Securing Communications for SCADA and Critical Industrial Systems

Tom Bartman and Kevin Carson
Schweitzer Engineering Laboratories, Inc.

Summary

- Communications as popular target
- More sophisticated criminals
- Threat vectors
- Mitigation
- New technology

SCADA and ICSs

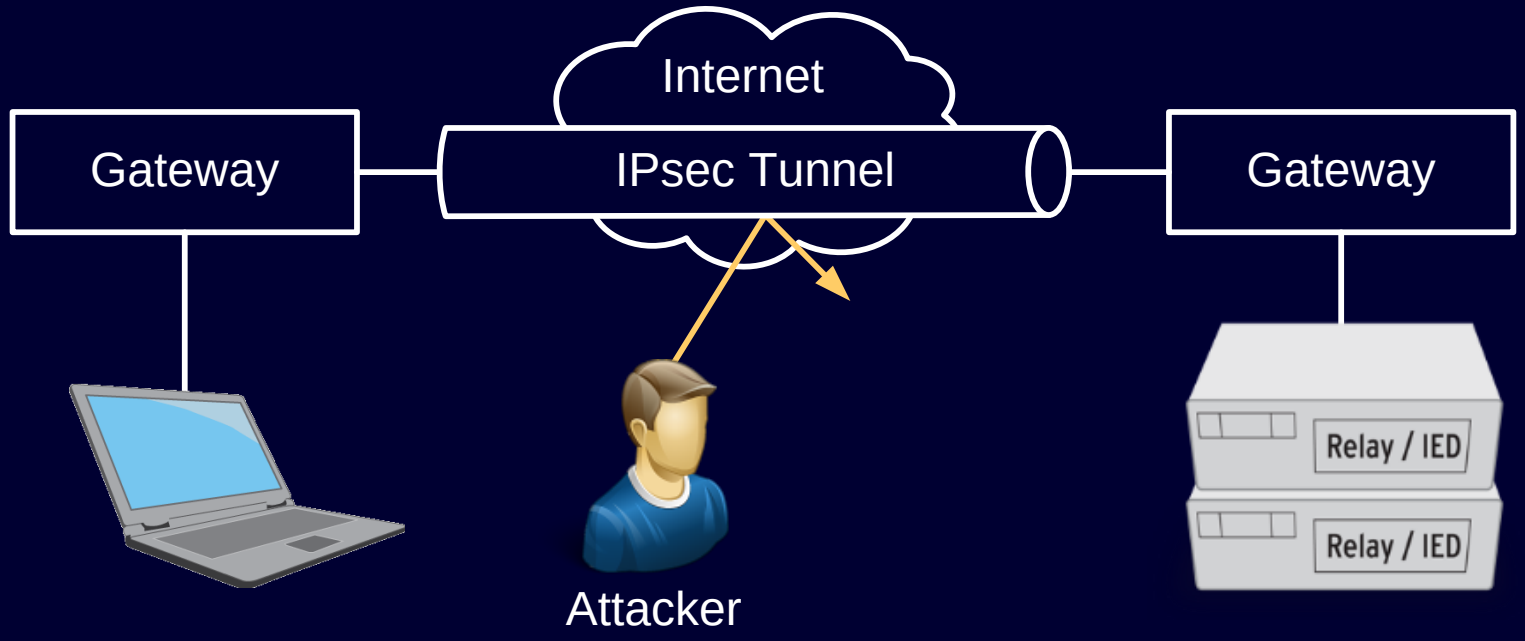
- SCADA and ICS communications are used to move electric power, gas, oil, water, petrochemicals, and transportation
- Protocols are in use today that rarely use authentication
- Energy sector is popular avenue for attacks

Threat Vectors

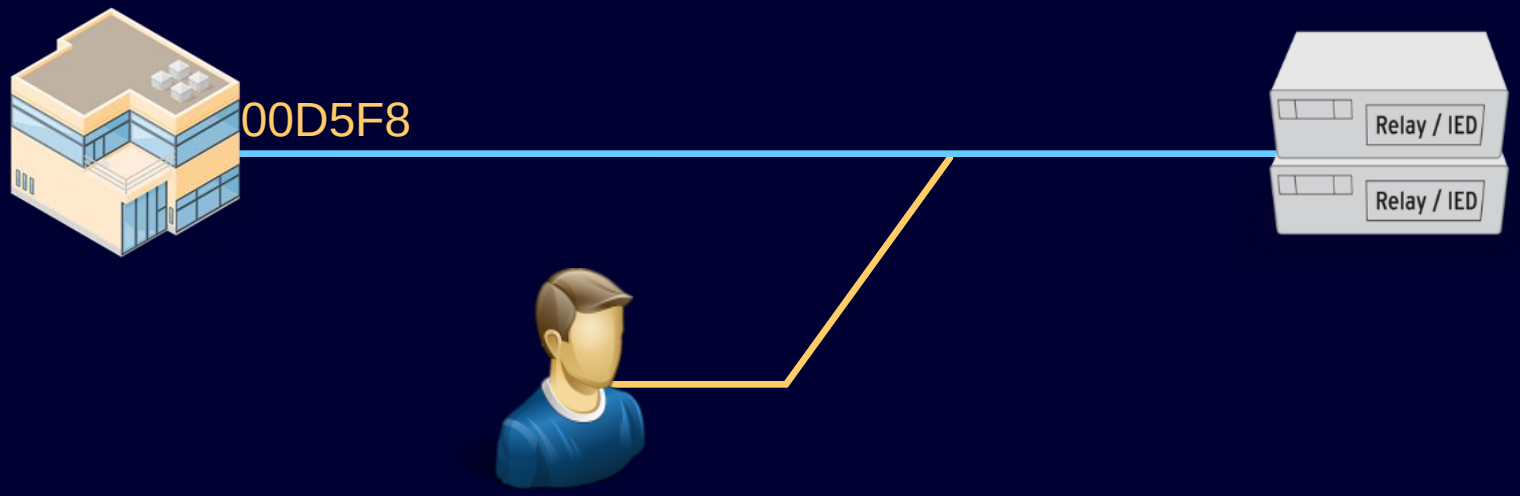
- Replay attacks
- Man-in-the-middle attacks
- Brute force attacks
- Dictionary attacks
- Denial of service (DoS) attacks
- War dialing
- Default passwords
- Data modification

