Sharad Agarwal

Research Scientist @ CERN

Incoming Information Security Postgrad @ UCL, London

Bachelor's in Computer Science and Engineering from VIT University

Previously:

Cyber Security Intern @ Gurugram Police Cyber Cell

Openlab Summer Student @ CERN OpenLab

Trainee/intern @ CERN Computer Security Team

Special Achievements:

BlackHat Academic Scholarship 2019

Research Papers in Cyber Security:

- Agarwal, S.; Oser, P.; Lueders, S. Detecting IoT Devices and How They Put Large Heterogeneous Networks at Security Risk. Sensors 2019, 19, 4107.
- Agarwal, Sharad, Oser, Pascal, Short, Hannah, & Lueders, Stefan. (2017, October 23). Internet of Things (IoT) security. Zenodo. http://doi.org/10.5281/zenodo.1035034
- Agarwal, Sharad, Oser, Pascal, Lueders, Stefan. (2018, June 12) Computer security: Smile, you're on camera…

Various Talks and other research papers …

https://sharad1126.github.io/

IoT Security

Gurugram Police Summer Internship 2020

Sharad Agarwal
European Organisation for Nuclear Research (CERN)

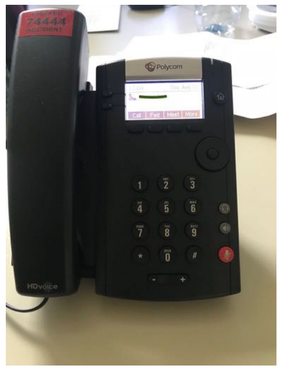
Internet of Things

where the web meets the physical world

Printer

Acces Card Reader

Media Layer Controller



IP Phones

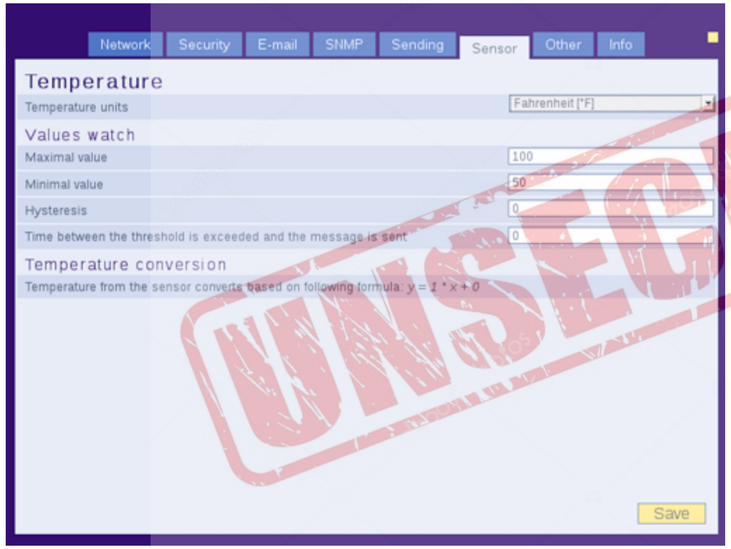
Routers

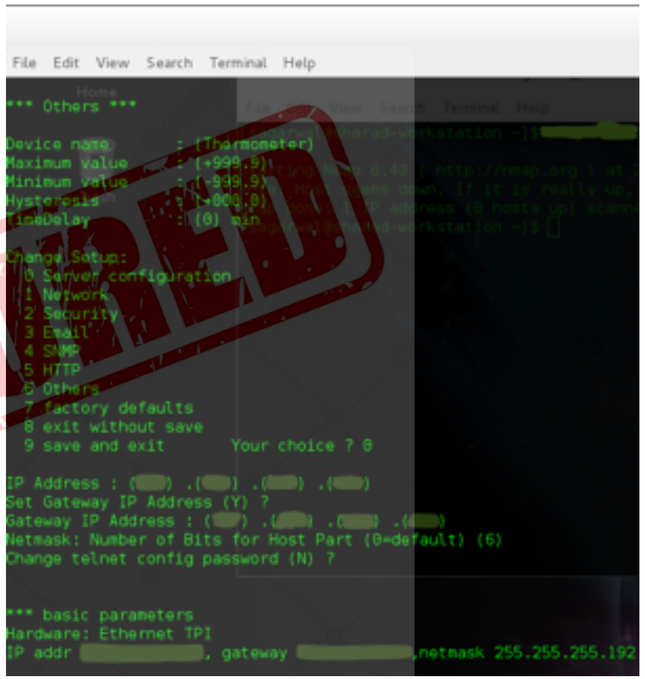
CCTV Cameras

We at CERN also do not have 100% secured IoT devices

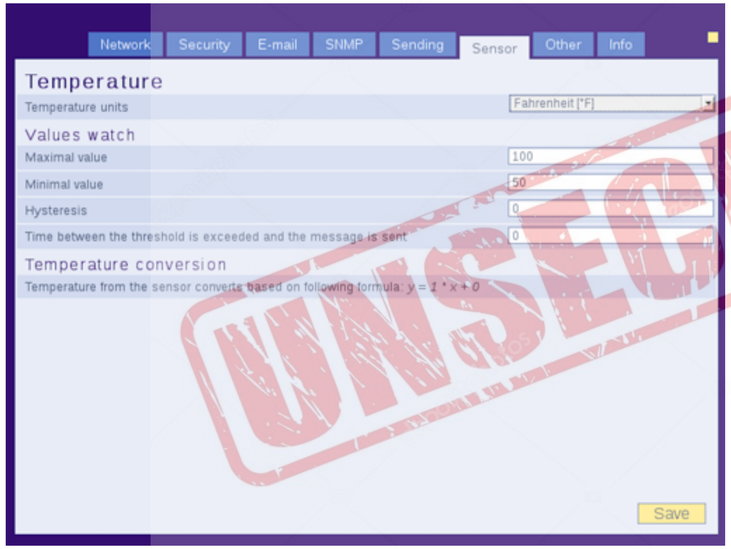
Let’s look into some cases of vulnerable devices found in CERN

