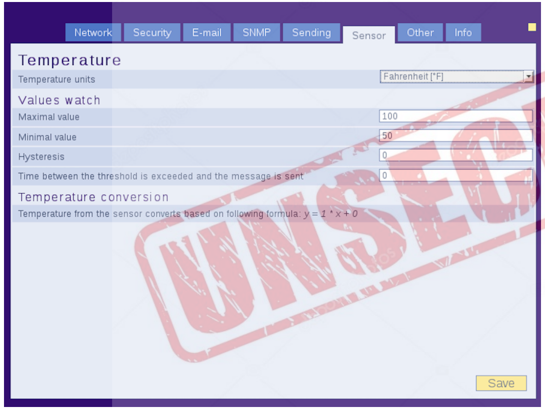
Detecting IoT Devices and How They Put Large Heterogeneous Networks at Security Risk

Sharad Agarwal (University of Wisconsin Madison and CERN)
Pascal Oser (Ulm University and CERN)
Dr Stefan Lüders (CERN)

IoT Security in Large Academic Organizations

Thermometer - TME - Settings



Temperature

Temperature units: Fahrenheit [°F]

Values watch

Maximal value: 100

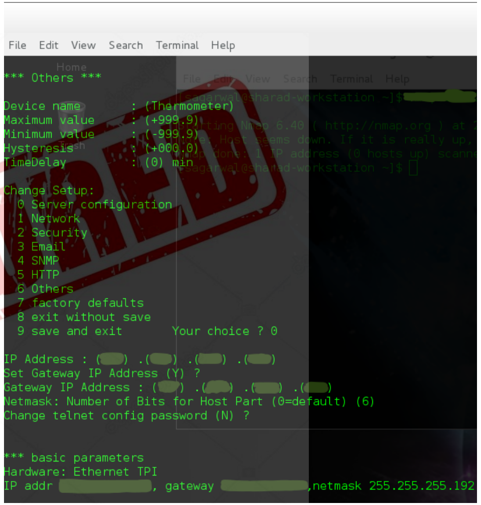
Minimal value: 50

Hysteresis: 0

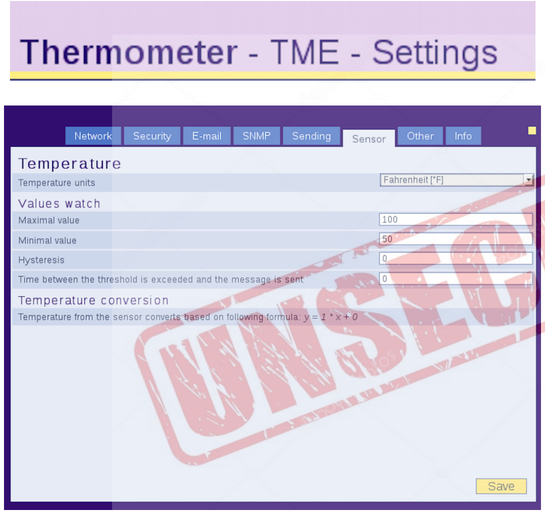
Time between the threshold is exceeded and the message is sent: 0

Temperature conversion

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



```
*** 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 ? 0

IP Address : ([redacted]) .([redacted]) .([redacted]) .([redacted])
Set Gateway IP Address (Y) ?
Gateway IP Address : ([redacted]) .([redacted]) .([redacted]) .([redacted])
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
```



Thermometer - TME - Settings

Temperature

Temperature units: Fahrenheit [°F]

