It is long past time to move reverse engineering of embedded devices for the OT community towards a more actionable and scalable direction.

Reverse Engineering OT Devices with ATT&CK® and ISA/IEC 62443 Part 4-2 Mapping as a Service

Isiah Jones
OT Cybersecurity Engineer

AIT
Applied Integrated Technologies

Reverse Engineering OT Devices with ATT&CK and ISA/IEC 62443 Part 4-2 Mapping as a Service

Introduction

It is long past time to move reverse engineering of embedded devices for the OT community towards a more actionable and scalable direction. Construction, engineering, and system integration firms; asset owners and operators; and even product vendors have struggled under the existing CVE focused regime. Reporting yet another product vulnerability and coming out with the same old "patching and network segmentation" as the panacea to mitigating everything does not work.

Why Reverse Engineering

At AIT we are constantly looking into current actions our community is taking and assessing the gaps that need to be addressed to move the ball forward. We believe reverse engineering should move towards an actionable analysis and mapping of vulnerabilities and weaknesses to the specific related ATT&CK tactics and techniques that could be used to exploit them. That then should be directly mapped to the ISA/IEC 62443 part 4-2 component security requirements which could be securely designed into the product.

Security Level 3 (SL-3) component capability technical requirements in part 4-2 should be part of every product manager's agile epic and user story. SL-3 requirements and testing should be a part of every product team sprint backlog on at least a biweekly basis. SL-3 covers a wider set of 4-2 requirements than the current status quo, bare minimum, approach of SL-1 and SL-2 that some product suppliers have attempted to implement.

This isn't just good for catching zero-day vulnerabilities. It can also be useful for continuous product improvements in an agile lifecycle. Vendors can start by focusing on the known exploitable vulnerabilities, their exploitable tactics and techniques, and specific standards requirements that could mitigate or prevent them.

Relevant Security Standards

Many security practices, frameworks, guidelines, and standards have requirements that require security capabilities, discovery, documentation, and testing of all components and subcomponents including bills of materials. Some examples include but are not limited to:

- NIST SP 800-160 Systems Security Engineering – System security requirements process, and verification and validation technical process phases
- ISA/IEC 62443 part 4-1 – Product Secure Development Lifecycle Maturity – Secure by design product development lifecycle practice requirements including secure by design, security requirement specification, attack mapping, threat modeling, independent security testing, continuous secure coding evaluation, considerations for third party components, handling, and fixing vulnerabilities etcetera
- ISA/IEC 62443 part 4-2 – Component Security Requirements – Security requirements for devices, firmware and software components and subcomponents
- NIST Cybersecurity Framework (NIST CSF) - Risk Assessment (ID.RA) - ID.RA-1: Asset vulnerabilities are identified and documented, Supply Chain Risk Management (ID.SC) - ID.SC-4:

Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations

- NIST SP 800-53rev5 & 82rev3 – CA-2 (Control Assessments), CA-8 (Penetration Testing), RA-3 (Risk Assessment), SA-11 (Developer Testing and Evaluation), SC-31 (Covert Channel Analysis), SR-6 (Supplier Assessments and Reviews), SR-10 (Inspection of Systems or Components)

What reverse Engineering Includes

Reverse Engineering should include but is not limited to:

- Supply chain tracing and checking for counterfeit and defective components (e.g., chips on a circuit board)
- Checking firmware builds including bill of material subcomponents
- Checking hardware components and subcomponents to verify bill of material
- Sourcing origin of components
- Software components and subcomponents to generate bill of materials
- Checking coding repositories
- Documenting zero-day vulnerabilities as well as known vulnerabilities
- Determining which ATT&CK tactics and techniques could be used to exploit components
- Determining which part 4-2 requirements if built into components and or subcomponents could defeat which ATT&CK tactics and techniques that would make zero day or known vulnerabilities no longer exploitable
- Product comparison report cards between competitors, versions, and families of products (including subcomponents that could be swapped out for more secure subcomponents within products)
- Continuous testing throughout the product agile lifecycle and lifespan of the product

Example Software Vulnerability Mapping:

AIT leverages tools such as ObjectSecurity ™ OT.AI ™ Platform to help scale and semi-automate reverse engineering analysis of common ICS, OT, IIoT, and IoT firmware and software to do our ATT&CK, and part 4-2 ISA/IEC 62443 mitigation mappings for customers. Product vendors can use this service to improve products. Engineering, Procurement and Construction (EPC) firms, system integrator firms, and asset owners and operators can use the information and AIT services to:

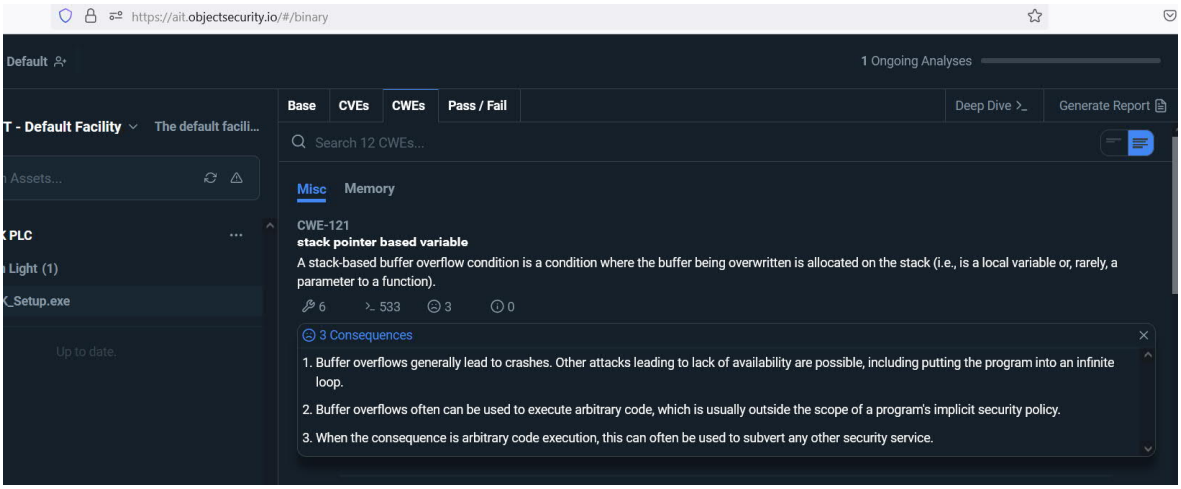
- Request required security features in procurement and project specifications during design build and purchasing phases of projects
- Shop for products that have built in secure design mitigations to discovered vulnerabilities and/or weaknesses

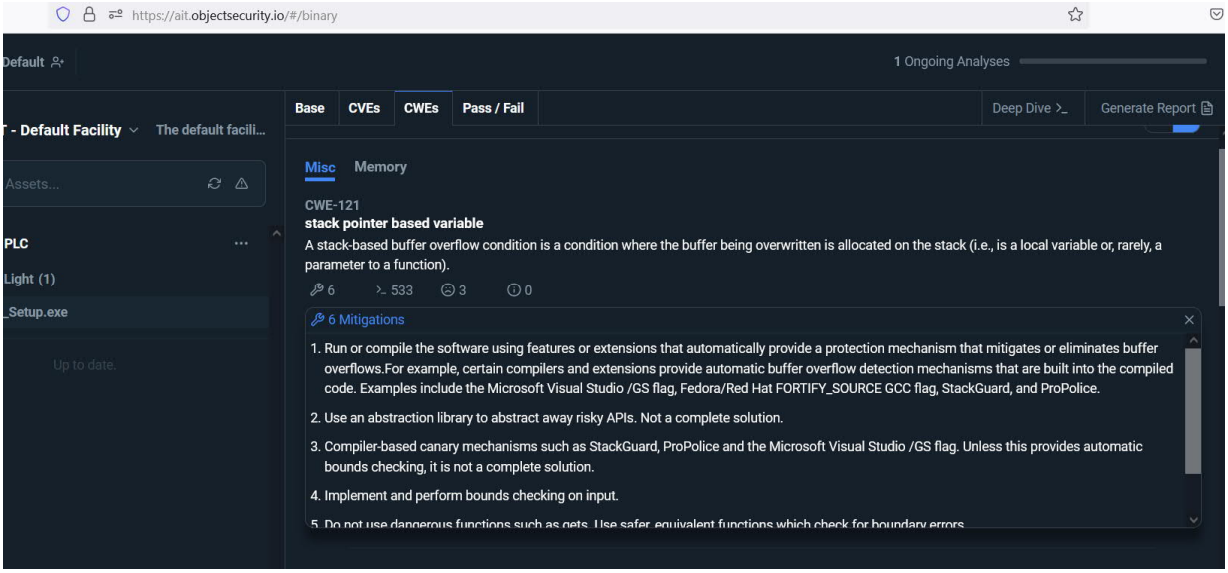
Below is an example of initial high-level analysis of a commonly used low-cost PLC's free programming software binary leveraging the ObjectSecurity ™ OT.AI™ platform.