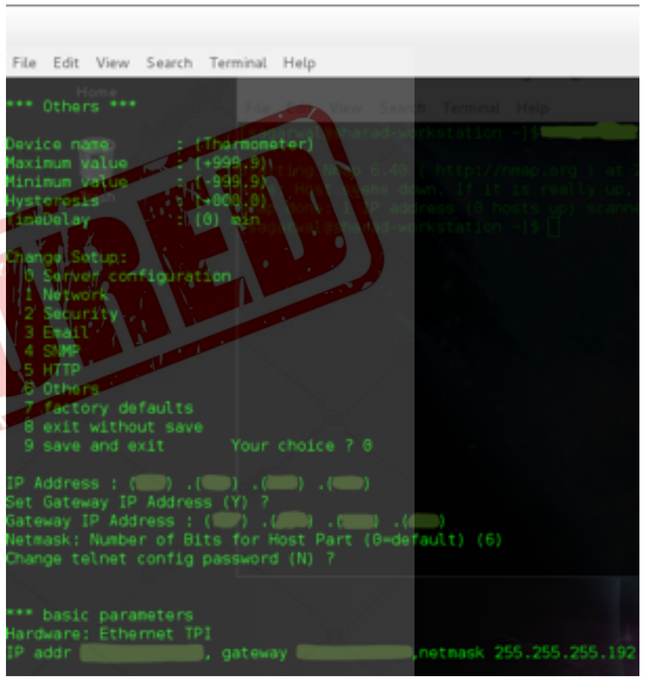
Thermometer - TME - Settings

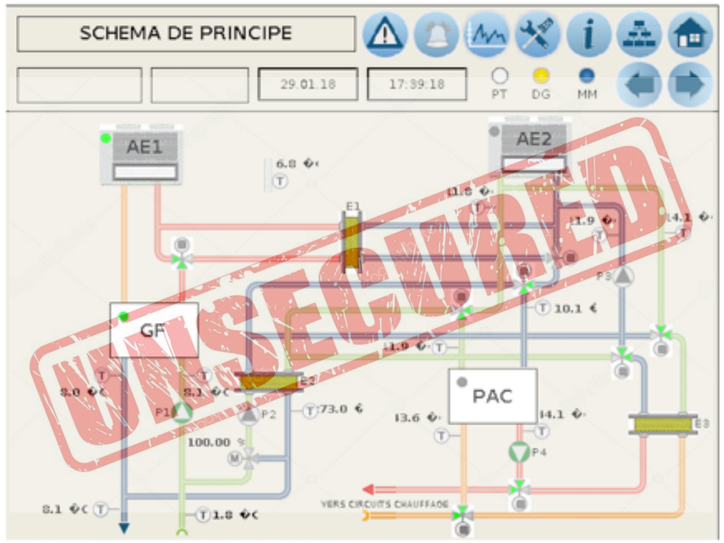




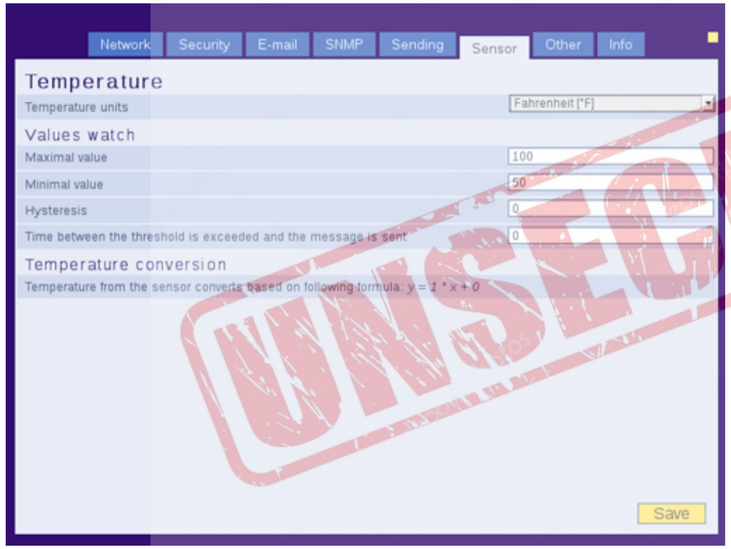
Thermometer - TME - Settings

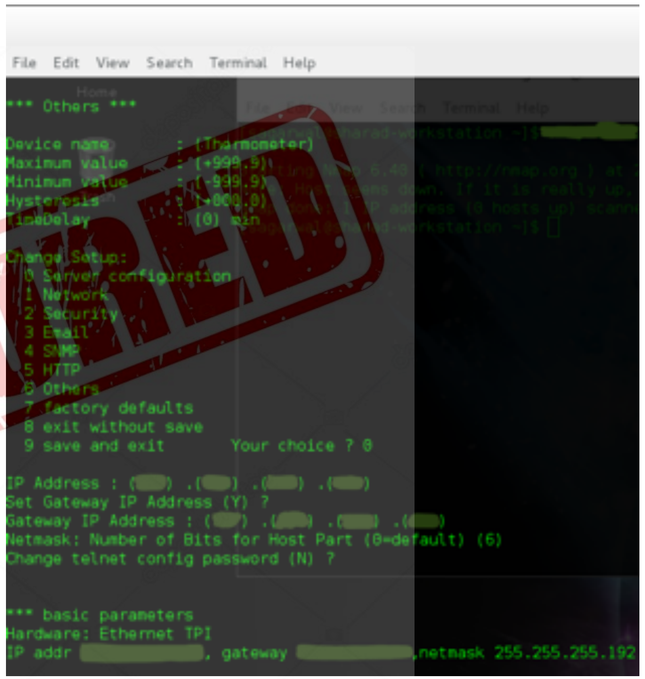


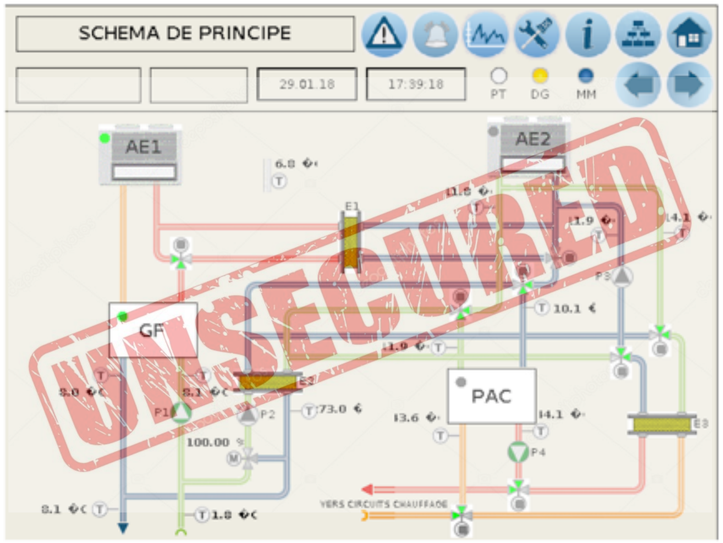




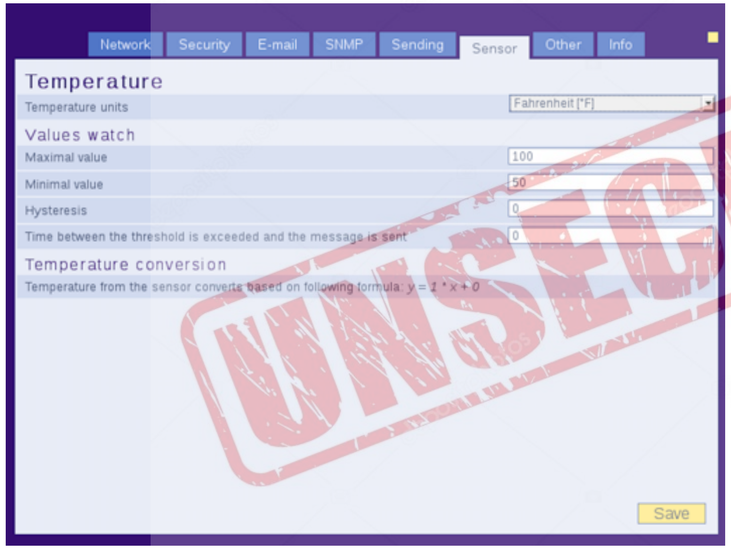
Thermometer - TME - Settings