Values watch

Maximal value: 100

Minimal value: 50

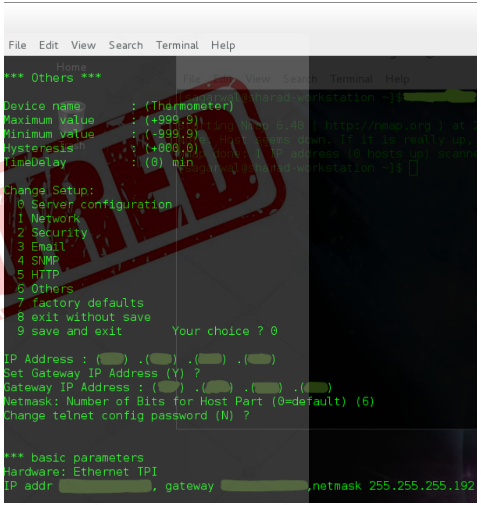
Hysteresis: 0

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

Temperature conversion

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

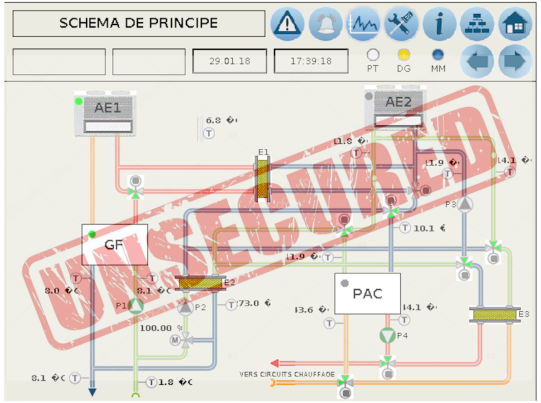
UNSECURED

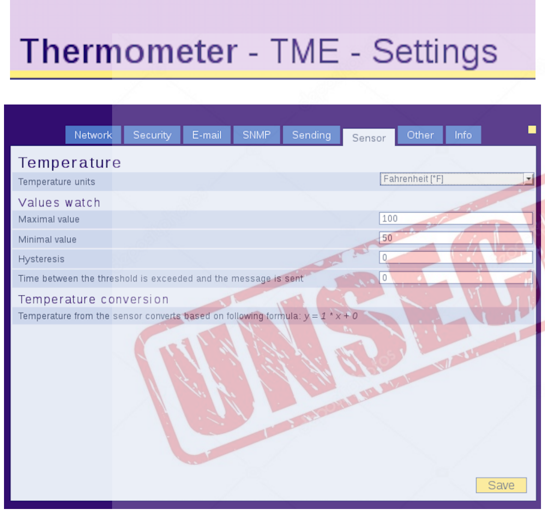


```
*** Others ***

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 ? 0

IP Address : ([redacted]) .([redacted]) .([redacted]) .([redacted])
Set Gateway IP Address (Y) ?
Gateway IP Address : ([redacted]) .([redacted]) .([redacted]) .([redacted])
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
```

```
[sagarwal@sharad-workstation ~]$ [redacted]
Starting Nmap 6.40 ( http://nmap.org ) at
Note: Host seems down. If it is really up,
Nmap done: 1 IP address (0 hosts up) scanne
[sagarwal@sharad-workstation ~]$
```

UNSECURED





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

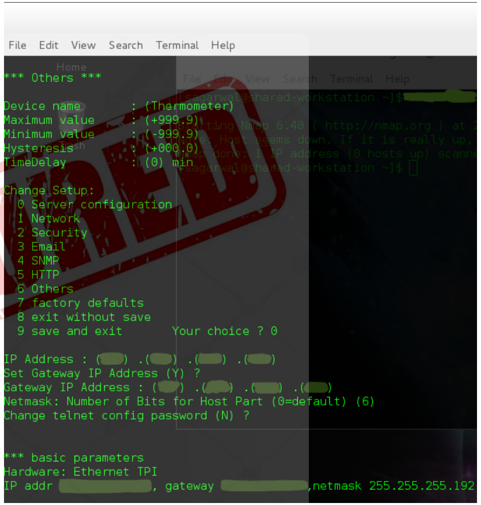
Hysteresis: 0

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

Temperature conversion

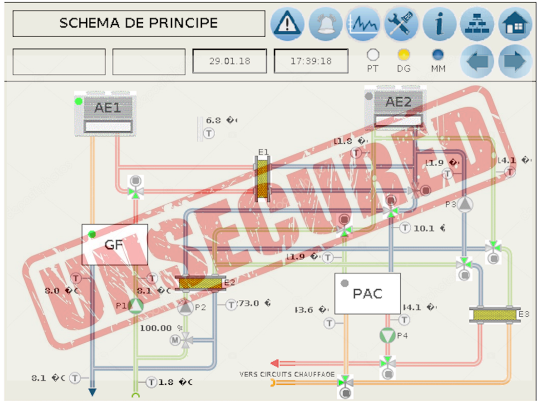
Temperature from the sensor converts based on following formula: *y = 1 * x + 0*

