ICS and IoT security labs

Rules of engagement / code of conduct

This document provides our take on the code of conduct for all users of the ICS & IoT security lab setup at the CS3STHLM conference. The lab is made available as a means to allow the attendees to test and do security tests against equipment, devices, components, etc., that are not generally available, and normally not available in such a way that they can be poked, probed, scanned, rebooted, crashed, without any consequences in a real-world plant or a dangerous physical process.

Objectives of the ICS security lab

Overall objective: **We want more secure devices, systems, applications, networks**. **We want to help protect our societies against attacks.** We believe that by having this proving ground and isolated environment with a lot of equipment, we can help vendors enhancing their products by eliminating security issues, vulnerabilities and other security errors. Think of it as crowdsourcing. Specifically, our objectives are:

1. **Allowing attendees to get hands-on access to hardware not normally available. The hardware is in an isolated sandboxed environment allowing for testing and tampering in ways that installed equipment cannot be.**
2. **To have people learn in a practical way about security in the ICS and IoT environments. Beginners, intermediate and advanced users should all have something to gain from using the ICS or IoT security lab**
3. **To find and fix security issues, by reporting them to vendors, via established channels and with well-known procedures. This process are ensured by KraftCERT, the Norwegian ICS CERT**
4. **To use attacks as basis to provide better defense, thus new IDS signatures, new IoC's, mitigation techniques, etc. are as important output from the lab as finding vulnerabilities**
5. ***To have a fun time doing all the above***

Being the good neighbour

We hope to foster a good spirit for all persons and stakeholders involved in the ICS and IoT security. We act as the good neighbour by inviting all others to our party (i.e. the ICS security lab), and we hope that the party goers repay this favor by being nice and gentle to others at the party, the working personnel (e.g. the people working with the equipment) and the vendors, the venue and the lab equipment. Being the good neighbour really boils down to – *don't behave like an idiot*. **More specifically, this mean:**

1. Handle vulnerability information in a sane and adult manner. The idea that we have, and that we sincerely hope is shared with any CS3STHLM attendee that uses the lab, is that we want broken things fixed. We do not think being a good neighbour is misusing the information to break, or break-into, real-world ICS or IoT equipment. We do not endorse selling zero-days, etc.
2. Not releasing information on a vulnerability publicly, but have it reported through KraftCERT who will coordinate handling of vulnerability information with you, vendor(s), other stakeholders, and the public
3. Not knowingly destroying things - equipment (e.g. uploading manipulating firmware, reconfiguring things in a destructive way), or wiki pages,
4. Not taking all available bandwidth with my network scanner running in insane scan mode,
5. No hardware hacking. Unless you have gotten an explicit permission from CS3STHLM staff
6. Leaving the devices in the same shape that you found them, e.g. same passwords, same config, etc. Important - Restart a device or network service that you might have hung or crash.
7. Having an open mind and share information and knowledge with others at CS3STHML

Not being a good neighbor will remove your access to the lab.

Vulnerabilities

ICS and IoT security labs

Most equipment and devices in the environment are old, run old versions of firmware or applications. Many vulnerabilities are believed to exist in the software that is used in this equipment. If you use the ICS/IoT security lab, you should report new vulnerabilities to the e-mail address for the ICSlab. This address is used to communicate with representatives of KraftCERT, which will in turn be the point of contact to vendors or security contacts within the different companies so they can make a fix or make a workaround.

Detection and protection

All things that can be found for detection and protection of old or new vulnerabilities are of interest to create and to make available to the public. We encourage anyone to share yara scripts, snort rules, bro scripts, etc. with the official contact, so they can be distributed for all to use in their detection/protection.

Reporting

Reporting a vulnerability should include some important basic information, such as:

- Make, model, type, version of the device and its software
- What has happened (e.g. authentication bypass, XSS, web directory traversal, etc.)
- How you triggered the event/fault/vulnerability
- Any Proof-of-Concept that might be used to repeat or validate the claim
- Any suggestions for mitigations, fixes, ids signatures, yara rules, etc.
- Contact information to you, the one that discovered the issue
- Finally, a note describing if you want to be credited for the discovery or not (i.e. if you want anonymity)

Send reports to icslab@cs3sthlm.se or, if you have any questions, contact the physical person supervising the ICS/IoT lab in the CS3STHLM geek lounge.

Don't release public information about the vulnerability. Coordinating all information handling with KraftCERT who is in charge of the vulnerability handling.

The ICS/IoT Lab "competition"

If you find something interesting (e.g. ***a vulnerability, a stupid default config***, etc.), or if you develop something useful (e.g. ***snort signature, a bro script, yara rules, new ELK grok filters***, etc.), report it! Report submitted to the official address, you participate in the ICS lab competition. Your name, type of reported item (vulnerability, better defense) and time of reporting will be added to the official information board. If you want to remain anonymous, you can note that in your vulnerability report.

All persons that finds zero day vulnerabilities in an ICS or IoT equipment and reports them: A diploma, free attendance to CS3STHLM 2018 and various prices from our sponsors.

Other prices in the competition include: attendance to CS3STHLM 2018, ICS/IoT gear, various prices from our sponsors, etc.

Public sharing of information

We will record all the network traffic that happens in the lab environment. These recordings will be used for security research, to validate old or new vulnerabilities. The recordings might be made public, after a period related to disclosure procedures with CERTs, vendors, etc.

We will make reported IoC's, IDS signatures, security tricks, etc. available publicly after the conference, related to disclosure procedures with CERTs, vendors, etc.