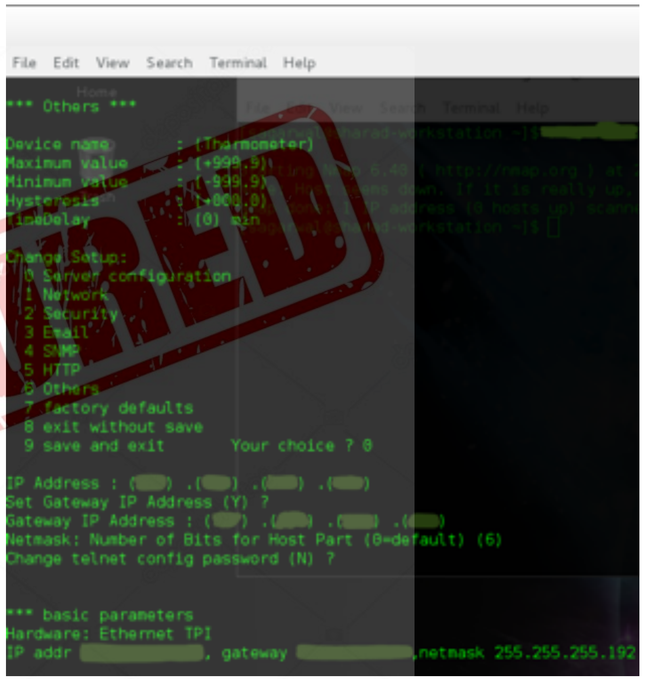


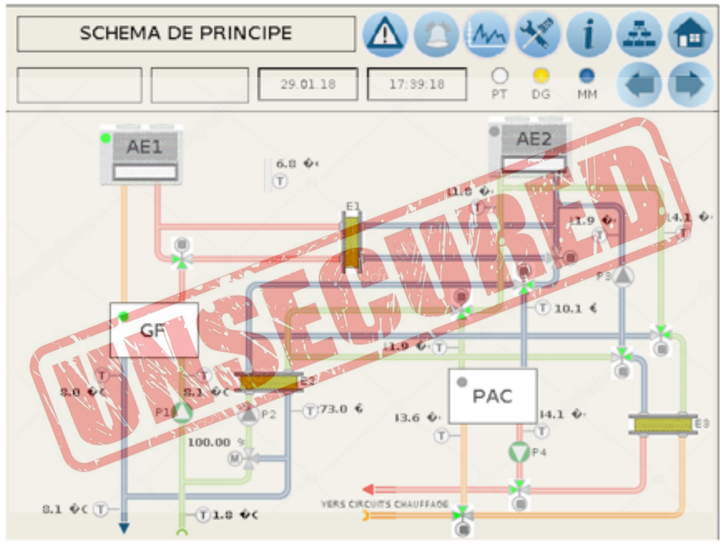




Thermometer - TME - Settings



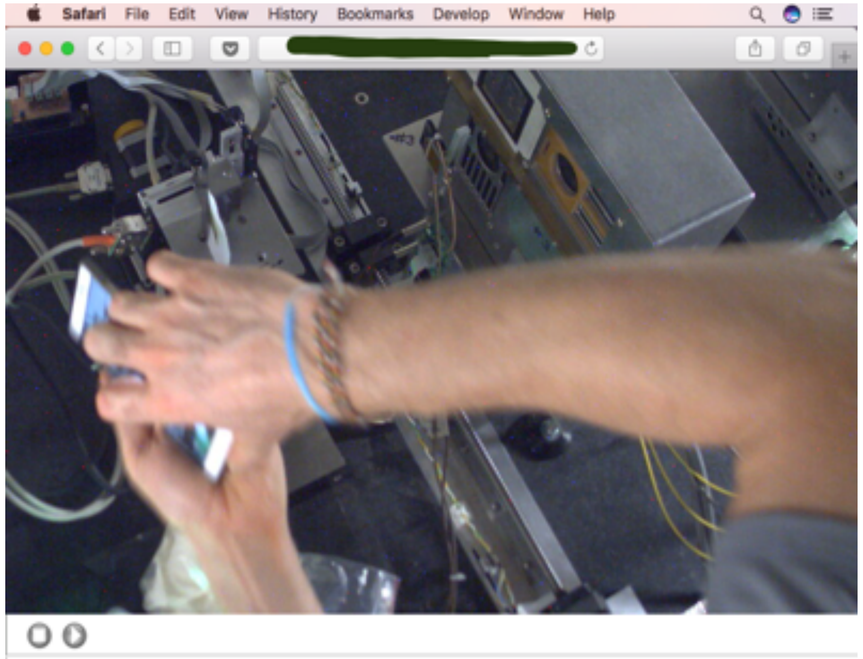


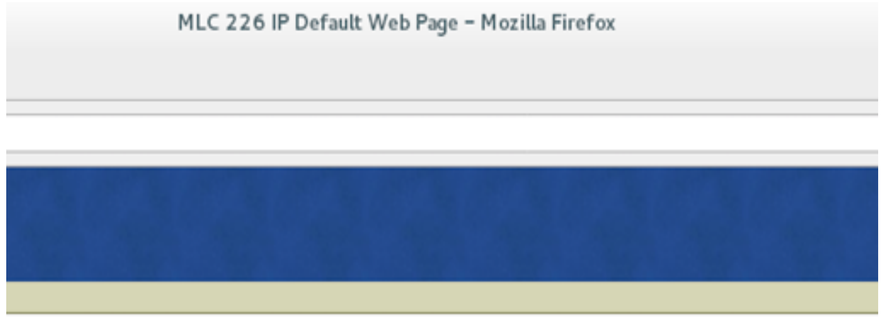


Devices like thermometers oscilloscopes, programmable logic controllers, used in physics organizations should be secured.

