Industrial Control System (ICS) Security Using TNC Technology

November 19, 2013, 1:00PM EST
No Sound?
This is a streaming audio event. Make sure the sound on your PC is turned on.

Questions?
Type your questions using the Ask a Question Text Box
Today’s Presenters

David Mattes, Founder, Asguard Networks
Mattes has developed network security appliances that help companies connect their industrial assets in a way that is highly secure, cost-effective and easy-to-use. He is the founder and lead developer for ompad, an open source IF-MAP server. Prior to Asguard Networks, Mattes was with The Boeing Company where he developed architecture and implementations for managing legacy connectivity for industrial control systems, embedded wireless controllers for hydraulic testing, a secure mobile factory workstation, and other applications.

Eric Byres, CTO and Vice President Engineering, Tofino Security
Byres is recognized as one of the world’s leading experts in the field of SCADA security, and with a background as a process controls engineer, he has a unique combination of deep technical knowledge plus practical field experience. He has written extensively on Stuxnet, leads various industry standards groups and has consulted with governments and enterprises.

Lisa Lorenzin, Principal Solution Architect, Juniper Networks
Lorenzin specializes in security and mobility solutions and has worked in a variety of Internet-related roles since 1994, with more than a decade of that focused on network and information security. She is currently concentrating on enterprise security - including network segmentation, end-to-end identity-based access control, and integration of mobile security.
Industrial Control Systems Network

Control and Monitoring

- HMI
- MTU

Backup Control Center

- CDMA
- Modem
- TCP-MODBUS
- DNP3
- ICCP

Substation ICS

- RTU
- PLC

Internet

Copyright 2013 Trusted Computing Group
Infrastructure Challenges

- Designed for safety, not security
- Standard applications, OSes seldom patched
- Susceptible to a variety of attacks
- Lack forensic capabilities
- Logging for operations, not communication
Goal: Integrated ICS & IT Intranet

INSECURE CONNECTIVITY

IDEAL INTEGRATED ICS AND IT INTRANET
Integration Drivers

- Geographically dispersed systems
- Responsiveness
- Business agility
- Cost savings
- Compliance
- Security
- Safety
Security Challenges

Attacker

Corporate Network

HMI Computer

PLC
Solution: Secure Overlay Network
For a customer POC, you will receive a license valid for 30 days.
For internal Juniper use, you will receive a license valid for 90 days.

TCG: Standards for Trusted Systems

- Virtualized Platform
- Mobile Phones
- Printers & Hardcopy
- Network Security
- Security Hardware
- Desktops & Notebooks
- Servers
- Authentication
- Storage
- Applications:
  - Software Stack
  - Operating Systems
  - Web Services
  - Authentication
  - Data Protection

Copyright 2013 Trusted Computing Group
Open Architecture for Network Security
- Completely vendor-neutral
- Strong security through trusted computing
- Original focus on NAC, now expanded to Network Security

Open Standards for Network Security
- Full set of specifications available to all
- Products shipping since 2005

New Standard for Industrial Control Systems
- Aligns with ISA100.15 Backhaul Network Architecture
- Aligns with IETF standards for PKI and identity-based comms
Problems Solved by TNC

- **Network and Endpoint Visibility**
  - Who and what’s on my network?

- **Endpoint Compliance**
  - Are devices on my network secure?
  - Is user/device behavior appropriate?

- **Network Enforcement**
  - Block unauthorized users, devices, or behavior
  - Grant appropriate levels of access to authorized users/devices

- **Security System Integration**
  - Share real-time information about users, devices, threats, etc.
TNC Architecture

Endpoint

Enforcement Point

Policy Server

Metadata Access Point (MAP)

MAP Clients

Copyright 2013 Trusted Computing Group
Dynamic Connectivity and Trust Management

IF-MAP COORDINATION

UNTRUSTED IP NETWORK

Backhaul Connectivity
- Any link type: Ethernet, Cell, WiFi, WiMax, SatCom, etc.
- Backhaul authentication

Protection
- Authentication
- Confidentiality
- Integrity
- Policy Enforcement

OVERLAY NETWORK

ISOLATION BOUNDARY

IP OVER BACKHAUL

TRANSPARENCY

Existing ICS protocols
Layer 2 VPLS

ICS OPS CENTER

FIELD ICS
Solution – Intelligent Isolation

Provisioning Client

Enforcement Point

MAP

Attacker

Corporate Network

STOP

OpenHIP Overlay (Virtual “Wire”)

Enforcement Point

HMI Computer

PLC

Tofino Endbox

Tofino Endbox

Provisioning Client

Enforcement Point

HMI Computer

OpenHIP Overlay (Virtual “Wire”)

Attacker

Corporate Network
Next Steps and Call to Action

- Design ICS security solutions customized for your unique environments.
- Contact vendors and insist on acquiring TCG-certified ICS security solutions based on the TNC and ISA standards.
- Deploy solutions in pilot first, observe and correct issues, then deploy into production.
- For more information on TCG technologies and architects guides, visit [www.trustedcomputinggroup.org](http://www.trustedcomputinggroup.org)
Questions?

Post your question now.