



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/>



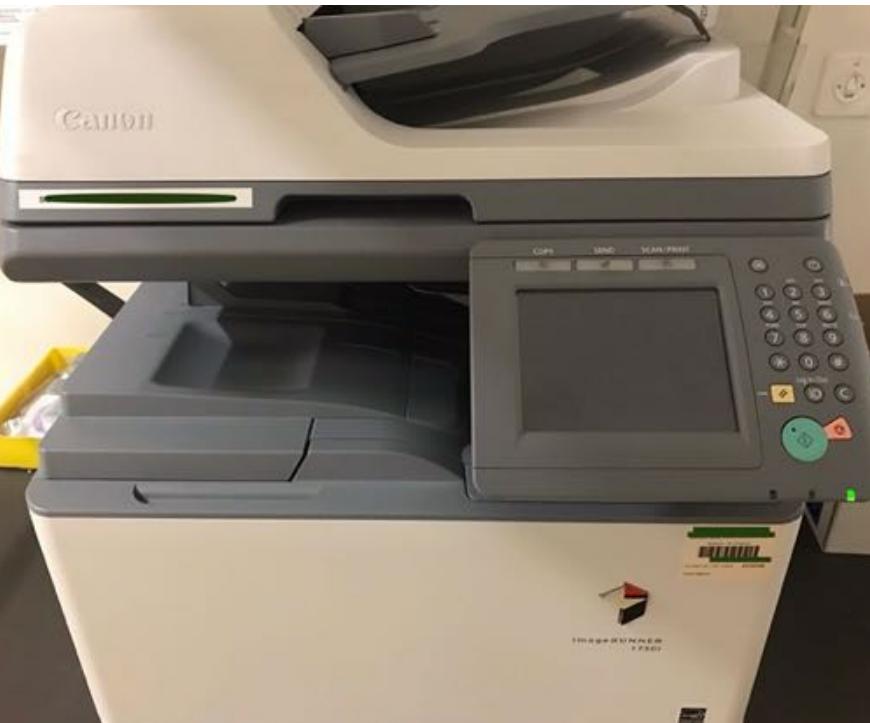
IoT Security

Gurugram Police Summer Internship 2020

Sharad Agarwal
European Organisation for Nuclear Research (CERN)

Internet of Things

where the web meets the physical world



Printer



Access Card Reader



Media Layer Controller



IP Phones

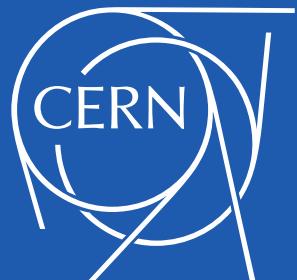


Routers



CCTV Cameras

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



Sharad Agarwal



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

Thermometer - TME - Settings

Network Security E-mail SNMP Sending Sensor Other Info

Temperature

Temperature units Fahrenheit [°F]

Values watch

Maximal value 100

Minimal value 50

Hysteresis 0

Time between the threshold is exceeded and the message is sent 0

Temperature conversion

Temperature from the sensor converts based on following formula: $y = 1 \cdot x + 0$

UNSECURE

Save

File Edit View Search Terminal Help

Home *** Others ***

Device name : (Thermometer)
Maximum value : (+999.9)
Minimum value : (-999.9)
Hysteresis : (+000.0)
TimeDelay : (0) min

Change Setup:
0 Server configuration
1 Network
2 Security
3 Email
4 SNMP
5 HTTP
6 Others
7 factory defaults
8 exit without save
9 save and exit Your choice ? 8

IP Address : () .() .() .()
Set Gateway IP Address (Y) ?
Gateway IP Address : () .() .() .()
Netmask: Number of Bits for Host Part (0=default) (6)
Change telnet config password (N) ?

*** basic parameters
Hardware: Ethernet TPI
IP addr [REDACTED], gateway [REDACTED], netmask 255.255.255.192



Sharad Agarwal

Thermometer - TME - Settings

Network Security E-mail SNMP Sending Sensor Other Info

Temperature

Temperature units Fahrenheit [°F]

Values watch

Maximal value 100

Minimal value 50

Hysteresis 0

Time between the threshold is exceeded and the message is sent 0

Temperature conversion

Temperature from the sensor converts based on following formula: $y = 1 * x + 0$

UNSECURED

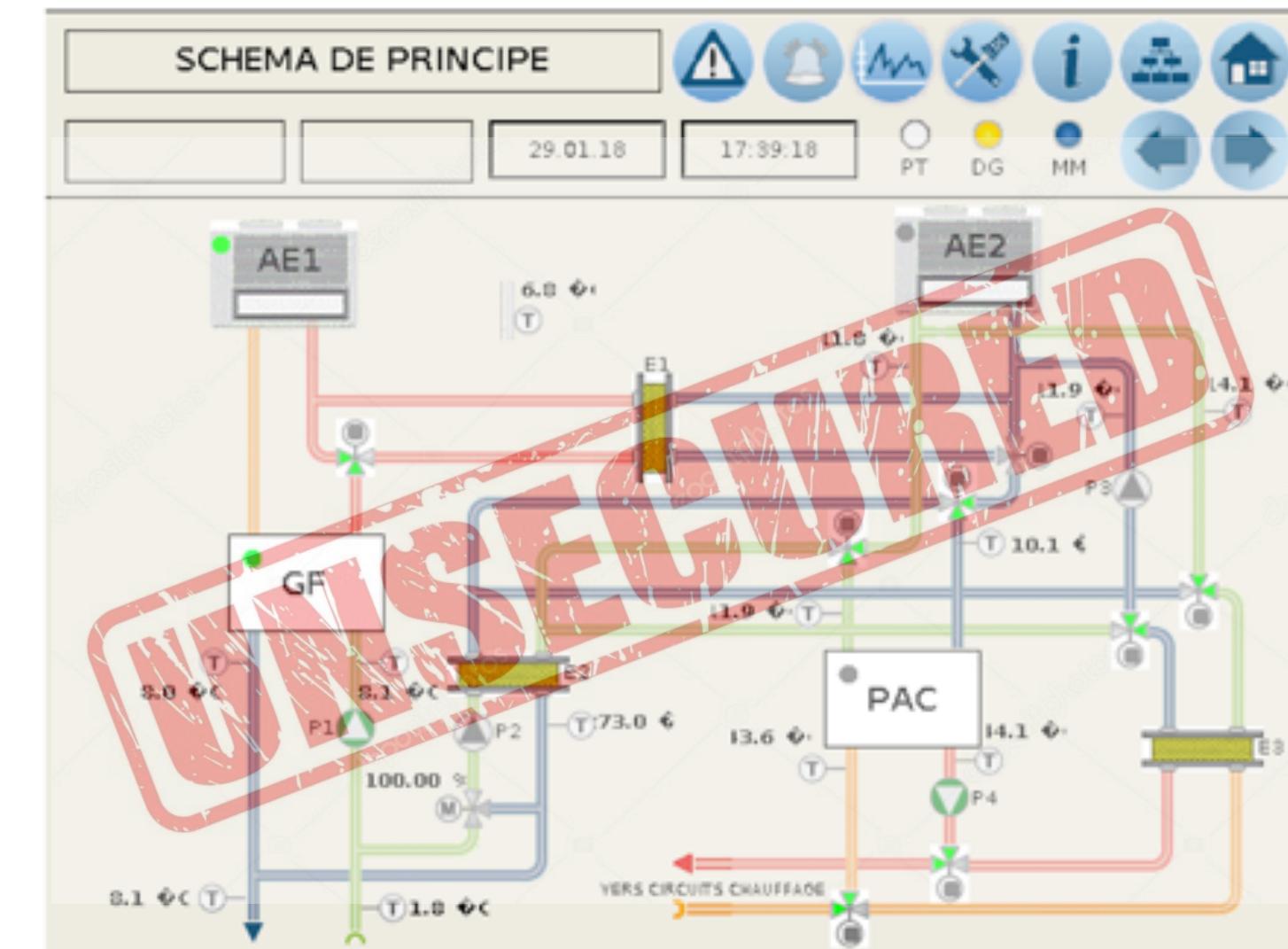
Save

File Edit View Search Terminal Help

Home *** Others *** Device name : (Thermometer) Maximum value : (+999.9) Minimum value : (-999.9) Hysteresis : (+000.0) TimeDelay : (0) min Change Setup: 0 Server configuration 1 Network 2 Security 3 Email 4 SNMP 5 HTTP 6 Others 7 factory defaults 8 exit without save 9 save and exit Your choice ? 8

IP Address : () .() .() .() Set Gateway IP Address (Y) ? Gateway IP Address : () .() .() .() Netmask: Number of Bits for Host Part (0=default) (6) Change telnet config password (N) ?

