INL/CON-22-69227-Revision-0

CyTRICS: Vulnerability Analysis Tailored for Critical Infrastructure

October 2022

Changing the World's Energy Future

Hannah Pearson Kleinheider

Idaho National Laboratory

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

INL/CON-22-69227-Revision-0

CyTRICS: Vulnerability Analysis Tailored for Critical Infrastructure

Hannah Pearson Kleinheider

October 2022

Idaho National Laboratory
Idaho Falls, Idaho 83415

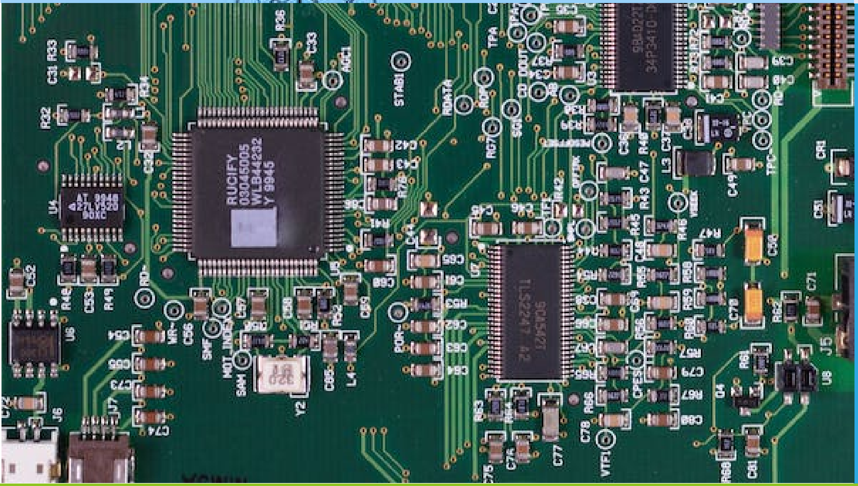
http://www.inl.gov

Prepared for the
U.S. Department of Energy
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

```
mov     rbp, rsp
mov     DWORD PTR [rbp-4], edi
mov     DWORD PTR [rbp-8], esi
mov     DWORD PTR [rbp-12], edx
mov     eax, DWORD PTR [rbp-4]
imul    eax, DWORD PTR [rbp-8]
mov     edx, eax
mov     eax, DWORD PTR [rbp-12]
add     eax, edx
sub     eax, DWORD PTR [rbp-4]
pop     rbp
```


October 8th, 2022

Hannah Pearson Kleinheider



CyTRICS: Vulnerability Analysis Tailored for Critical Infrastructure

About me

- **Cyber Security Researcher**
- Working at **Idaho National Laboratory** for the past 2.5 years
  - Former intern, so I've actually been around for longer than that
- **M.S. in Information Security** from Carnegie Mellon's Information Networking Institute
- **B.S. in Computer Science**, and B.S. in Math, from University of Idaho

Overview and context

- **CyTRICS** (Cyber Testing for Resilient Industrial Control Systems) created in 2018
  - Department of Energy program supported by **6 DOE national laboratories**
  - Originated as an INL LDRD (lab-directed research and development) project

OAK RIDGE National Laboratory

INL Idaho National Laboratory

Pacific Northwest NATIONAL LABORATORY

NREL NATIONAL RENEWABLE ENERGY LABORATORY

Lawrence Livermore National Laboratory

CyTRICS Objectives

1. **Identify components** of systems used in critical infrastructure, with an emphasis on identifying common components
2. **Identify vulnerabilities** affecting critical infrastructure and correlate them to common, shared components

What makes CyTRICS unique

- **SBOMs** (Software Bills of Materials) and **HBOMs** (Hardware Bills of Materials)
  - Inform and enrich vulnerability analysis
  - Enables correlation of vulnerabilities in components to systems that use those components
- **Vendor partnerships**
  - Provide equipment for testing and describe typical configurations
  - Assist with setting up a representative system for testing
  - Respond to reported vulnerabilities by patching and notifying their customers
- CyTRICS is well-equipped to analyze control systems for vulnerabilities due to the combined expertise in both control systems and cyber security research

Overview of testing

- Prioritization of systems based primarily on impact, prevalence, and availability
- Vendors sign testing agreements and provide equipment and documentation
- Control systems experts configure systems in a lab environment
- Cyber researchers (like me) take things apart, identify components, and find, document, and report vulnerabilities
- Test artifacts are collected in a repository
  - SBOMs (software bills of materials)
  - HBOMs (hardware bills of materials)
  - Reports
- Data scientists analyze data and gather insights

