Bringing Identity Standards into the World of Critical Infrastructure

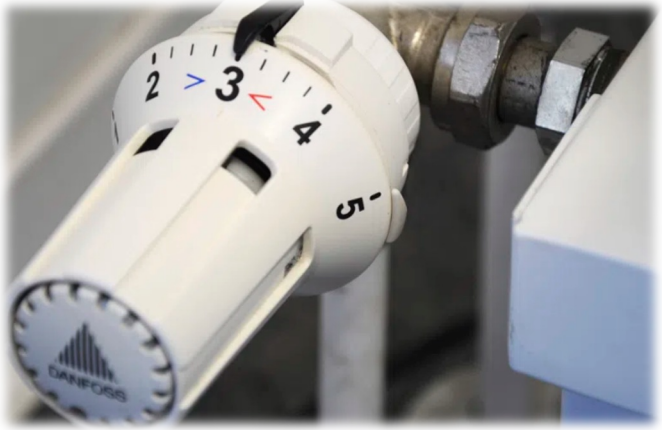
Steve Venema, PhD, CISSP

Distinguished Engineer, Office of the CTO

ForgeRock

Control Systems have evolved

Mechanical Thermostats



Digital Thermostats

Connected Thermostats

What is OT?

OT = Operational Technology

- *Hardware and software that detects or causes a change in the physical world, through the direct monitoring and/or control of industrial equipment, assets, processes and events [Wikipedia]*

Related Terminology

- Process Control Systems (PCS)
- Industrial Control Systems (ICS)
- Cyber-Physical Systems (CPS)
- Distributed Control Systems (DCS)
- Supervisory Control and Data Acquisition (SCADA)

What is Critical Infrastructure?

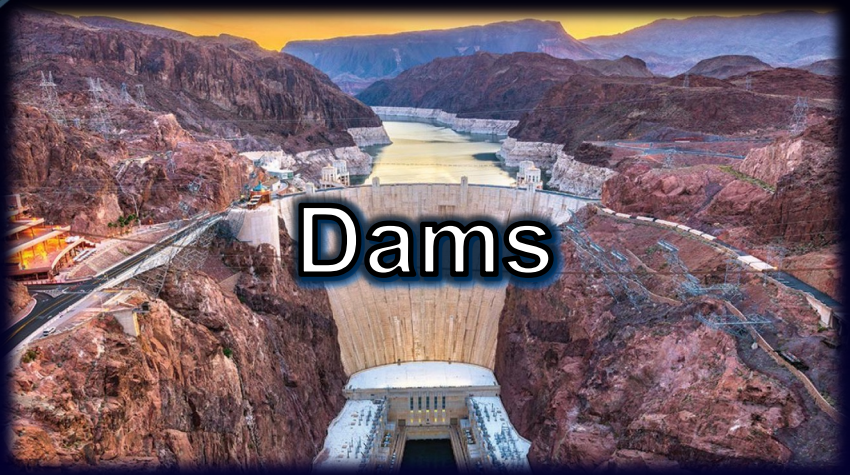
Why do we care?

CISA Definition

…assets, systems, and networks, whether physical or virtual, [that] are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

CISA: 16 Critical Infrastructure Sectors

CISA: 16 Critical Infrastructure Sectors



CISA: 16 Critical Infrastructure Sectors

CISA: 16 Critical Infrastructure Sectors

Information Technology

Nuclear Reactors, Materials and Waste

Hypothesis

Modern identity standards can improve the security posture of OT and CI systems by helping to bridge the IT/OT divide

History: OT and CI have a “long tail” problem

- Hundreds of legacy protocols remain in use today
  - Usage varies by sector and vendor
  - Many incompatible with standard IT systems and networks
  - Cross-vendor interop hasn’t been a top priority
- System lifecycles of decades, unlike IT’s 3-5 years
- Historically, security has depended on isolating OT systems from each other and from IT systems

The Mythical Airgap

IT/OT Convergence: The pressures build

- Connectivity increases across traditional isolation boundaries
  - Drivers: increase visibility and efficiency, lower opex
  - Began in earnest in the mid-to-late 1990's

