OT Attack Vectors

Common attack paths targeting industrial control systems

OT Security Learning Series

Document 420 | January 2026

Contributors: Matthias Niedermaier

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction **3**

2 Network-Based Vectors **3**
2.1 IT/OT Boundary Attacks . . . 3
2.2 Protocol Exploitation . . . 4
2.3 Man-in-the-Middle Attacks . . . 4

3 Remote Access Vectors **4**

4 Physical Vectors **4**
4.1 Direct Physical Access . . . 4
4.2 Removable Media Risks . . . 5

5 Supply Chain Vectors **5**
5.1 Vendor Access Risks . . . 5

6 Human Vectors **5**
6.1 Social Engineering . . . 6
6.2 Insider Threats . . . 6

7 Wireless Vectors **6**

8 Attack Chain Example **6**

9 Defensive Priorities **7**

10 Summary **7**

11 Further Reading **7**

1 Introduction

Information

Attack vectors are the paths or methods attackers use to gain access to OT systems. Understanding these vectors is essential for implementing effective defenses. OT environments face both IT-style attacks and OT-specific threats targeting industrial protocols and processes.

Attack vector categories:

- **Network-based** – Exploiting network connectivity
- **Physical** – Direct access to equipment
- **Supply chain** – Compromised vendors or components
- **Human** – Social engineering and insider threats
- **Wireless** – Exploiting RF communications

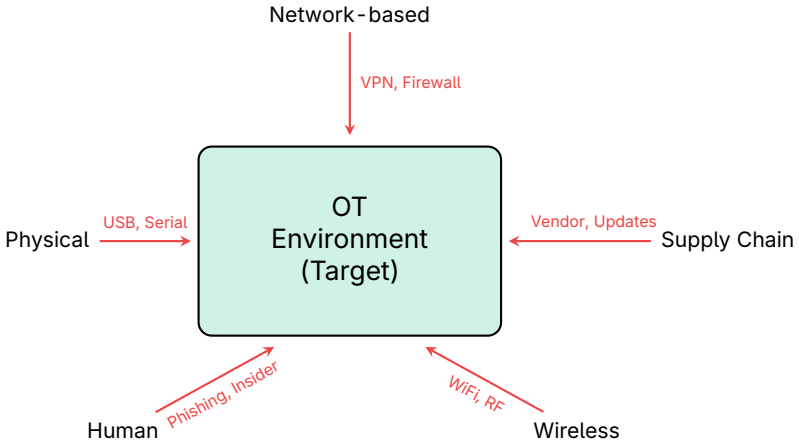

Figure 1: Attack Vectors Targeting OT Environments

2 Network-Based Vectors

2.1 IT/OT Boundary Attacks

Vector	Description
Firewall misconfiguration	Overly permissive rules allowing lateral movement
VPN compromise	Stolen credentials or vulnerabilities in VPN
Jump server exploitation	Compromising shared administration points
Historian pivoting	Using data historians as bridge to control networks
DMZ bypass	Exploiting poorly segmented DMZ architecture

Table 1: IT/OT Boundary Attack Vectors

2.2 Protocol Exploitation

Critical

Industrial protocols lack authentication:

- Modbus – No authentication, commands accepted from any source
- DNP3 – Optional security features rarely enabled
- EtherNet/IP – CIP protocol has limited security
- S7comm – Legacy protocol with weak authentication
- OPC Classic – DCOM-based with known vulnerabilities

2.3 Man-in-the-Middle Attacks

- ARP spoofing to intercept OT traffic
- Modifying commands between HMI and PLCs
- Injecting false data into historian
- Intercepting engineering uploads/downloads

3 Remote Access Vectors

Vector	Attack Method	Risk
VPN credentials	Phishing, credential stuffing	HIGH
RDP exposure	Brute force, BlueKeep exploits	CRITICAL
Vendor backdoors	Default/hardcoded credentials	HIGH
TeamViewer/AnyDesk	Compromised remote tools	HIGH
Cellular modems	Exposed management interfaces	MEDIUM

Table 2: Remote Access Attack Vectors

Warning

Remote access is one of the most exploited vectors in OT attacks. The Ukraine power grid attacks (2015/2016) used stolen VPN credentials to gain initial access.