*** basic parameters Hardware: Ethernet TPI IP addr [REDACTED], gateway [REDACTED], netmask 255.255.255.192



Sharad Agarwal

Thermometer - TME - Settings

Network	Security	E-mail	SNMP	Sending	Sensor	Other	Info
<h2>Temperature</h2>							
Temperature units	Fahrenheit ("F)						
<h3>Values watch</h3>							
Maximal value	100						
Minimal value	50						
Hysteresis	0						
Time between the threshold is exceeded and the message is sent	0						
<h3>Temperature conversion</h3>							
Temperature from the sensor converts based on following formula: $y = 1 \cdot x + 0$							
<input type="button" value="Save"/>							

The screenshot shows a terminal window with a menu bar at the top. The menu bar includes 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. Below the menu bar, there is a red watermark with the word 'REDACTED' repeated twice.

The main area of the terminal displays configuration parameters:

- Device name : (Thermometer)
- Maximum value : (+999.9)
- Minimum value : (-999.9)
- Hysteresis : (+000.0)
- TimeDelay : (0) min

Below these parameters, there is a 'Change Setup:' section with the following options:

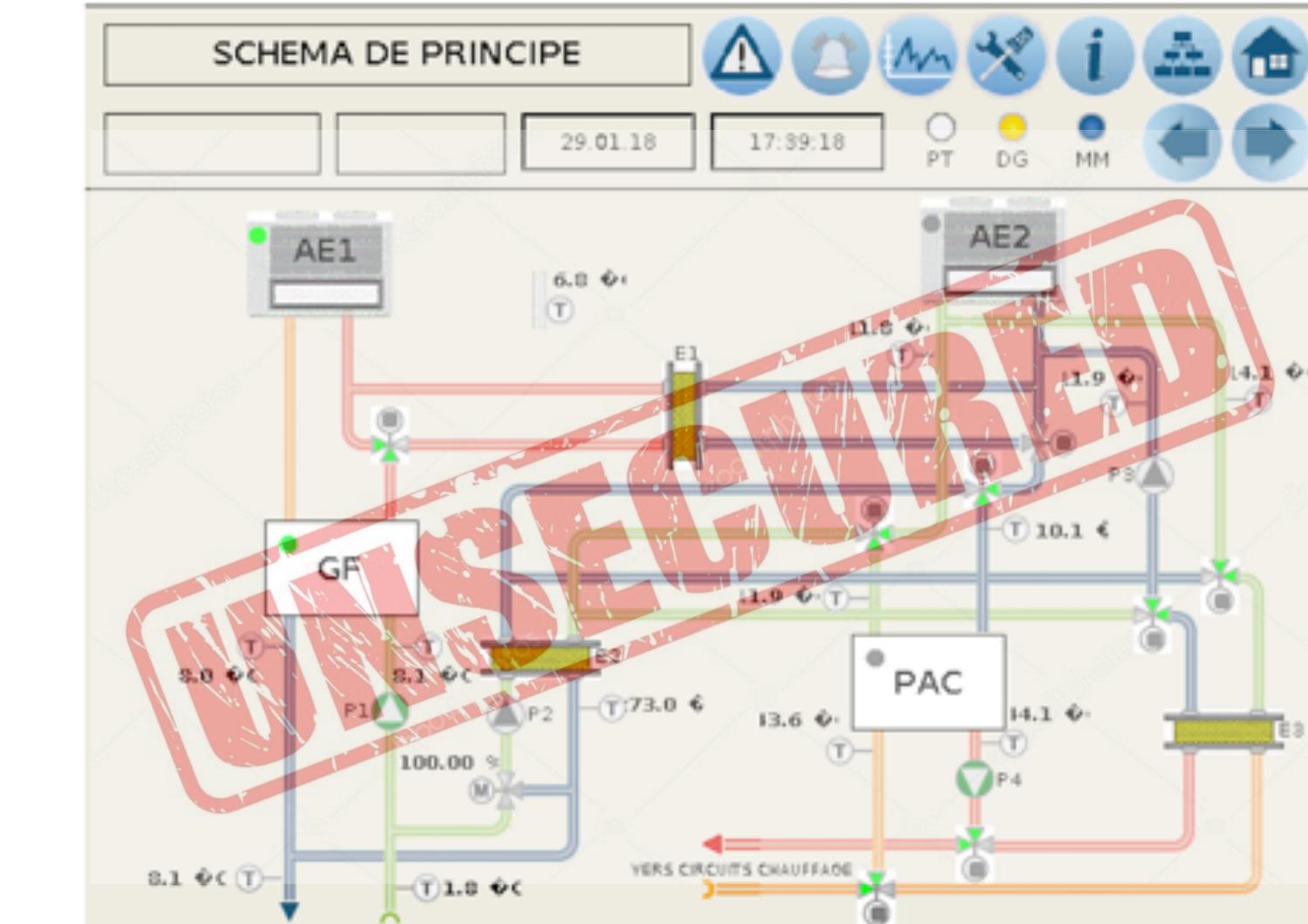
- 0 Server configuration
- 1 Network
- 2 Security
- 3 Email
- 4 SNMP
- 5 HTTP
- 6 Others
- 7 factory defaults
- 8 exit without save
- 9 save and exit

To the right of the setup options, the text 'Your choice ? 0' is displayed.

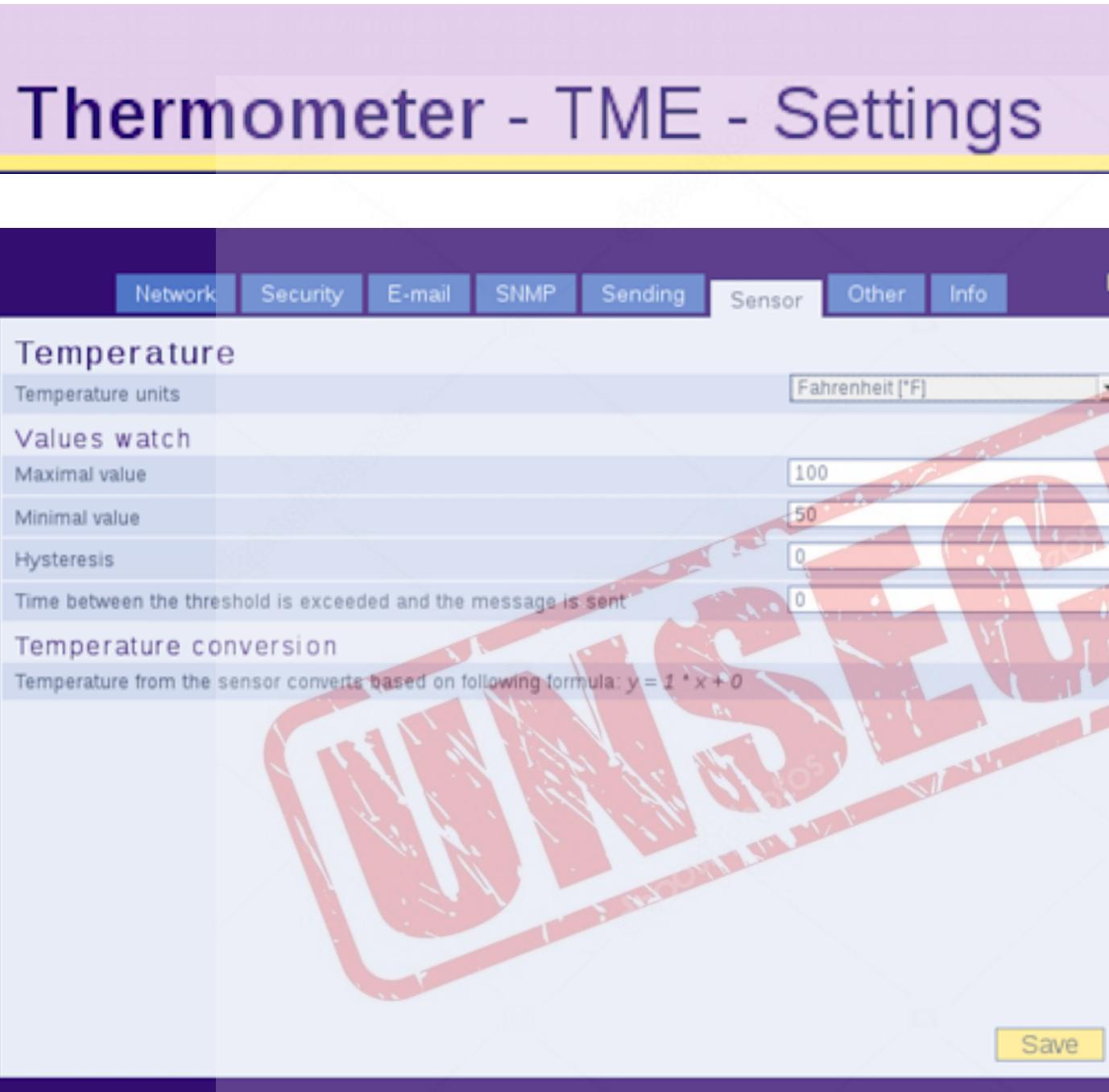
At the bottom of the terminal window, several configuration prompts are shown:

- IP Address : () .() .() .()
- Set Gateway IP Address (Y) ?
- Gateway IP Address : () .() .() .()
- Netmask: Number of Bits for Host Part (0=default) (6)
- Change telnet config password (N) ?