Securing Internet Protocol

- IPsec
- Encryption and authentication
- Logging

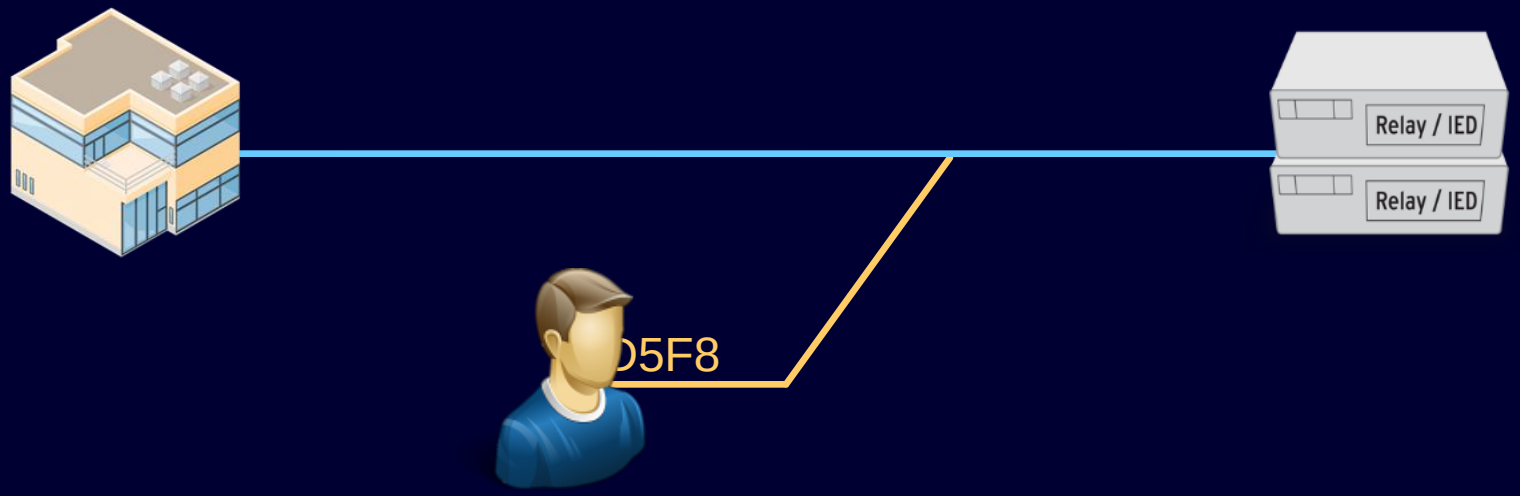


Replay Attack With Encryption



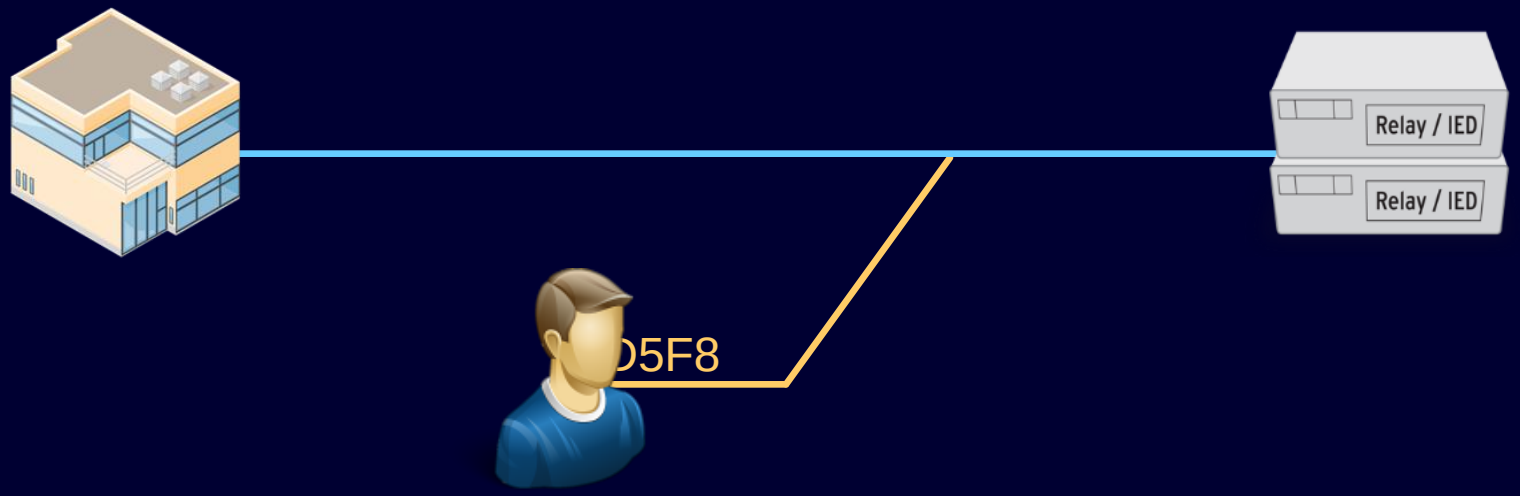
Attacker is able to see encrypted command