The inexpensive PLC brand we analyzed for this example is usually less than $100 for a controller with basic IO. Its programming software is free to download online. It is often used in manufacturing plants, buildings, and facilities. In oil and gas, they are especially popular for pumps, tanks, pick stations,

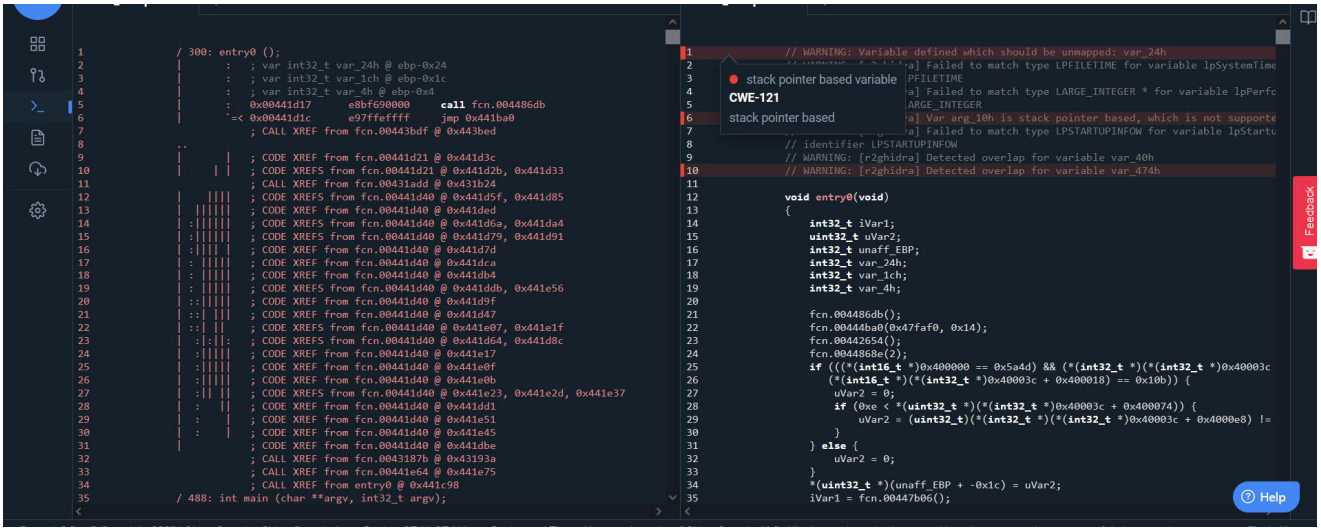
etcetera. Inexpensive and common brands of controllers and their programming and configuration software often gets overlooked in traditional cybersecurity.

ObjectSecurity ™ OT.AI ™ Platform found no Common Vulnerability Exposures (CVEs) in the current version of the PLC programming software. However, the platform found several Common Weakness Enumeration (CWEs). The ObjectSecurity ™ OT.AI ™ Platform Screenshots below is an example of a CWE-121 stack pointer-based variable weakness.





The platform also flags the CWE within the binary disassembly so the analyst, researcher, engineer, developer, or end user can quickly find where the CWE occurs. Automating some of the traditionally manual reverse engineering steps for firmware and software binaries particularly larger binaries, provide the ability to scale more consistent reviews.



*Note: CWE 121 stack pointer-based value are a common weakness across several different binary types including:

- Common, freely downloadable, protocol calibration and configuration explorer tools
- Common, freely downloadable, protocol middleware driver, connector, conversion, and data historian applications
- Common and freely downloadable versions of SCADA applications
- Other inexpensive PLCs with freely downloadable programming software

Knowing that attackers could use the CWE information to create new exploits, AIT chooses not to reveal the specific versions of software binaries used in the test in accordance with our responsible disclosure policy.

