RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: HTA-W03

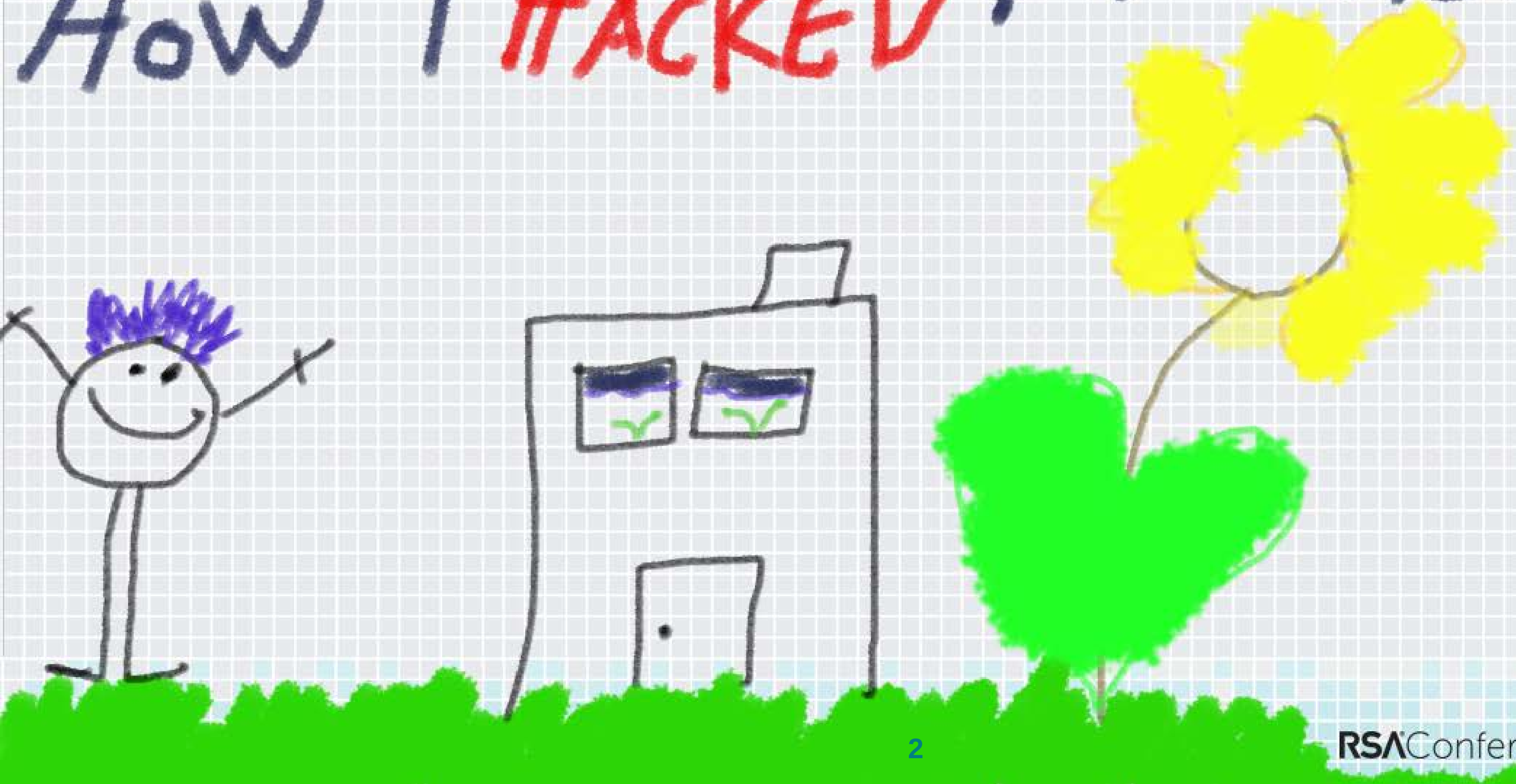
How Vulnerable Are Our Homes? - The Story of How My Home Got Hacked

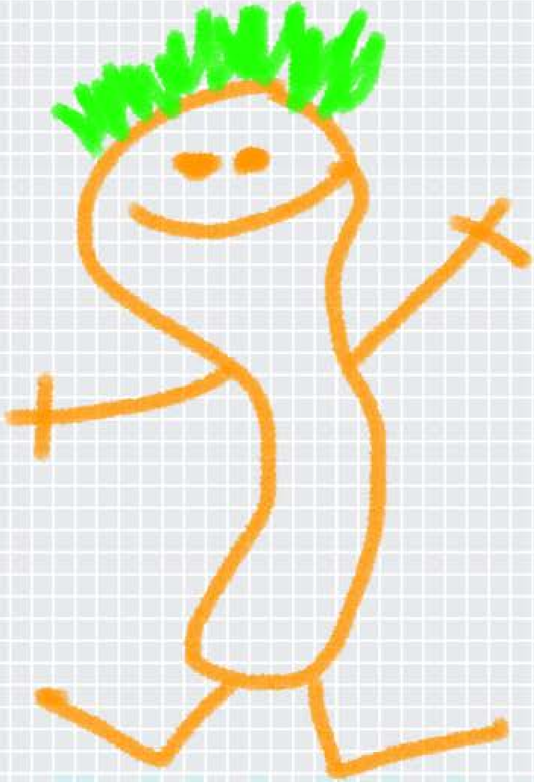
David Jacoby

Security Evangelist – Kaspersky Lab
@JacobyDavid

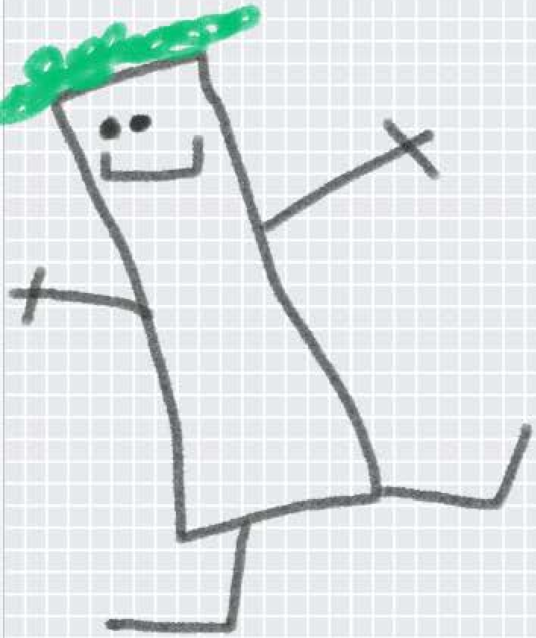
#RSAC

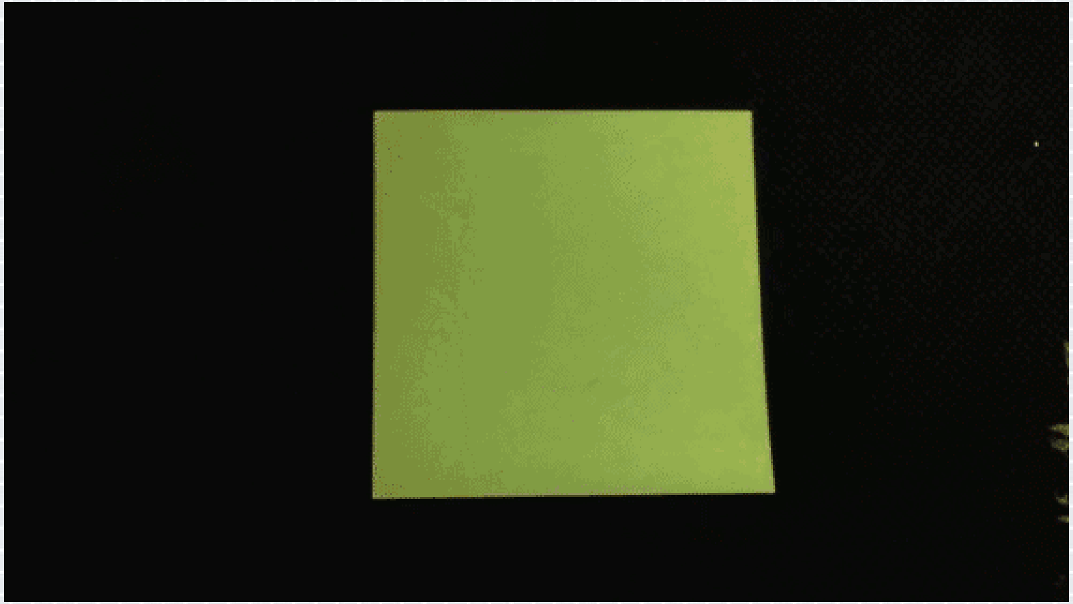
How I Hacked My Home!