At the very bottom of the window, the text '*** basic parameters' is followed by 'Hardware: Ethernet TPI' and 'IP addr [REDACTED], gateway [REDACTED], netmask 255.255.255.'

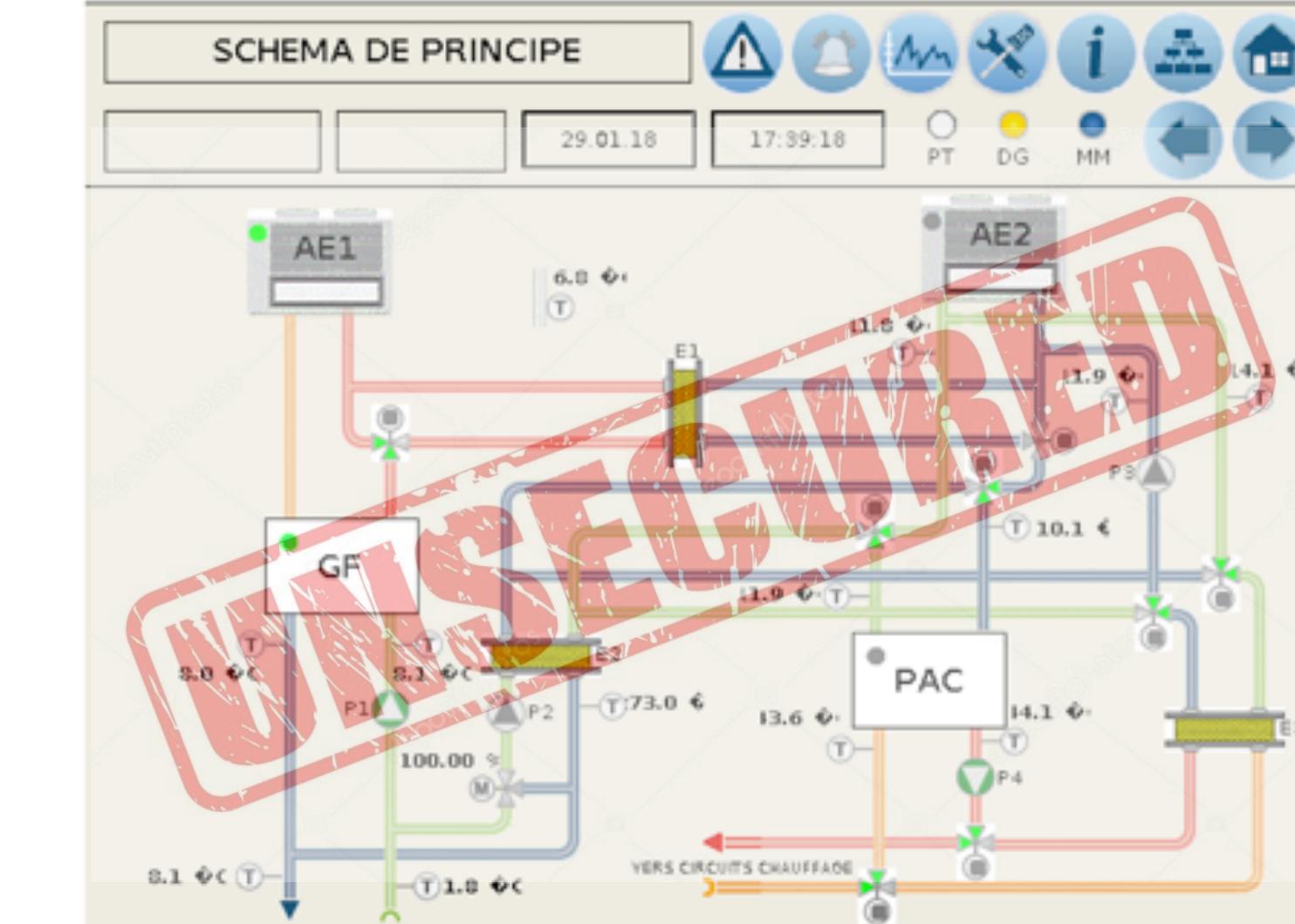


Sharad Agarwal



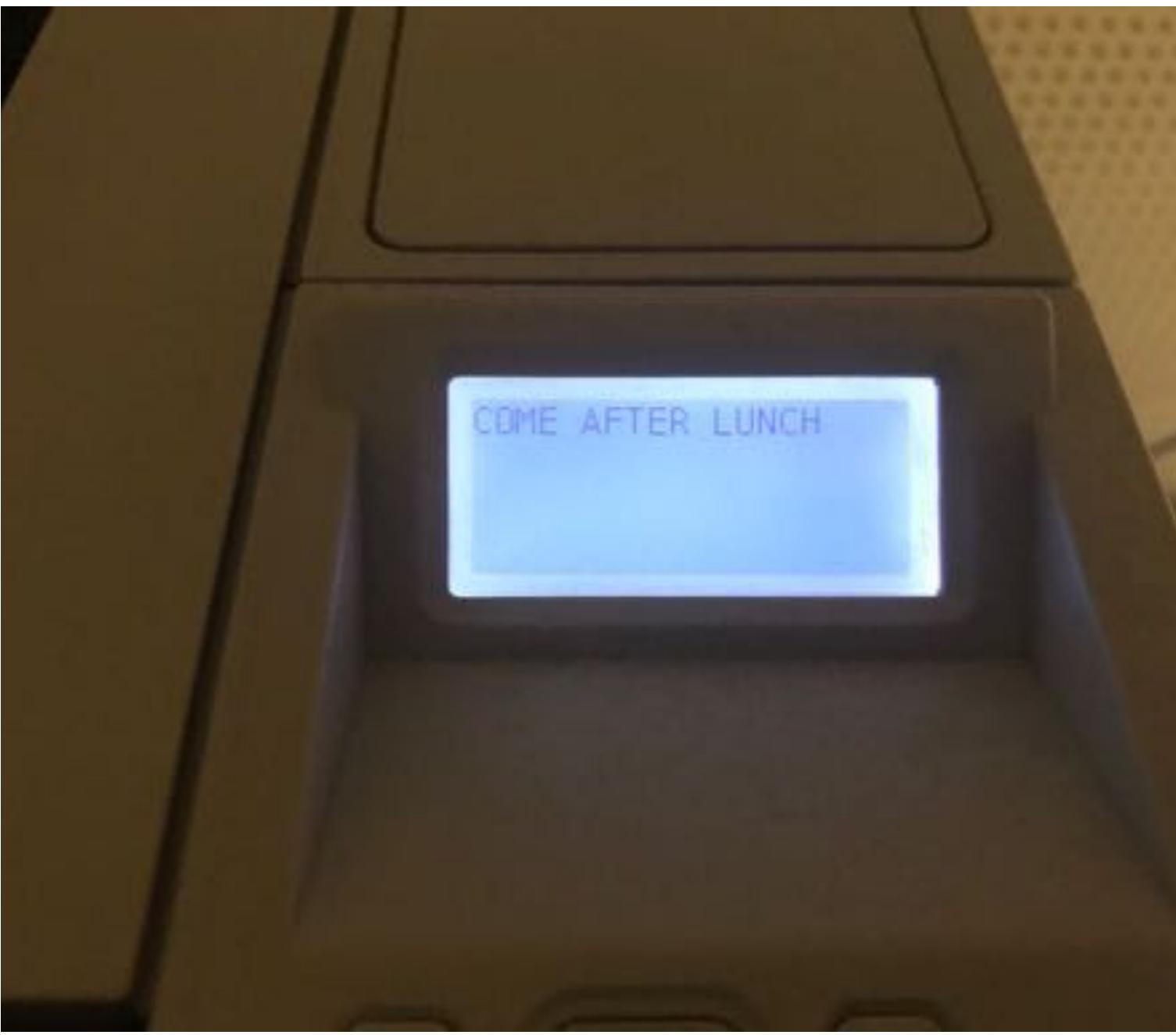
```
File Edit View Search Terminal Help
Home *** Others ***
Device name : (Thermometer)
Maximum value : (+999.9) at 25.48 ( http://rasp.org ) at
Minimum value : (-999.9) If it goes down, if it is really up,
Hysteresis : (+000.0) If IP address (0 hosts up) scan
TimeDelay : (0) min
Change Setup:
0 Server configuration
1 Network
2 Security
3 Email
4 SNMP
5 HTTP
6 Others
7 factory defaults
8 exit without save
9 save and exit Your choice ? 8
IP Address : ( ) .( ) .( ) .( )
Set Gateway IP Address (Y) ?
Gateway IP Address : ( ) .( ) .( ) .( )
Netmask: Number of Bits for Host Part (0=default) (6)
Change telnet config password (N) ?

*** basic parameters
Hardware: Ethernet TPI
IP addr [REDACTED], gateway [REDACTED], netmask 255.255.255.192
```