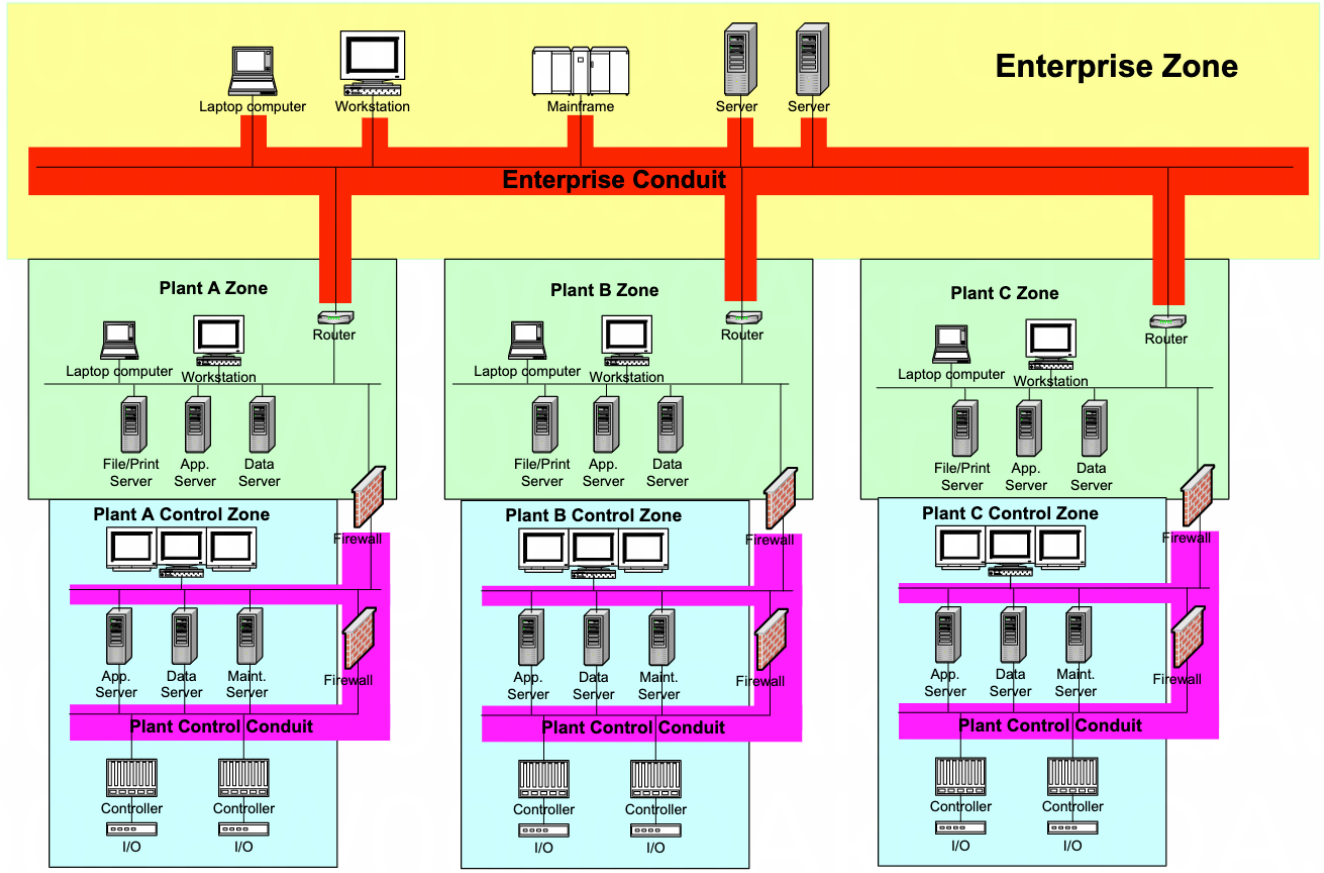
- Accelerants
  - Growing need for remote support due to skillset shortages
  - Vendors increasingly offering Cloud-only OT services
  - Growing use of real-time, cloud-based data lakes to manage costs
  - Growing intersection with IoT & IIoT – e.g., home automation

Current Best Practices – Security Architecture

ISA99 ⇔ IEC 62443

- Zones
  - Groups of assets with shared security requirements
  - Generally implicit trust between devices within a (sub)zone
- Conduits
  - Connections between (sub)zones
  - Firewalls to control flows