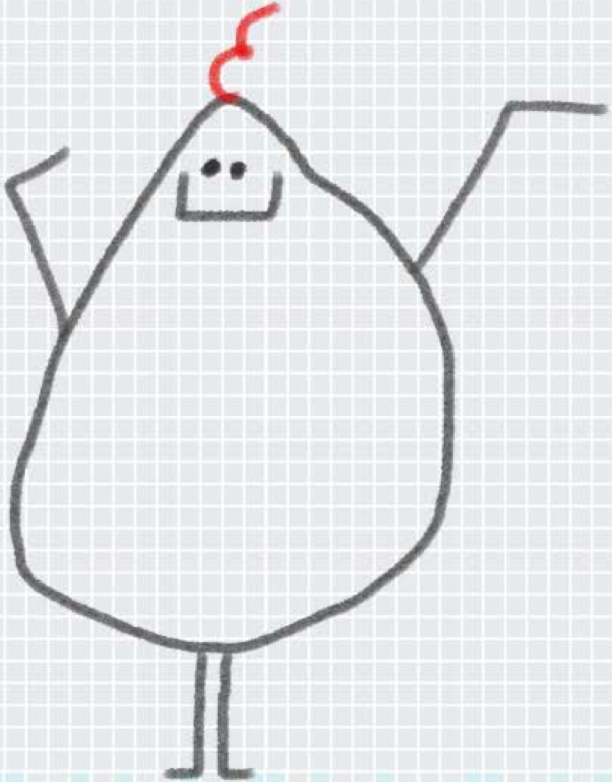


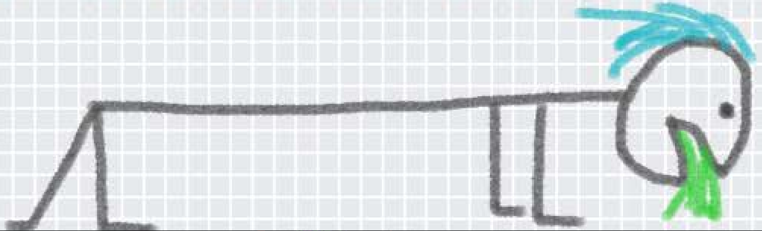
DAVID JACOBY





HACK!

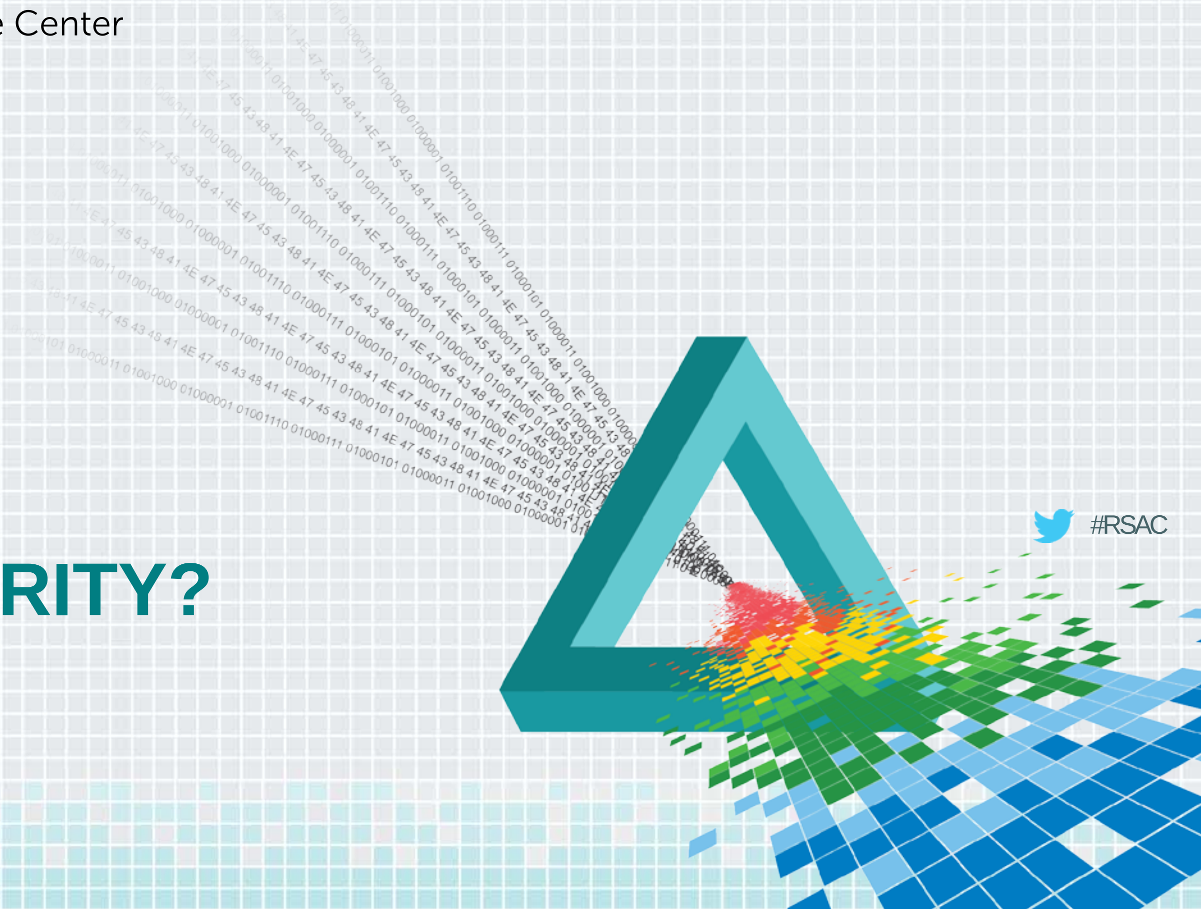




ABSOLUT
Country of Sweden
VODKA
This superb vodka
IMPORTED

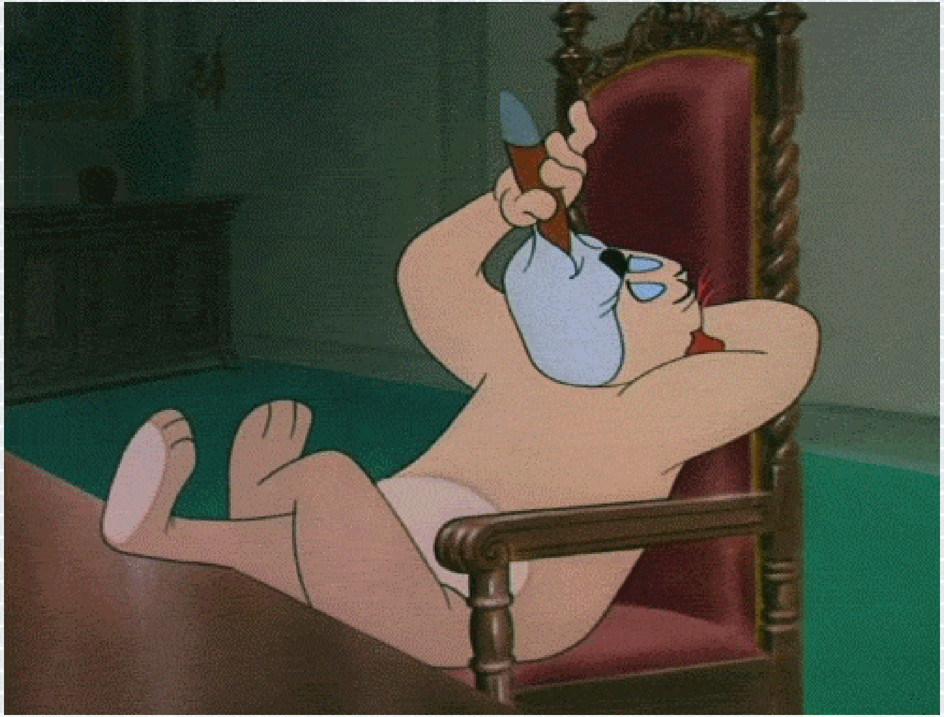
RSAConference2015

San Francisco | April 20-24 | Moscone Center

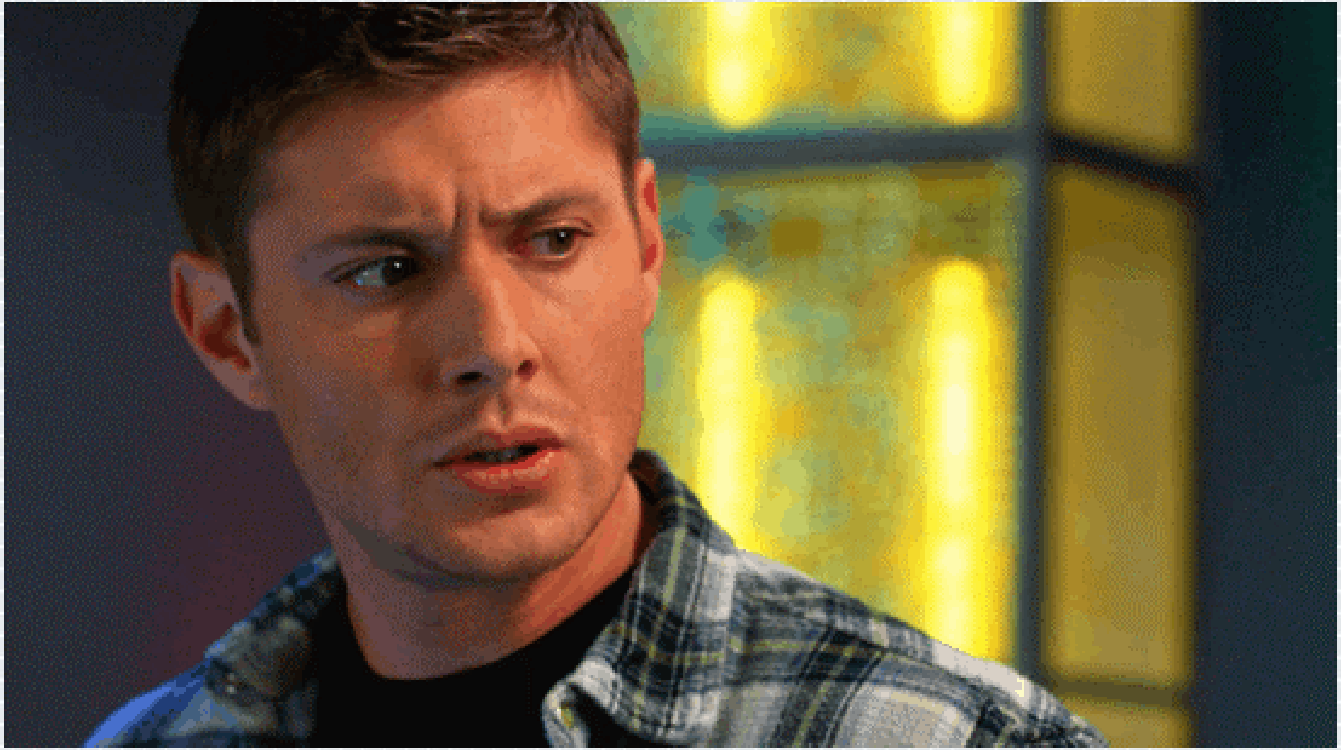


#RSAC

WHAT IS IT-SECURITY?