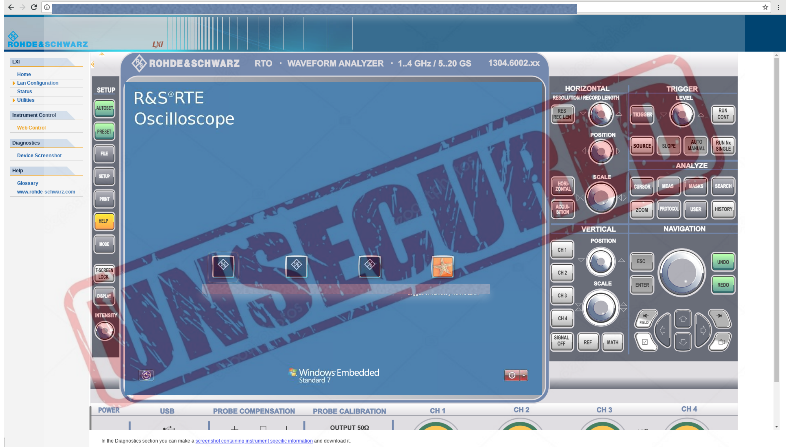
Save



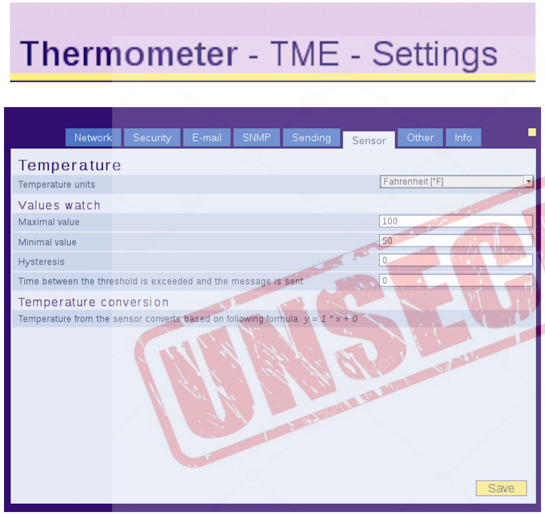
```
*** Others ***

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 ? 0

IP Address : ([redacted]) .([redacted]) .([redacted]) .([redacted])
Set Gateway IP Address (Y) ?
Gateway IP Address : ([redacted]) .([redacted]) .([redacted]) .([redacted])
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
```

```
[sagarwal@sharad-workstation ~]$ [redacted]
Starting Nmap 6.40 ( http://nmap.org ) at
Note: Host seems down. If it is really up,
Nmap done: 1 IP address (0 hosts up) scanne
[sagarwal@sharad-workstation ~]$
```





In the Diagnostics section you can make a screenshot containing instrument specific information and download it.



Thermometer - TME - Settings

Temperature

Temperature units: Fahrenheit [°F]

Values watch

Maximal value: 100

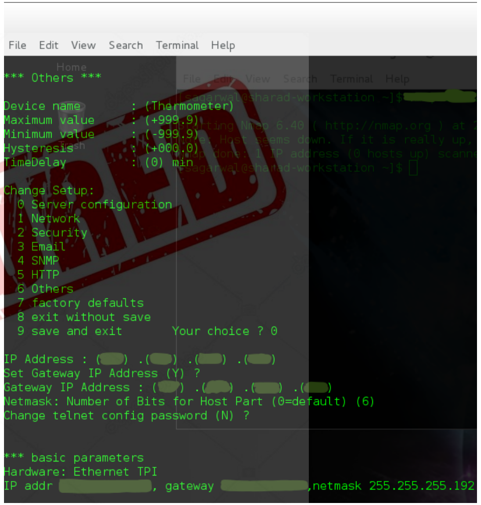
Minimal value: 50

Hysteresis: 0

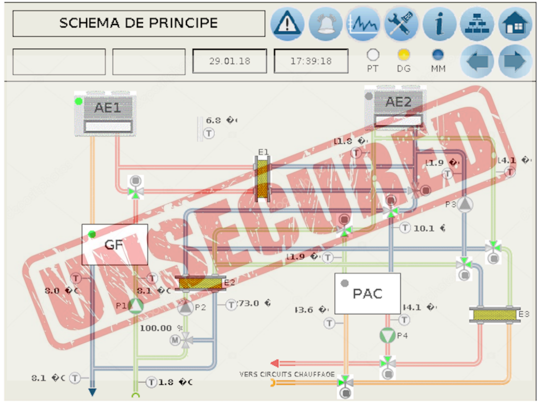
Time between the threshold is exceeded and the message is sent: 0

