IIoT and Security – An External View

Matthias Luft, mluft@ernw.de
Stefan Kiese, skiese@ernw.de

ERNW

- Vendor-independent
- Established 2001
- 65 employees, 42 FTE consultants
- Continuous growth in revenue/profits
  - No venture/equity capital, no external financial obligations of any kind
- Customers predominantly large/very large enterprises
  - Industry, telecommunications, finance

ERNW
providing security.

ERNW Mission

- Integrity
- Independence
- Technical Competence
- Open Access to Knowledge

ERNW
providing security.

whoami

- Matthias Luft
- CEO of ERNW GmbH
- IT Security since 2006
  - Hypervisor/virtualization/network security
  - Production security since 2010
    - “Shopfloor Micro Segmentation with Industrial Firewalls”
    - Author of ENISA’s “Hardware Threat Landscape and Good Practice Guide”
- From pentester to researcher to consultant to team lead

“Hi, I’m a consultant.”

ERNW
providing security.

whoami

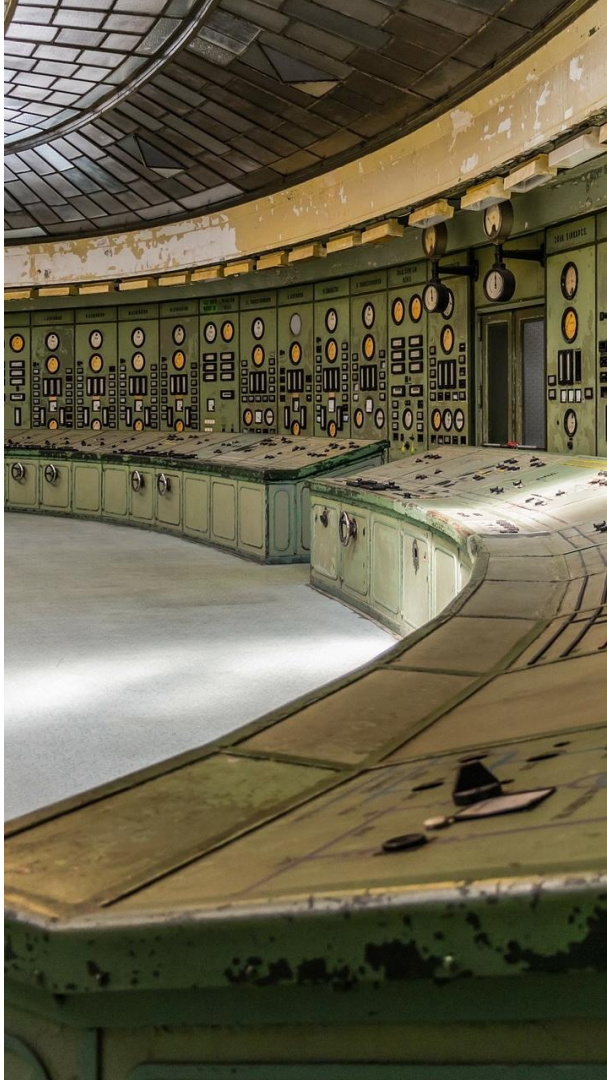
- Stefan Kiese
- Security Researcher @ERNW GmbH
- IT Security since 2010
  - Embedded & RF Security
- E.g.
  - “Dropping the MIC; picking up the keystore” – Extracting CISCO Manufacturer Installed Certificates
  - Author of ENISA’s “Hardware Threat Landscape and Good Practice Guide”

“Hi, I’m a Hacker!”

ERNW
providing security.

ERNW and IIoT

- Penetration Tests/Vulnerability Assessments
- Risk Assessments
- Design Review/Architecture
  - Particular focus on network architecture
- Security Concepts



Agenda

- Industrial Internet of Things – Current State
- IIoT Security Challenges
- Case Studies & Potential Security Approaches

Adventures in Attacking Wind Farm Control Networks

ERNW
providing security.