TT
TABB TV
seriöst brann han?



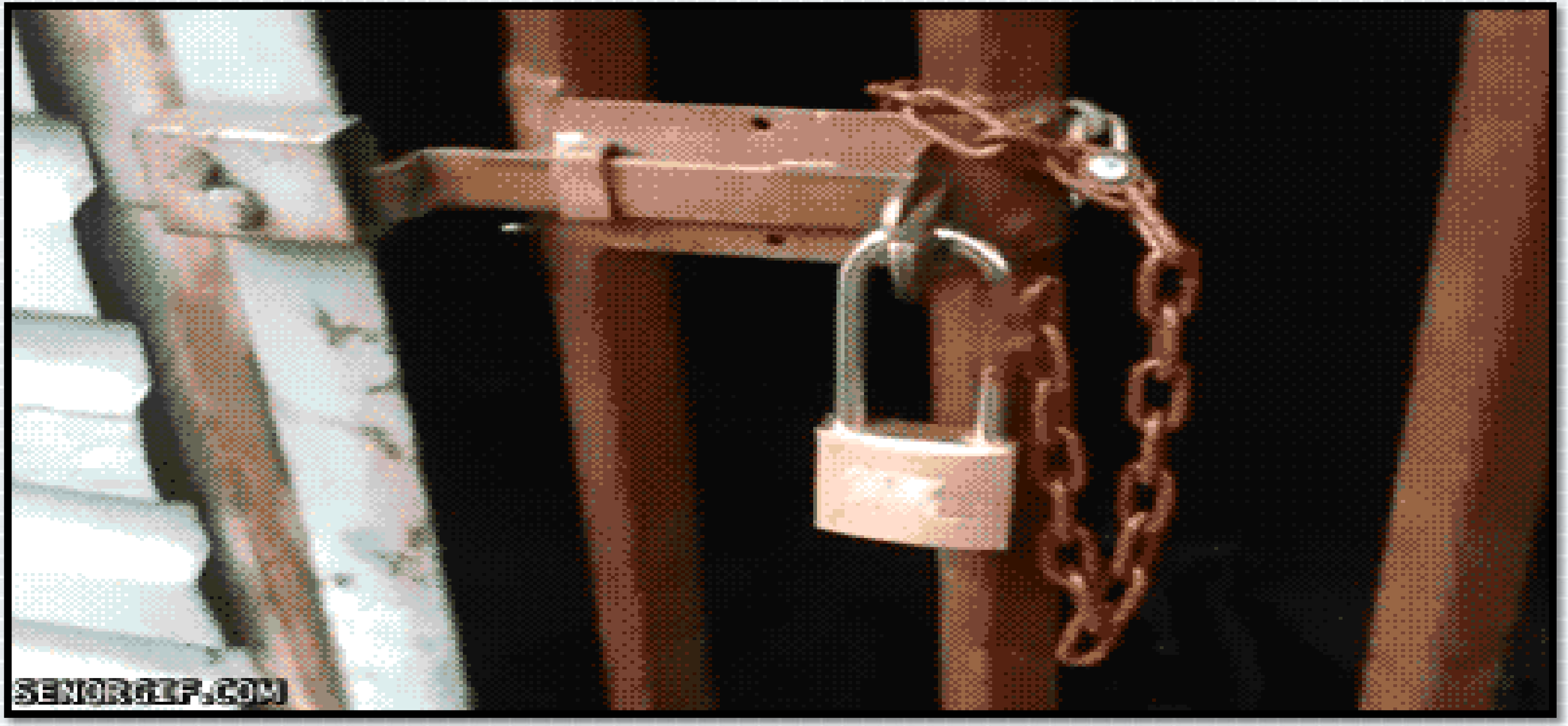
4GIFs.com

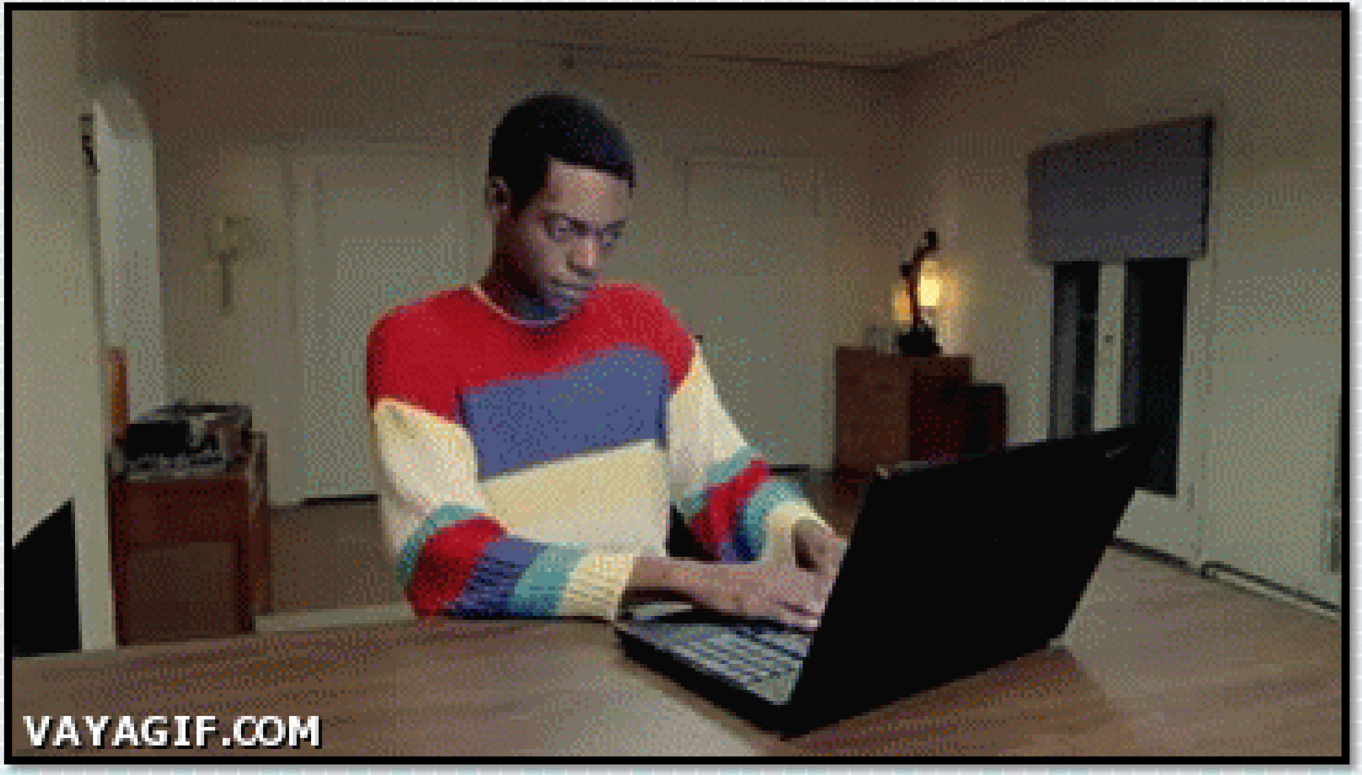
4GIFs
.com

4GIFs
.com

ForGIFs.com

Virus Download


SENORGIF.COM

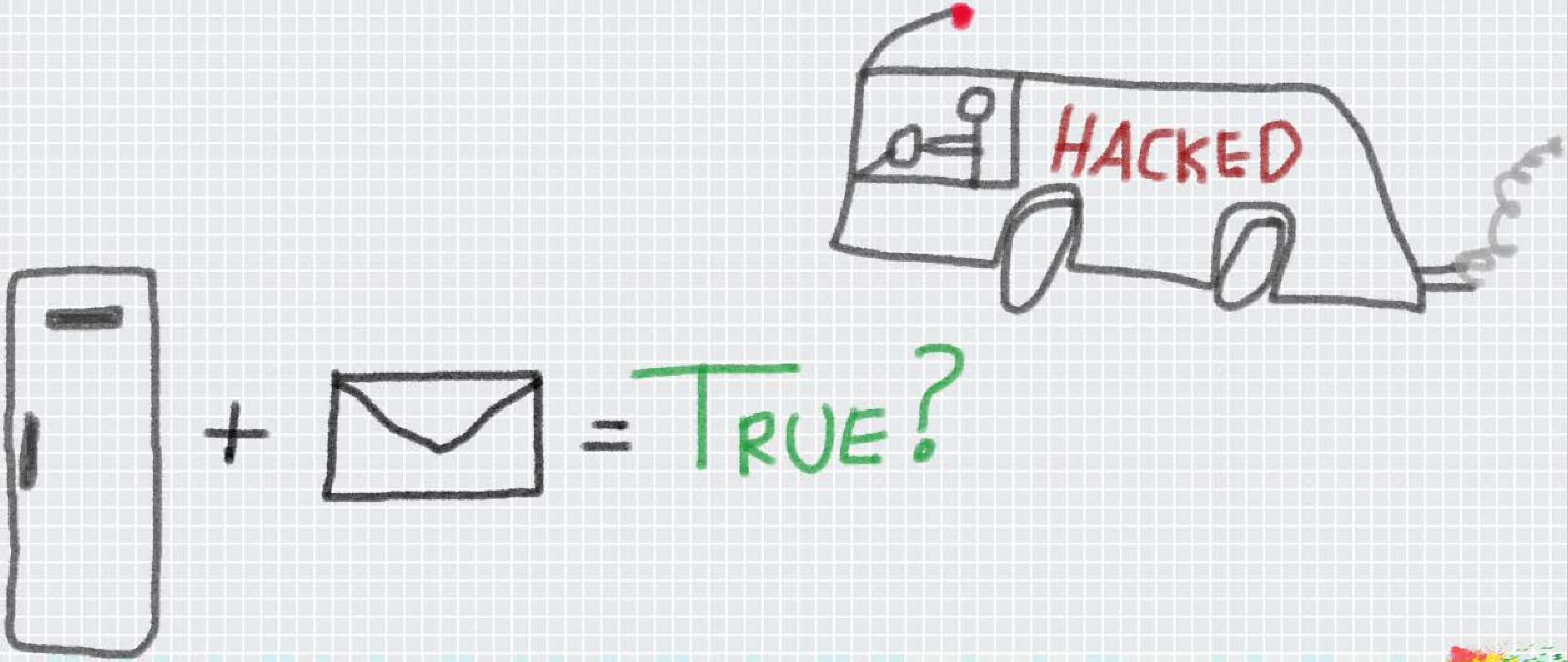

VAYAGIF.COM

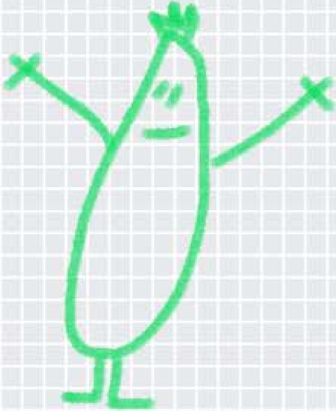
RSAConference2015

San Francisco | April 20-24 | Moscone Center

#RSAC

WHAT IS IOT SECURITY?


HACKED
+
=
TRUE?

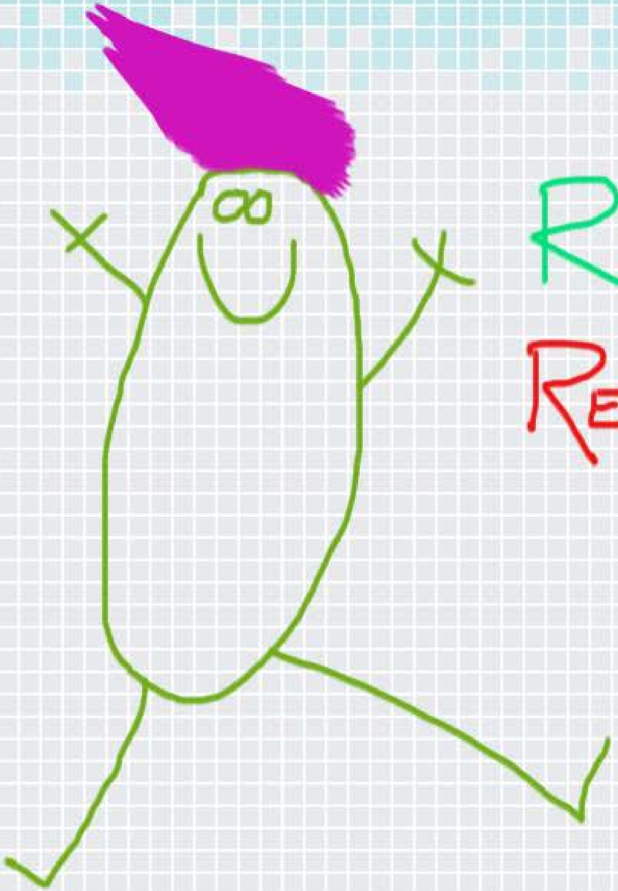


OMG!

OMG!

