Minimizing Attack Surfaces in IT/OT Environments

Viktor Szulcsányi

Doctoral School on Safety and Security Sciences, Óbuda University

Presentation Agenda

- Introduction: Why This Matters

- IT vs. OT Differences

- Case Studies

- Attack Surface Identification Methods

- Mitigation Strategies

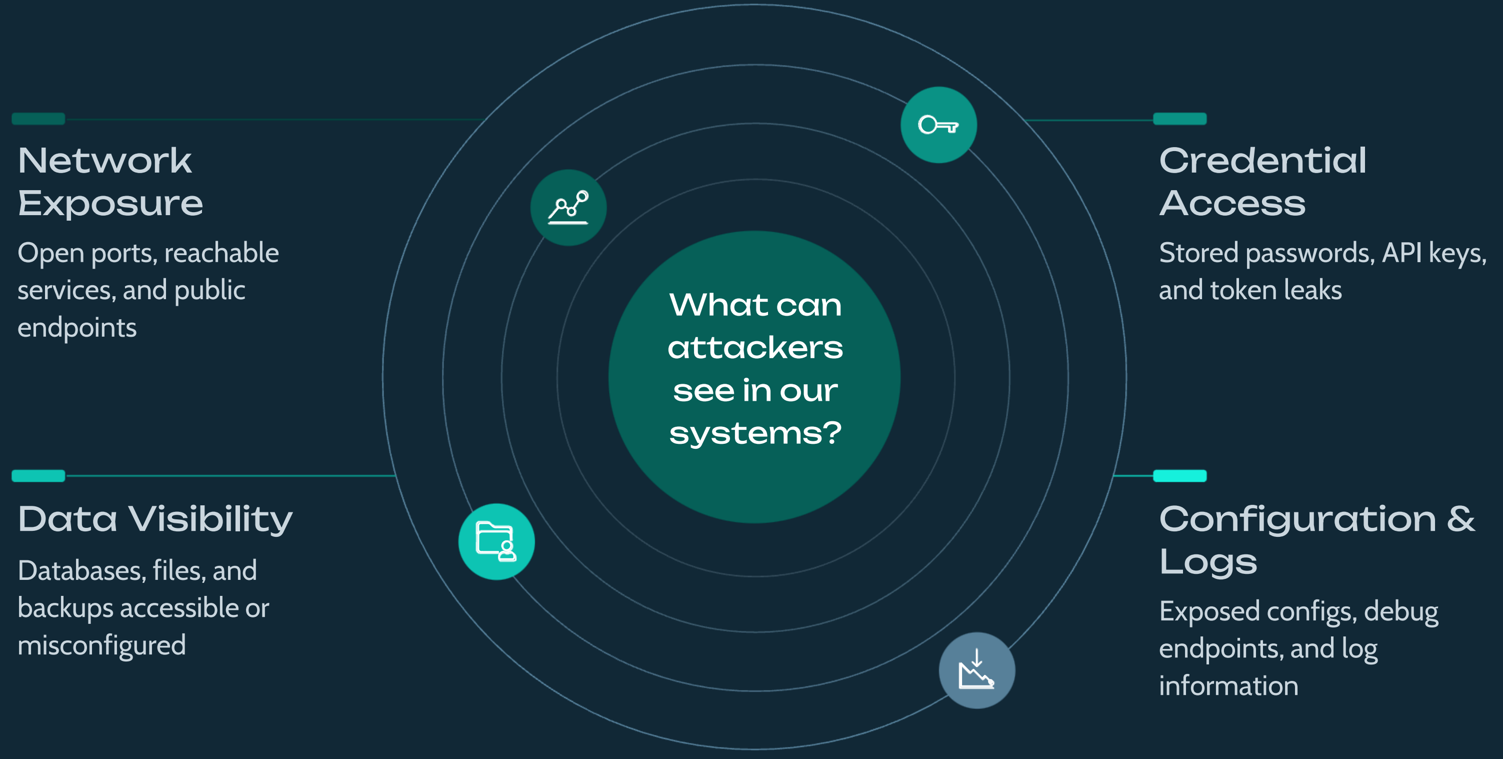
- Conclusion

Why This Matters in 2025

The Challenge

Digital transformation has dramatically expanded the attack surface across both IT and OT systems. In 2024, attacks targeting operational technology with physical consequences reached record levels across energy, water utilities, and manufacturing sectors.

Central question: "What can attackers see in our systems?"