Successful Replay Without Authentication



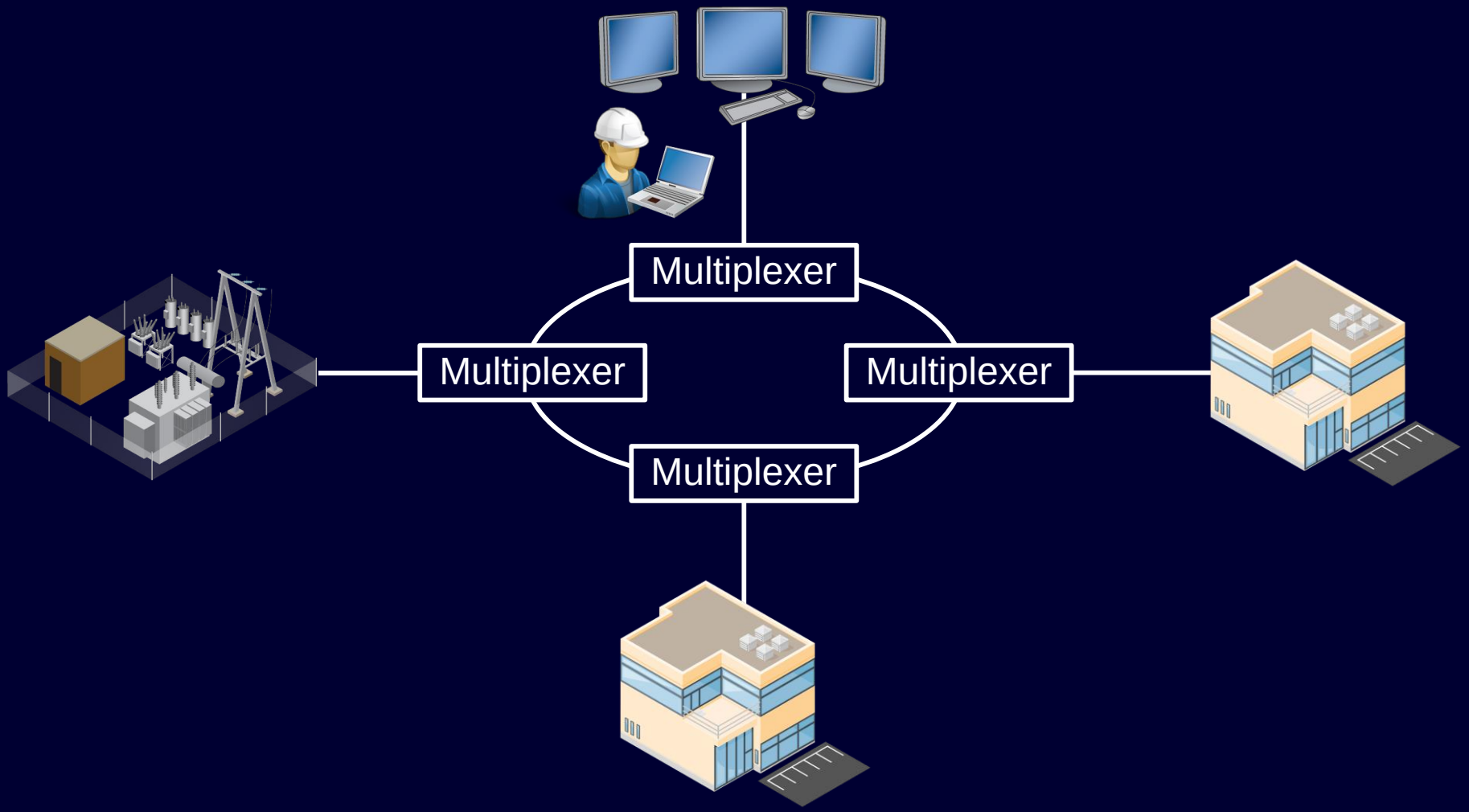
Attacker replays command

Unsuccessful Replay With Authentication

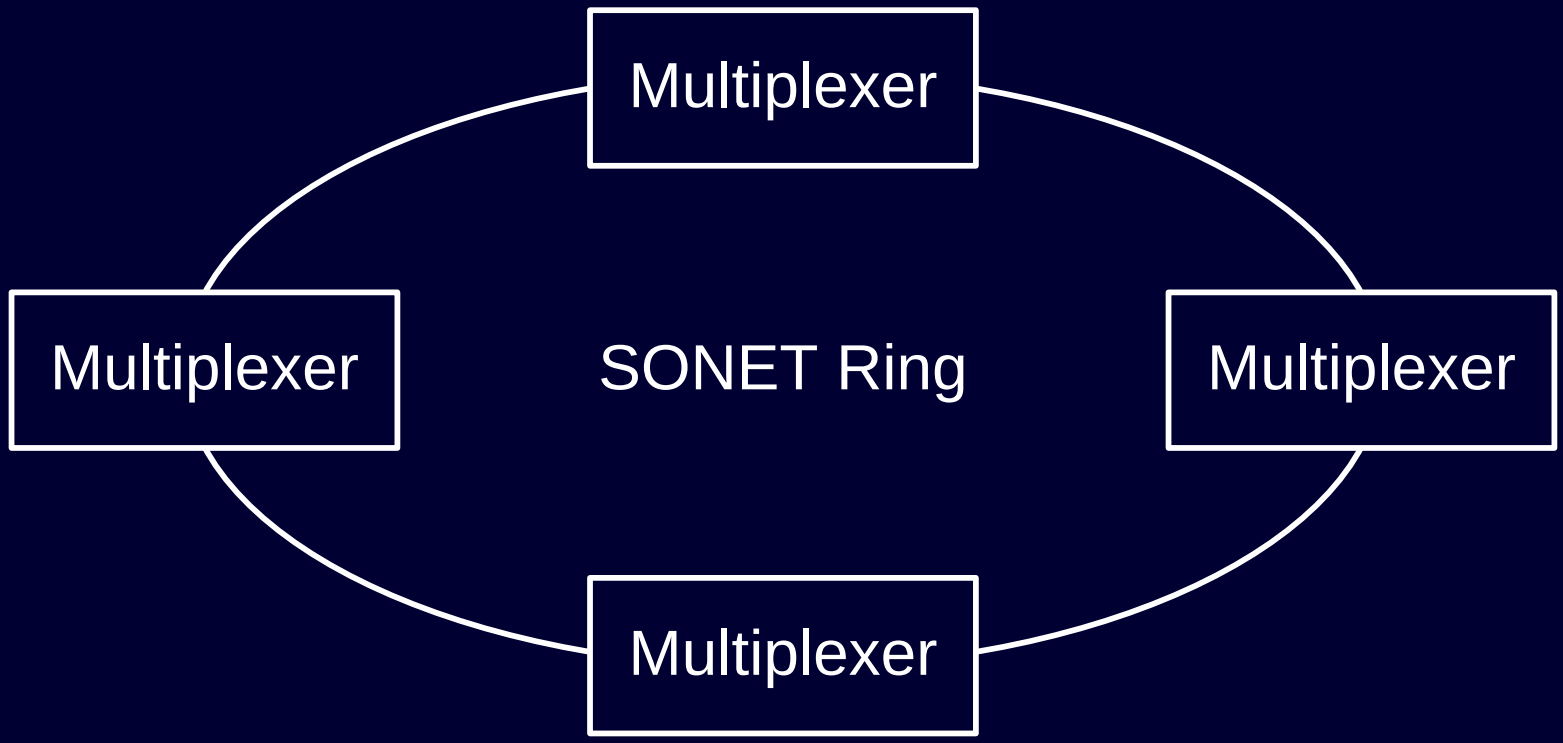


Attacker replay command is rejected

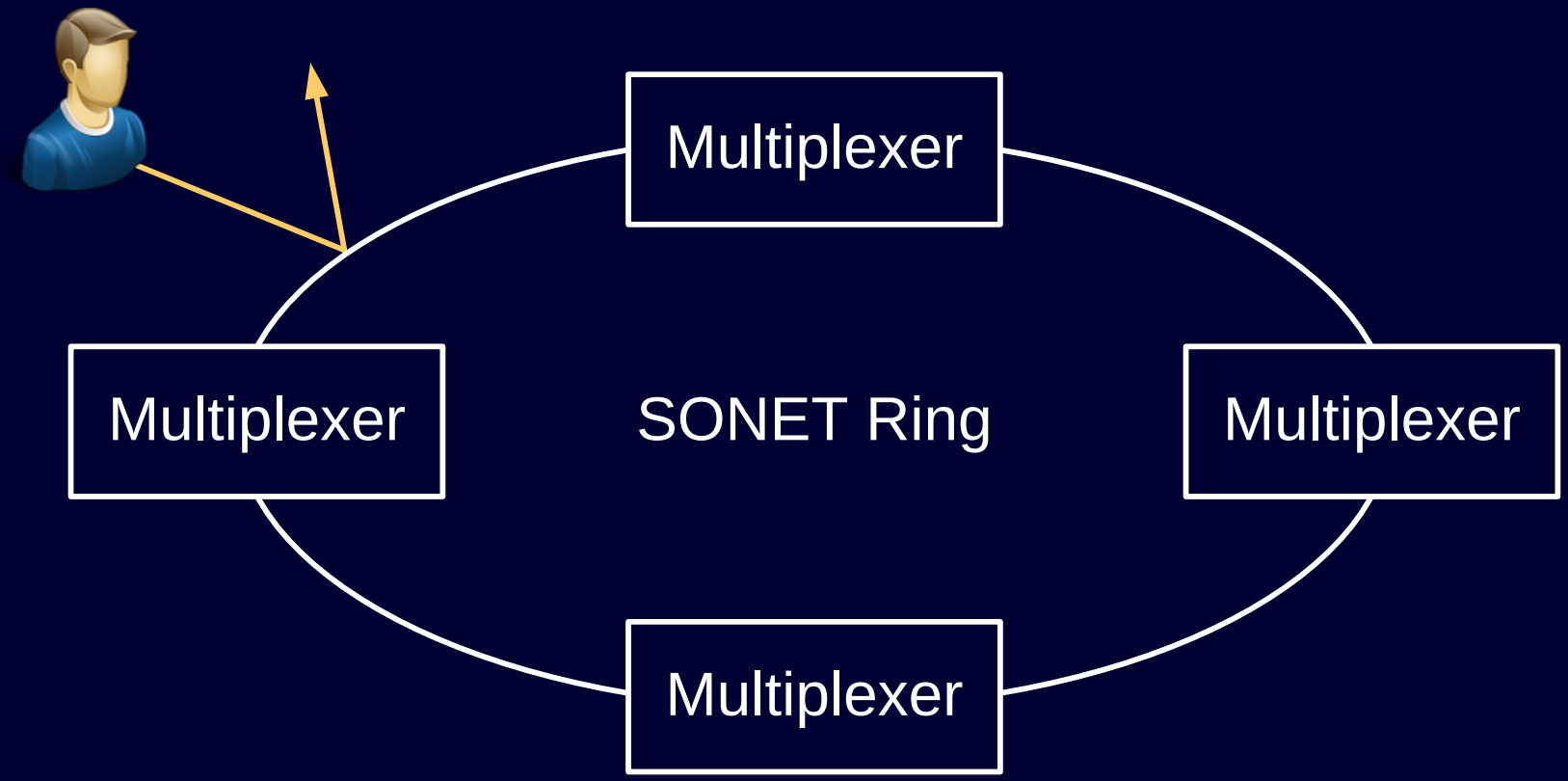
SONET Communications Network



Encrypt WAN Connections