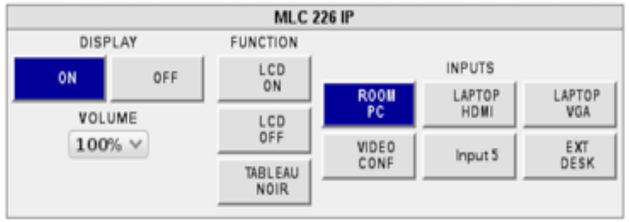
Printers - where I was able to write anything on the display screen

Real time streaming CCTV Camera

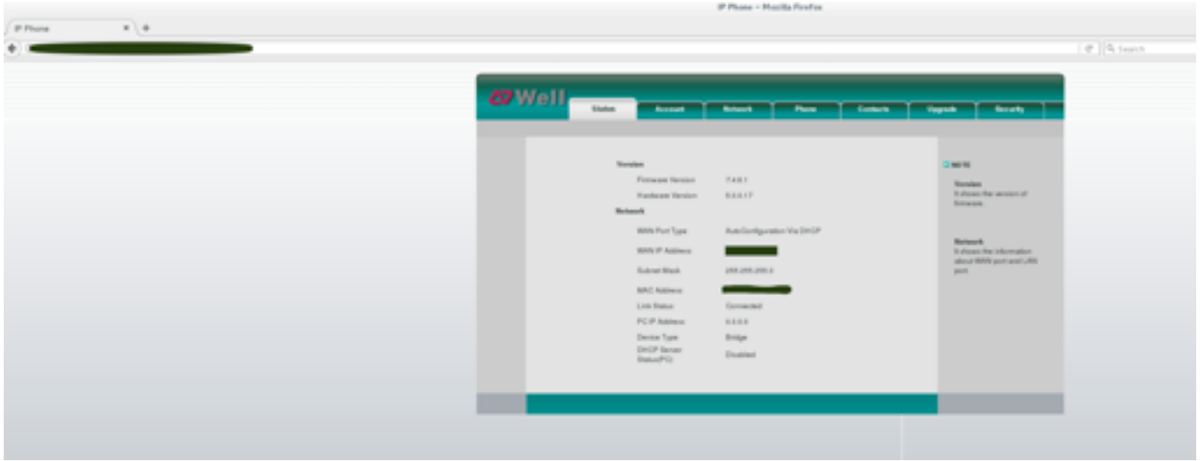




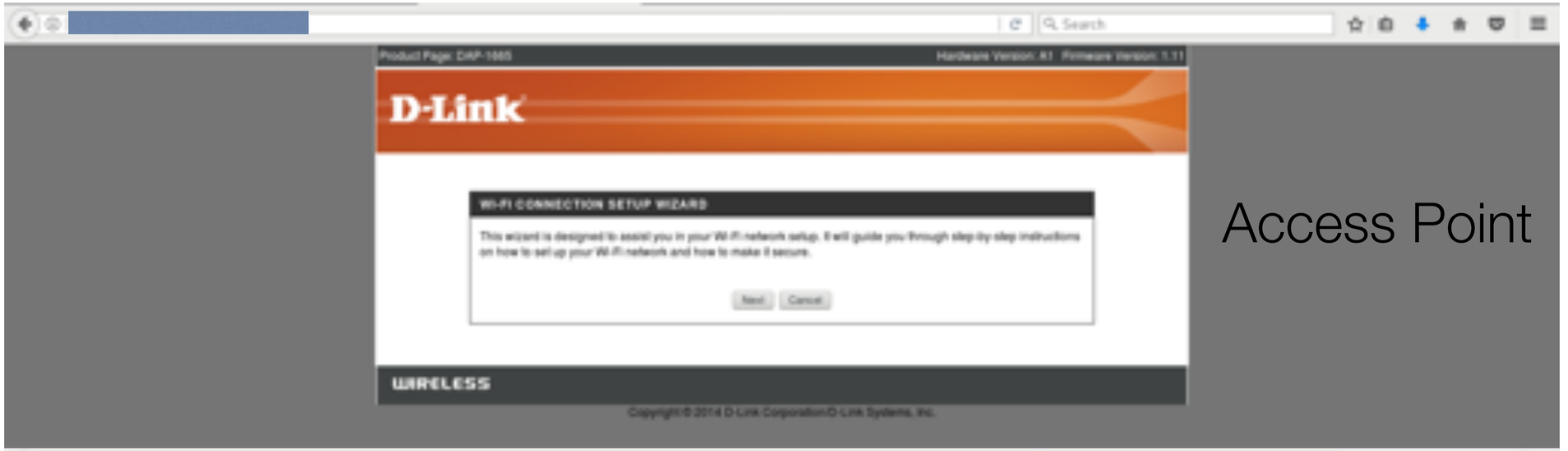
Conference room controllers



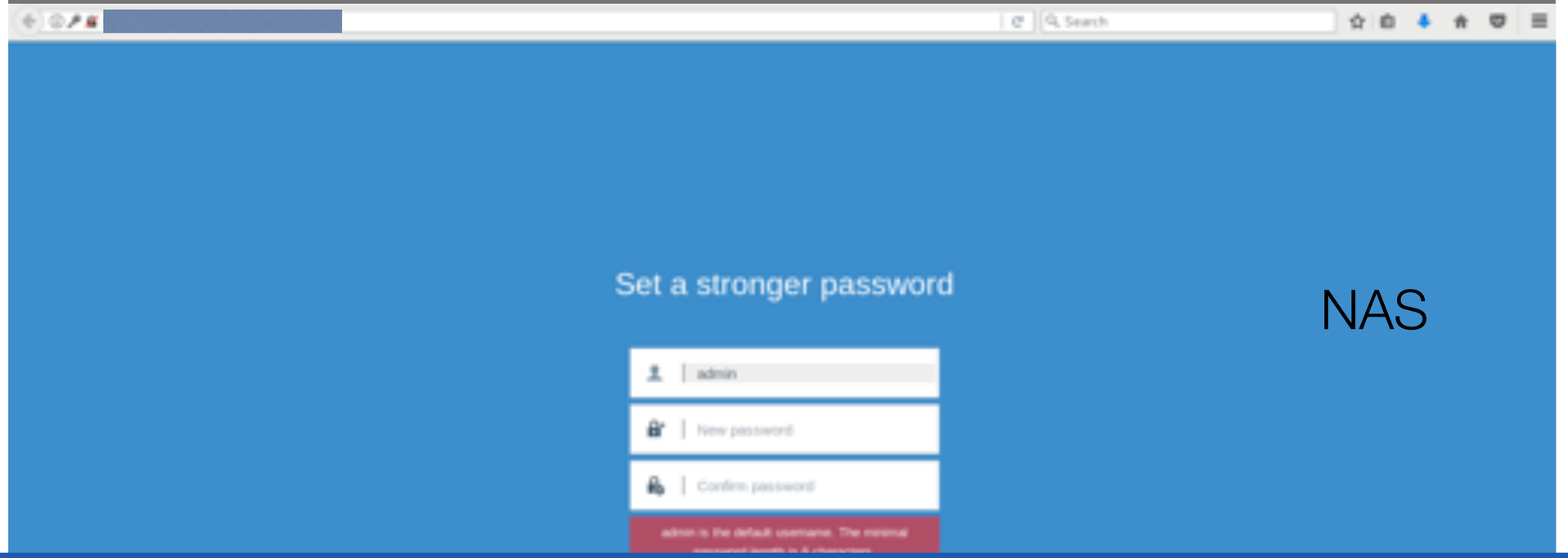
IP Phone



Non Configured Devices

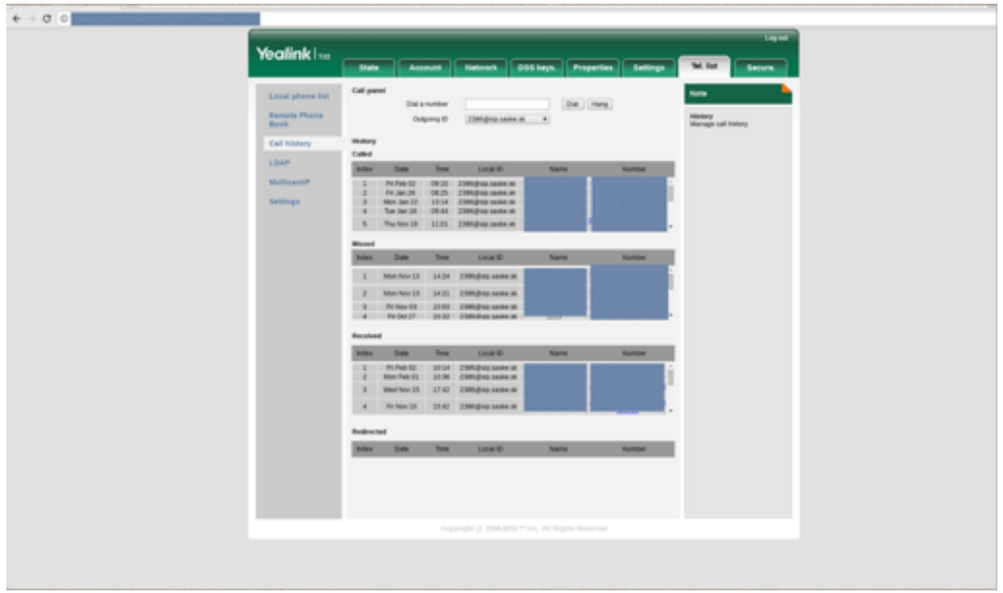


Access Point



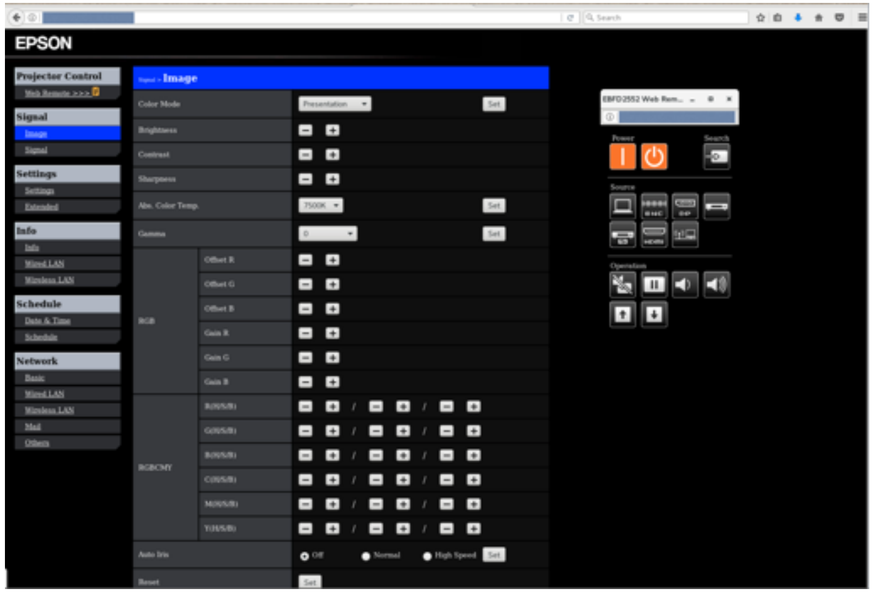
NAS

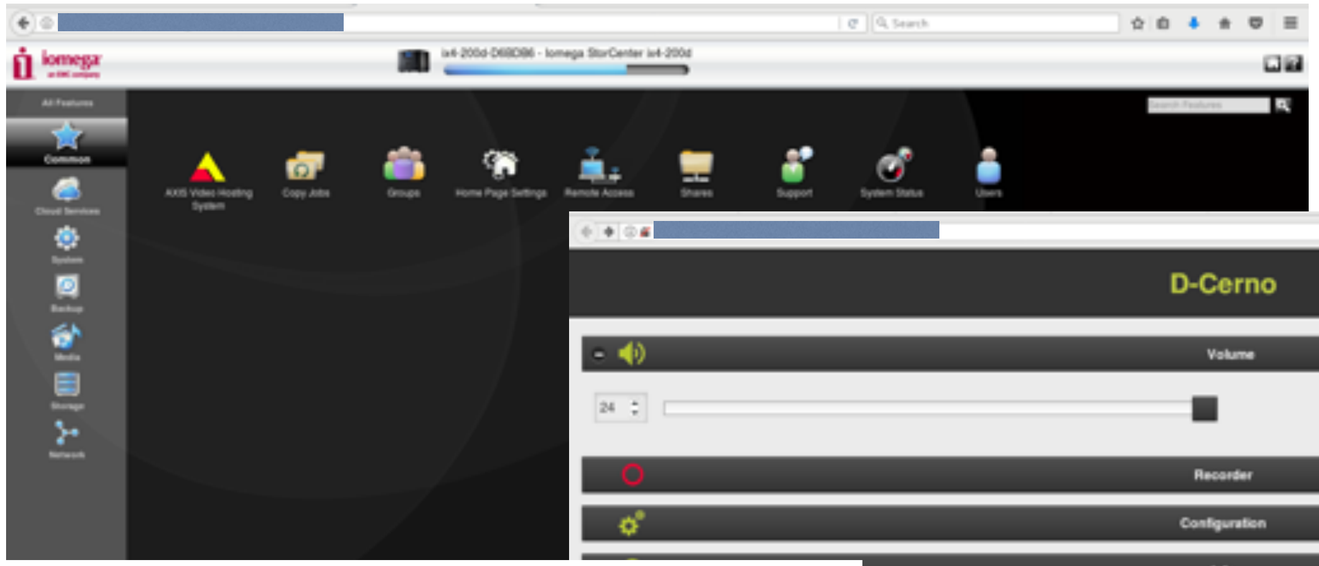
Easily Vulnerable Devices

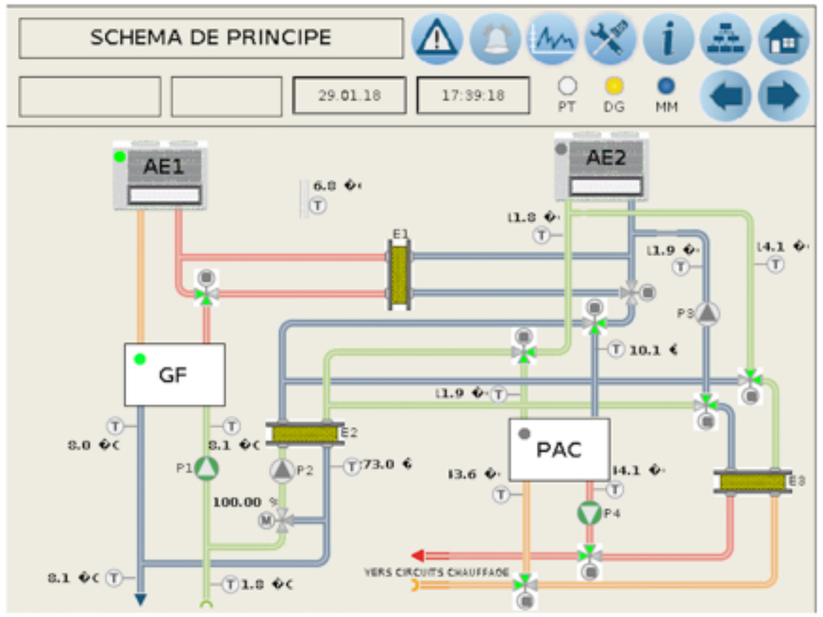


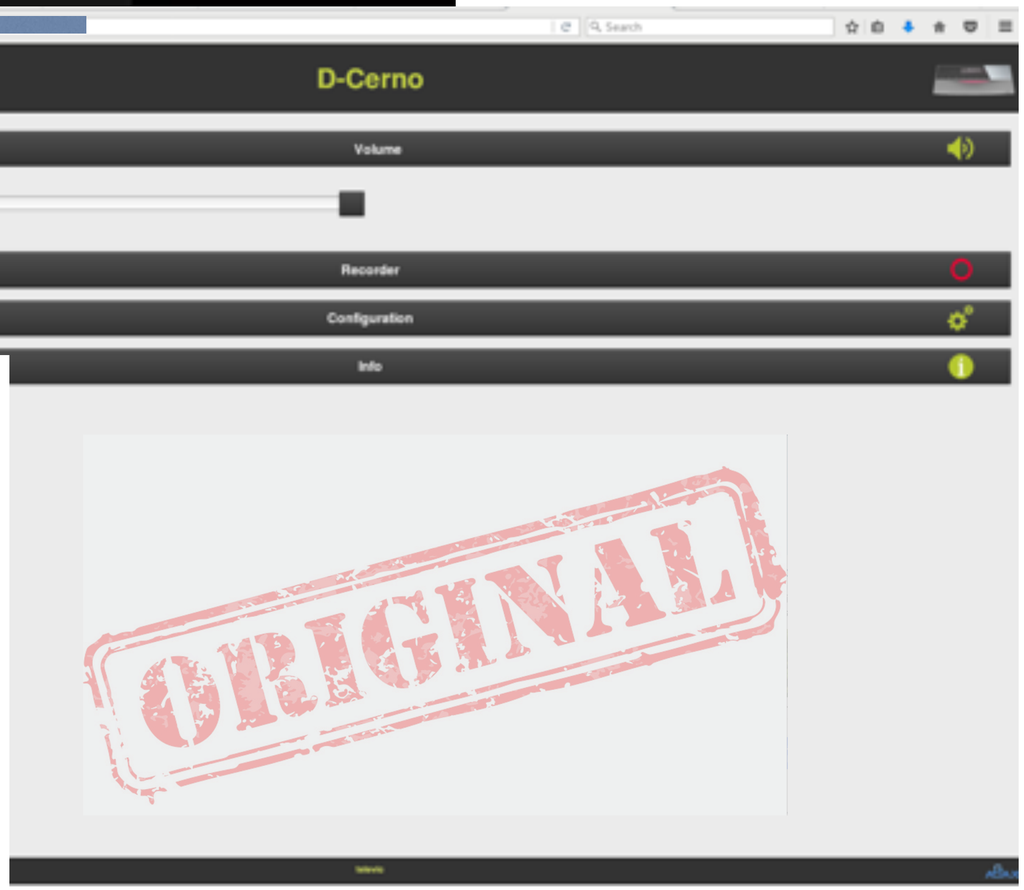
IP Phones - Can access contacts,