Vendor partners

- Schneider Electric: https://www.energy.gov/ceser/articles/doe-ceser-partners-schneider-electric-strengthen-energy-sector-cybersecurity-and
- Hitachi Energy: https://www.energy.gov/ceser/articles/doe-announces-hitachi-abb-power-grids-participation-cytrics-program
- More which have not been publicly announced

Testing process overview

Enumeration	Vulnerability Analysis
Check-In: Establish a baseline condition for system and configurations.	**Check-In:** Establish a baseline condition for system and configurations.
Initial Enumeration: Enumerate interfaces and services. Conduct a minimal evaluation of the security and operational constraints of the system before engaging in an in-depth analysis.	**Initial Vulnerability Analysis:** Perform tests to understand the security model of a system, enumerate interfaces, identify services, evaluate security controls, and identify vulnerabilities.
Hardware Enumeration: Analyze the physical hardware components that enable component identification. Note: this step is not performed for software-only enumeration.	**Hardware Testing:** Extract firmware, access in-circuit debug ports, and analyze hardware security features. Different levels of disassembly and removal will be performed as defined in the test plan.
Software Enumeration: Identify components, such as libraries, operating systems, and dependencies, including third-party libraries, operating systems, and utilities within the software and firmware.	**Software Analysis:** Discover and analyze functionality to identify relevant weaknesses in the security of the system.
	Targeted Testing: Execute tests designed to further explore potential weaknesses or issues discovered within the analysis phase. This might require further realism, including full-scale operation of the system. Mitigations for identified vulnerabilities as well as specific counterfeit detection activities can be developed during this step.
Check-out: Document the final state of the system, including any changes in system functionality or capability based on the tests performed.	**Check-out:** Document the final state of the system, including any changes in system functionality or capability based on the tests performed.

Check-in

- Configure a system to be representative of a realistic deployment
  - Team includes sector-specific experts such as power engineers
  - Vendors provide assistance with configuration, as they would for a customer

Initial exploration

- Understanding context
  - What are the security boundaries?
  - What is the environment in which the system operates?
    - Next to safety, availability is generally the highest priority
    - What are the physical processes that the system is controlling?
    - What could go wrong if the system is misused?
- Become familiar with configuration software, operator workstations, engineering workstations, HMIs, etc. as well as the specific system under test
- What ports are open? What network protocols are used to communicate? Which services are communicating? Which communications are encrypted? How are networks segmented? And so on...
- What protections are in place?

Enumeration

- Creating bills of materials (BOMs)
  - Hardware
    - Opening up physical devices and extensively photographing them
    - Identifying components involved in data storage, memory, processing, and communication
  - Software
    - Lots of scripting to identify all the different files present (often 10's of thousands of files)
    - Additional manual identification of components through software reverse engineering (this is the primary approach when creating SBOMs for firmware)
- Producing SBOMs and identifying components relates to vulnerability analysis
  - We look for published vulnerabilities and determine whether or not they apply

Vulnerability analysis

- Test out security boundaries, based on information gathered about the system and the physical processes it controls
- Determine whether known vulnerabilities in a component apply to the system
- Search for new vulnerabilities
  - Conduct targeted testing to prove vulnerability with proof-of-concept exploit

Disclosure process

- We report vulnerabilities as we find them, after a review by DOE
- Provide vendors the earliest opportunity to begin patching, rather than waiting until an assessment is complete
- We also document what we looked at and encourage vendors when we see things they are doing right

Success thus far

- Vulnerabilities in GE relays, discovered during the 2018 proof-of-concept phase https://www.cisa.gov/uscert/ics/advisories/icsa-21-075-02
- Hitachi Energy patched three vulnerabilities identified by CyTRICS researchers
  - Certificate verification vulnerability: CVE-2021-22278
  - Insecure boot: CVE-2021-35535
  - Insufficient security controls: CVE-2021-35534
- Many more have been reported and are in the process of being patched

Recommendations for testing

- Team up with an expert on the infrastructure sector in which the system you are testing is used
  - Understand the physical environment the system operates in and the processes it controls
- Ask vendors how a system is typically configured in the field
  - Understand the security model and requirements
- Identify system components and check whether known vulnerabilities in those components are exploitable in the system under test
- Provide positive feedback on system features that have been well-designed and implemented with security in mind
- Encourage vendors to maintain an accurate inventory of the components in their products
  - Vendors can and should produce their own BOMs
  - It is particularly important to maintain a list of third-party components that are being used
- Encourage vendors to track disclosed vulnerabilities in the third-party components they use and assess whether those known vulnerabilities in components are exploitable in their products
- Encourage vendors to provide timely patches and security bulletins to their customers

Idaho National Laboratory

hannah.kleinheider@inl.gov

@h4nn4rchy