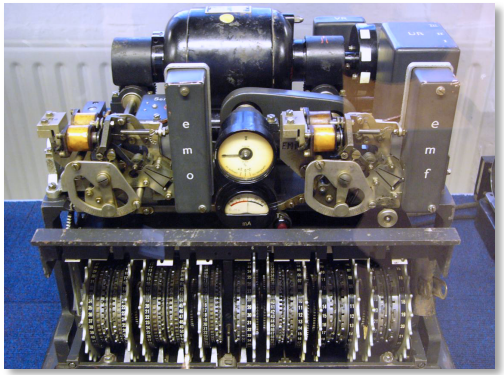
- Harder to scale as the environment scales
- No entirely passive monitoring options

IT crypto defense approaches not appropriate in industrial networks

- SSL stripping or continuous bulk decryption of an industrial network likely inappropriate
- Slows ability to diagnose and respond to process borne threat

How Cryptography Impacts ICS Security Monitoring

Cryptography for integrity and cryptography for confidentiality impacts security program differently



- Integrity focused program:
  - Allows network and host monitoring
  - Blocks some attacks
- Confidentiality focused program:
  - Adds complexity to security program
  - Requires endpoint modification
  - Slows ability to diagnose and respond to process borne threat


THANK YOU
DRAGOS
SEL
SCHWEITZER
ENGINEERING
LABORATORIES
DUKE
ENERGY®