TRAFICOM
Liikenne- ja viestintävirasto

Component-level security: Can we trust the software in industrial components?

Goal of this presentation

- By the end of this session you will:
- Understand the embedded software layer in OT components
- Recognize how attackers exploit component-level weaknesses through real-world cases
- Identify the cyber risks facing OT supply chains and the mitigations available. From management to developers.

- If we have time: discussion about AI

TRAFICOM

Starting from basics

Terminology

What is Cyber (security)?

What is embedded software layer?

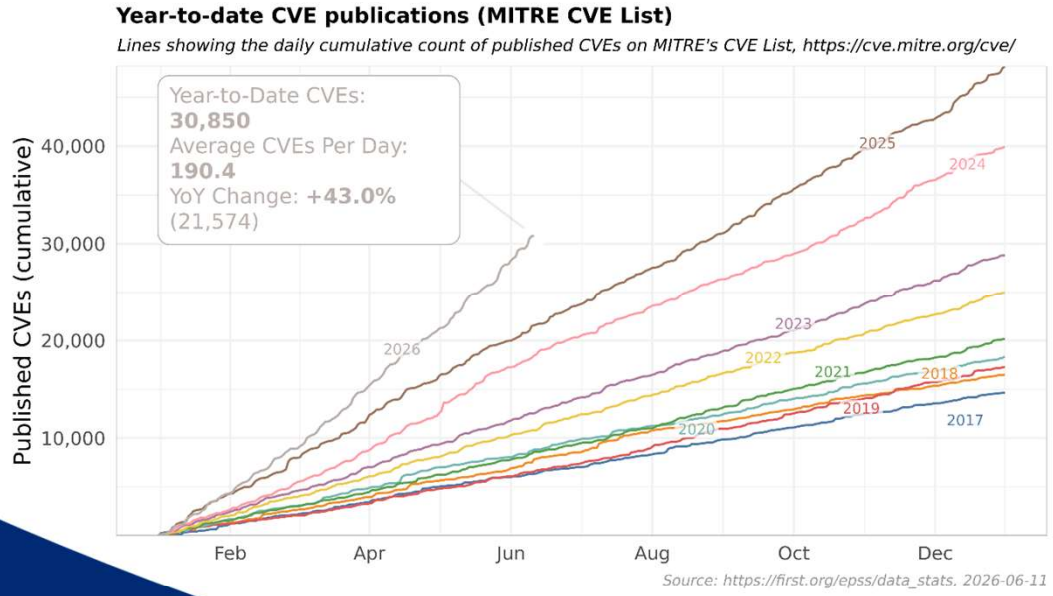
What are supply chain attacks?

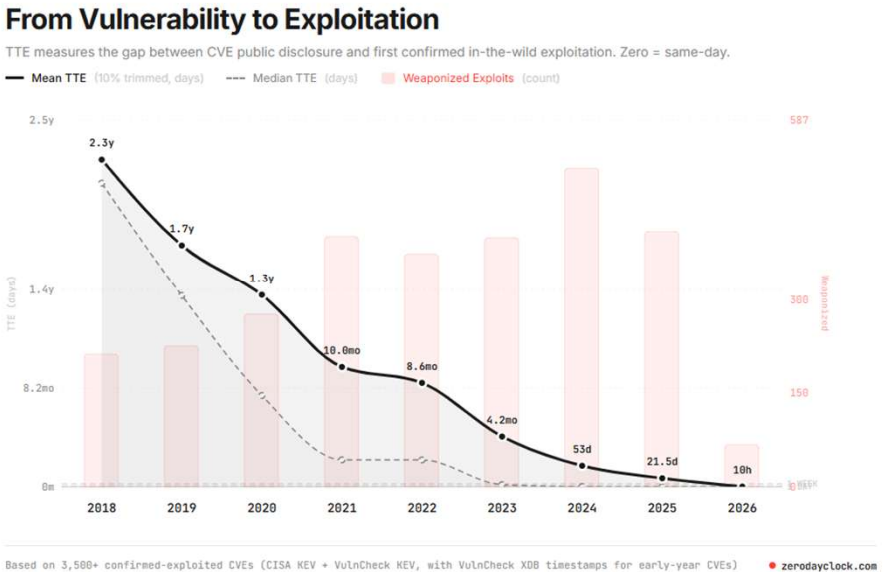
Cyber security is...