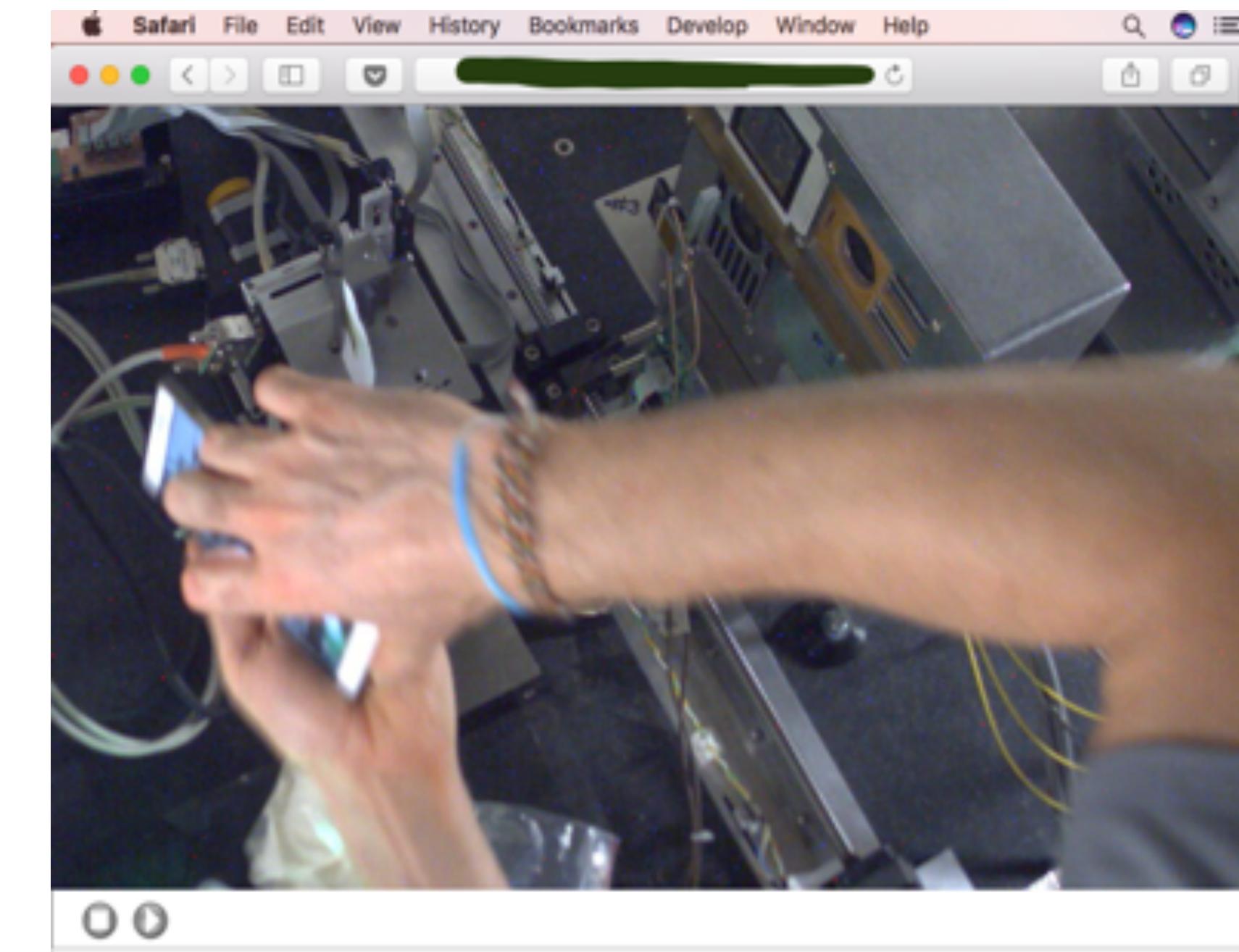
Devices like thermometers
oscilloscopes, programmable logic
controllers, used in physics organizations
should be secured.

Sharad Agarwal

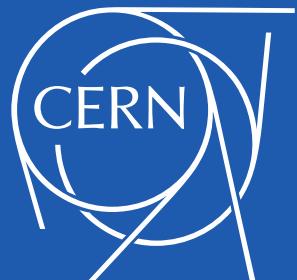


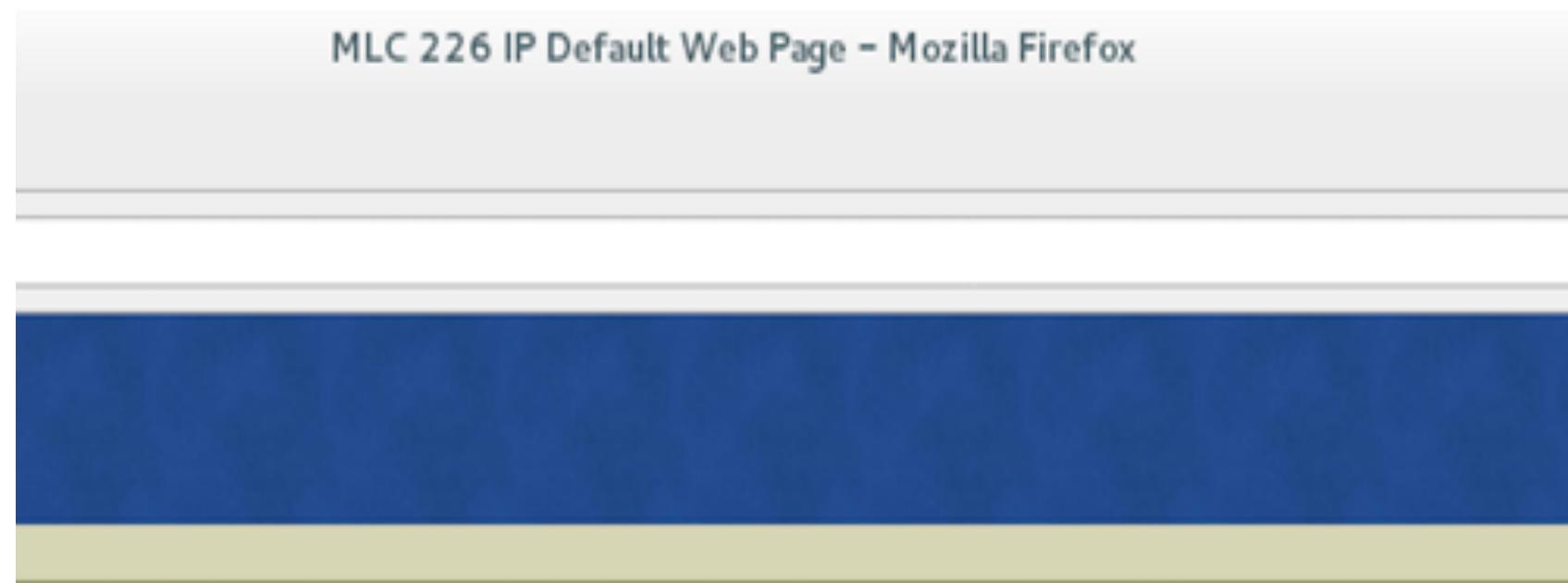
Printers - where I was able to write anything on the display screen