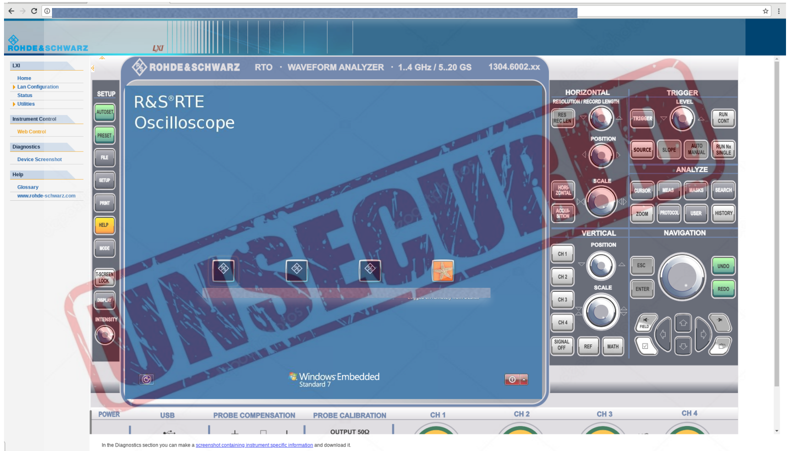
Temperature conversion

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



```
*** 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 ? 0

IP Address : ([redacted]) .([redacted]) .([redacted]) .([redacted])
Set Gateway IP Address (Y) ?
Gateway IP Address : ([redacted]) .([redacted]) .([redacted]) .([redacted])
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
```





In the Diagnostics section you can make a screenshot containing instrument specific information and download it

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

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

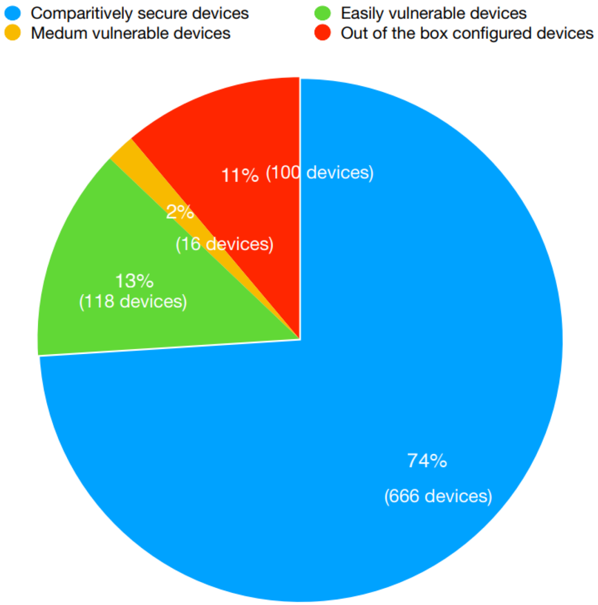
Some statistics from research done at CERN

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)