Mapping ATT&CK Tactics and Techniques to CWE-121:

Often the status quo is to report and register a CVE, assign it a CVSS score and push out alerts saying to do network segmentation and patching. This method doesn't actually fix the problem and will never improve products in the ecosystem. It does not help asset owners, operators; EPC, or system integrators know what specific technical capability requirements from part 4-2 to request in the components they use. It does not help product teams prioritize specific SL-3 capabilities in components and subcomponents regardless of whether they are trying to certify the product against the full 4-2 list or not. Ultimately, it delays rapid, incremental improvements that could mitigate today's already known and commonly used ATT&CK tactics and techniques.

In the PLC programming software binary example, ObjectSecurity ™ OT.AI ™ Platform flagged a "CWE-121 stack pointer-based variable." CWE-121 weaknesses invite stack-based buffer overflow style attacks. We discovered that there were no public ATT&CK Enterprise, Mobile, or ICS tactics and techniques directly mapped to CWE-121. Based on attacker behaviors in the past and AIT experiences, the closest obvious ATT&CK tactics and techniques we could find that attackers could potentially use to exploit CWE-121 in components are:

- ATT&CK Enterprise Tactic – Execution with Technique - Exploitation for Client Execution https://attack.mitre.org/techniques/T1203/

- ATT&CK for ICS Tactic – Initial Access with Technique – Supply Chain Compromise https://collaborate.mitre.org/attackics/index.php/Technique/T0862

With further research and testing one could argue that there are additional tactics and techniques that have been or could be used by attackers to take advantage of CWE-121. This is one reason AIT believes reverse engineering software and firmware binaries with mapping to ATT&CK and part 4-2 ISA/IEC 62443 should be a focused service in the ICS, OT, IIoT, IoT, Embedded, and Cyber-Physical Systems communities.

Mapping Part 4-2 ISA/IEC 62443 Component Requirements as Product Mitigations:

Often it is overlooked that a part 4-2 component requirement may in fact have mitigated commonly used ATT&CK tactics and techniques used to exploit CVEs and CWEs both known and zero day. It should baffle society then as to why the mappings are not regularly performed and used to directly inform product improvement sprints every month. For several years now the status quo in the community has focused too much on finding zero days and registering CVEs only for the guidance to be "patch and segment." That is no longer good enough for asset owners, operators, or system integrators in an evolving dynamic and interdependent ecosystem of 'systems of systems,' smart things, devices, and components.

As an example of mapping, below are some of the existing ISA/IEC 62443 part 4-2 technical capability requirements for components (e.g., hosts OS, platforms, software, firmware, and embedded hardware) that could mitigate, deny, contain, or counter CWE-121:

- Embedded Device Requirement - EDR 3.2 – Protection from malicious code – Which states, "The embedded device shall provide the capability to protect from installation and execution of unauthorized software." The rational supplemental guidance even gives some protection examples such as:
    - Removable media control
    - Sandbox techniques
    - Restricted firmware update
    - No Execute (NX) bit
    - Data execution prevention (DEP)
    - Address space layout randomization (ASLR)
    - Stack corruption detection
    - Mandatory access controls

For CWE-121, it is reasonable to expect that stack corruption detection could be used to counter, limit, or at least detect CWE-121 stack pointer based variable related exploits used to target the stack-buffer weaknesses in components. Another requirement example could include:

- Component Requirement - CR 3.5 – Input validation - Which states, "Components shall validate the syntax, length and content of any input data that is used as an industrial process control input or input via external interfaces that directly impacts the action of the component."

One should note that in part 4-2, many general Component Requirements (CR) are to be applied across all common component types (embedded device, host, network device, software, or firmware,

etcetera). Both EDR 3.2 and CR 3.5 should be implemented in products of all component types to limit or eliminate CWE-121 stack-based weaknesses.

All reverse engineering and attack mapping efforts by the community and by AIT should include focused analysis and mappings of CVE and CWE to ATT&CK tactics and techniques where applicable. We also need to flag part 4-2 component technical requirements that should be implemented in the discovered vulnerable products. AIT believes this will move the community towards regular actionable improvements in the ecosystem, rather than continue to just create a barrage of endless CVEs that overwhelm asset owners, integrators, governments, and product suppliers. This reverse engineering and mapping as a service could finally focus the industry on remediating common trends such as CWE-121 being common across all the software and firmware binaries tested.