Real time streaming
CCTV Camera

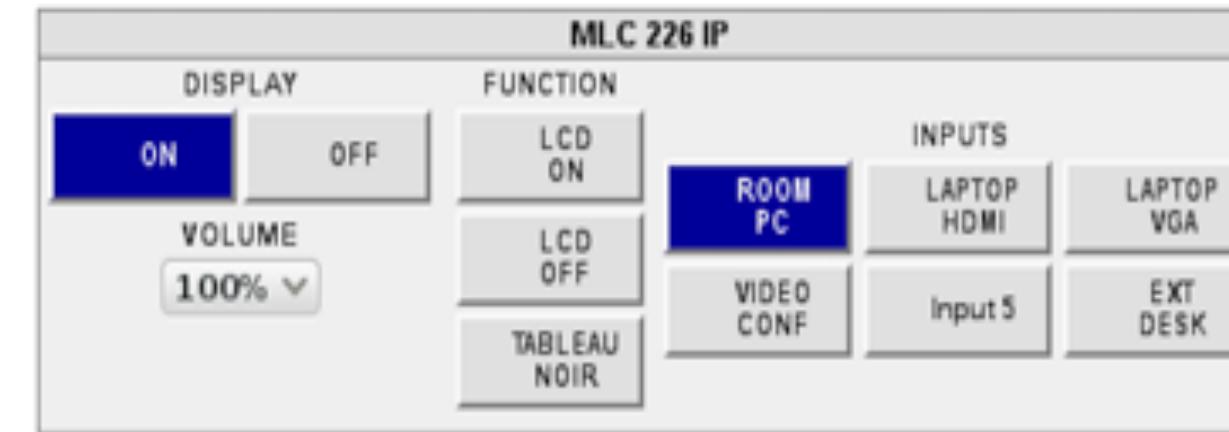


Sharad Agarwal



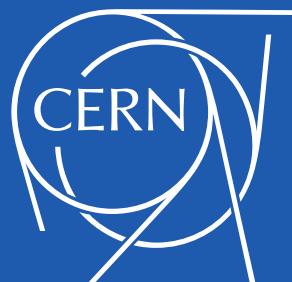


Conference room controllers



IP Phone

A screenshot of a web browser window showing the configuration page for an IP phone. The title bar says 'IP Phone - Mozilla Firefox'. The main content area displays various network settings, including 'Status' (Firmware Version: 7.4.0.1, Hardware Version: 8.0.0.1), 'Network' (WAN Port Type: AutoConfiguration Via DHCP, WAN IP Address: [redacted], Subnet Mask: 255.255.255.0, MAC Address: [redacted], Link Status: Connected, PC IP Address: 192.168.1.10, Device Type: Bridge, DHCP Server: Enabled), and 'Logs' (IP Log: [redacted]). The page has a green header bar with the 'Well' logo.



Sharad Agarwal

Non Configured Devices



Sharad Agarwal

Product Page: DAP-1665 Hardware Version: A1 / Firmware Version: 1.11

D-Link

Wi-Fi CONNECTION SETUP WIZARD

This wizard is designed to assist you in your Wi-Fi network setup. It will guide you through step-by-step instructions on how to set up your Wi-Fi network and how to make it secure.

Next Cancel

WIRELESS

Copyright © 2014 D-Link Corporation/D-Link Systems, Inc.

Set a stronger password

admin

New password

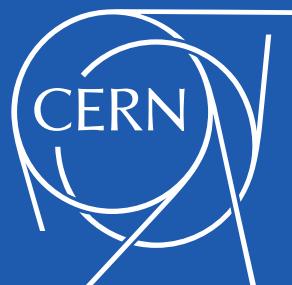
Confirm password

admin is the default username. The minimal recommended length is 8 characters.

Access Point

NAS

Sharad Agarwal



Easily Vulnerable Devices



Sharad Agarwal

The screenshot shows the Yealink web-based management interface. On the left, there's a sidebar with links like 'Local phone list', 'Remote Phone Book', 'Call history', 'LDAP', 'MulticastIP', and 'Settings'. The main area has tabs for 'Call panel' (with fields for 'Dial a number' and 'Output ID'), 'History' (with a search bar), and 'Logs'. Under 'Logs', there are four sections: 'Called' (5 entries), 'Missed' (4 entries), 'Received' (4 entries), and 'Redirected' (1 entry). Each section has columns for 'Index', 'Date', 'Time', 'Local ID', 'Name', and 'Number'. At the bottom left, it says 'Copyright © 2009-2012 ** Inc. All Rights Reserved.'

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

Projectors used in meeting rooms

The screenshot shows the EPSON Projector Control software. The main window is titled 'EPSON' and has a tab for 'Image'. It includes sections for 'Signal' (selected), 'Settings', 'Info', 'Schedule', 'Network', and 'RGB' and 'RGBCY' color calibration controls. On the right, there's a sidebar with 'Power' (on/off), 'Search', 'Source' (with icons for input sources), and 'Operation' (with icons for volume, brightness, and other controls). A small window titled 'EBF02552 Web Rom...' is also visible.

Sharad Agarwal

SCHEMA DE PRINCIPE

AE1 AE2 GF PAC

6.0 °C 11.8 °C 11.9 °C 14.1 °C

11.8 °C 11.9 °C 10.1 °C 14.1 °C

13.6 °C 73.0 °C 14.1 °C

VERS CIRCUITS CHAUFFAGE

29.01.18 17.09.18

PT DG MM

D-Cerno

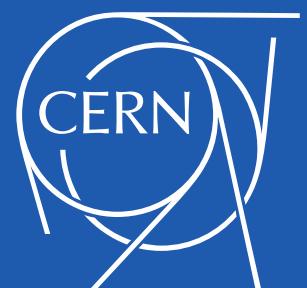
Volume

Recorder Configuration Info

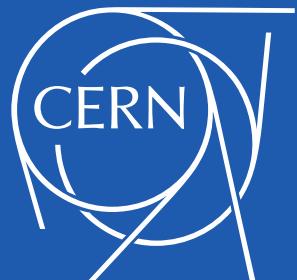


And Many More

Sharad Agarwal

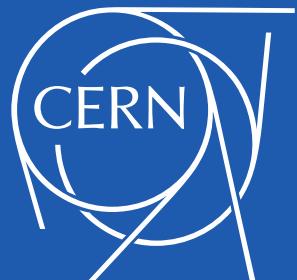


Medium Vulnerable Devices



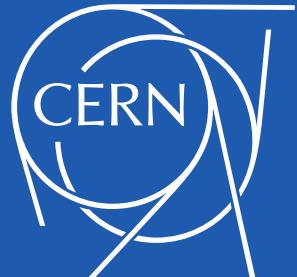
Sharad Agarwal

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



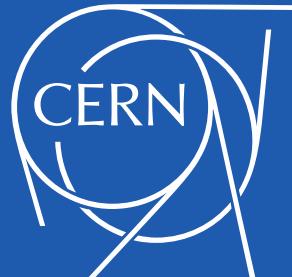
Sharad Agarwal

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



Sharad Agarwal

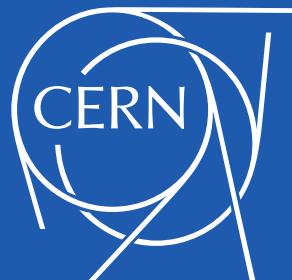
We have developed a tool that detects IoT Devices and provides model, manufacturer, and firmware details which will be used to predict the security risk score for an IoT device



Sharad Agarwal

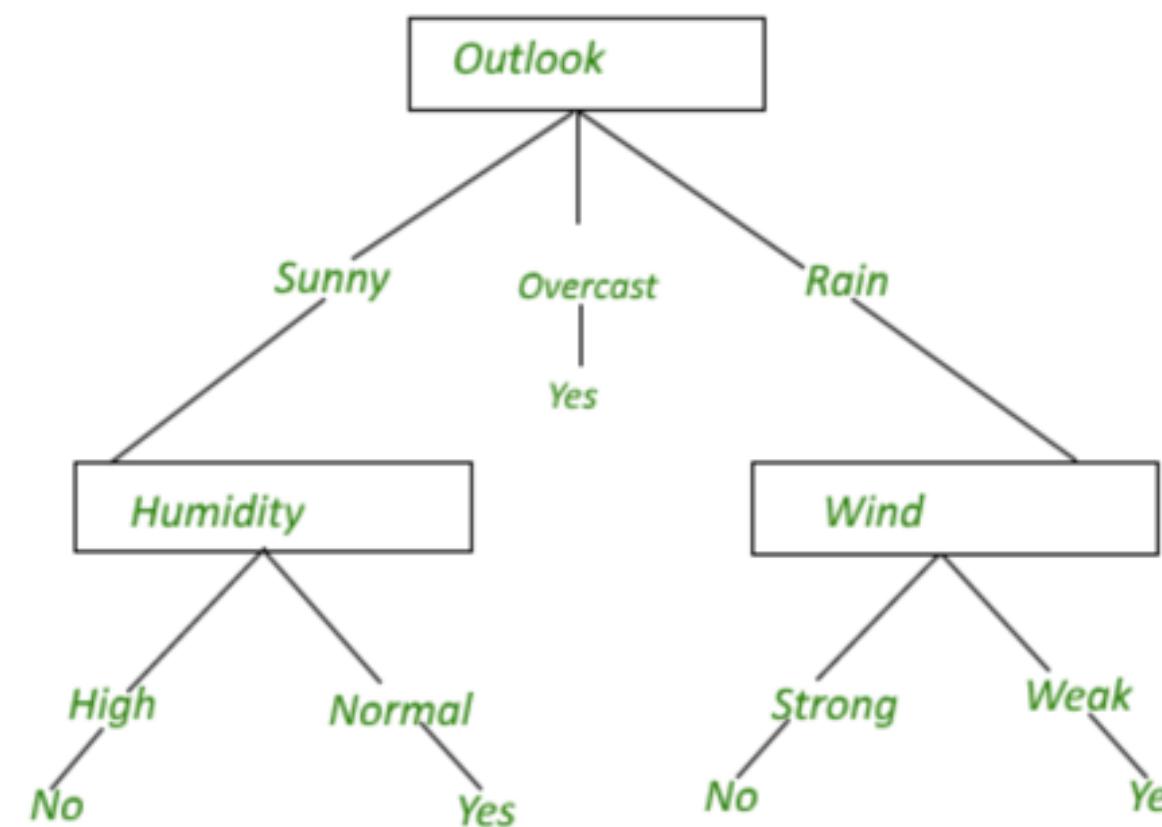
So how we did this :