Current State

Cyber attack hits German train stations as hackers target Deutsche Bahn

share

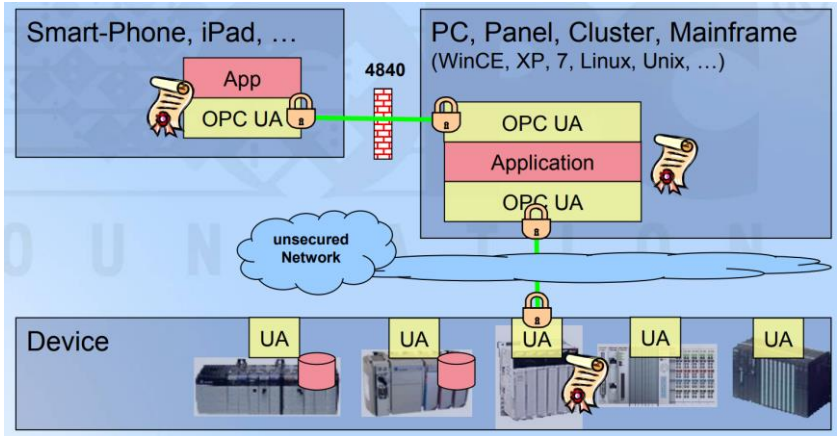
Alert (IR-ALERT-H-16-056-01)

Cyber-Attack Against Ukrainian Critical Infrastructure

Original release date: February 25, 2016

A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case

By **JOSEPH BERGER** MARCH 25, 2016



CONNECTED MACHINES	REMOTE MONITORING	
Sensors	Network	Integration

Built-in sensors
- Existing machine sensors

External sensors
- Temperature
- Vibration
- Amperage

Connectivity
- Bluetooth
- Wi-Fi
- LoRa
- RFID

Management
- IoT middleware

Accumulation
- Data management

Existing data
- PLC
- CMMS
- ERP
- Data historian
- Industry standards
- Original equipment manufacturer parameters

Current State

Making maintenance smarter

Predictive maintenance and the digital supply network

PLM + MES + ERP = Closed-Loop Product Lifecycle

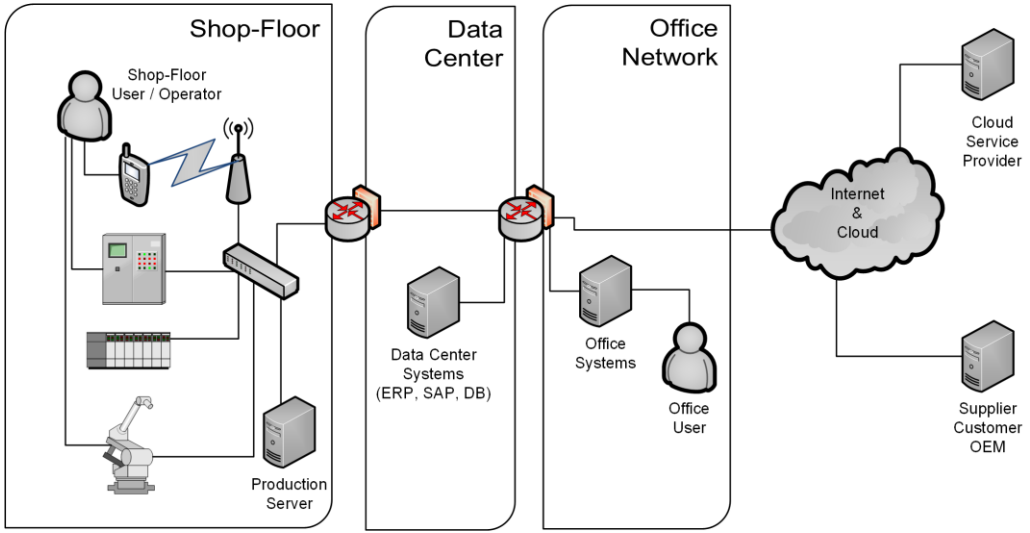
ERNW
providing security.

Current State - Summary

- Security Level:
  - Not at a new record high
- At the same time:
  - Plans/requirements to increase exposure.

Industrial Internet of Things

- Interconnectivity between
  - different shop-floors
  - ERP
  - Office
  - external Partners
  - …
- Drivers:
  - Predictable Maintenance
  - Just in Sequence production
  - Optimization of Production Processes



ERNW
providing security.

Relevant Distinctions

- Sensor/PLC vs.
  Panel PC vs.
  Full-Blown Industrial PC

- Soft- and hardware settings are very different!

ERNW
providing security.