Encrypted WAN Connections Stop Interception



Ethernet Communications

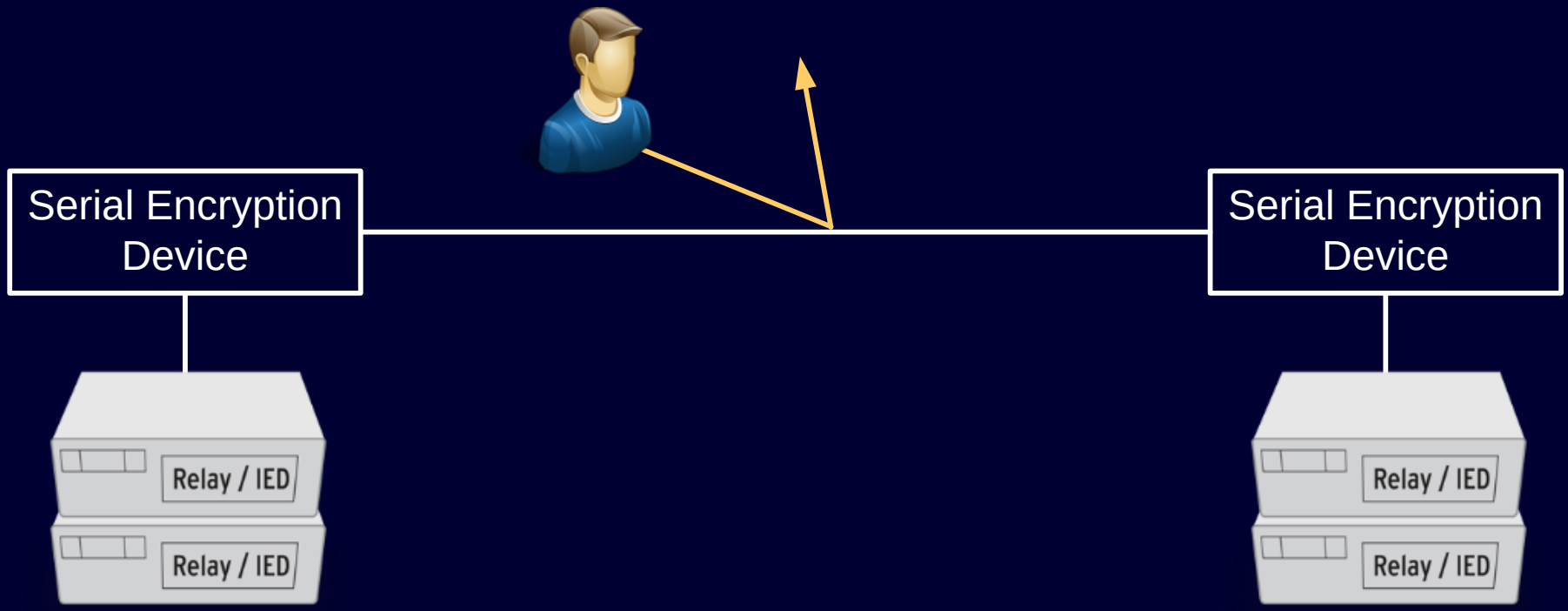
- Replay attack prevention via encryption and authentication
- MAC address count lock
- MAC address time lock (capture endpoints during commissioning)
- Tamper detection using link status in new technology