MY DEVICES

NAS
THX
WIFI
HP
DVD

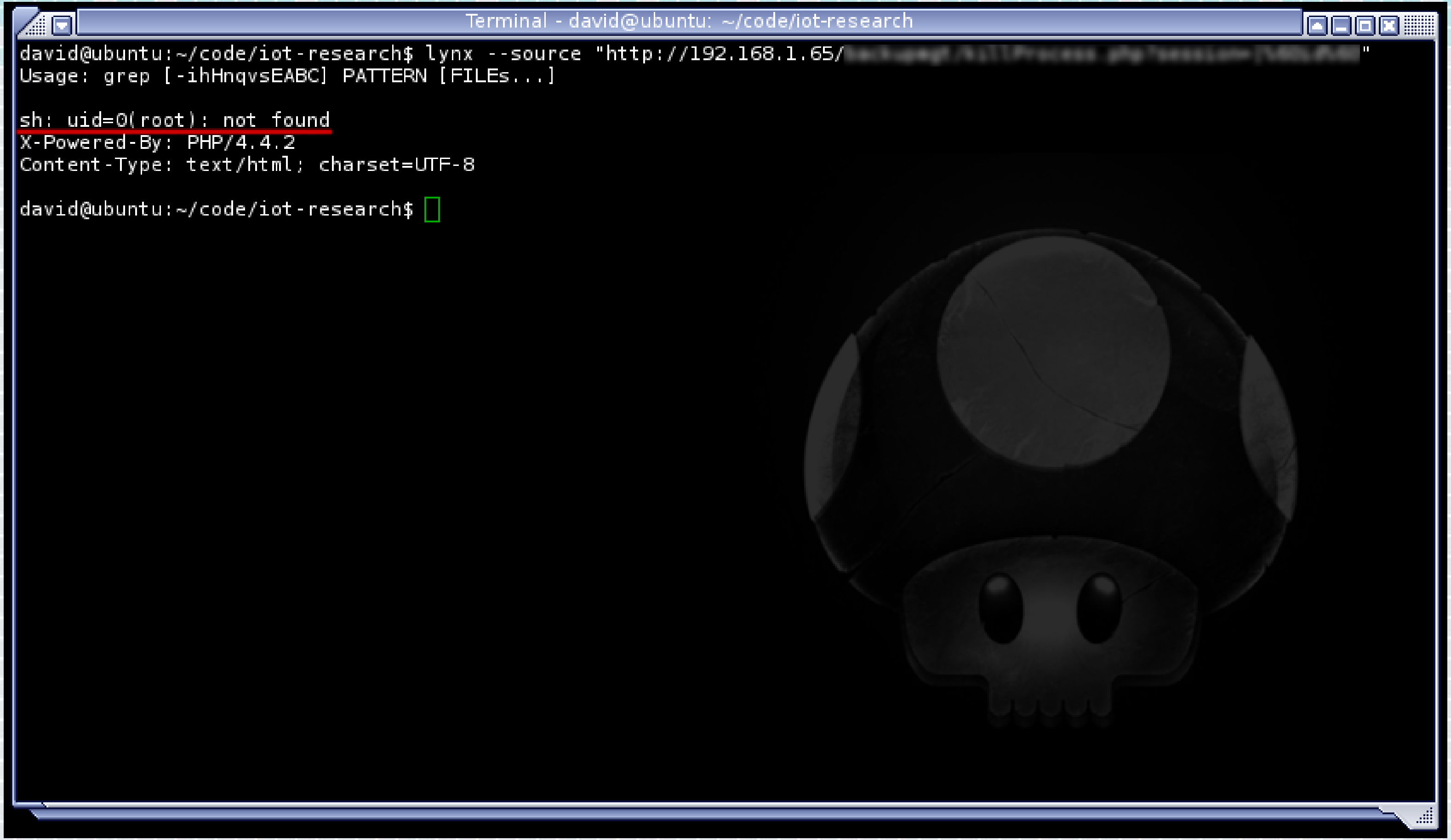


REMOTE PRE-AUTH r00t VULN

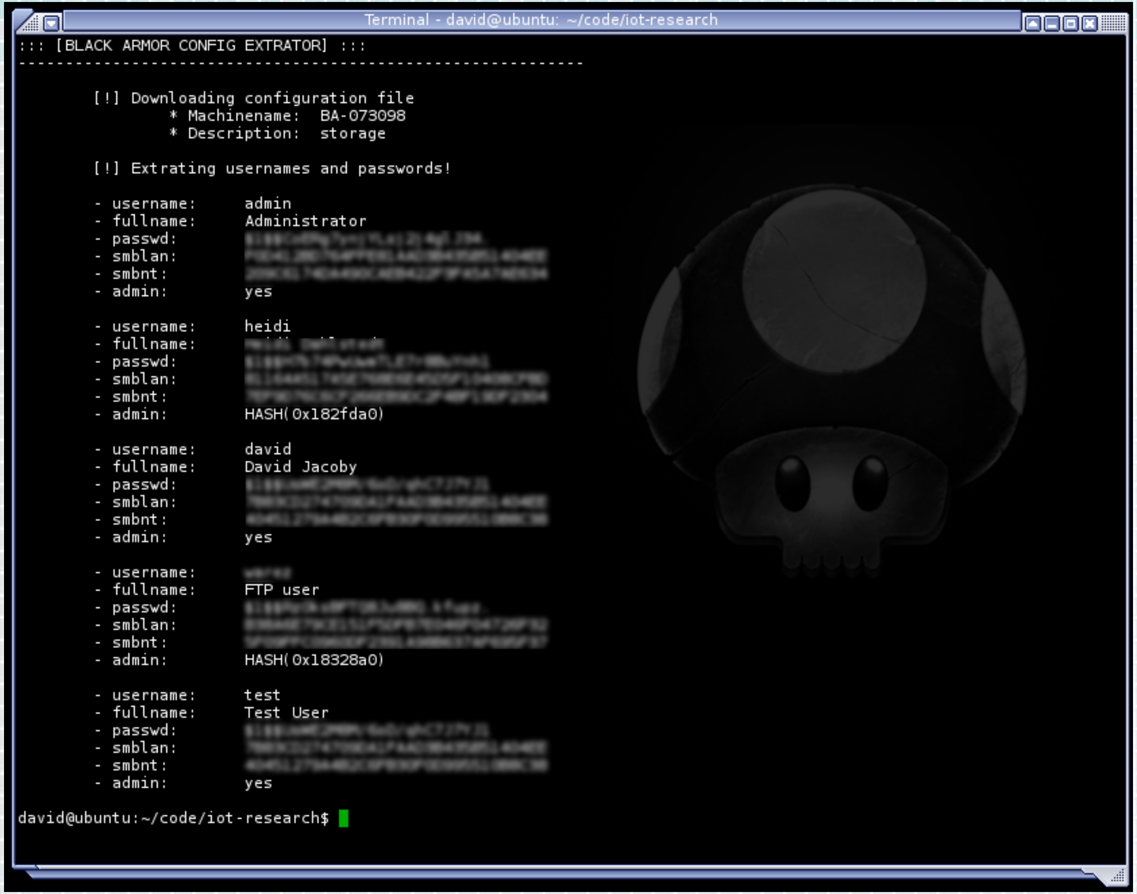
REMOTE PRE-AUTH CONFIG DOWNLOAD

TROJANIBLE

NAS



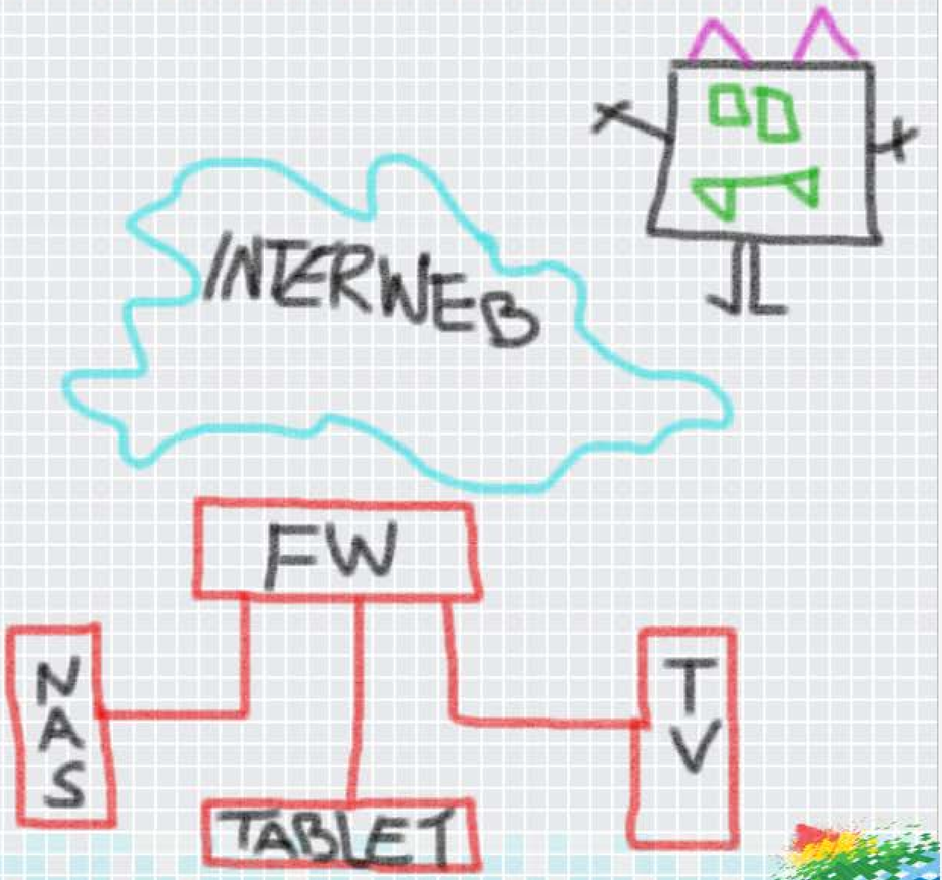
```
david@ubuntu:~/code/iot-research$ lynx --source "http://192.168.1.65/[redacted]"
Usage: grep [-ihHnqvsEABC] PATTERN [FILEs...]

sh: uid=0(root): not found
X-Powered-By: PHP/4.4.2
Content-Type: text/html; charset=UTF-8

david@ubuntu:~/code/iot-research$ 
```



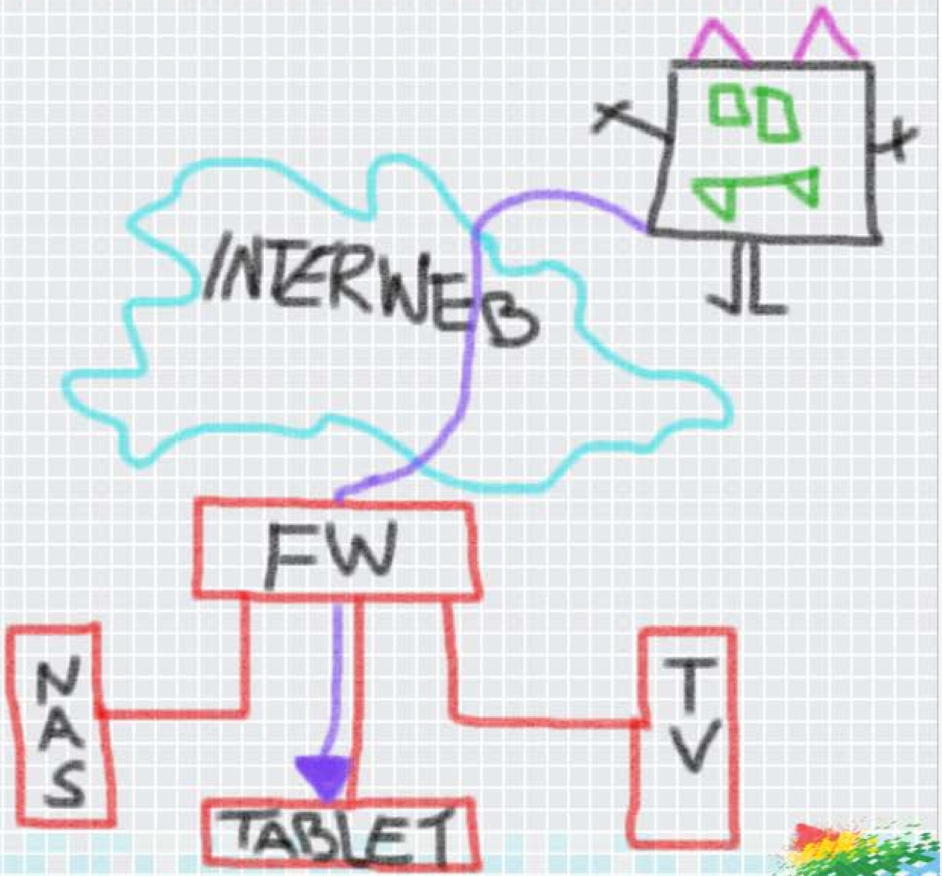
```
::: [BLACK ARMOR CONFIG EXTRATOR] :::
-----------------------------------------------------------

        [!] Downloading configuration file
                * Machinename:   BA-073098
                * Description:   storage

        [!] Extrating usernames and passwords!

        - username:     admin
        - fullname:     Administrator
        - passwd:       [redacted]
        - smblan:       [redacted]
        - smbnt:        [redacted]
        - admin:        yes

        - username:     heidi
        - fullname:     [redacted]
        - passwd:       [redacted]
        - smblan:       [redacted]
        - smbnt:        [redacted]
        - admin:        HASH(0x182fda0)

        - username:     david
        - fullname:     David Jacoby
        - passwd:       [redacted]
        - smblan:       [redacted]
        - smbnt:        [redacted]
        - admin:        yes

        - username:     [redacted]
        - fullname:     FTP user
        - passwd:       [redacted]
        - smblan:       [redacted]
        - smbnt:        [redacted]
        - admin:        HASH(0x18328a0)

        - username:     test
        - fullname:     Test User
        - passwd:       [redacted]
        - smblan:       [redacted]
        - smbnt:        [redacted]
        - admin:        yes

david@ubuntu:~/code/iot-research$ 
```

HACKING IT REMOTELY!