Challenges

- IIoT Protocol Characteristics
- Network Exposure
- Maintenance Access
- Update and Vulnerability Management
- Physical Security
- Establishment of Trust
- Security Testing

ERNW
providing security.

Protocols & Network Exposure

- Industrial systems were designed to work in a “closed” environment
- Safety and availability were top priority
- Communication was designed in a “point-to-point way”, like
  - Serial, RS485, CAN, Fieldbus
- Security therefore based on/achieved by physical connections

ERNW
providing security.

Categorization Regarding Use Case

- Process automation protocols
- Industrial control system protocols
- Building automation protocols
- Power system automation protocols
- Automatic meter reading protocols
- Automobile / Vehicle protocol buses

(src: wikipedia.org)

ERNW
providing security.

Categorization Regarding Origin/Characteristicss

- Fieldbus
- Ethernet/LAN
- Wireless
  - LAN-like
  - Bus-like

- + real-time or safety-oriented variations

Categorization Regarding their Origin

- Fieldbus
  - CAN
  - Serial
  - ModBus
  - Profibus
- Ethernet/LAN
  - See above in TCP/IP version ;-)
  - OPC-UA
  - SMB
  - MQ-TT
  - DDS
- Wireless
  - LAN - See LAN
  - Bus-like
    - Zigbee
    - Bluetooth

ERNW
providing security.

“Bus” vs “LAN”

- Systems with only bus-like connectivity need a gateway
  - Common example: Temperature sensors in production system used to predict maintenance
    - Queried via ZigBee
    - Data pushed into analytics cloud by gateway
- Security issues come into play when sensors are to be made widely exposed.

Network Isolation

- Most industrial systems not designed for operation in an untrusted environment are now connected to several other network systems
  - Violating the PERA model
- Operation systems used on shop floor are often EOL and cannot be replaced by current secure operating systems because of compatibility
- ICS often do not have the capability for (strong) authentication and authorization
- ICS systems are designed for safety and availability – Appling IT Security measures may break them

- => Network-level controls often only viable approach

ERNW
providing security.

Approaches

- Integrate shop floor networks into overall zoning model
  - Including classification
- Same firewall management processes/tools
- Enforce intermediate/gateway systems
- Monitoring

ERNW
providing security.

Particular Focus: SMB

- Various industrial malware families use SMB for lateral movement/infections.
- SMB must be in focus of overall network filtering design.

ERNW
providing security.

“But our shop floor network is isolated”

- Rarely fully the case:
  - Maintenance access
    - Unpatched service laptops
    - Remote access/network connections
  - Multi-million EUR/USD manufacturing systems as phone chargers
  - Updates via USB drives

ERNW
providing security.

Case Study

- 12 factory sites
- Maintenance via service laptops
- Different production system families
- Single-point-of-failure production systems
- Distribution of files/updates via USB drives or SMB

ERNW
providing security.

Case Study

- Introduction of MES triggered network changes
- Changes to be used to analyze security posture
- Most relevant threats:
  - Malware

ERNW
providing security.

Case Study

- Evaluation of security benefit of network segmentation of
  - Factories
  - Production system families
  - SPOF production systems
  - Arbitrary combinations of those
- Operational feasibility:
  - Number of network segments ranging from 1 to 276
- Micro segmentation was evaluated as well

ERNW
providing security.

Security Benefit?

- Segmentation of Factories:
  - Containment to one site
- Production system families:
  - No real security benefit, ensuring that malware can reach all vulnerable systems
- SPOF production systems:
  - Isolation between regular and SPOF systems, ensuring minimal viable operation

ERNW
providing security.

Solution

- Zoning factories and SPOF systems
- Central file exchange hubs
  - Reducing need for USB
  - Clear filtering model, incoming network traffic for hubs, nowhere else
    - Containment!
- Establishment of contractual controls for service providers/maintenance
- Introduction of AV terminals

ERNW
providing security.

Applicability?

- Target environment heavily SMB-based
- Similar communication structures exist for OPC-UA/MQ-TT as well and can be used to develop network zoning models

ERNW
providing security.

Update and Vulnerability Management

Advisory (ICSA-18-107-03)

Rockwell Automation Stratix Services Router

CVSS v3 9.8

- **ATTENTION**: Exploitable remotely/low skill level to exploit.
- **Vendor**: Rockwell Automation
- **Equipment**: Allen-Bradley Stratix 5900 Services Router
- **Vulnerabilities**: Improper Input Validation, Improper Restriction of Operations within the Bounds of a Memory Buffer, Use of Externally-Controlled Format String.