call logs and use it to call

Projectors used in meeting rooms









And Many More

Medium Vulnerable Devices

Before securing the IoT device, get to know the network on which it is running on.

To secure your devices, get to know the devices on your network.

We have developed a tool that detects IoT Devices and provides model, manufacturer, and firmware details which will be used to predict the security risk score for an IoT device

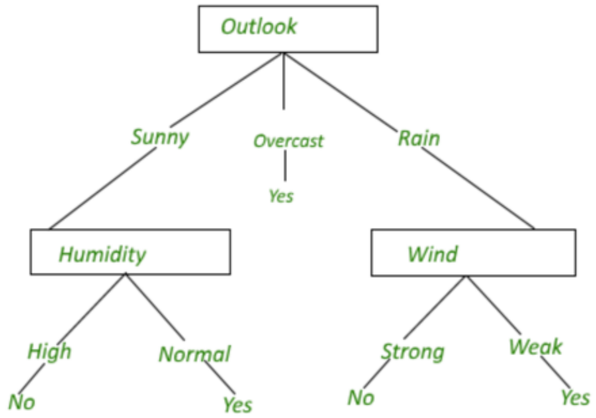
So how we did this :

1. Developed a Machine Learning tool which uses Random Forest Algorithm using TCP Timestamps with a precision of 93.61% and accuracy of 99.67%

2. Developed a tool which analyses webpages to detect the IoT devices and gives manufacturer, model name and firmware version and store these details in a JSON file.

Random Forest Algorithm

- Supervised Learning Approach
- Builds Multiple decision trees and merges them together to to get a more accurate and stable precision



Decision Tree

- Decision Tree generally formulates a set of rules and predicts the result
- The Random Forest algorithm randomly selects observations and features to build several decision trees and then averages the results