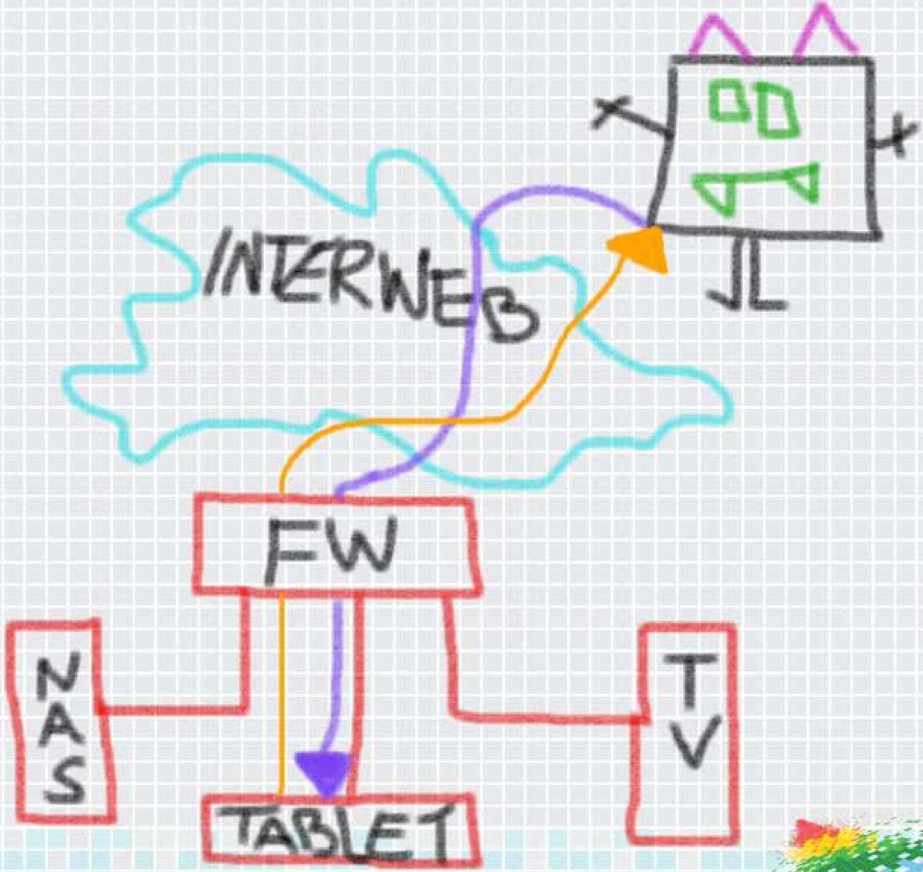
MY NORMAL SETUP



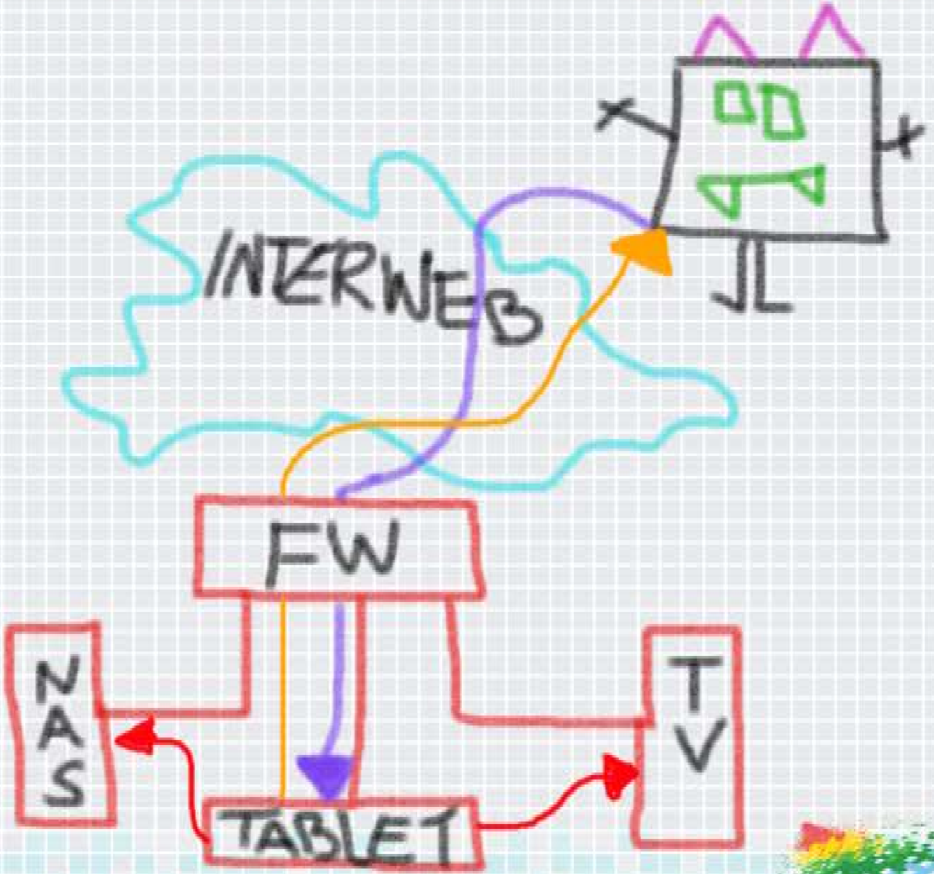
SEND LINK!



