Network Function Insertion for Reliable and Secure Control Messaging Over Commodity Transport

Deniz Gurkan, Nicholas Bastin, Stuart Baxley
University of Houston
Resiliency against Threat Vectors in Commodity Transport

- Sensor data and control directives from oil/gas production facilities are transmitted unencrypted using unreliable transport protocols over lossy network infrastructures
- Network threats evolve on a time scale significantly faster than the upgrade schedules of industrial equipment
Resiliency Solution: Network Function Insertion

• Decouple the implementation of secure, reliable transport from the actual industrial hardware

• Provide agility in responding to new threats without downtime or vendor upgrades

• Design and implement a network function which can be deployed without infrastructure disruption into existing ICS
Resiliency through Policy Enforcement

• Network transport quality
  • Loss
  • Delay
  • Re-ordering

• Threat vectors: injection attacks
  • Signed packets: Integrity of the system – system control data:
    • Injection by an external third party
    • Injection by an internal third party
  • Encryption: Privacy – system sensor data:
    • Listening by a third party
POLICY: control knobs with trade-off

• A lossy network:
POLICY: control knobs with trade-off

- A lossy network:

Existing protocols: retransmissions, lost connections, end point (not flow-specific) tuning

Custom POLICY: delayed but GUARANTEED delivery

Custom POLICY: NO delivery unless IN-ORDER
Resiliency – Network Transport Quality

- Loss, delay, re-ordering
POLICY: control knobs with trade-off

- A lossy network:

Custom POLICY: GUARANTEED delivery – delayed on lost packets
Resiliency – Attack Vectors: injections

• Integrity of the system (system control/sensor data), privacy (sensor data)
Resiliency against attacks

Existing protocols: end to end protection with firewalls, without signed packets *per flow*
POLICY: guarantee access by authorized personnel and keep sensor/control data private

Custom POLICY: signed and encrypted packets of the flow
Reconfigurable ICS Scenario on UH Testbed

• Support *multiple concurrent arbitrary isolated* topologies, with MTS (Managed Topology Services) orchestration system:
  • Software-defined networking scenarios
  • Critical infrastructure security
  • Internet of things
  • Computer networking education

• UH Testbed Resources:
  • Over 1000 1Gb and 10Gb switch ports from Brocade, Cisco, Dell/Force10, HP, Intel, and Pica8
  • Over a dozen SDN switches
  • A variety of specialized forwarding devices (NPUs, hybrid server-switches, etc.) from Caros, Cavium, Freescale, Intel, and Znyx
  • Over 250 general purpose CPU cores and 1.5TB of ram across two dozen servers
  • Over 100TB of raw storage capacity and 24 line-rate taps
Network Function Insertion: Testbed Setup

• Number of sites
• Sensors per site
• Sensor emulation software at sensor nodes
• Management emulation software at remote console

• Loss
• Delay
• Reorder

• Without a NF - baseline behavior of the network
• With NF - network function software at NF nodes
Project Next Steps

• Reference implementation that achieves representative ICS scenarios with configurable loss and delay.
• A test suite for the reference implementation using the UH Testbed.
• A specification document for the network function deployment and logical functionality.
• Analysis to show the level of resiliency achieved through the network function deployment.
• Validation and verification results of our implementation and testbed setup in collaboration with PNNL.
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

http://cred-c.org
@credcresearch
facebook.com/credcresearch/

Funded by the U.S. Department of Energy and the U.S. Department of Homeland Security