NetScanIoT tool

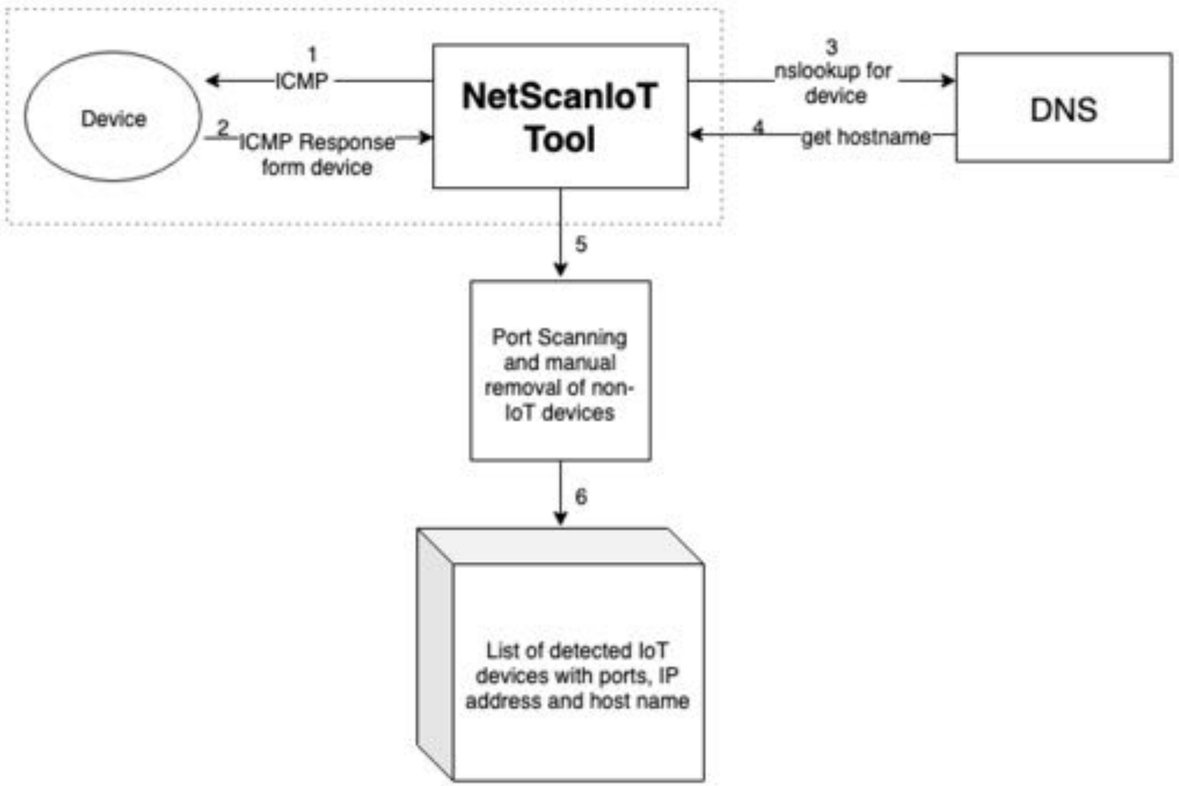
+

Web-IoT Detection (WID) tool

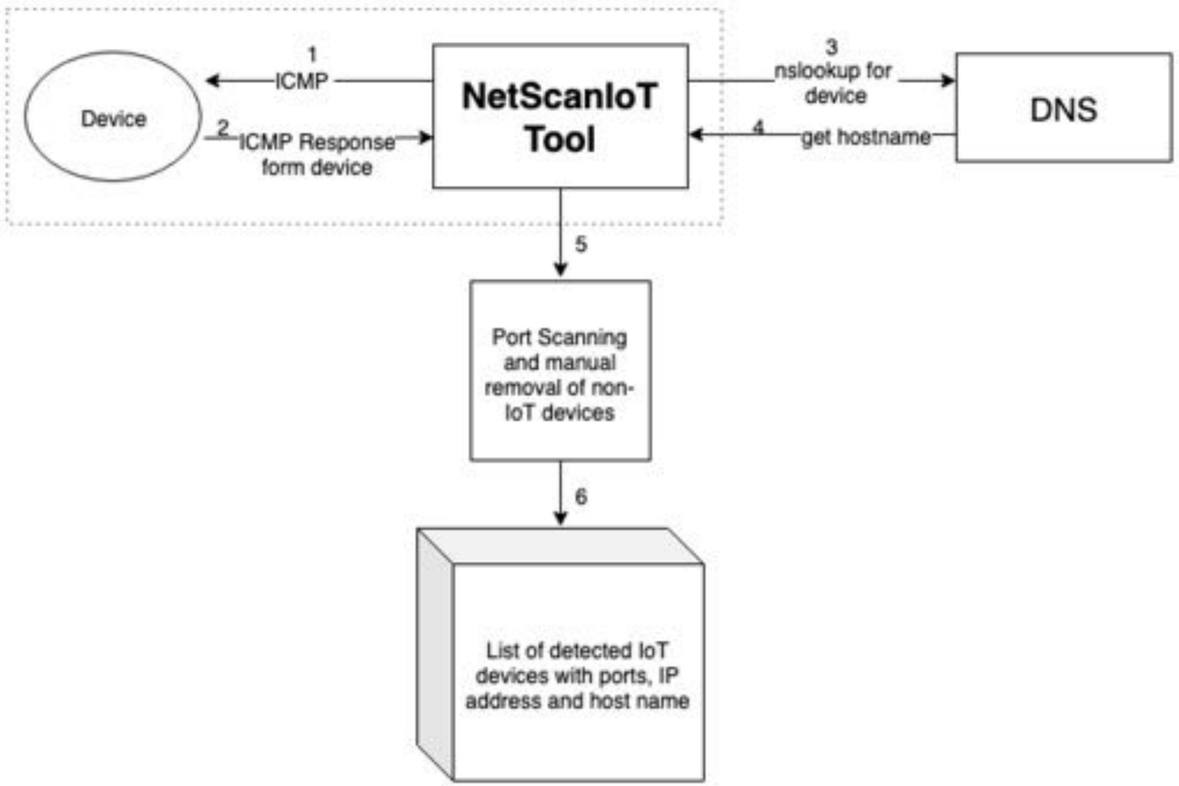
=

IoT device with it’s model, manufacturer and firmware version

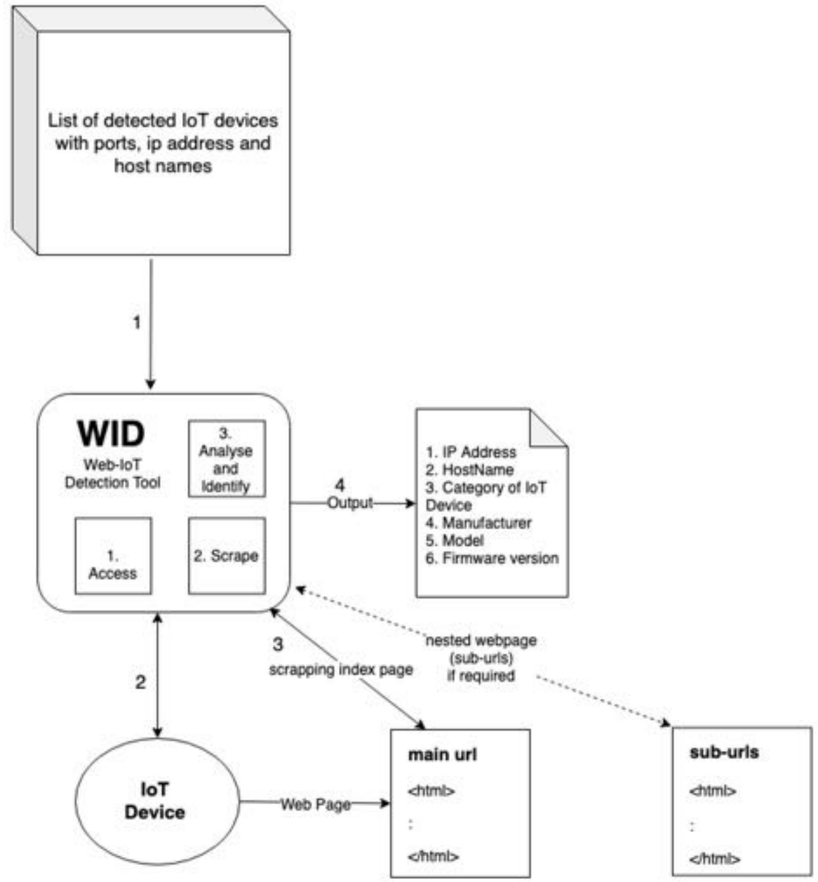
NetScanIoT Tool



NetScanIoT Tool



Web-IoT Detection Tool



Web Analysis for detecting IoT Devices

- Scan the General Purpose Network at CERN to detect the IoT Devices
- After trying a lot of popular web scrapping methods - wget, curl, scrapy, python request package, etc, we found the final solution as selenium with chrome driver
- Analysed a lot (100s) of webpages manually
- Detected the Manufacturer, Model and Firmware version of the device
- Constructed a tool to automate the the output of IoT device detection using BeautifulSoup