Wireless Communications

- Bluetooth® keeps cabinet doors closed
- New radio transceivers support encryption and authentication

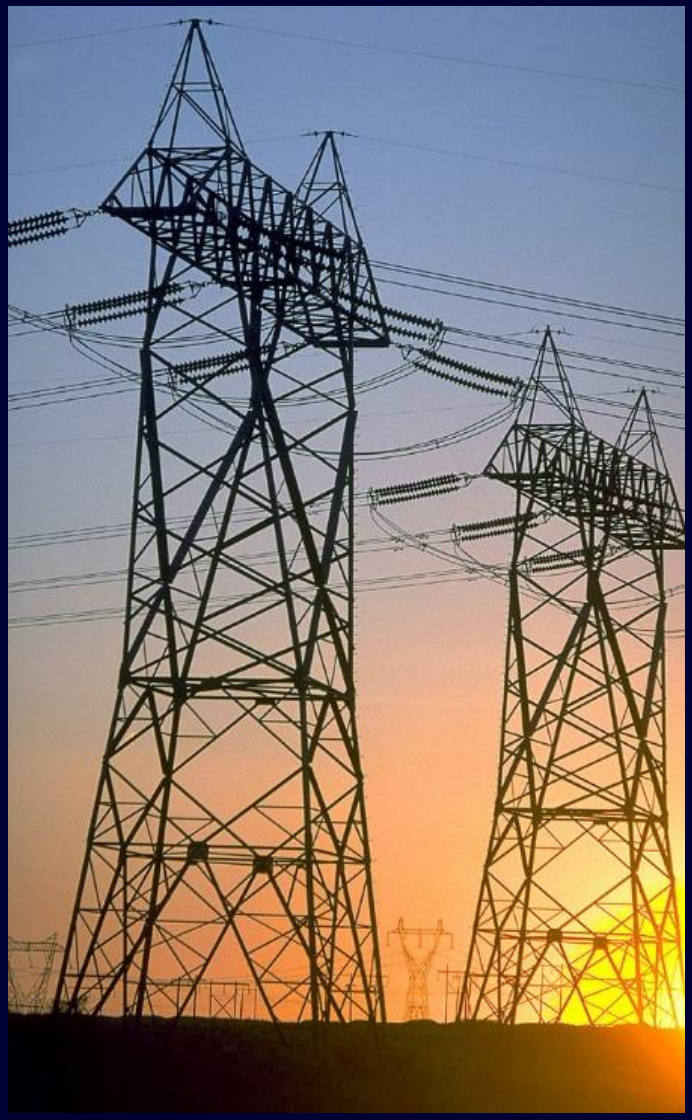
Serial Communications

- Serial communications are still widely used
- Serial encryption devices provide secure wrapper