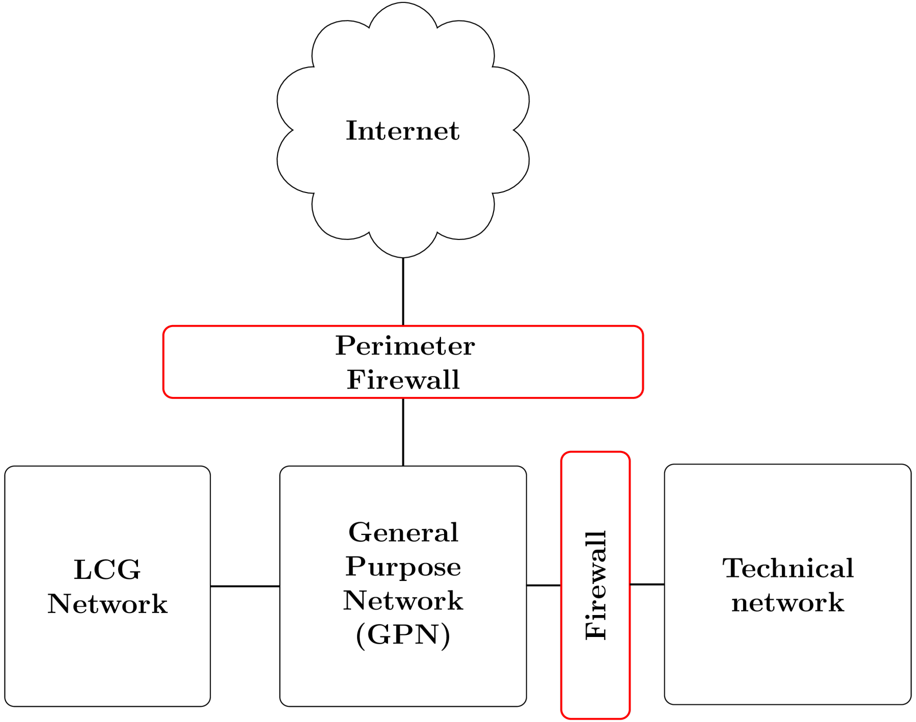
(a)

Vulnerability Classification



(b)

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



CERN Network

There are 1000s of devices installed and running on the CERN network. It consists mainly of two parts:

1. General Purpose Network (GPN): All users have access to this network.

2. Technical Network (TN): Only selected users have access to this network.

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

We developed tools to automatically detect and identify IoT devices running on a network