Advisory (ICSA-18-088-02)

Siemens TIM 1531 IRC

CVSS v3 9.8

ATTENTION: Exploitable remotely/low skill level to exploit.

Vulnerability: Missing Authentication for Critical Function

Advisory (ICSA-13-084-01)

Siemens CP 1604 and CP 1616 Improper Access Control

Advisory (ICSA-12-102-04)

Siemens Scalance X Buffer Overflow Vulnerability

Original release date: April 11, 2012 | Last revised: May 08, 2013

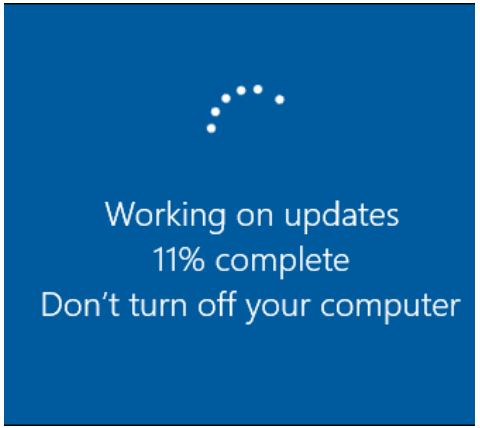
Print Tweet Send Share

ERNW
providing security.

Challenges of Patching

- Reliability requirements resulting in extensive testing
- No over-the-air update capabilities guaranteed
  - Read: Internet connectivity ;-)

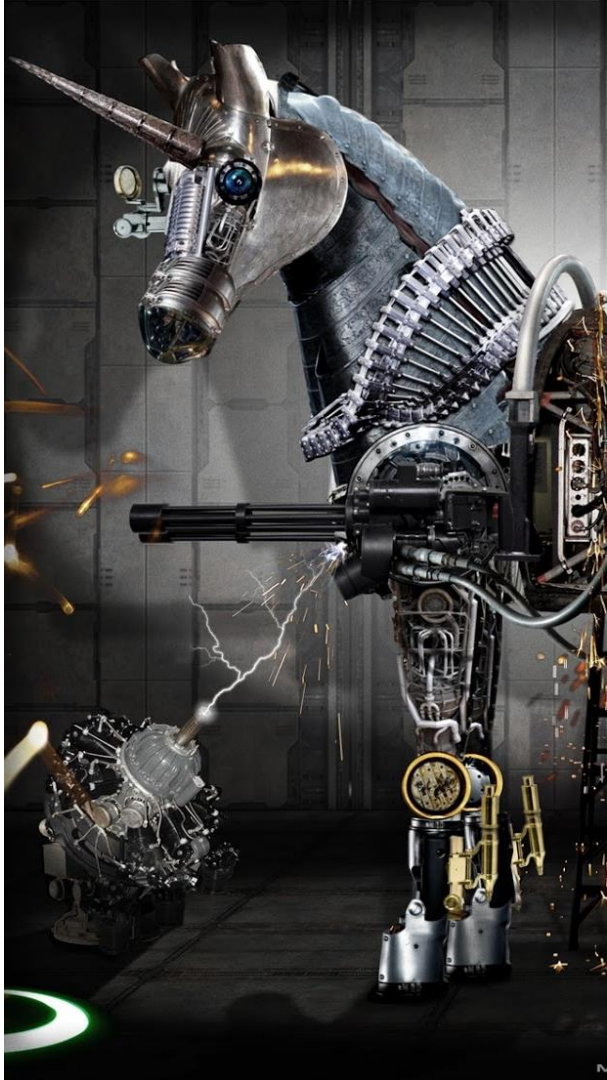
- Important Effort: FDA striving to make modern update capabilities mandatory!



ERNW
providing security.

Agile Fairy Dust & Industrial

- Merging DevOps & Embedded/Industrial
  - Proposing ShopDevOps? ;-)
- Current trend:
  - Software delivery via containers also in industrial/embedded environments



ERNW
providing security.

Container Benefits

- Room for another one day workshop and discussion.
- Benefits:
  - Development environment == production environment
  - Ecosystem focused on software delivery
    - Thus update delivery
  - Added process isolation and control
    - Avoiding side-effects/cohesion

ERNW
providing security.