Network Segmentation Model



Security improvements are clearly needed
May 2022 Trend Micro ICS/OT Security Survey

- 900 respondents from companies with 1000+ employees
  - Industries: manufacturing, electric utilities, oil and gas
  - Countries: US, Germany, Japan
  - Questions focused on cyberattack experiences in the past 12 months
- Results
  - 44% had 6-10 cyberattack disruptions – balanced across OT & IT
  - Average damages of $2.8M
  - Top reason to strengthen ICS/OT security: Prevent recurrence of incidents

The State of Industrial Cybersecurity, Trend Micro Survey Report, May 2022

Where are the Identity-related challenges?
User / Operator Level

- Increasing rate of account and entitlement changes
- User authN often uses local accounts and passwords
  - Also shared accounts or no authN
  - Access speed is critical for safety and can trump security

Identity standards can help keep accounts & entitlements in sync

Where are the Identity-related challenges?
Device Level

- Too much trust within a zone
- Static firewall-based rules
- Lack of standard device onboarding
- Lack of standard SBOM inventory
- Lack of standard device health attestation

What tools are in our toolbox?

- OAuth2
- SAML Federation
- OIDC
- SCIM
- X.509, OCSP
- SCEP

Problem solved, right?? Not so fast!

Understanding OT Domain Limitations

- OT systems usually have a reverse priority triad
- OT systems are often delay-intolerant
- OT systems may use standard IT components, but not in a standard way

Any use of Identity standards must **adapt**
to OT domain requirements

Is Zero Trust applicable to OT?

- **Zero Trust**
  - Focused on resource protection
  - Trust is never granted implicitly but must be continually evaluated
- **Zero Trust architecture encompasses**
  - Identity (person and nonperson entities)
  - Hosting environments
  - Access management
  - Interconnecting infrastructure
  - Credentials
  - Endpoints
  - Operations
- **See:**
  - NIST SP 800-207: Zero Trust Architecture
  - NIST SP 800-82: Guide to OT Security (Rev. 3 draft)

What would Zero Trust look like for OT?
The future I'd like to see

GOAL:
Security +
Interoperability

- Leverage existing standards and IT best practices where possible
- OT-specific profiles will be needed

- **Provisioning:**
  - OEM-provided X.509 identities for secure onboarding
  - Operator can replace identity after onboarding
- **Authentication:**
  - Devices authenticate peer devices, services and personnel
- **Authorization:**
  - System-level authorization policy
  - Device-level enforcement
- **Logging & Audit:**
  - Standardized event and logging streams

Approaches for Improved User Security & UX

- Poor user authentication practices stem from:
  - Fast access requirements
  - Constrained device HMIs
  - Cost of change
- Strong authentication allows
  - Improved access control granularity
  - Improved accuracy of auditing
- FIDO offers some interesting possibilities
  - Fast authentication
  - Near-field/BLE for constrained HMI devices

How can these ideas help?

- None are cure-alls to today's cyberattacks by extortionists, terrorists and nation-states, but they can help!
  - Increased visibility into OT systems operations
  - Increased granularity of authorization policies
  - Reduced "blast radius" of compromises
- Many OT cyberattacks come through the supply chain
  - Ex: 2014 DragonFly, 2020 Solar Winds, 2022 "Pipedream" toolkit
  - Best practices need to extend up into the supply chain

What can you do to help?

- OT Operators:
  - Raise the bar with your OEM vendors and integrators
- OT OEM Vendors:
  - Look to apply security & identity standards into product lines & roadmaps
  - Learn from customers seeking to improve IT/OT convergence
- Identity Professionals:
  - Develop a deeper understanding of the OT and Identity domains
    - Lots of OT training opportunities: CISA, SANS Institute, etc.
  - Participate in standards communities such as ISA to make sure that the perspectives of Identity professionals are at the table

Hypothesis

Modern identity standards can improve the security posture of OT and CI systems by helping to bridge the IT/OT divide

The way forward

It will take a lot of time to make progress on this, but its important to start the conversation, seek consensus and get started!

Thank You!

Steve.Venema@ForgeRock.com