NetScanIoT tool

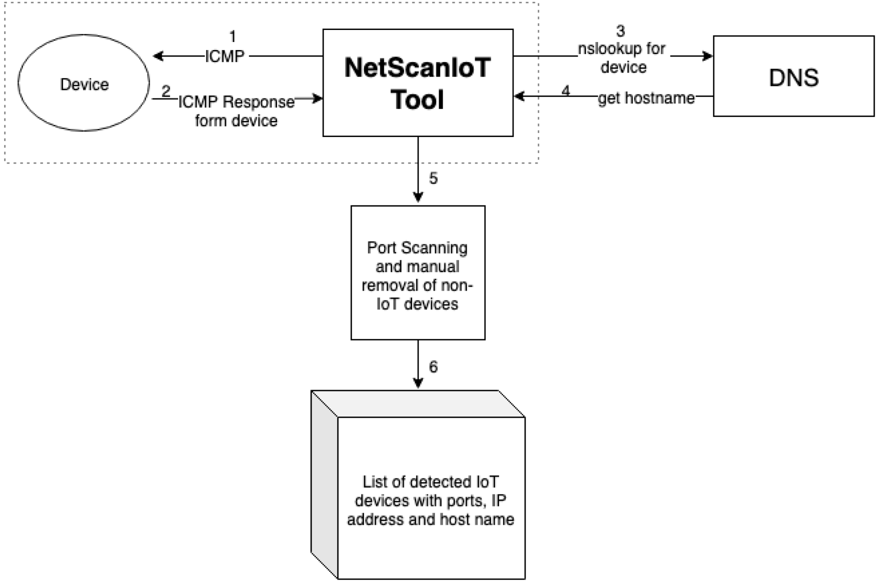
+

Web-IoT Detection (WID) tool

=

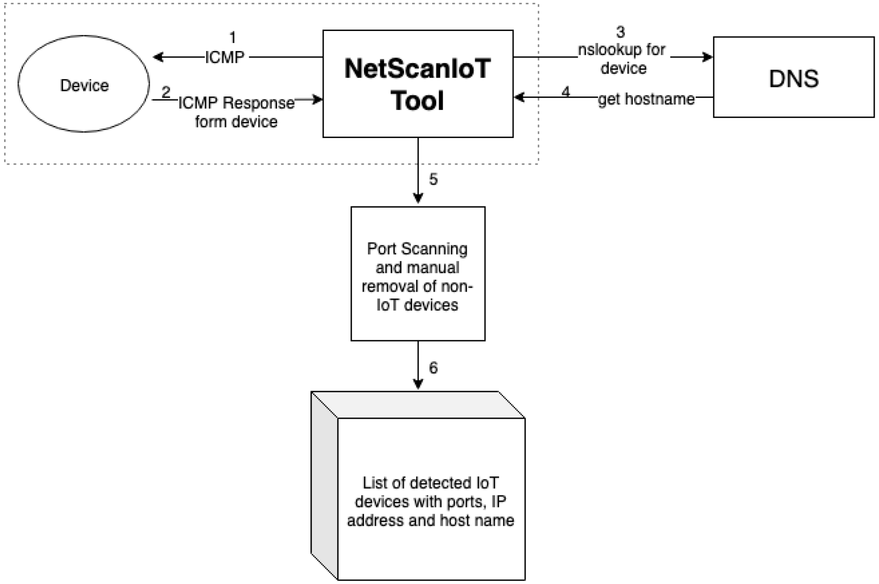
IoT device with it’s model, manufacturer and firmware version

NetScanIoT Tool



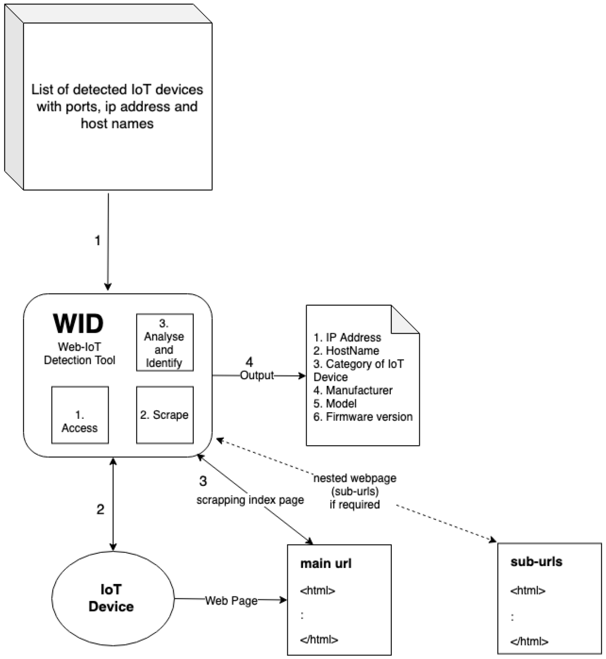
Device
1
ICMP
2
ICMP Response form device
NetScanIoT Tool
3
nslookup for device
4
get hostname
DNS
5
Port Scanning and manual removal of non-IoT devices
6
List of detected IoT devices with ports, IP address and host name