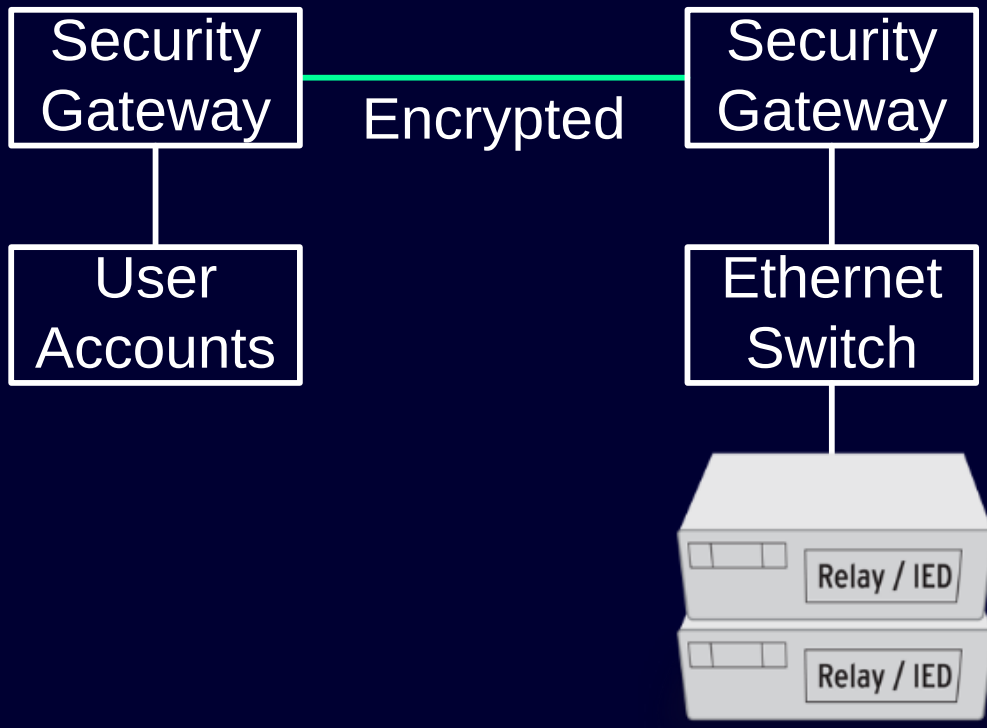


Precise Time

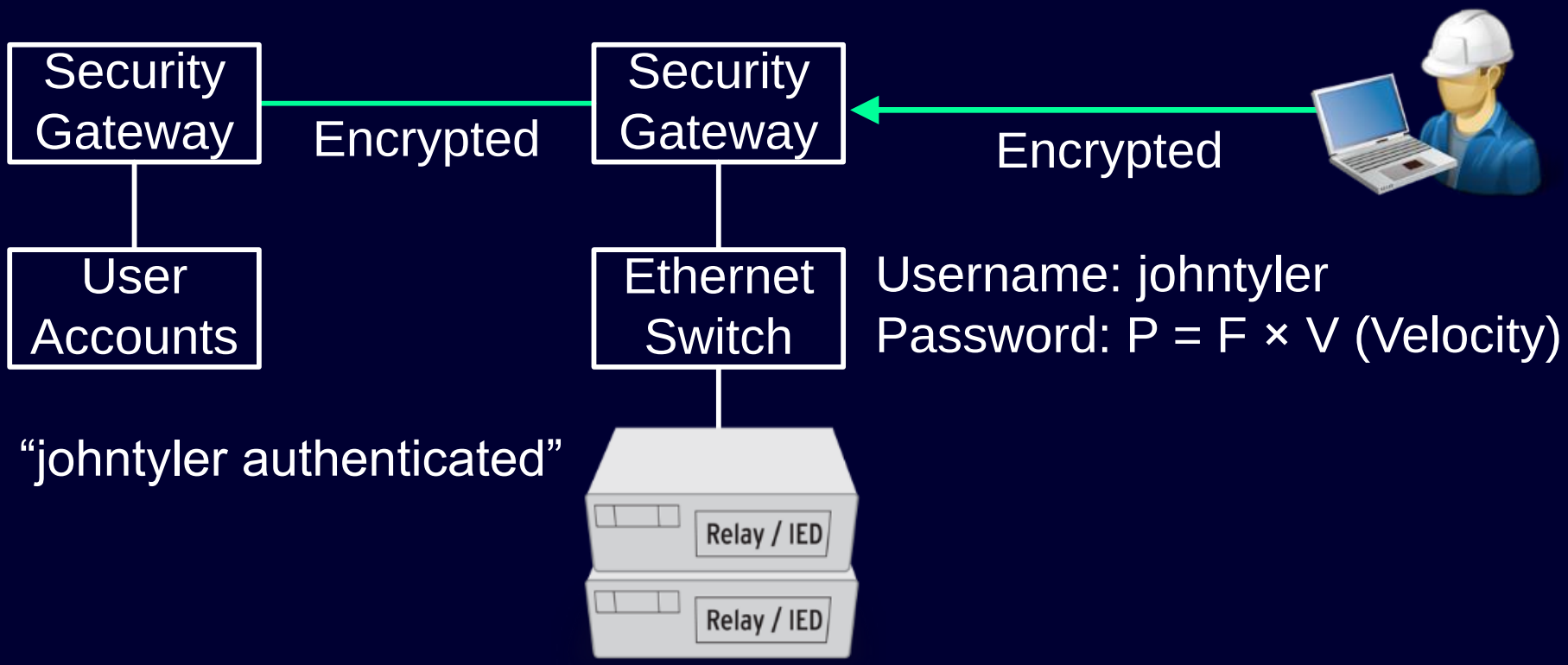
- Critical component in power systems
- Precision time and date-stamped logging
- Distribution over SONET networks



Password Management



Password Management



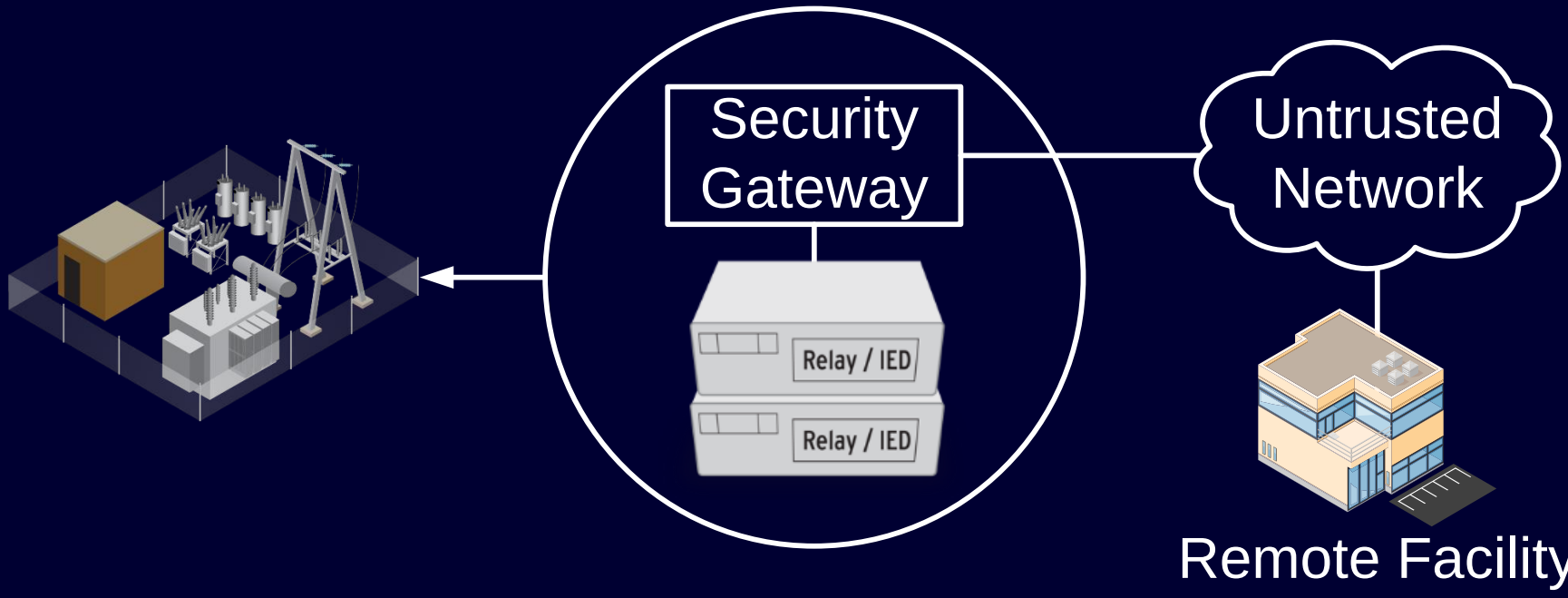
Backdoor Passwords and Maintenance Accounts

- Cause significant threat exposure
- Are used for equipment access

Insist that your devices have no such mechanisms in place!

Engineering Access

- Utility engineer – engineering access is biggest risk
- Endpoints must be firewalled