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 get a more accurate and stable precision



- 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

Decision Tree

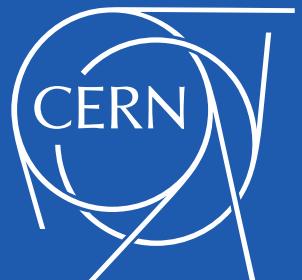
NetScanIoT tool

+

Web-IoT Detection (WID) tool

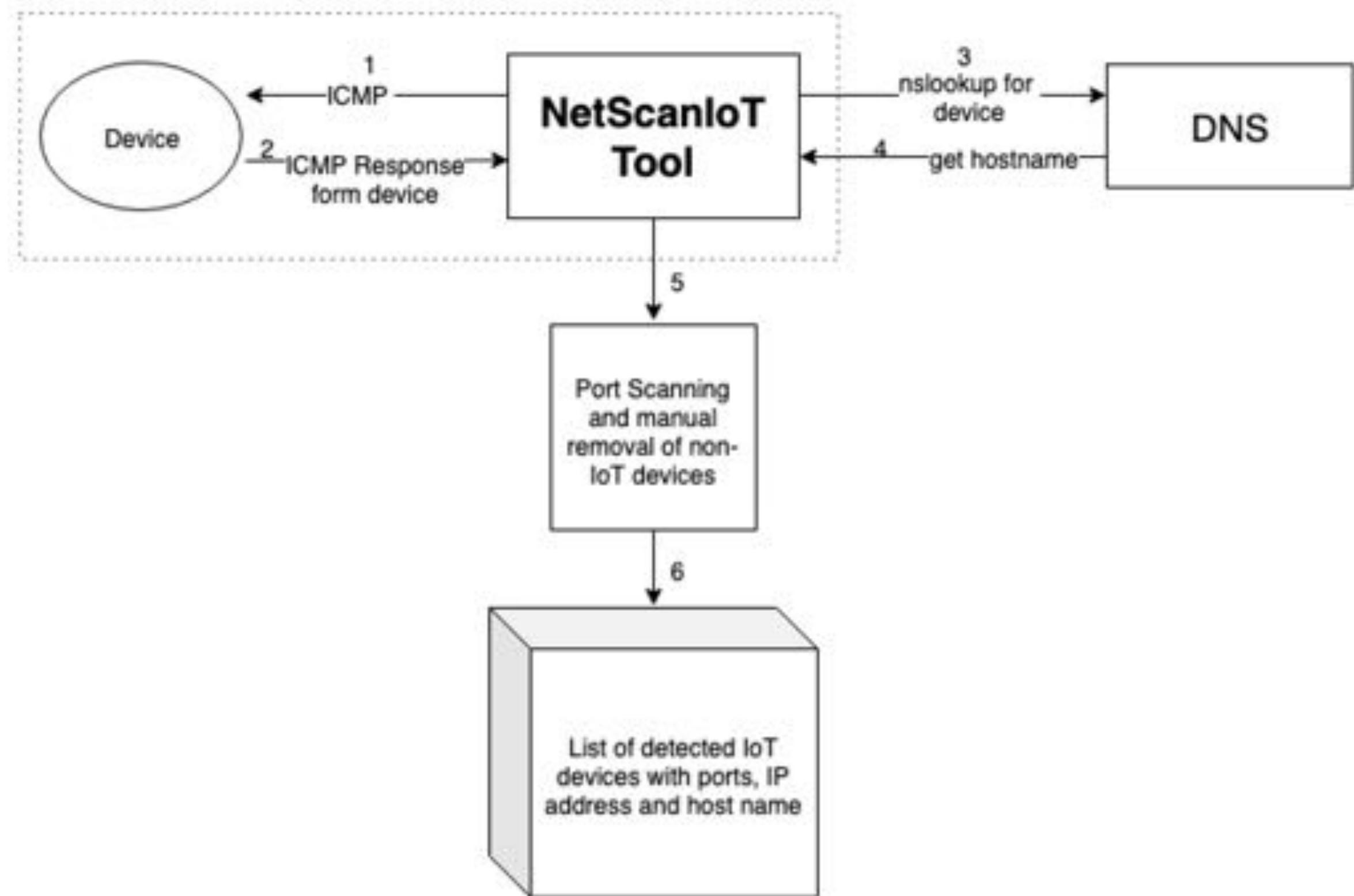
=

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

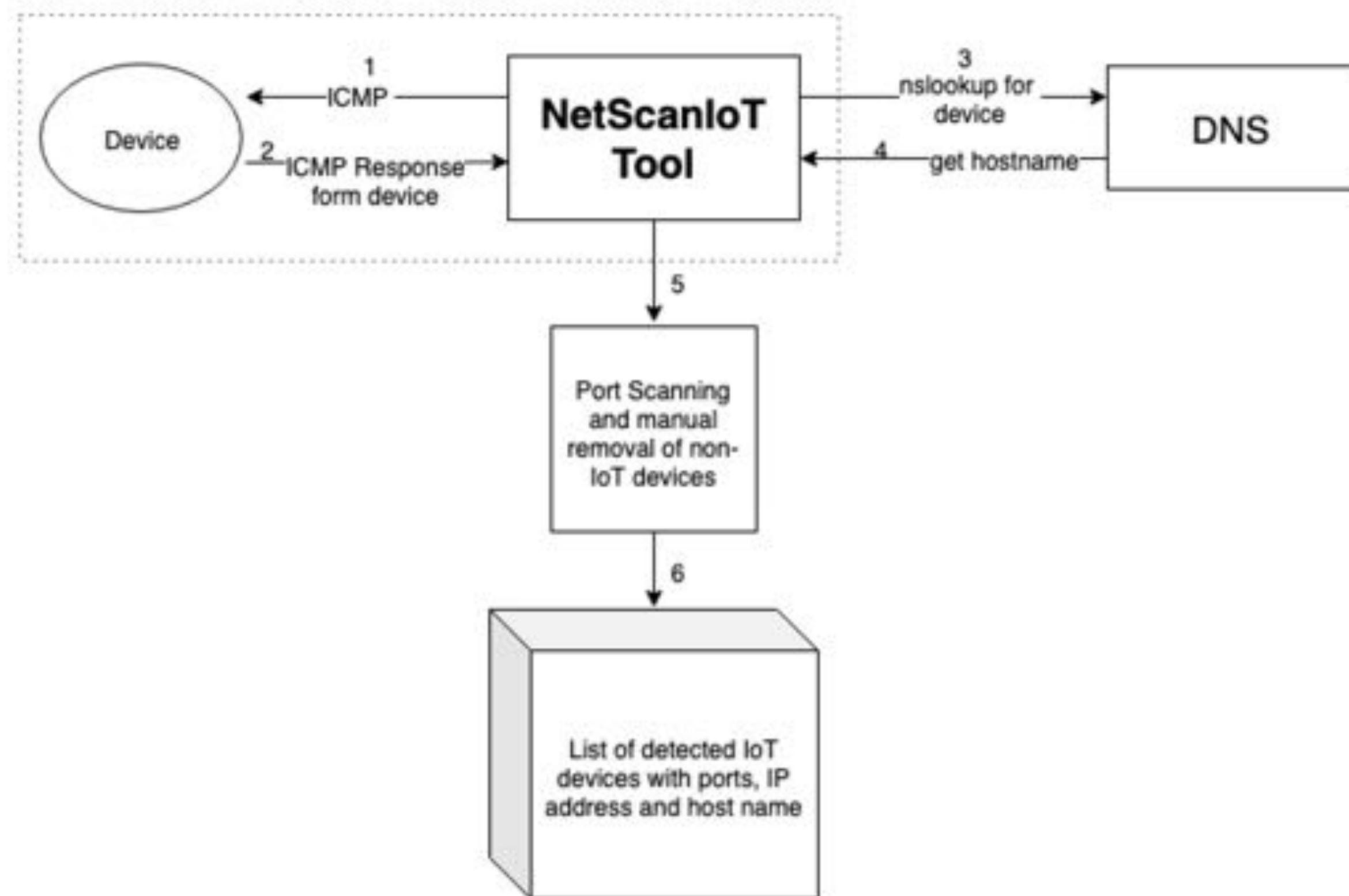


Sharad Agarwal