NetScanIoT Tool

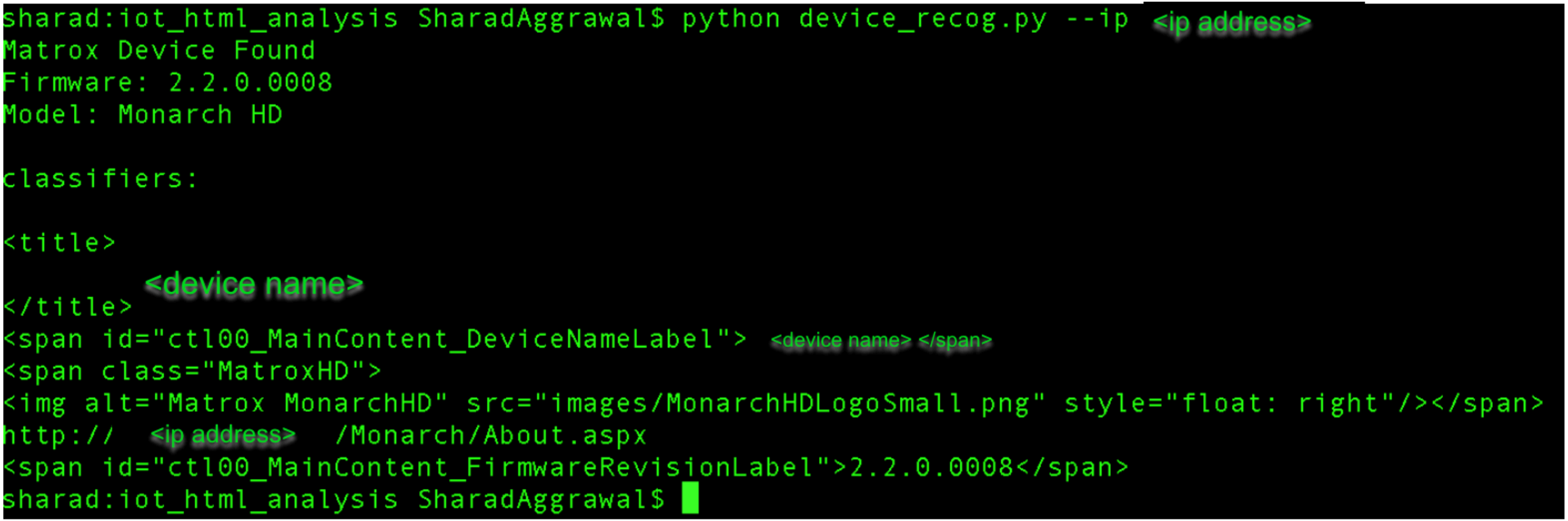


Device
1
ICMP
2
ICMP Response form device
NetScanIoT Tool
3
nslookup for device
4
get hostname
DNS
5
Port Scanning and manual removal of non-IoT devices
6
List of detected IoT devices with ports, IP address and host name