What can attackers see in our systems?

Network Exposure

Open ports, reachable services, and public endpoints

Credential Access

Stored passwords, API keys, and token leaks

Data Visibility

Databases, files, and backups accessible or misconfigured

Configuration & Logs

Exposed configs, debug endpoints, and log information

Internet-Connected OT

Rapid spread of OT devices with direct internet access

Remote Access Standard

Remote connectivity becoming default operational model

Supply Chain Risks

Exponentially growing vulnerabilities in service chains

IT vs. OT: Different Attack Surface Realities

IT Environment

- Rapid change, regular updates
- Logical attack surface (services, APIs, cloud)
- Focus: confidentiality, integrity, availability (CIA triad)

OT Environment

- Long lifecycle devices (10-20+ years)
- Often non-updateable or updates require downtime
- Industrial protocols (Modbus, DNP3, S7comm) often lack authentication
- Focus: safety, uninterrupted process operations

IT/OT Convergence

Single network → dual security perspectives → expanded, complex attack surface with amplified risk

Why Minimizing Attack Surface Is Critical

OT systems were never designed for internet connectivity. Each misconfiguration can halt entire operations.

→ **Common Weak Points**

Default passwords, outdated firmware, remote maintenance access, public admin interfaces

→ **Attacker Tools (2023-2024)**

Shodan, Censys, leaked credentials, open GitHub repositories, legacy VPNs without MFA

→ **Direct Impact**

Lack of attack surface management leads directly to operational disruptions with physical consequences

Case Study: Internet-Exposed OT Devices

The Discovery

Between 2023-2024, Microsoft, Dragos, and CISA issued alerts: tens of thousands of OT devices accessible directly from the internet across water utilities and energy sectors.

Critical Problems Identified

- Internet-connected PLCs without protection
- No firewall or VPN implementation
- Open remote access (RDP) ports
- Factory default passwords maintained

Key Lesson: Without active ASM, attackers have better visibility into your infrastructure than you do.

Data Manipulation

Operation Disruption

Physical Damage Potential

Case Study: Colonial Pipeline (2021)

1 **The Vulnerability**

Unused VPN account password leaked on dark web. No multi-factor authentication implemented.

2 **The Attack**

Single compromised credential granted access to critical systems.

3 **The Impact**

Fuel supply disruption across U.S. East Coast. National emergency declared.

Attack Surface Connection

Every existing access point—even dormant ones—is part of your attack surface. If Colonial Pipeline had implemented ASM combined with CTI:

- Leaked password detected in real-time
- Account blocked immediately
- Complete shutdown prevented

> This incident remains the **benchmark example of attack surface management failure.**

Case Study - MOVEit Transfer Mass Exploitation (2023)

One of the best examples of modern attack surface exploitation

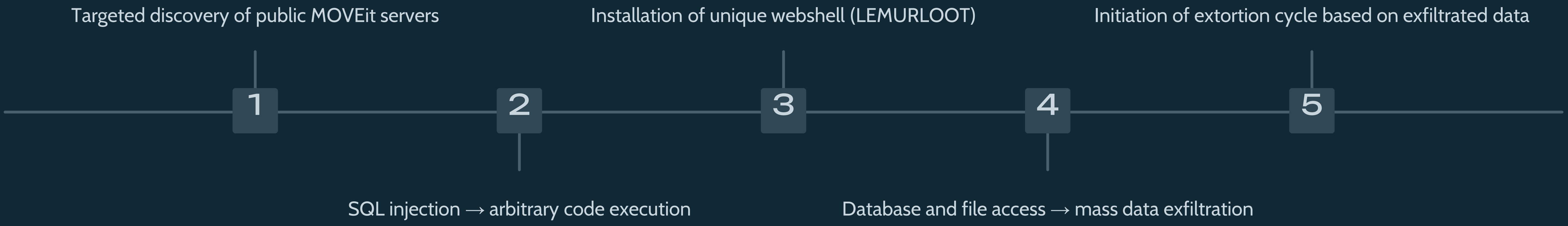
What was MOVEit Transfer?

- Widely used managed file transfer (MFT) system
- Used in government, finance, energy, and enterprise sectors
- Often directly exposed to the internet (HTTPS interface) for sensitive data transfer

What happened in May 2023?