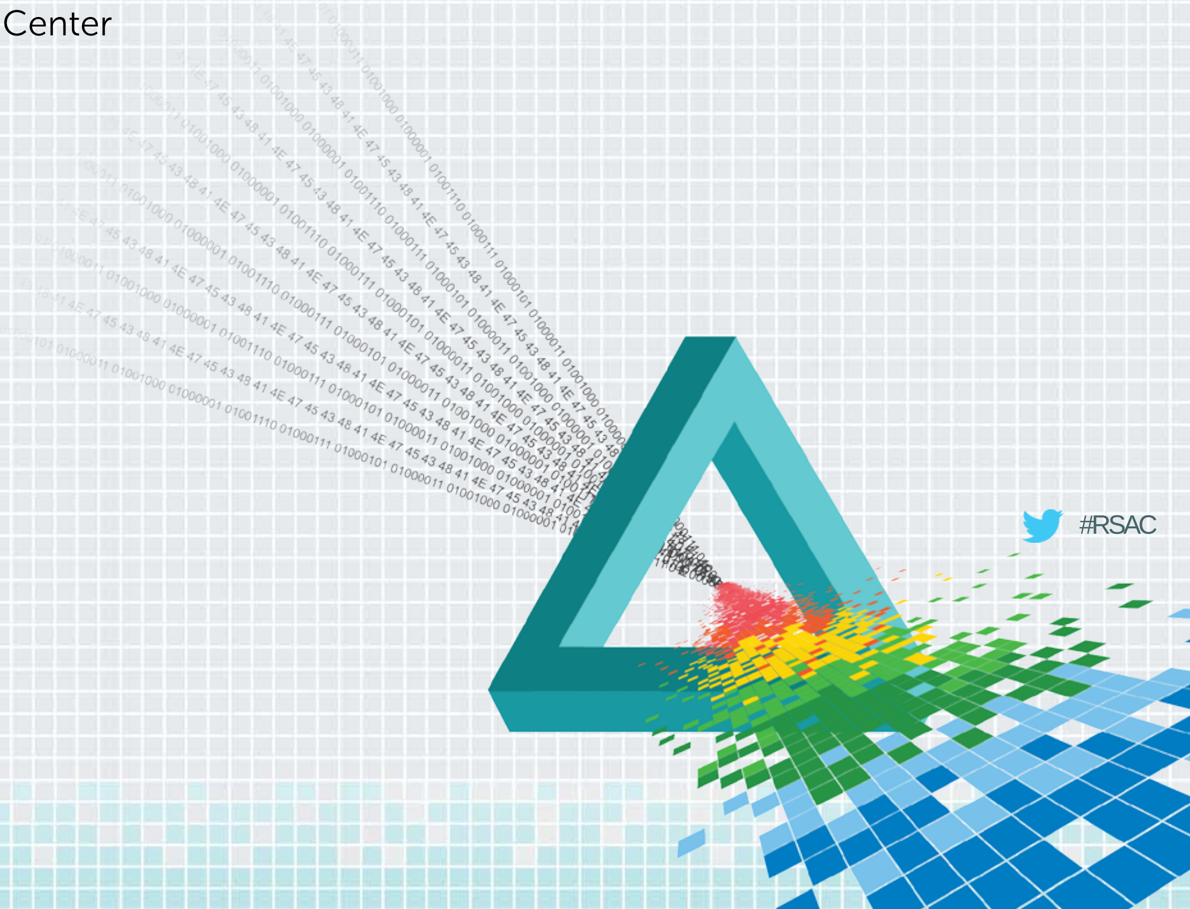
VISITS LINK



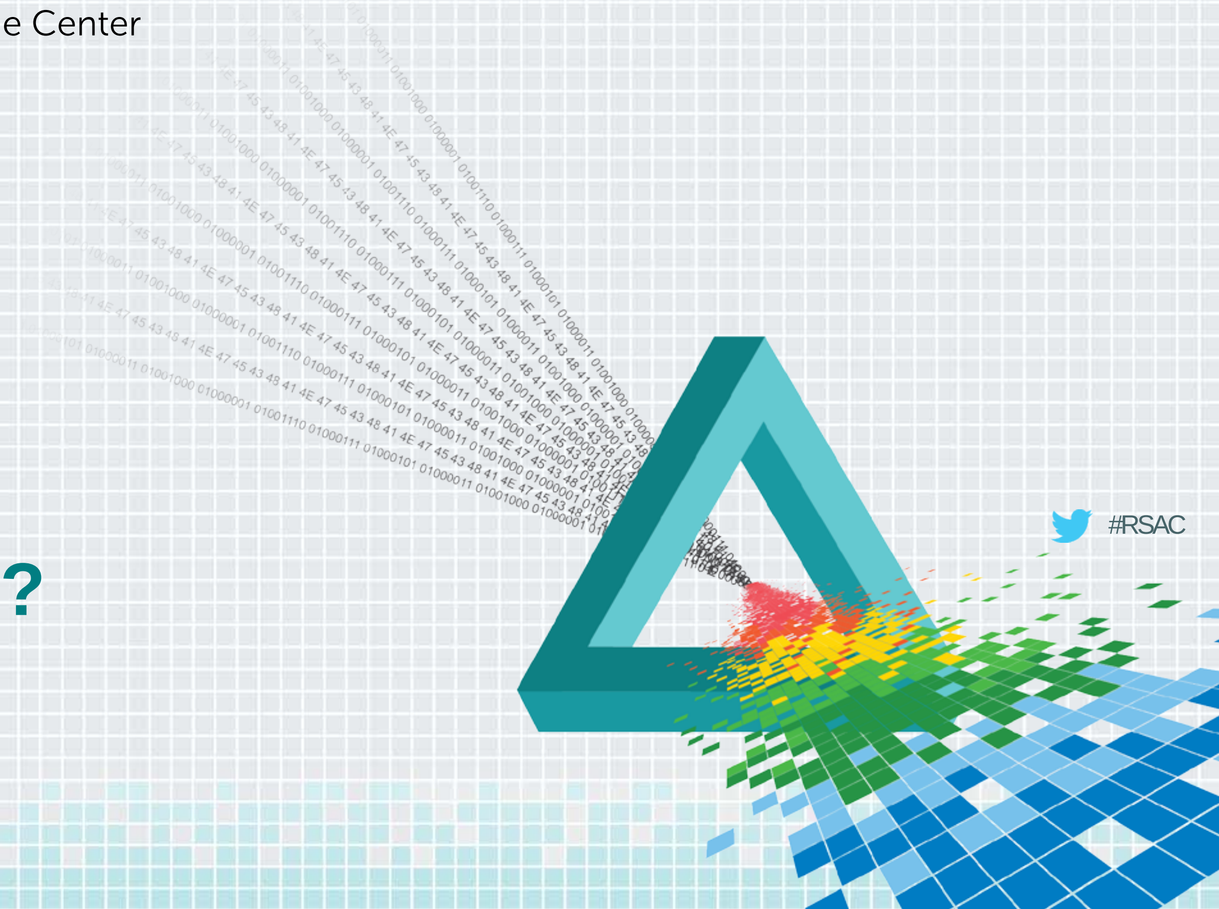
STARTS SCANNING



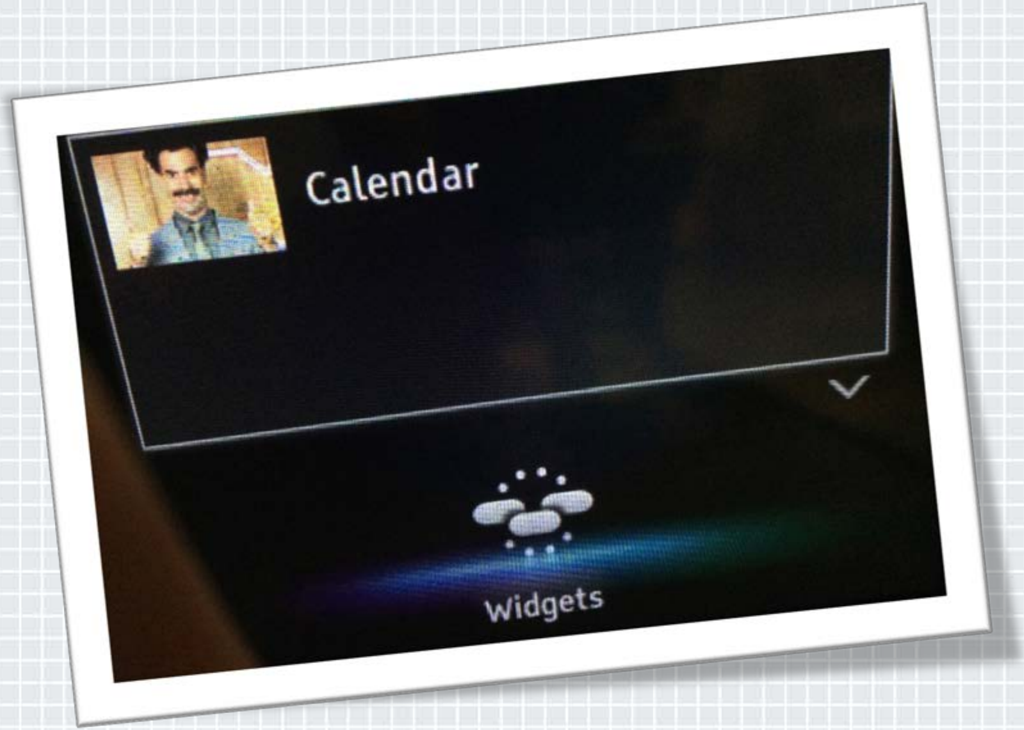
LIVE DEMO!!!



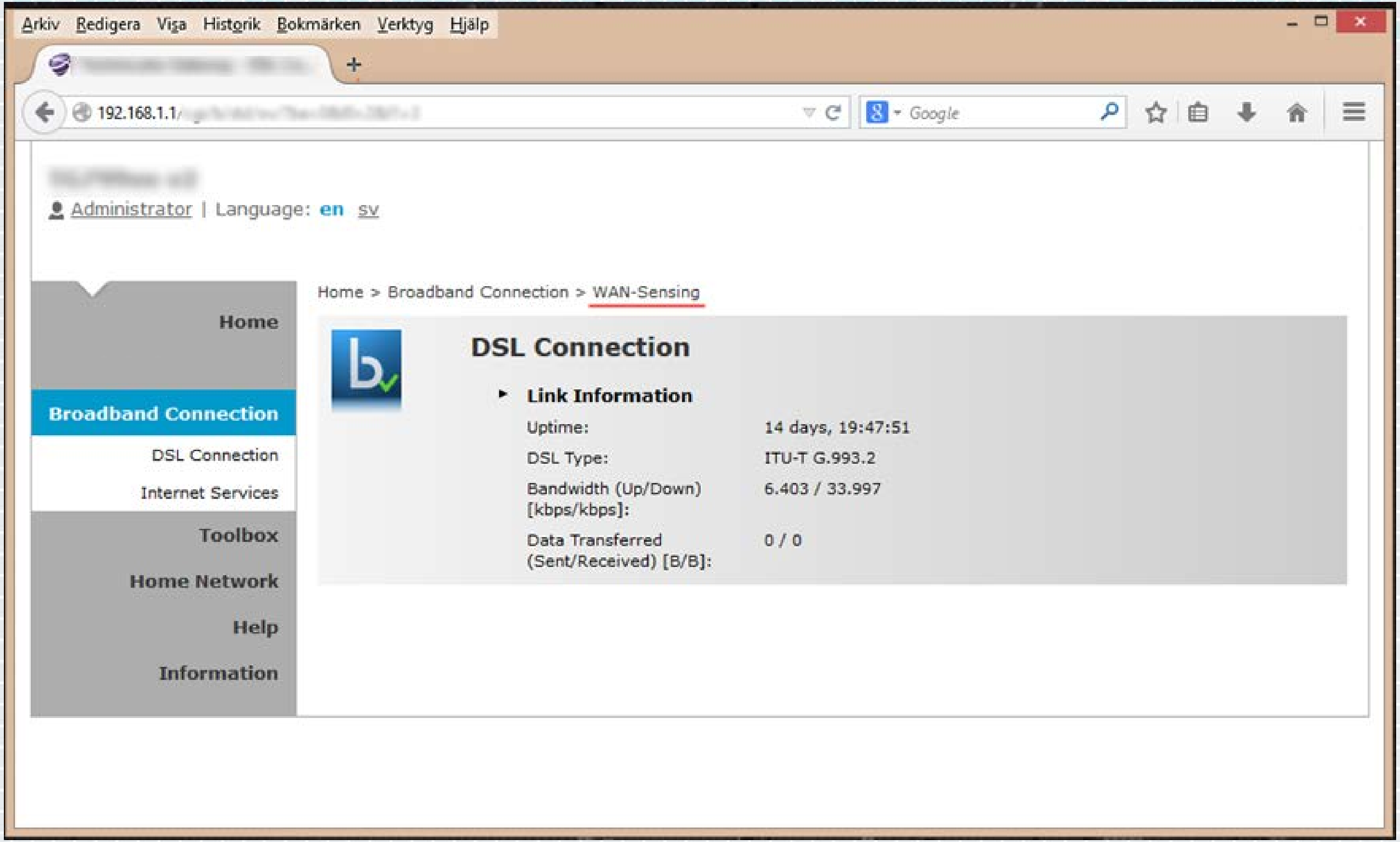
OTHER DEVICES?