Recommendations for the Community

This is the beginning of a new service AIT wishes to offer the community. We believe the community at large should also move in this direction as often and consistently as possible. Here are our recommendations for each of the community stakeholder groups:

Recommendation for Product Vendors

- Design components with security level 3 (SL-3) part 4-2 of ISA/IEC 62443 as a baseline for embedded devices, firmware, embedded hosts, and software applications
- Report self-discovered vulnerabilities with the applicable ATT&CK tactics and techniques that threat actors could use to potentially exploit the vulnerabilities and/or weaknesses
- Reference the part 4-2 requirements that can be enabled in your products so that EPC, Architecture and Engineering (AE) firms, system integrators, consultants, government, and asset owners and operators are aware of which specific features can be enabled in the vulnerable product as a mitigation to the discovered vulnerability and/or weakness
- Work with specialized security firms such as AIT to add continuous reverse engineering and mapping into your product, component, and subcomponent lifecycles

Recommendation for EPCs, AE and System Integrators

- Select, purchase, design, document, implement, integrate, and configure SL-3 part 4-2 of ISA/IEC 62443 capable components (e.g., embedded devices, firmware, software and embedded host operating systems or platforms). *Note: it is especially important that extra focus is given to packaged unit vendors and skid vendors and the components they are selecting in their solutions (e.g., bioreactors, fillers, mixers, palletizers, chillers, boilers, air handling units, etc.)
- Require the collection and testing of all software and firmware binaries for all products in the bill of materials so that zero-day and known weaknesses are discovered as early in the design build project schedule as possible. Ideally leveraging automated tools like ObjectSecurity ™ OT.AI ™ Platform lets AIT help scale this dynamic effort during busy brownfield retrofit and greenfield new build projects.
- Contract specialized OT security firms such as AIT to conduct penetration testing, security reviews, validation, verification, and assessments during design build and factory and site acceptance testing (FAT/SAT) phases of projects. This will ensure that SL-3 features are working as expected and properly configured, programmed, (e.g., PLC Top 20) and integrated.

Recommendation for Governments

- Designate which critical infrastructure sectors and types of assets, components and systems within your community, county, city, state, and country are highly critical capabilities and thus are mandated to only use components and devices that are SL-3 capable from part 4-2 of ISA/IEC 62443 technical foundational security requirements and feature capabilities
- Provide tax, insurance, and regulatory incentives and investments favorable to businesses who create and implement SL-3 baseline features and product capabilities from ISA/IEC 62443 part 4-2

Recommendation for Asset Owners and Operators

- Contract specialized ICS/OT security firms such as AIT to conduct penetration testing, security reviews, validation, verification, and assessments during design build, construction, factory and site acceptance testing (FAT/SAT) phases of projects to ensure that SL-3 features are working as expected and properly configured, programmed, and integrated
- Ensure that EPC, AE, and integrators select part 4-2 SL-3 capable products as part of design specifications and procurement requirements for all retrofits, upgrades, and new greenfield projects. Creating such specifications is something AIT's ICS/OT Cyber Mission Assurance Capabilities (CMAC) team can help with.
- Contract specialized ICS/OT security firms such as AIT to conduct at least annual penetration testing, red teaming, and vulnerability assessments of your existing production environments post go-live, commissioning, and cutover from the EPC, integrator, AE, and product vendors
- Contract specialized security firms such as AIT to leverage reverse engineering tools and map your OT software and firmware to common ATT&CK tactics and techniques with recommended ISA/IEC 62443 part 4-2 component technical requirements. This will identify product feature improvements that asset owners and operators should request from vendors in their purchasing, procurement, and vendor supply chain management requirements

Conclusion and contact us

AIT recognizes that this effort is hard and advanced in many cases; however, we believe it should be a focus area for the community. With our staff, tools, and growing list of partners, we have positioned ourselves to make this a consistent and beneficial service to society. AIT's security engineering professionals have experience reverse engineering hardware, firmware and software for embedded components, devices, applications and systems for commercial and government customers and their supply chain subcomponents. AIT's ICS/OT security engineers are regular contributors and members of ISA/IEC 62443 and ISA84.00.09 standards committee working groups. Our security engineers are regular contributors to national security, CVE, and FFRDC organizations. Additionally, AIT's staff maintain current GICSP, CISSP, and other relevant certifications. To seek out security reverse engineering and mapping services please contact us at otcyber@ait-i.com.

ObjectSecurity, ObjectSecurity Logo Design, OT.AI, and the OT.AI Logo Design are trademarks of ObjectSecurity LLC. All other trademarks, logos, and brand names are the property of their respective owners. All rights reserved.