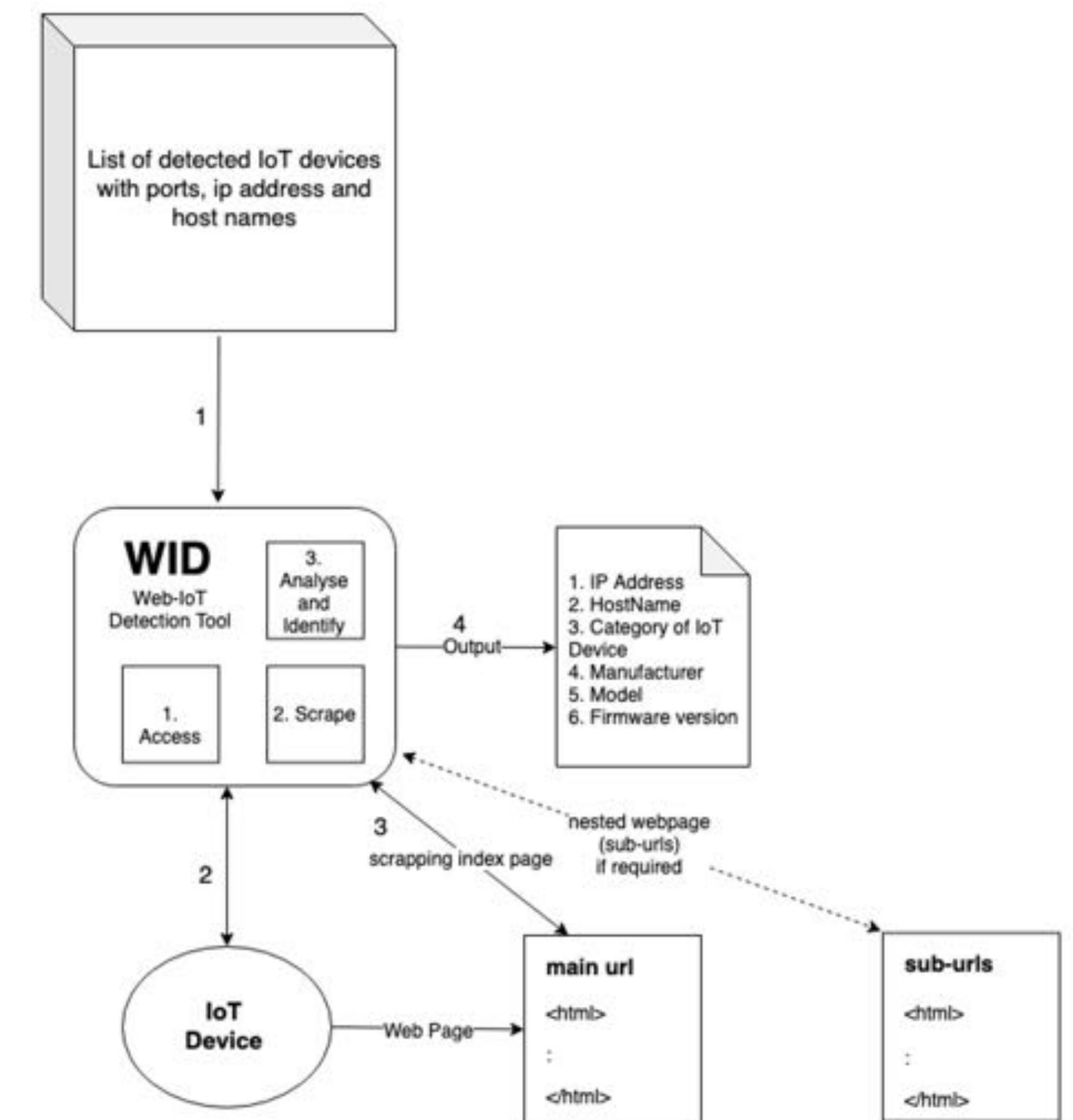
NetScanIoT Tool



NetScanIoT Tool

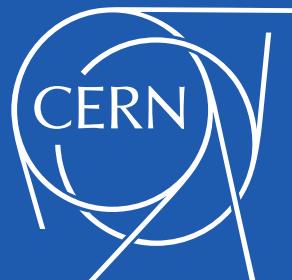


Web-IoT Detection Tool



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

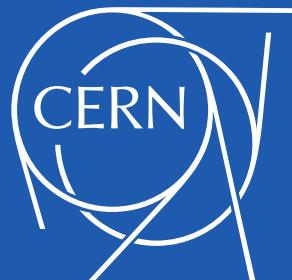


Snapshot of our WID tool output

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

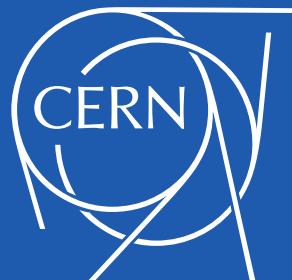
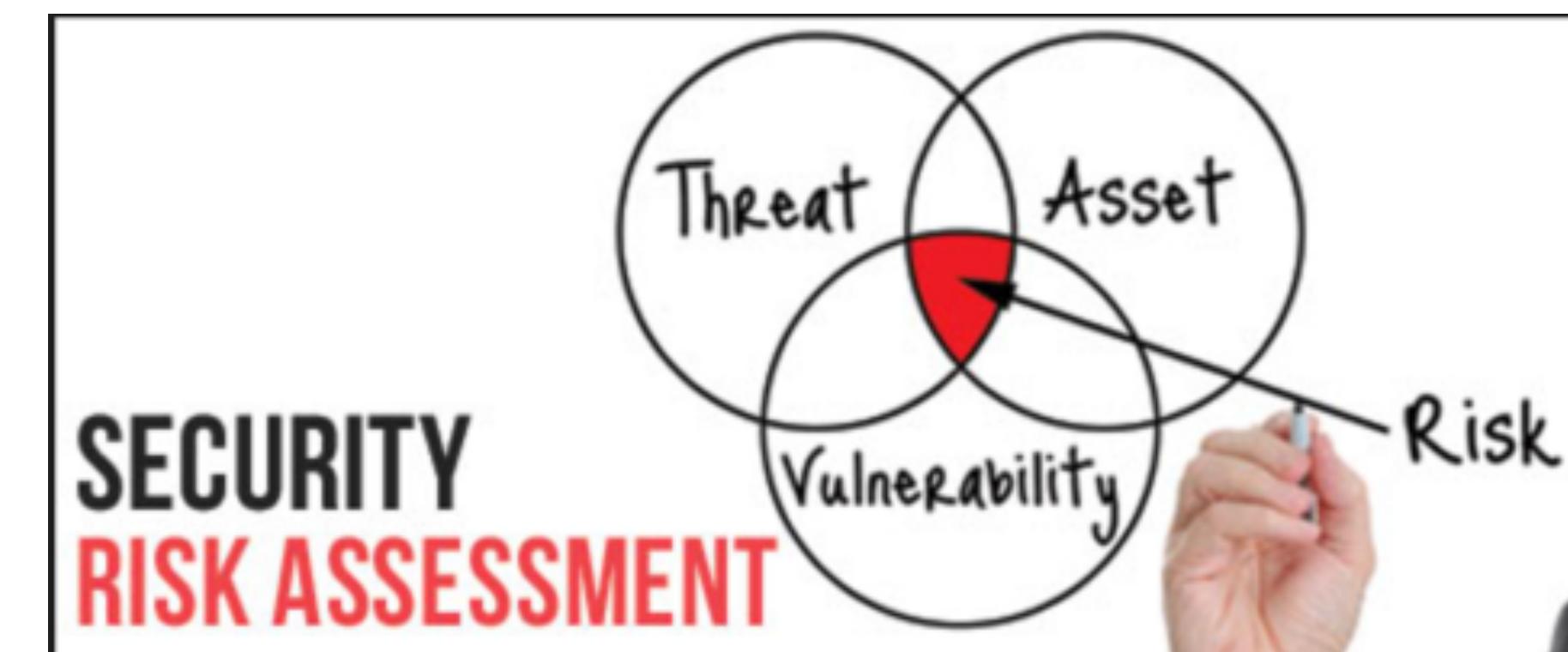
classifiers:

<title>
    <device name>
</title>
<span id="ctl00_MainContent_DeviceNameLabel"> <device name> </span>
<span class="MatroxHD">
</span>
http:// <ip address> /Monarch/About.aspx
<span id="ctl00_MainContent_FirmwareRevisionLabel">2.2.0.0008</span>
sharad:iot_html_analysis SharadAggrawal$
```



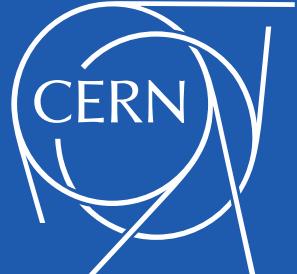


Finally after the development of these tools, we worked to predict the Security Risk Score of these IoT Devices



Sharad Agarwal

Some statistics from research done at CERN



Sharad Agarwal

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

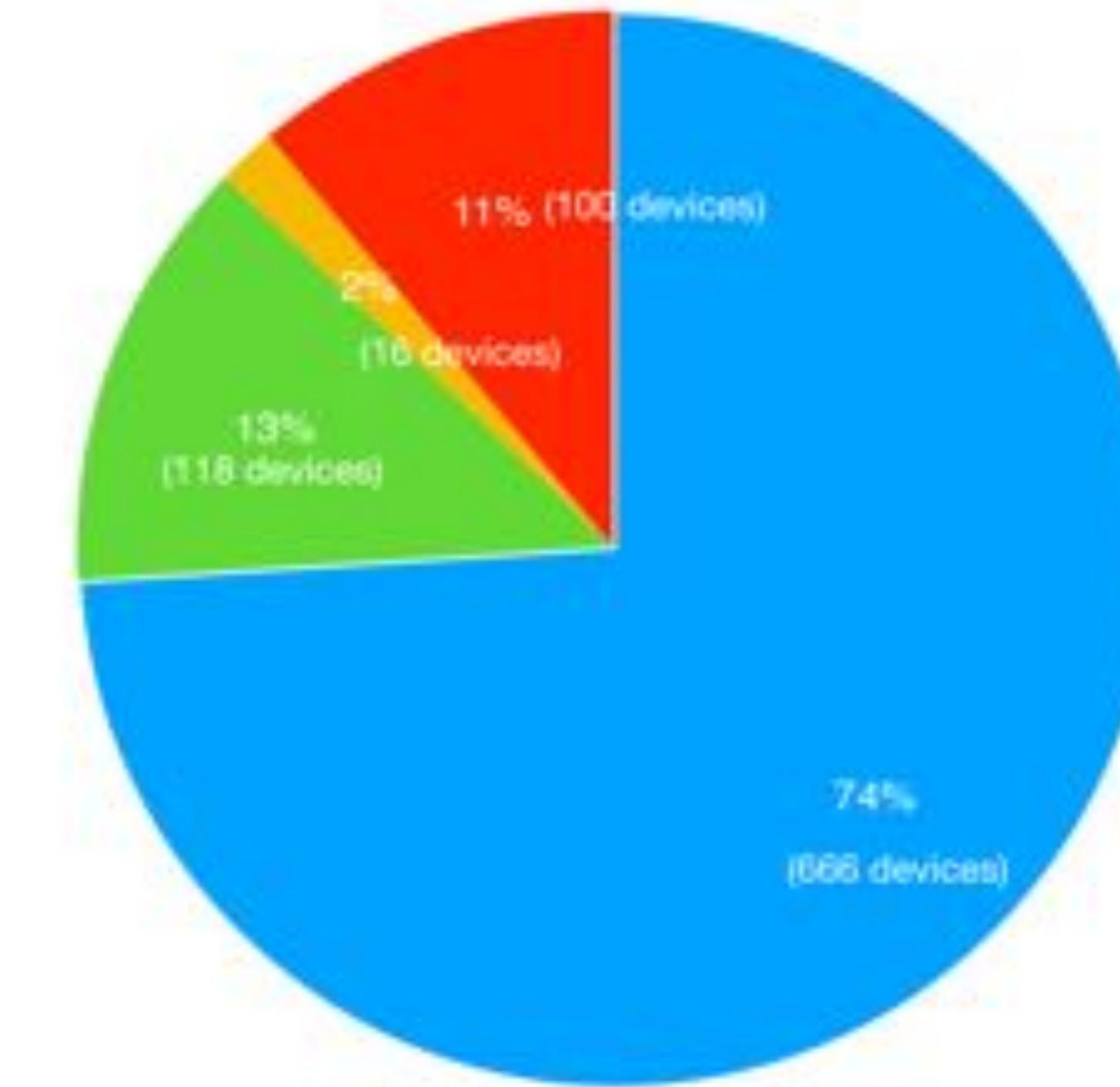
Vulnerability Classification

IoT Devices at CERN

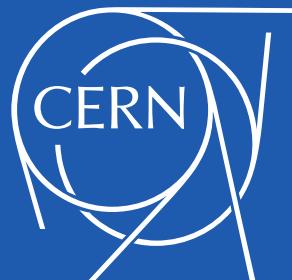
1. Switches
2. Routers
3. Thermometers
4. Programmable logic controllers (PLCs)
5. Close circuit television cameras (CCTVs)
6. Sensors
7. Oscilloscopes
8. Ip phones
9. AnywhereUSBs - network attached USB hubs
10. Network attached storage (NAS) servers
11. Printers
12. Projectors
13. MediaLink controllers (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)

● Comparitively secure devices
● Medium vulnerable devices
● Easily vulnerable devices
● Out of the box configured devices



(b)



Sharad Agarwal



Sharad Agarwal

Want to know more ?

Checkout our
recently published paper
here:

[https://www.mdpi.com/
1424-8220/19/19/4107](https://www.mdpi.com/1424-8220/19/19/4107)



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

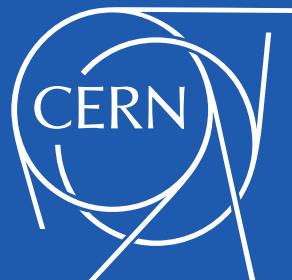
* Correspondence: sharad.agarwal@cern.ch; Tel.: +33-769-465-489

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



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



Sharad Agarwal

<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.

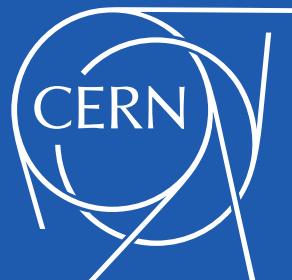
If you are a beginner, you should have a look at the [Books](#) and [Case Studies](#) sections.

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 commercial products.

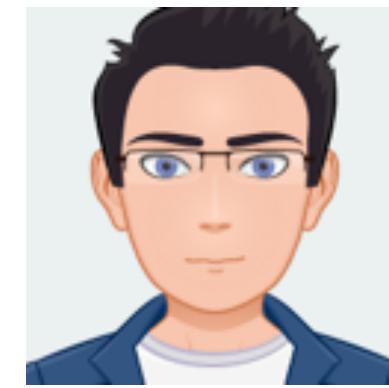
Contents

- [Software Tools](#)
 - [Analysis Frameworks](#)
 - [Analysis Tools](#)
 - [Extraction Tools](#)
 - [Support Tools](#)
 - [Misc Tools](#)
- [Hardware Tools](#)
 - [Bluetooth BLE Tools](#)
 - [ZigBee Tools](#)
 - [SDR Tools](#)
 - [RFID NFC Tools](#)
- [Books](#)
- [Research Papers](#)
- [Case Studies](#)
- [Free Training](#)
- [Websites](#)
 - [Blogs](#)
 - [Tutorials and Technical Background](#)
- [Conferences](#)

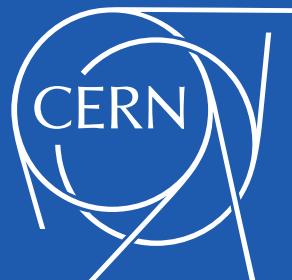


Sharad Agarwal

How to contact me:



<https://sharad1126.github.io/>



Sharad Agarwal