Container & Embedded

- Performance: Should be feasible for >= panel PC
- Sample Memory footprint, x86_64:
  - Docker 1.13: 390MB
  - Overhead per container: 5MB
- Dedicated projects with embedded scope available:
  - resin OS
  - SkiffOS
  - HypriotOS

ERNW
providing security.

Shop Floor System Evolution

- Case Study
- Six to seven digit EUR/USD production system
- Multiple systems involved
- Central industrial PC for operation

ERNW
providing security.

2008

- Windows XP embedded
- Default accounts, usernames == passwords
- No Windows patching
- Apache versions with RCE vulnerabilities
- Remote maintenance:
  - IPsec connection to target network required

ERNW
providing security.

2009

- Windows XP embedded
- Standard remote attack surface minimized
  - Removal of features, deactivation of services
  - Use of local firewall
  - Patch process
- Complex (yet fixed) passwords
- Additional hardware firewall on demand
- But now:
  - .net Remoting
  - IPC$ jumped back into availability
- Remote maintenance:
  - IPsec connection to target network required

ERNW
providing security.

2013

- Windows XP embedded
- Remote attack surface minimal
- Local attack surface wide open
  - Hardcoded credentials
  - Binary planting in home-grown update services + various other proprietary services

ERNW
providing security.

2014

- New remote maintenance solution
- Support case:
  - Triggered by help desk
  - Deployment of clean baseline maintenance VM
  - Connection of VM to incoming (i.e. triggered by end customer) IPsec tunnel
- Only vulnerability:
  - SSH MitM

ERNW
providing security.

2014

- Upgrade of Industrial PC to Windows 7
- Continuous test bed with regard to new malware samples
- Kiosk breakout required USB HID descriptor fuzzing
- Upcoming deployment of a custom Windows Shell

ERNW
providing security.

2017

- Custom Windows Shell in place
- Current working step:
  - Update management and increased isolation leveraging Windows containers

ERNW
providing security.

Physical Security

- Authentication
  - For maintenance access?
    - See case study
  - For daily operation?
- USB
  - Again, production systems used as phone chargers
  - Use of “dirty” USB media

ERNW
providing security.

Establishing Trust

- Bold opening statement:
  - Machine certificates and trust stores incl. lifecycle infrastructure should be one of the first discussions of every product development/shop floor projects
- Strong requirements for:
  - Signature verification
  - Establishment of trusted communication channels

ERNW
providing security.

Case Study Data Hub

- Data Hub development project
- Industrial server to aggregate data for various systems/sensors
- Linux-based
- Custom, light-weight web services for communication
- To be deployed in fully unknown network infrastructure
- Lifecycle via APT repository
- Only requirement: Internet-uplink

ERNW
providing security.

Challenges

- Maintenance access
- AAA backend infrastructure
- Establishing communication with client devices
  - Discovery out of scope

ERNW
providing security.

Establishing Communication Channels

- No DNS entries
- No known IP ranges
- Off-channel verification not operationally feasible.
- Deployment of machine certificates from newly established CA.

- Implementation of custom “pinning” upon first connection.

ERNW
providing security.

Maintenance Access

- Backend service is pulled on a regular basis
- Job to enable maintenance access stored in backend
  - Including a one-time password
  - Which can then be checked out by service technician
  - Optional approval in hub web interface
  - For offline systems: Check out RFC4226
- Remote maintenance comparable, using reverse SSH tunnels to SSH non-interactive jump host

ERNW
providing security.

Vendor Trust

- Make security requirements mandatory in RFP phases
- Request extensive proof of security quality assurance from vendors
  - One-page “We do security best practices” is not enough
  - Pentest results can be shared, if everything is performed properly
  - They don’t need to be confidential.
    - And even if so, you’re running strictly confidential or highly critical operations on the products, right?

ERNW
providing security.

Summary

- Network zoning/filtering model essential
- Leverage modern AAA approaches
- Push for strong software lifecycles
- Challenges vendors for security transparency

ERNW
providing security.

Thank You For Your Attention!

Discussion!

mluft@ernw.de
skiese@ernw.de

@uchi_mata
@net0Ski

www.ernw.de

www.insinuator.net