Snapshot of our WID tool output

```
sharad:iot_html_analysis SharadAggrawal$ python device_recog.py --ip <ip address>
Matrox Device Found
Firmware: 2.2.0.0008
Model: Monarch HD

classifiers:

<title>
        <device name>
</title>
<span id="ctl00_MainContent_DeviceNameLabel"> <device name> </span>
<span class="MatroxHD">
<img alt="Matrox MonarchHD" src="images/MonarchHDLogoSmall.png" style="float: right"/></span>
http://  <ip address>  /Monarch/About.aspx
<span id="ctl00_MainContent_FirmwareRevisionLabel">2.2.0.0008</span>
sharad:iot_html_analysis SharadAggrawal$
```

Finally after the development of these tools, we worked to predict the Security Risk Score of these IoT Devices

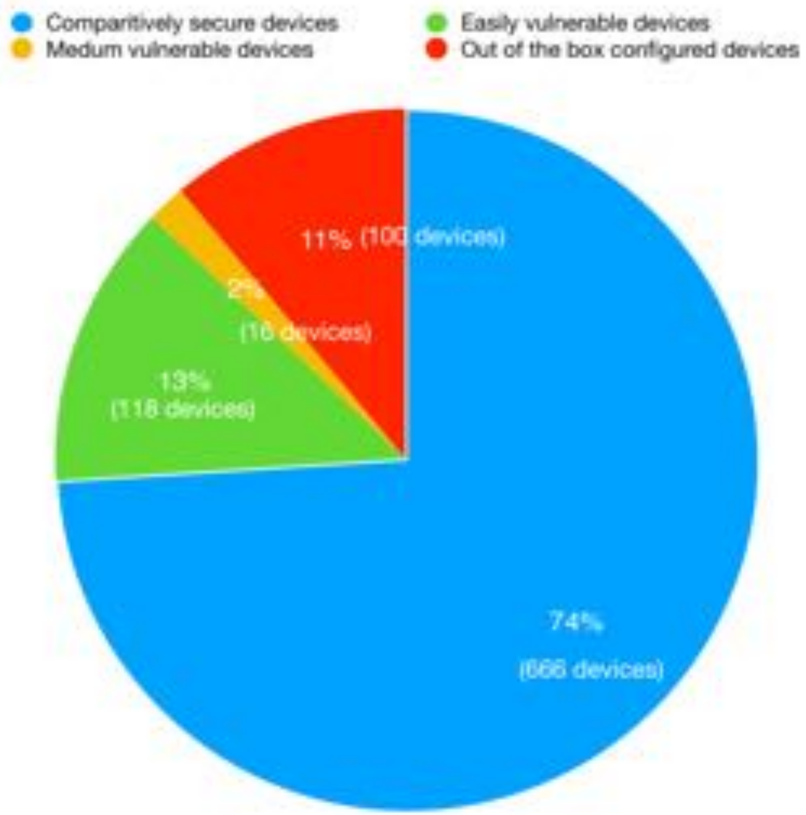
Some statistics from research done at CERN

The current basis is 900 IoT devices, detected to be connected to CERN's General Purpose Network

IoT Devices at CERN
1. Switches
2. Routers
3. Thermometers
4. Programmable logic controllers (PLCs)
5. Close circuit television cameras (CCTVs)
6. Sensors
7. Oscilloscopes
8. Ip phones
9. AnywhereUSBs - network attached USB hubs
10. Network attached storage (NAS) servers
11. Printers
12. Projectors
13. MediaLink controllers (MLCs)
14. Conference microphones and video streaming devices
15. Integrated lights out (iLOs) - HP server management
16. Info screens
17. Power supplies
18. Arduinos
19. Raspberry Pis
20. Intelligent platform management interfaces (IPMIs)

(a)

Vulnerability Classification



(b)


That's it?

Want to know more ?

Checkout our recently published paper here:

https://www.mdpi.com/1424-8220/19/19/4107

sensors

MDPI

Technical Note

Detecting IoT Devices and How They Put Large Heterogeneous Networks at Security Risk

Sharad Agarwal [1,2,*], Pascal Oser [3,4] and Stefan Lueders [3]

1 CMS Experiment, European Organization for Nuclear Research (CERN), 1211 Geneva, Switzerland
2 Department of Physics, University of Wisconsin Madison, Madison, WI 53706, USA
3 CERN Computer Security Team, European Organization for Nuclear Research (CERN), 1211 Geneva, Switzerland; p.oser@cern.ch (P.O.); Stefan.Lueders@cern.ch (S.L.)
4 Institute of Distributed Systems, Ulm University, Helmholtzstraße 16, 89081 Ulm, Germany
* Correspondence: sharad.agarwal@cern.ch; Tel.: +33-769-465-489

Received: 14 August 2019; Accepted: 19 September 2019; Published: 23 September 2019

check for updates

Abstract: The introduction of the Internet of Things (IoT), i.e., the interconnection of embedded devices over the Internet, has changed the world we live in from the way we measure, make calls, print information and even the way we get energy in our offices or homes. The convenience of IoT products, like closed circuit television (CCTV) cameras, internet protocol (IP) phones, and oscilloscopes, is overwhelming for end users. In parallel, however, security issues have emerged and it is essential for infrastructure providers to assess the associated security risks. In this paper, we propose a novel method to detect IoT devices and identify the manufacturer, device model, and the firmware version currently running on the device using the page source from the web user interface. We performed automatic scans of the large-scale network at the European Organization for Nuclear Research (CERN) to evaluate our approach. Our tools identified 233 IoT devices that fell into eleven distinct device categories and included 49 device models manufactured by 26 vendors from across the world.

Keywords: Internet of Things; security; vulnerabilities and protective measures; control network security; operation in multi-user environments; risk assessment

https://github.com/fkie-cad/awesome-embedded-and-iot-security

Awesome Embedded and IoT Security

> A curated list of awesome resources about embedded and IoT security. The list contains software and hardware tools, books, research papers and more.

Botnets like Mirai have proven that there is a need for more security in embedded and IoT devices. This list shall help beginners and experts to find helpful resources on the topic.
If you are a beginner, you should have a look at the Books and Case Studies sections.
If you want to start right away with your own analysis, you should give the Analysis Frameworks a try. They are easy to use and you do not need to be an expert to get first meaningful results.

> *Items marked with ✖ are comercial products.*

Contents

How to contact me:

https://sharad1126.github.io/