Web-IoT Detection Tool



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$ █
```

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

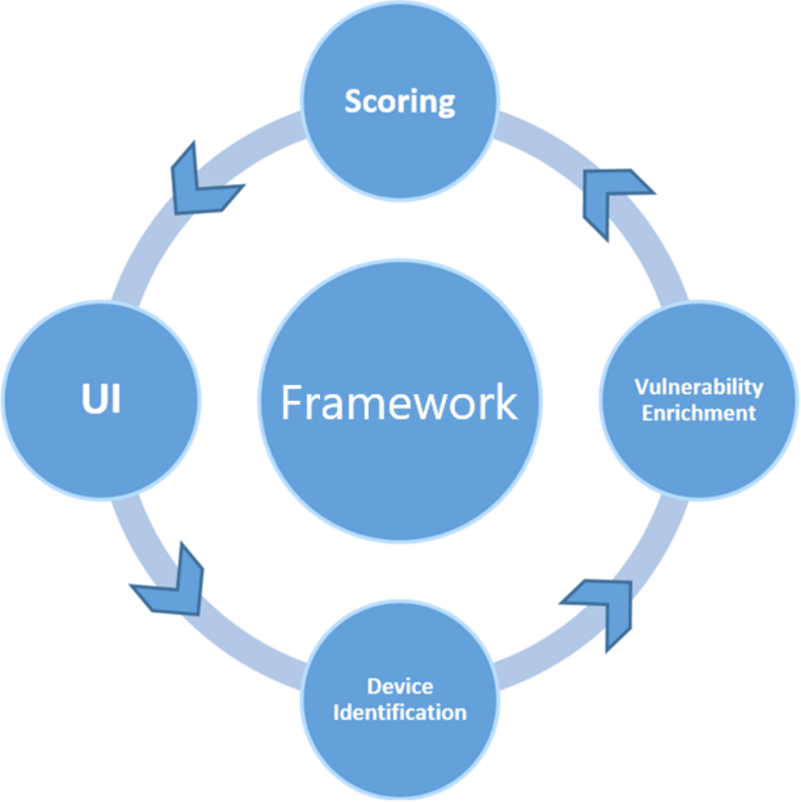
Received: 14 August 2019; Accepted: 19 September 2019; Published: 23 September 2019

check for updates

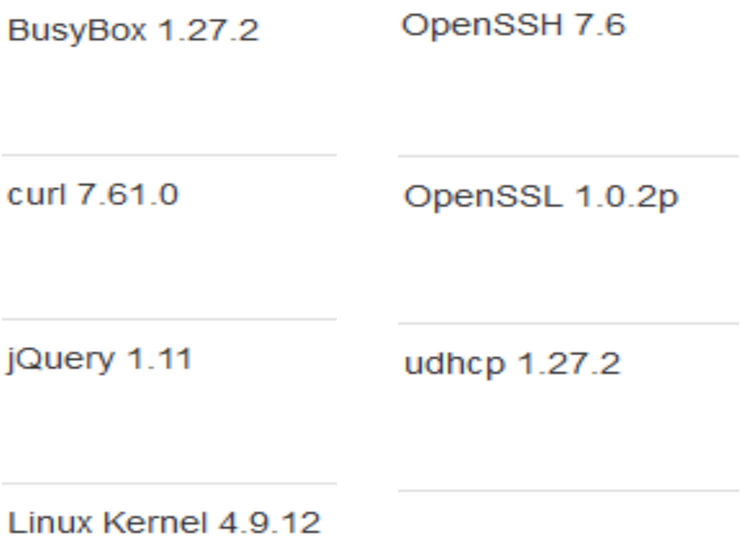
Abstract: The introduction of the Internet of Things (IoT), i.e., the interconnection of embedded devices over the Internet, has changed the world we live in from the way we measure, make calls, print information and even the way we get energy in our offices or homes. The convenience of IoT products, 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

One can now use the identified information to execute IoT risk assessments



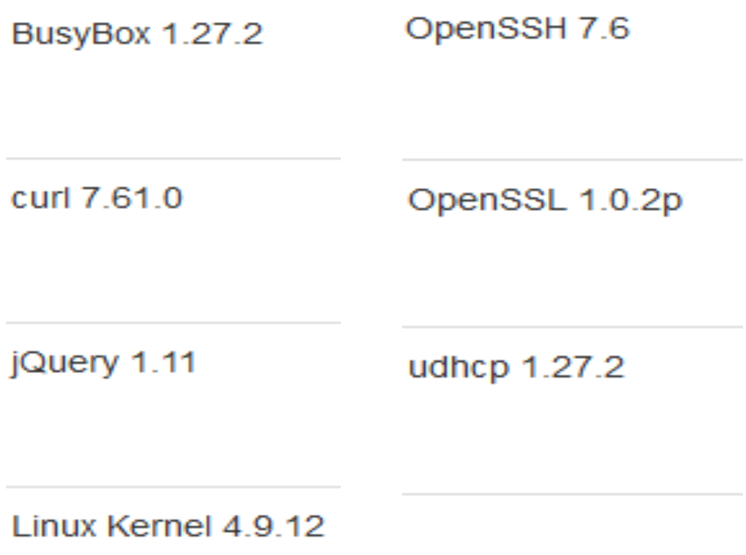
Information for the Risk Assessment



BusyBox 1.27.2	OpenSSH 7.6
curl 7.61.0	OpenSSL 1.0.2p
jQuery 1.11	udhcp 1.27.2
Linux Kernel 4.9.12	

Axis M2026-LE-Mk-II, Firmware 8.50.1

Information for the Risk Assessment



BusyBox 1.27.2	OpenSSH 7.6
curl 7.61.0	OpenSSL 1.0.2p
jQuery 1.11	udhcp 1.27.2
Linux Kernel 4.9.12	

Gathering vulnerabilities of all found libraries

Axis M2026-LE-Mk-II, Firmware 8.50.1

Risk Assessment

- Based on public vulnerabilities for
  - firmware contained libraries
  - the device model

- Allows to show users the risks exposed by their devices

Questions?

sharad.agarwal@cern.ch
(Device Identification)

p.oser@cern.ch
(Risk Assessment Framework)

References:

- Agarwal, S.; Oser, P.; Lüders, S. Detecting IoT Devices and How They Put Large Heterogeneous Networks at Security Risk. Preprints 2019, 2019080295 (doi: 10.20944/preprints201908.0295.v2).
- 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. Securing IoT Devices at CERN (2018, June). IT Lightning Talks: session #16. Available at: https://cds.cern.ch/record/2624930
- Agarwal, Sharad. Internet of Things (IoT) Security (2017, Aug). CERN openlab summer students' lightning talks 1. Available at: https://cds.cern.ch/record/2280014
- Agarwal, S.; Oser, P.; Lueders, S. Detecting IoT Devices and How They Put Large Heterogeneous Networks at Security Risk. *Sensors* **2019**, *19*, 4107.