- Cybersecurity is the **art of protecting** networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information. (CISA)
- Cybersecurity is the **practice of protecting** people, systems and data from cyberattacks by using various technologies, processes and policies. (IBM)
- **measures taken to protect** a computer or computer system (as on the Internet) against unauthorized access or attack (Merriam-Webster)

Todays situation

More vulnerabilities, faster exploitation





SOURCES first.org/epss/data_stats, haettu 12.6.2026
ja zerodayclock.com, haettu 12.6.2026.

Todays situation

VPN’s are still popular attack vectors

- For example, routers, VPN systems, and firewalls that have not been updated pose a risk to both organizations and private home users.
- Attackers exploit new vulnerabilities even within hours.
  - Attackers also look for vulnerabilities in the content of released updates, which exposes outdated versions to attacks shortly after the update is released.

Phising is not most common attack vector anymore

31 %

Data breaches now begin with exploiting vulnerabilities. Previously, the most common method of hacking globally was using login credentials stolen through phishing.

SOURCE Verizon 2026 Data Breach Investigations Report verizon.com/about/news/breach-industry-wide-dbir-finds, haettu 8.6.2026.

OT-systems cyber threats

Hacktivism: opportunistic disruption generates visibility

Hacktivists search the Internet for poorly protected systems, such as exposed administration panels, which can be breached using simple techniques.

Their goals include disrupting the target and using any collected information for influence operations. Hacktivists may, for example, share the data they obtain on social media.

BUSINESS IMPACTS

- disruption of system operations
- becoming a tool for information influence
- unwanted media attention

Espionage: information is power : and money

State-sponsored and financially motivated actors conduct espionage to gain a competitive advantage or to support political intelligence gathering.

A state may be interested in areas such as innovations, energy or defense policy, or supply chains, while a competitor may focus on methods, product development, or customers.

METHODS OF ESPIONAGE

data breach, for ex. unsecured network edge devices

social engineering, for ex. targeting OT specialists on social media

open-source intelligence (OSINT)

phishing, for ex. email

Sabotage: a deliberate precision strike that cripples operations

The motive for sabotage may be financial gain or state-driven influence. The perpetrators can be cybercriminals or state actors. A competitor or even an insider employee may also take part in sabotage.

Attackers prepare by studying the target through open sources and tailoring the attack to match the target.

BUSINESS IMPACTS

- Compromising operational continuity
- Significant financial damage
- Psychological effects

Embedded software layer

- Software that is built into a device at the component level, not installed or managed by the end user, but shipped as part of the hardware itself

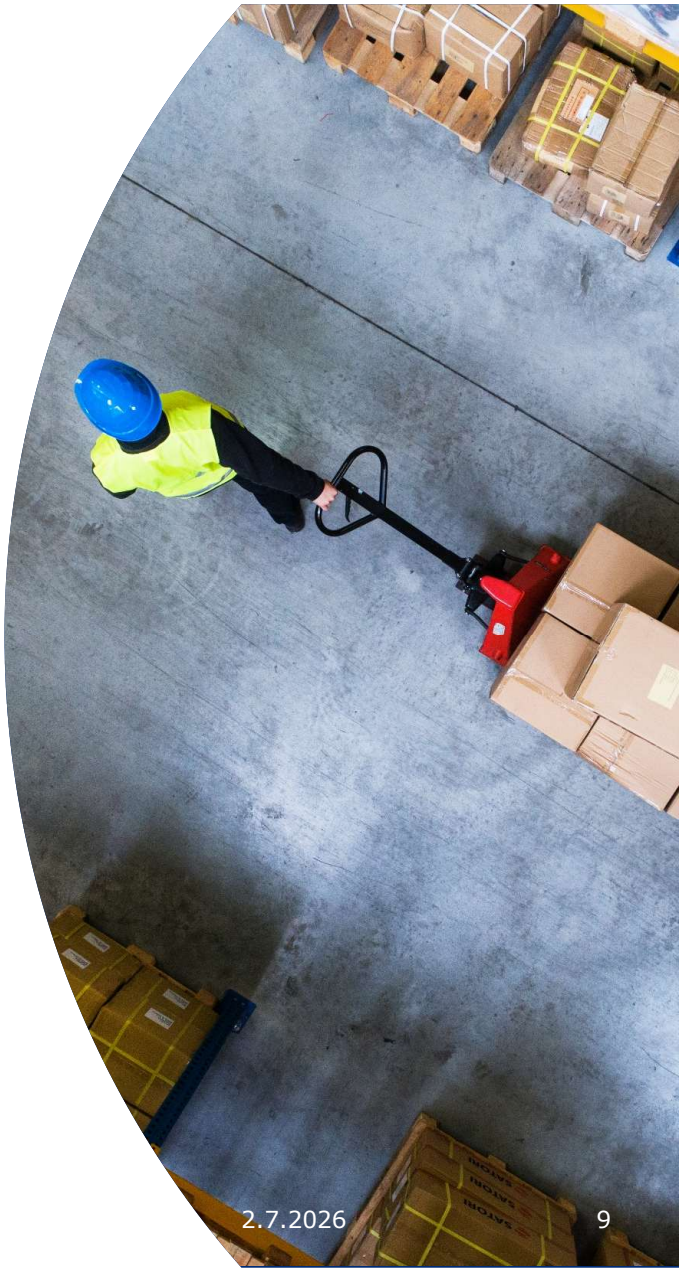
Includes:

- Firmware (low-level software controlling hardware behavior)
- Bootloaders (controls what runs at startup)
- Embedded OS (e.g. VxWorks, embedded Linux, RTOS)
- Application logic (PLC ladder logic, function blocks)
- Third-party libraries and components bundled by the vendorKey characteristic:

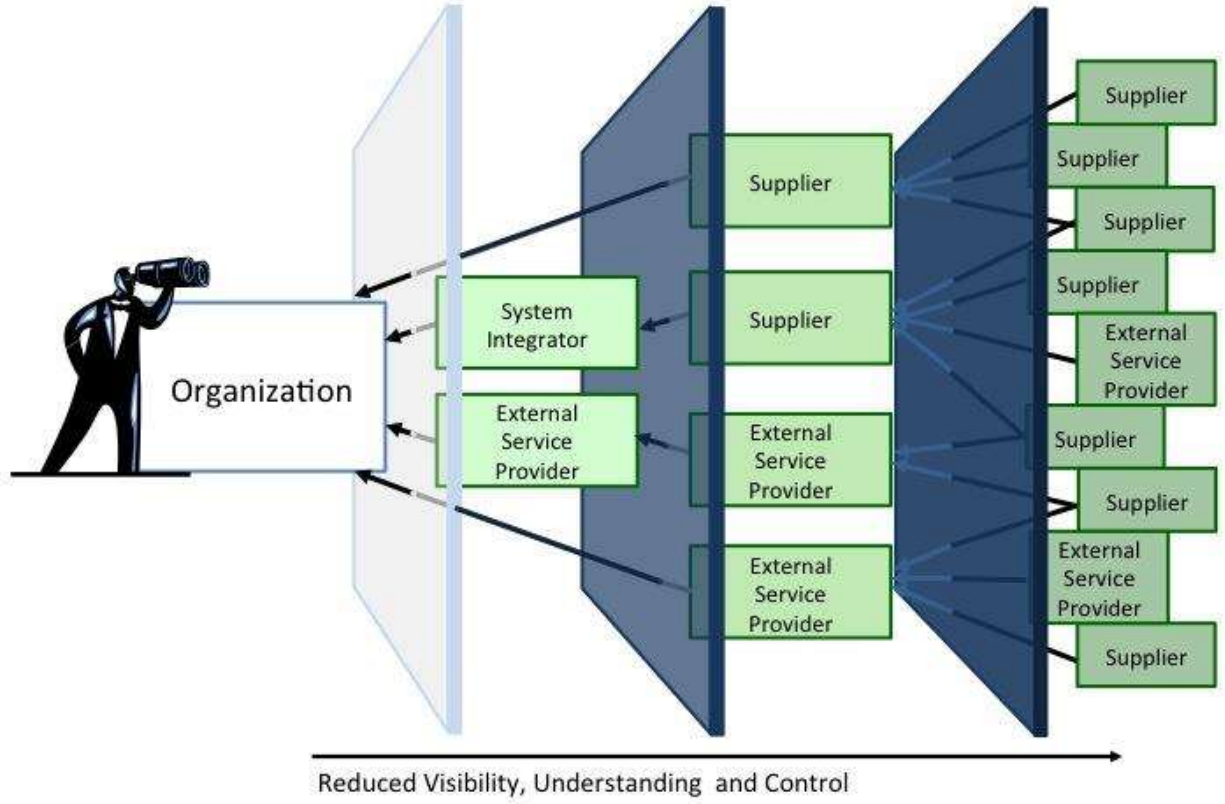
The end user typically has no visibility into what's in it, no control over how it's updated, and no easy way to verify its integrity.