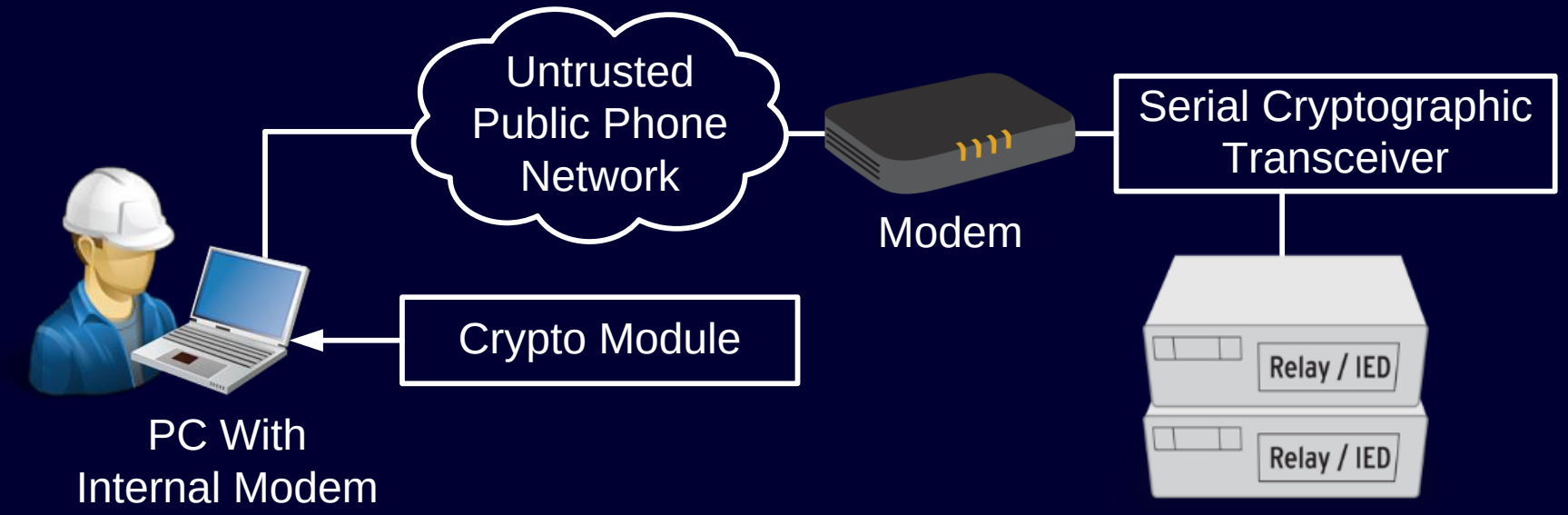


Dial-Up Modems Still Widely Used

- Disconnect when not in use
- Whitelist inbound numbers
- Use modem call-back feature

Secure Dial-Up Engineering Access

- Secure dial-up access protects serial communications
- Field engineers are given unique cryptographic identities



Whitelist Technology

- Was developed by U.S. Department of Energy and several partners
- Is based on whitelist malware protection
- Monitors system services
- Mitigates malware, rootkits, and zero-day exploits
- Eliminates frequent antivirus signature patches

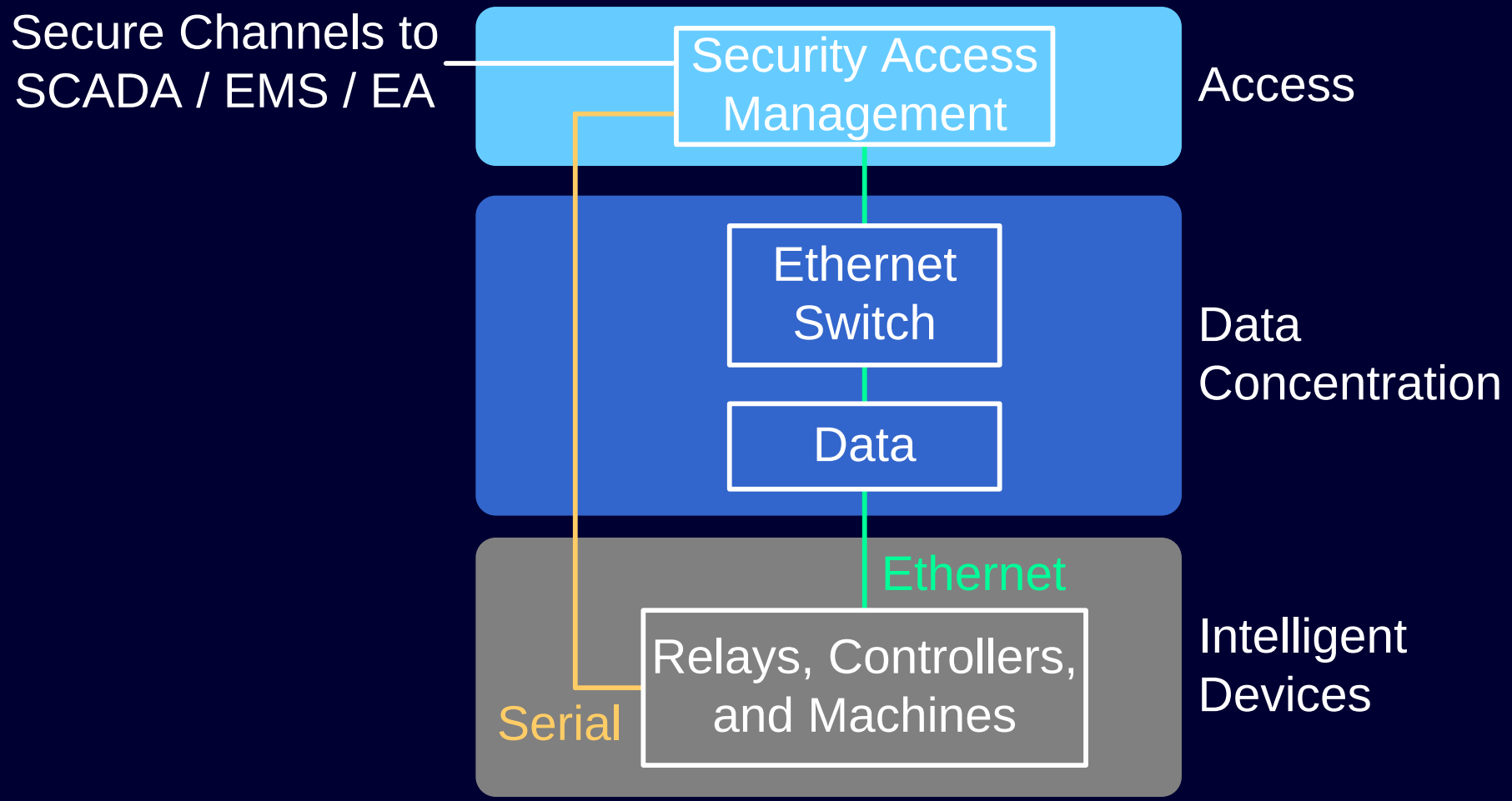
Tamper Detection

- New technology detects break-in or tampering
- Sensors detect movement, light levels, and binary sensors

Tamper Detection

- Optical sensor or binary input detects door opening
- Accelerometer detects jolt or movement
- Tilt sensor detects someone physically handling device
- Combination of sensors reduces false alarms
- Alarms are sent out-of-band

Establish Zones of Protection



New Generation of Computers

- MTBF many times that of typical industrial computers
- SCADA, automation, data concentration, monitoring, and control

New Generation of Computers

- No moving parts (spinning drives, fans)
- Error-correcting memory
- Harsh environments
- Operation when exposed to ESD, vibration, shocks, bumps, EMI fields, and RF interference
- Wide range of applications (LDAP, automation, network intrusion detection)