- A critical 0-day SQL injection vulnerability (CVE-2023-34362) was discovered in the MOVEit web interface
- The vulnerability was actively exploited before a patch was released
- The Cl0p ransomware group launched an automated attack campaign against internet-exposed servers

Attack Timeline



1 Targeted discovery of public MOVEit servers

2 SQL injection → arbitrary code execution

3 Installation of unique webshell (LEMURLOOT)

4 Database and file access → mass data exfiltration

5 Initiation of extortion cycle based on exfiltrated data

Case Study - MOVEit Transfer Mass Exploitation (2023)

Affected Organizations and Consequences

- Over 2,500 organizations affected worldwide
- Tens of millions of personal data records compromised
- Affected sectors: government, banking, financial services, airlines, energy, healthcare and educational institutions
- Examples: BBC, British Airways, Shell, US government agencies

Why is this important from an attack surface perspective?

Attackers exclusively exploited publicly accessible services

Many organizations didn't know if they were using MOVEit or how it was accessible

Key success factors: public, discoverable services; automatable 0-day exploit; missing ASM visibility; slow detection and response

The MOVEit incident clearly demonstrated that a single internet-exposed service is sufficient to cause a global-scale data breach affecting thousands of organizations within days. Attackers discover exposurebefore organizations realize it exists.

Identifying IT Attack Surface with ASM Tools

DNS & Port Discovery

Subdomain enumeration and open port identification across all domains

Shadow IT Discovery

Unauthorized devices, services and applications identification

API Exposure

Public and private API endpoint security assessment

Cloud Resources

Public cloud asset analysis (S3, Azure Blob, storage buckets)

Vulnerability Scanning

Version analysis, configuration review (Nessus, OpenVAS, Qualys)

Third-Party Services

Outsourced provider security posture evaluation

Common Tools: Shodan, Censys, SecurityTrails, Nmap | **ASM Platforms:** Randori, Palo Alto Cortex Xpanse, Microsoft Defender EASM

Identifying OT Attack Surface

Critical Difference: Active port scanning on OT devices can be prohibited or dangerous. Passive methods are essential.

01

Passive Network Observation

SPAN/TAP implementations for non-intrusive monitoring

02

ICS-Specific Asset Discovery

Specialized tools can help in automating asset discovery in a non-intrusive way

03

Remote Access Inventory

Complete cataloging of all remote connectivity points

04

Vendor Relationship Audit

Third-party maintenance access review and control

05

Legacy Access Points

Old network devices and legacy IP gateways identification

06

Network Segmentation Mapping

OT network zone documentation and boundary verification

Minimizing Attack Surface: IT & OT Strategies

IT Environment

- ### Service Reduction

  Disable unnecessary services and close unused ports

- ### Access Control

  Eliminate public interfaces (RDP → VPN → MFA)

- ### Patch Management

  CTI-driven prioritization of vulnerability remediation

- ### Zero Trust Architecture

  Implement least-privilege access controls

- ### Microsegmentation

  Consistent firewall policies and network isolation

- ### Credential Monitoring

  Dark web surveillance for leaked authentication data

OT Environment

- ### IT/OT Separation

  Network segmentation with DMZ implementation

- ### Secure Remote Access

  Time-limited connections, jump hosts, mandatory MFA

- ### Vendor Access Control

  Supervised third-party maintenance with logging

- ### Internet Isolation

  Complete elimination of public OT device exposure

- ### Firmware Updates

  Scheduled maintenance windows for system updates

- ### Password Hygiene

  Replace default credentials, enforce strong policies

- ### Configuration Monitoring

  Real-time change detection and alerting

Conclusion - Strengthening Our Digital Defenses

Holistic Attack Surface Management

Effective security requires a comprehensive approach to identifying and mitigating vulnerabilities across both IT and OT domains. Continuously monitor and reduce potential entry points for attackers.

Tailored IT vs. OT Strategies

Recognize the fundamental differences between IT and OT environments. Implement distinct, yet integrated, security measures that respect operational criticality and unique technical challenges.

Lessons from Real-World Incidents

Case studies highlight the devastating impact of successful attacks. Learning from these incidents is crucial for refining defense strategies and preventing similar breaches.

Proactive & Continuous Security

A reactive stance is no longer sufficient. Prioritize proactive measures, continuous monitoring, and regular updates to stay ahead of evolving threats and ensure resilience.

Minimizing attack surfaces is not a one-time task but an ongoing commitment to safeguarding critical infrastructure and sensitive data in an increasingly connected world.

Thank You for Your Attention!