Supply chain

- Imagine that you run a company: you buy a new shiny device, which is a very good device, it has all security certificates and promised to be secure.
  - Does it really do all those things it promises?
- Long supply chain before getting the product
  - When you decide you trust the product, you also decide to trust its supply chain.



Supply chain management



https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-161.pdf

Supply chain attacks

Three of the top ten threats for 2030 are directly relevant to what we're discussing today.

This graphic is a few years old now, ENISA published it around 2022.

But threats are materializing already.

Technical findings

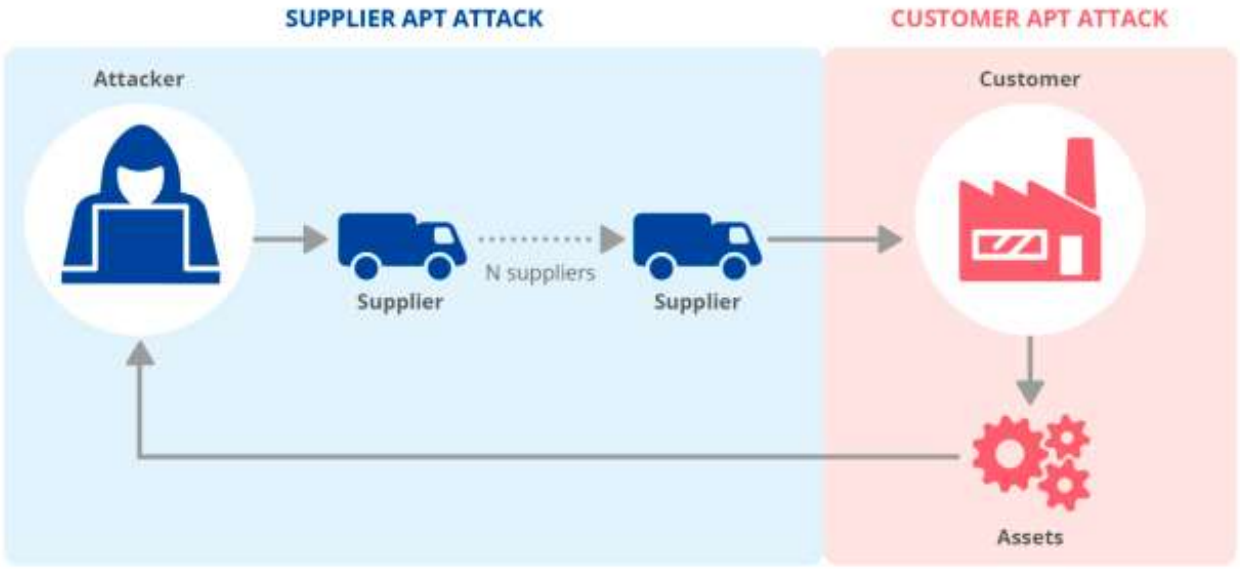
- Obsolete & vulnerable software.
- Insecure handling of updates.
- Development features were still active.
- The product used reference implementations as such.
- Too wide attack surface, large number of open ports and unused services.
- Hidden undocumented credentials.
- Remote management that is usable by the manufacturer without users' consent.
  - Sometimes this is even undetectable to the user.
- Insecure handling of input data, often leading to unauthenticated access or remote code execution.
- Various issues in www-based management interfaces (often basic OWASP Top 10 vulnerabilities).
- Insecure radio interfaces, Wi-Fi and other technologies (i.e. no encryption or authentication).
- The overall maturity of the product is too low, it looks like an early prototype.

Findings on product maturity

- The maturity level of security of OT products is moderately polarized. Some manufactures meet the requirements easily, while the others do not.
- Correcting defects found during inspection is time-consuming.
- The manufacturer's own ability to assess the cybersecurity of its product is not sufficient.
- Security challenges are aggravated by
  - **long supply chains**
  - **large numbers of stakeholders**
  - and increased integration among components and ecosystems.

Attack vectors

- **Firmware tampering**
  - malicious code inserted during manufacturing or via a compromised update mechanism
- **Malicious software updates**
  - legitimate update channels used to distribute backdoored versions
- **Hardcoded backdoors**
  - undocumented interfaces left in by the vendor
- **Compromised dependencies**
  - vulnerable or malicious third-party libraries
- **Maintenance access abuse**
  - vendor remote access used as an entry point



66%

of analysed supply chain attacks, the compromised supplier did not know : or was not transparent about : how they were breached.