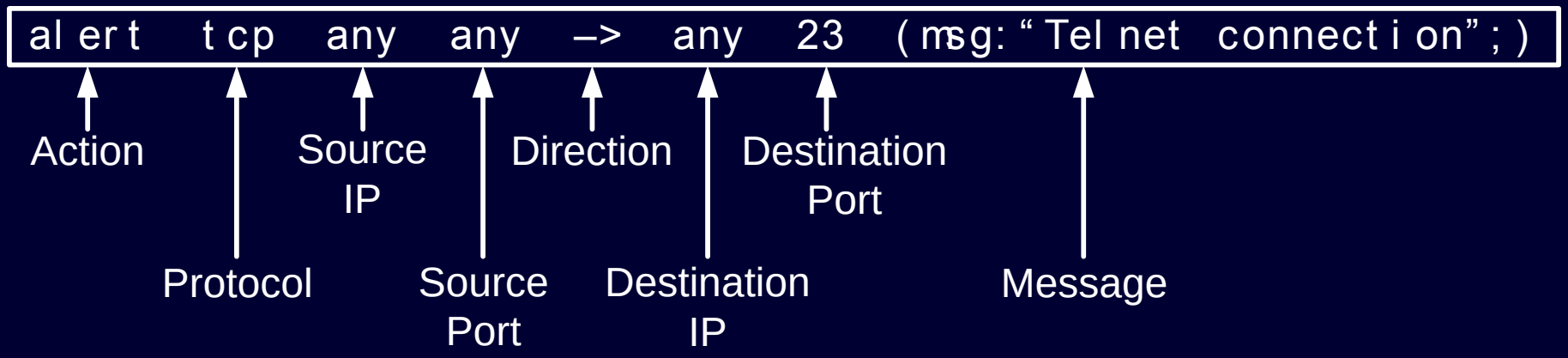
Network Intrusion Detection

- Reliable option with new rugged computers
- Important piece in security framework
- Detection of network breach provided

Network Intrusion Detection

- Monitors inbound and outbound traffic
- Records access attempts, port scans, probes, buffer overflow attempts, and more
- Provides deep packet inspection and rule-based alerts

Rule Determines How to Inspect Each Packet

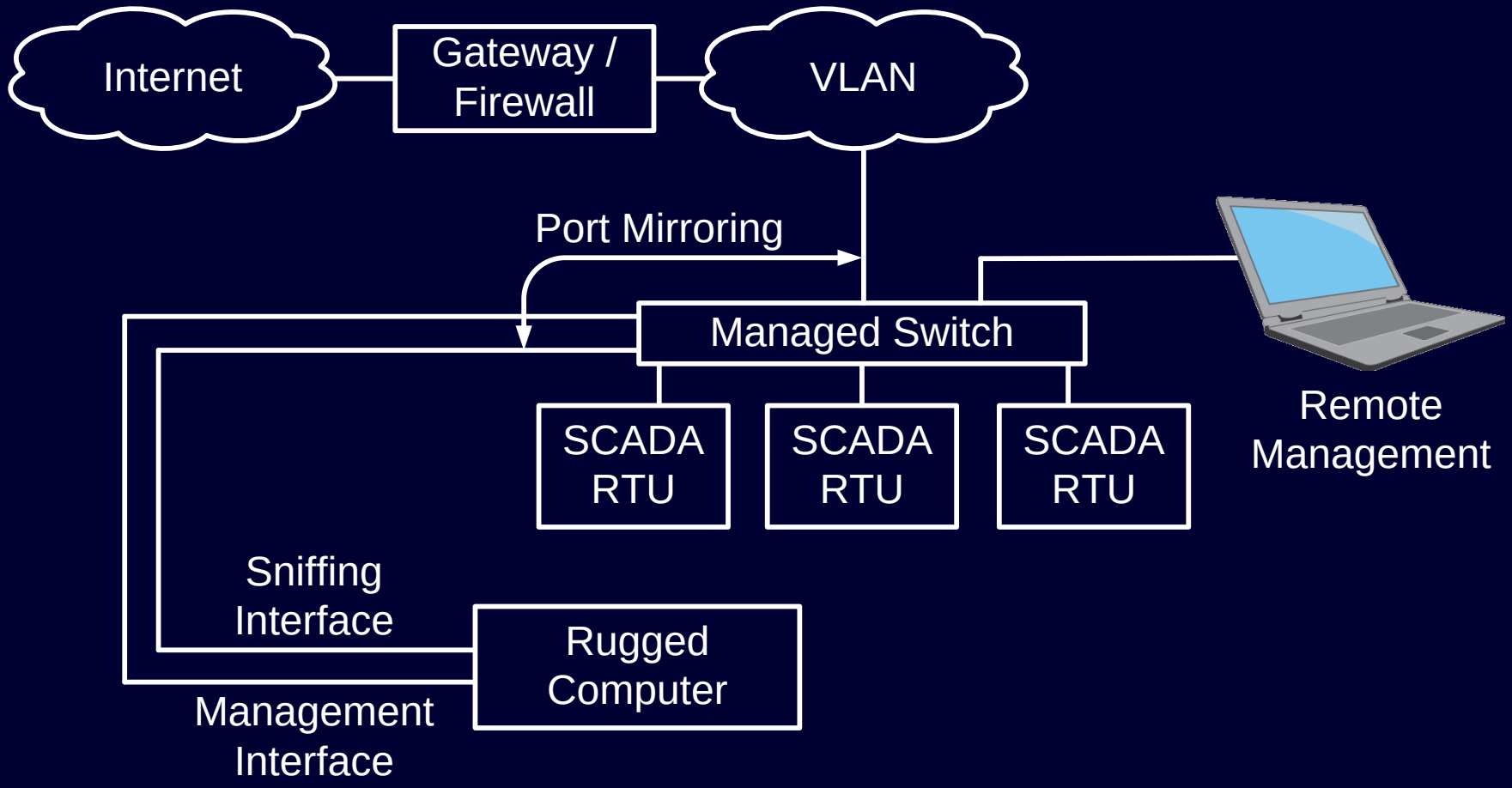


Network Intrusion Detection

- Detects traffic from within (i.e., between devices)
- Example – Modbus® TCP buffer overflow

```
alert tcp $MODBUS_Client any -> $MODBUS_Server 502 \
dsize:>300; msg:"Illegal Modbus TCP Packet Size";)
```

Network Intrusion Detection



Best Practices

- Know your system endpoints
- Have USB flash drive policy
- Review logs periodically
- Lock down engineering access
- Consider insider threats (access rights)
- Keep device firmware up to date

Conclusion

- Communications require end-to-end authentication to be secure
- Compensating controls are available for legacy protocols
- Layered security should be established
- Many new technologies are available

Questions?