Network Reliability Monitoring Using Statistical Modeling and Data Analysis to Measure the Health and Security of ICS

Jim Gilsinn
Kenexis
Jim Gilsinn

- Senior Investigator, Kenexis Consulting
  - ICS Network & Security Assessments & Designs
  - Developer, Dulcet Analytics, Reliability Monitoring Tool
- International Society of Automation (ISA)
  - ISA99 Committee, Co-Chair (ISA/IEC 62443 Standard Series)
  - ISA99-WG2, Co-Chair (ICS Security Program)
Overview

- Introduction
- Communications Method Affects Metrics
- Network Security Monitoring
- Communications in ICS/SCADA Networks
- What Can Network Reliability Monitoring Show?
- When & How to Test
- ICS/SCADA Performance Metrics
- MITM Example
- Summary
Introduction

• Determinism is one key req. for ICS/SCADA
• Determinism can be affected by many factors:
  – Individual device performance
  – Network performance
  – Intra- & inter-system interactions
  – Security settings
• Some factors can be planned for
• Some factors need to be measured in place
• Network measurements need to be tailored for ICS/SCADA
Comm. Method Affects Metrics

Master/Slave

Publish/Subscribe

Report by Exception
What is NSM?

• “the collection, analysis, and escalation of indications and warnings to detect and respond to intrusions.”

• “a way to find intruders on your network and do something about them before they damage your enterprise.”

The Practice of Network Security Monitoring, Richard Bejtlich
When NSM Won’t Work?

• “…if you can’t observe the traffic that you care about, NSM will not work well.”

• “Node-to-node activity, though, is largely unobserved at the network level.”

The Practice of Network Security Monitoring, Richard Bejtlich
Example ICS/SCADA Network: Upper-Level Architecture

- Most Traffic Crosses Zone Boundaries
- Less ICS-Specific Protocols
- More Common Platforms
Example ICS/SCADA Network: Lower-Level Architecture

- Most Traffic Remains Within Zone
- Mostly ICS-Specific Protocols
- ICS-Specific Platforms
So... What Can You See?

~1ms Mean Measured Packet Interval

±10µs Jitter*

Beat Patter @ ~30s

Total Test ~65s

*Jitter is Variation From Expected Frequency
So... What Can You See?

- OS & application operations
  - Garbage collection
  - Antivirus checks & updates
  - On-screen operator commands
- Network anomalies
  - Network EMI interference
  - Signal degradation
  - Flaky connections
- Security-related incidents
When & How To Test

- Baseline Testing
  - FAT, SAT, Commissioning
  - After major changes
- Periodic Testing vs. Real-Time Testing
- Automated Testing & Analysis
ICS/SCADA Performance Metrics

• Easy
  – Mean
  – Minimum
  – Maximum

• Medium
  – Standard Deviation

• More Complex and/or Compute Intensive
  – FFT
  – Convolution
  – Correlation
MITM Example
Summary

- NSM is good
  - If you are doing it great
  - If not, maybe you should
- NSM can’t detect everything, especially for ICS/SCADA networks
- There are ways to measure network reliability in the lower layers
  - ICS/SCADA networks are particularly well suited to this
  - Relatively simple metrics are good enough to start
- Testing can show more than just security events