4 Physical Vectors

4.1 Direct Physical Access

- **USB devices** – Malware delivery (Stuxnet spread via USB)
- **Serial ports** – Direct connection to PLCs/RTUs
- **Network jacks** – Connecting rogue devices

- **Exposed equipment** – Substations, pump stations
- **Maintenance laptops** – Infected contractor equipment

4.2 Removable Media Risks

Media Type	Risk Scenario
USB flash drives	Malware autorun, BadUSB attacks
External hard drives	Infected backup restoration
SD cards	Compromised firmware updates
CDs/DVDs	Legacy systems without USB

Table 3: Removable Media Attack Vectors

5 Supply Chain Vectors

Critical

Supply chain compromises are difficult to detect:

- Trojanized software updates (SolarWinds-style)
- Compromised firmware from manufacturer
- Malicious code in third-party libraries
- Counterfeit hardware with backdoors
- Compromised vendor remote access

5.1 Vendor Access Risks

- Persistent vendor VPN connections
- Shared credentials among vendor staff
- Unmonitored maintenance sessions
- Vendor laptops connecting to OT networks
- Cloud-based vendor management platforms

6 Human Vectors

6.1 Social Engineering

Technique	OT-Specific Example
Phishing	Fake vendor security bulletin with malicious link
Spear phishing	Targeting control engineers with project files
Pretexting	Impersonating vendor support for credentials
Baiting	Dropping infected USB near control room
Tailgating	Following authorized person into secure area

Table 4: Social Engineering Techniques

6.2 Insider Threats

- Disgruntled employees with system access
- Contractors with excessive privileges
- Unintentional errors by operators
- Knowledge transfer during layoffs
- Credential sharing among staff

7 Wireless Vectors

Vector	Description
Rogue access points	Unauthorized WiFi bridging IT and OT
WiFi attacks	WPA2 cracking, evil twin APs
Bluetooth	Exploiting industrial Bluetooth devices
Cellular/LTE	Attacking exposed cellular modems
RF protocols	ZigBee, LoRa, WirelessHART vulnerabilities
Radio jamming	Disrupting wireless control communications

Table 5: Wireless Attack Vectors

8 Attack Chain Example

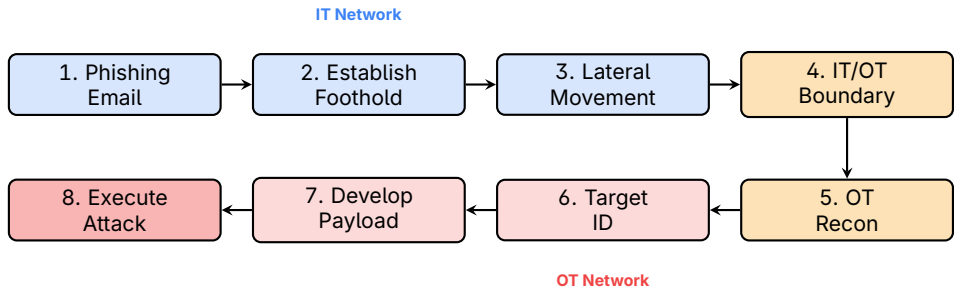

Figure 2: Typical OT Attack Chain Progression

Key Point

Typical OT attack progression:

1. **Initial Access** – Phishing email to corporate user
2. **Establish Foothold** – Malware on IT workstation
3. **Lateral Movement** – Pivot through IT network
4. **IT/OT Boundary** – Exploit jump server or historian
5. **OT Reconnaissance** – Map industrial network
6. **Target Identification** – Find critical controllers
7. **Develop Capability** – Create OT-specific payload
8. **Execute Attack** – Manipulate physical process

9 Defensive Priorities

Attack Vector	Primary Defense
Remote access	MFA, jump servers, session monitoring
Network-based	Segmentation, firewalls, IDS
Protocol attacks	Network monitoring, protocol validation
Physical access	Access controls, USB restrictions
Supply chain	Vendor management, integrity verification
Social engineering	Security awareness training
Wireless	WPA3-Enterprise, WIDS, RF monitoring

Table 6: Defenses by Attack Vector

10 Summary

Key Takeaways

- **Remote access** – Most commonly exploited initial vector
- **Protocol weakness** – Industrial protocols lack authentication
- **Physical access** – USB and direct connections remain threats
- **Supply chain** – Trusted vendors can be attack paths
- **Defense in depth** – No single control stops all vectors
- **Monitor boundaries** – IT/OT interface is critical chokepoint

11 Further Reading

Resources

- **MITRE ATT&CK for ICS**
  https://attack.mitre.org/techniques/ics/
- **CISA – ICS Attack Vectors**
  https://www.cisa.gov/topics/industrial-control-systems
- **NIST SP 800-82** – Guide to ICS Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

Part of the OT Security Learning Series