(ENISA, Threat Landscape for Supply Chain Attacks)

Why OT Environments Are Particularly Challenging

Downtime is not an option

- Updating or patching a software component often requires taking the system offline

Accepted risk from outdated components

- A certain level of known risk is deliberately tolerated. Running end-of-life software is often a conscious operational decision, not an oversight.

Software runs in layers

- The operator-facing HMI is just the surface. Underneath sit device drivers, embedded OSes, firmware, third-party libraries

The air gap illusion

- Maintenance laptops, vendor remote access, USB updates, and historian connections all create bridges that are rarely tracked or controlled.

Examples

Real life examples

XZ Utils backdoor

A malicious contributor spent two years infiltrating an open source project and inserted a backdoor into a core Linux compression library. Nearly made it into major distros. Perfect example of software supply chain compromise at the dependency level, and it was caught almost by accident.

SOURCE: Screenshots from Wired, SentinelOne, HackerNews

Real life examples

Unitronics PLC attacks

Iranian-linked group Cyber Av3ngers targeted water utilities in the US using default credentials on internet-exposed Unitronics PLCs. Directly OT, directly component-level assumptions about security.

SOURCE: Screenshots from CSO Online, The Hacker News

Iran-Linked Hackers Disrupt U.S. Critical Infrastructure by Targeting Internet-Exposed PLCs

Ravie Lakshmanan Apr 08, 2026

Iran-affiliated cyber actors are targe
critical infrastructures in the U.S., in
and intelligence agencies warned T

"These attacks have led to diminish

Iran-linked PLC attacks cause real-world disruption at critical US infra sites

News
Apr 8, 2026 • 5 mins

Operational disruptions and financial losses have already been reported, and six federal agencies say the campaign is ongoing.

What to do?

So can we trust the software in industrial components?

Trust, but verify

Tips for developers

- Choose a secure programming language
- Best practices for development
- Version control and configuration management
- Software bill of materials (SBOM) is a tool to identify what software consists of.
- Maintenance and updating of equipment and software. Also development tools.

TRAFICOM

Software procurement

THE RIGHT VENDOR PROTECTS MORE THAN JUST CODE – IT PROTECTS THE BUSINESS.

- Requirements as part of the procurement from the beginning, safety must be part of the contract
- If possible, get help from lawyers and developers.
- The customer doesn't just purchase the software. It determines the level of risk and quality the organization commits to.

TRAFICOM

Tips

- Identify whether you are subject to any regulations that the software must comply with (e.g. GDPR, NIS2 Directive, CRA and any industry-specific regulations)
- Define the organization's risk level together with management. Security is not a yes or no, it's a sliding scale.
- Include requirements
  - architecture, access control, logging, vulnerability management, and data protection
  - Verify through testing, reviews, and documentation
- Require adherence to secure software development principles

Tips for management

- Understand the impact of software security and risk management on business and its continuity

- Resources for the future
  - Safety doesn't happen by chance, it requires planning, management commitment and resourcing

TRAFICOM

3 categories for good practices

- Actors
  - Industry professionals (e.g. managers, engineers), end users and organizations
- Processes
  - not limited to the context of a single organization. Include interactions between stakeholders
- Technologies
  - These include hardware components, design recommendations, techniques, libraries or other software components to support the process throughout the entire supply chain

Conclusion

The Reality

- OT and supply chains are complex ecosystem
- Many different threats from physical to digital and the threat landscape keeps changing
- The embedded software stack is largely invisible to the operator
- Risk management plays a big role!

The Opportunity

- Incidents like XZ Utils and Unitronics are forcing the industry to take component-level s
- Regulations are catching up, NIS2 and CRA
- You don't need to solve everything at once. Define your risk level, start with procurement requirements, build from there

References

- Threat Landscape For Supply Chain Attacks https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
- Good Practices for Supply Chain Cybersecurity https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity
- FORESIGHT 2030 THREATS ENISA Foresight Cybersecurity Threats for 2030.pdf

THANK YOU!

Questions?

Contact information
cert@traficom.fi

AI Security problems

- AI is being adopted across every industry, including critical infrastructure and industrial environments
- IoT sensors and OT devices increasingly feed data into AI systems
- Ever increasing stress for Open source

- Manipulation of AI models
- Use of AI in cybercrimes -> attack automation and enhanced ability to evade detection
- Double edged sword: helps security and criminals

Thank you again

TRAFICOM
Liikenne- ja viestintävirasto