#RSAC


Calendar
Widgets

z



[redacted]

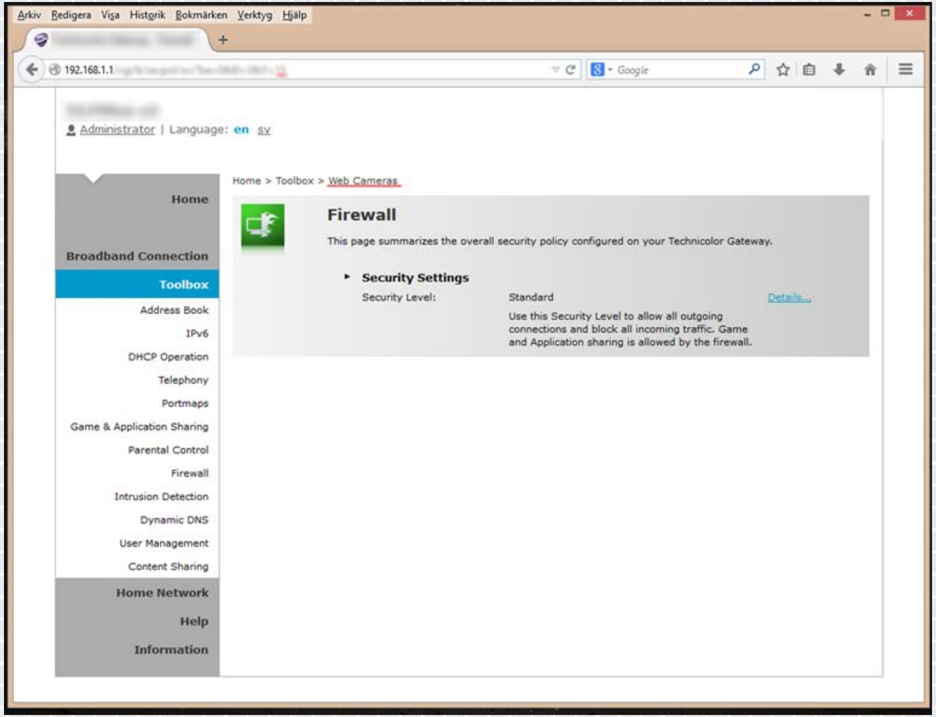
Administrator | Language: en sv

Home > Broadband Connection > WAN-Sensing

DSL Connection

▸ **Link Information**

Uptime:	14 days, 19:47:51
DSL Type:	ITU-T G.993.2
Bandwidth (Up/Down) [kbps/kbps]:	6.403 / 33.997
Data Transferred (Sent/Received) [B/B]:	0 / 0



[redacted]

Administrator | Language: en sv

Home > Toolbox > Web Cameras

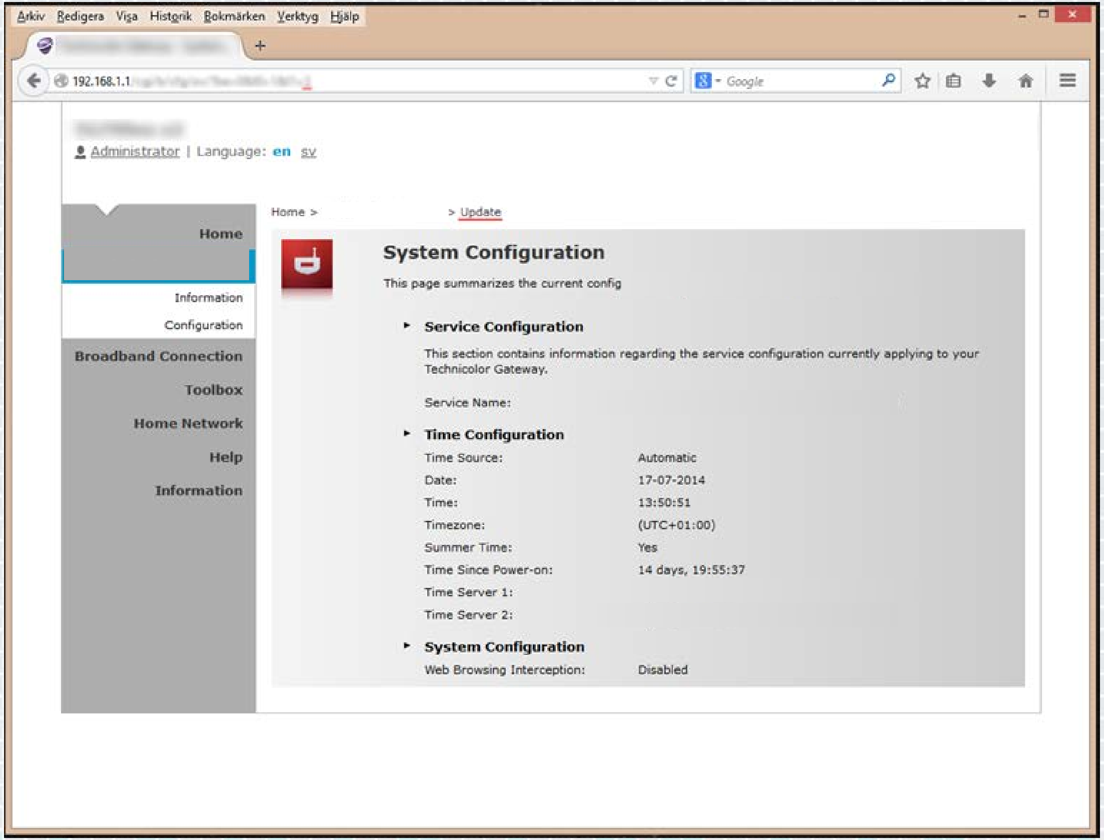
Firewall

This page summarizes the overall security policy configured on your Technicolor Gateway.

Security Settings

Security Level: Standard Details...

Use this Security Level to allow all outgoing connections and block all incoming traffic. Game and Application sharing is allowed by the firewall.



[redacted]

System Configuration

This page summarizes the current config

Service Configuration

This section contains information regarding the service configuration currently applying to your Technicolor Gateway.

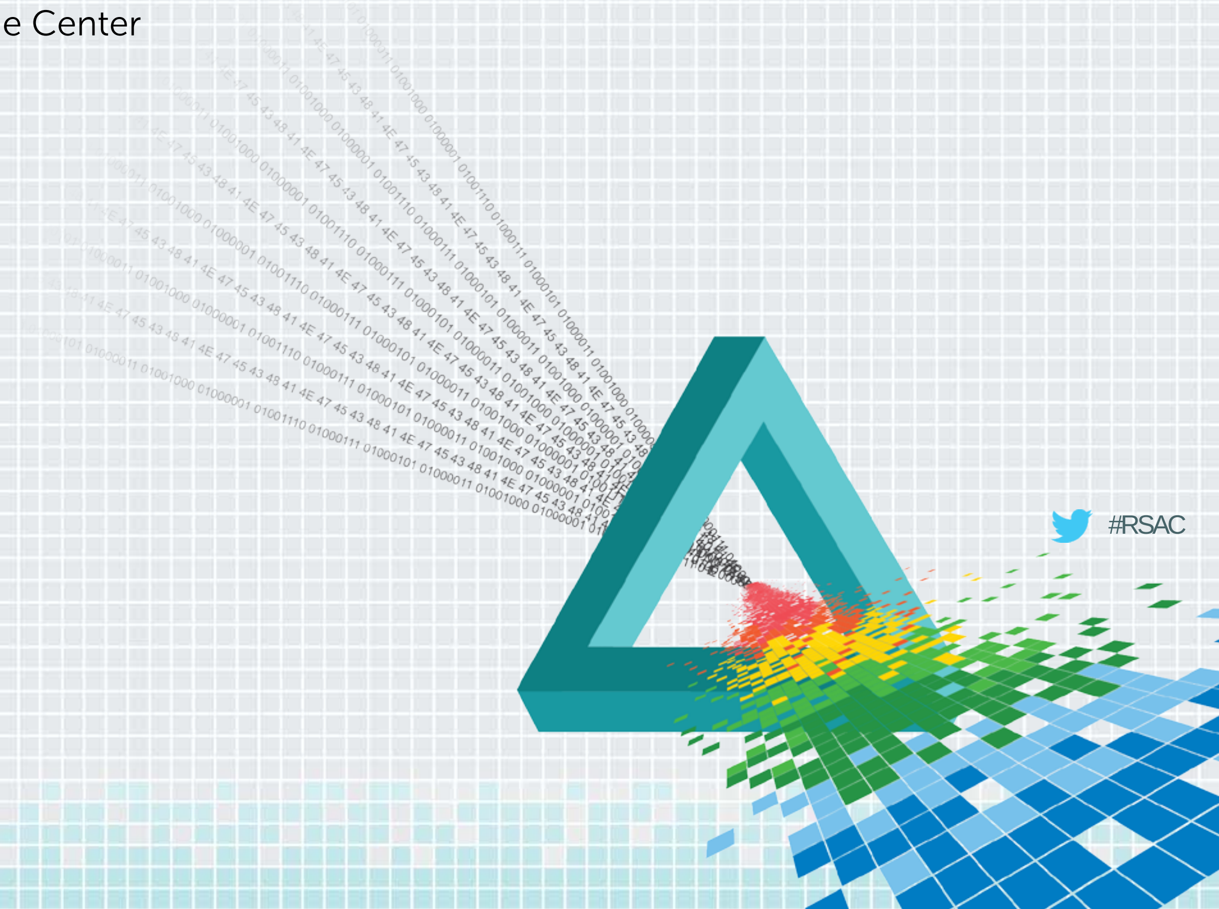
Service Name:

Time Configuration

Time Source:	Automatic
Date:	17-07-2014
Time:	13:50:51
Timezone:	(UTC+01:00)
Summer Time:	Yes
Time Since Power-on:	14 days, 19:55:37
Time Server 1:	
Time Server 2:	

System Configuration

Web Browsing Interception:	Disabled



#RSAC

CONCLUSION

CONCLUSIONS

- More and more devices gets connected!
- Bad guys are already hacking us!
- Exploitation is easy and effective

CONCLUSIONS

- Good solutions for software vendors
  - BuildItSecure.ly
  - I Am The Cavalry
  - OWASP
  - iEEE Guides

- No solutions / help for consumers