Security considerations for IoT

Pascal Oser

ulm university universität ulm

Work sponsored by the Wolfgang Gentner Programme
of the Federal Ministry of Education and Research: http://cern.ch/gentner

Introduction

- Failures in developing secure IoT
- How you can improve IoT security
- How we improve IoT security
- Summing-up

ANDY GREENBERG SECURITY 07.24.15 12:30 PM

AFTER JEEP HACK, CHRYSLER RECALLS 1.4M VEHICLES FOR BUG FIX

WIRED

The Argus

Rude awakening for dawn drivers

7:38am Friday 27th October 2006

Print Email Share

By Louise Acford »

Early morning motorists got a shock yesterday when digital car park signs were tampered with by computer hackers and were left displaying an obscene message.

The message appeared on all similar signs around Crawley at about 6.45am.

Thousands of motorists travelling into the town would have been subjected to the unsavoury advice.

The signs normally display the number of spaces available in the town's car parks and were installed about four years ago.

BBC | BBC iD | Menu | Search

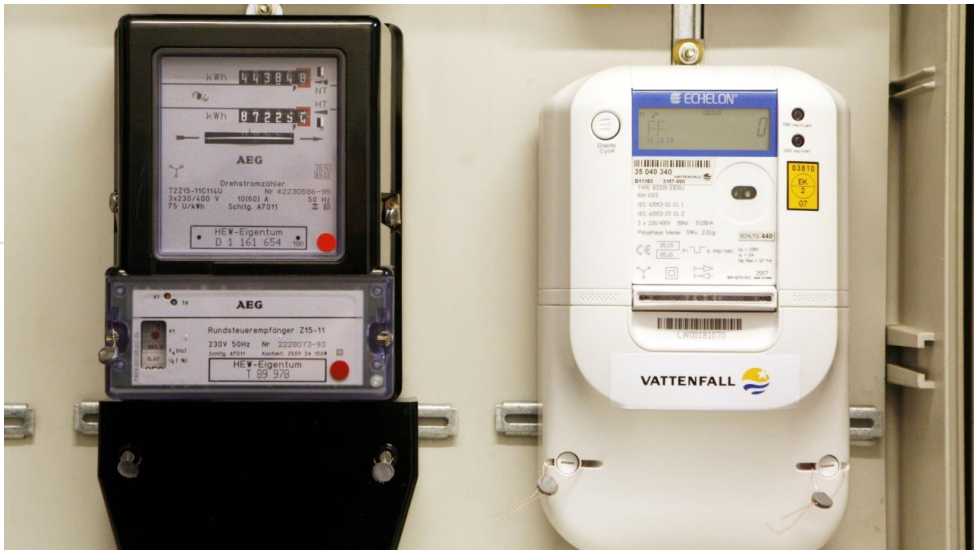
NEWS

Smart meters can be hacked to cut power bills

By Mark Ward

Technology correspondent, BBC News

16 October 2014 | Technology



- Encryption keys generated by device name (6 characters long)
- No authentication for pairing
- Guessable hardcoded administrator credentials
- Long network communication crashes the device

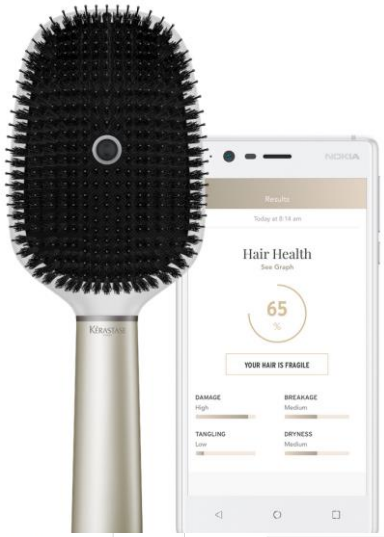
GERMANY

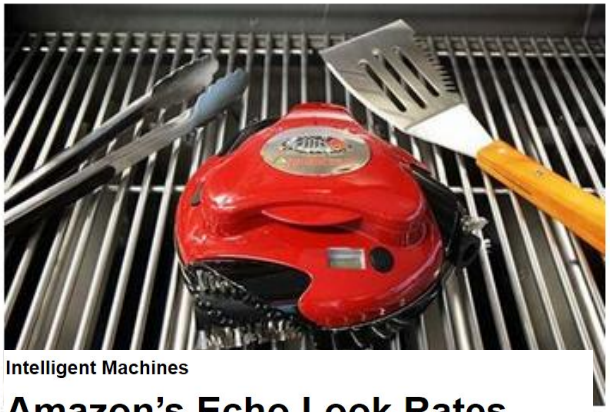
Deutsche Telekom 'hack' affects nearly a million cust

By Euro /2016

Hund had their broadband service cut off following a hack

IoT is everywhere





Intelligent Machines

Amazon's Echo Look Rates Your Outfits and Slurps Up Revealing Data

The company's latest smart assistant features a camera to help you choose what to wear—and photograph the inside of your house while it's at it.

by Jamie Condliffe April 27, 2017

BBC iD Menu Search

NEWS

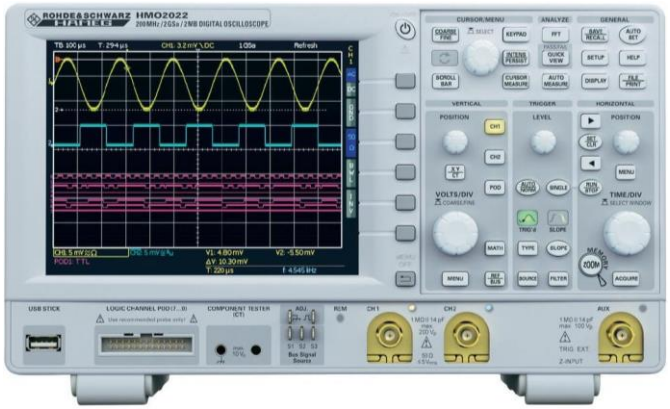
Not in front of the telly: Warning over 'listening' TV

9 February 2015 | Technology

Failures in developing secure IoT

How you can improve IoT security

Small selection of IoT at CERN

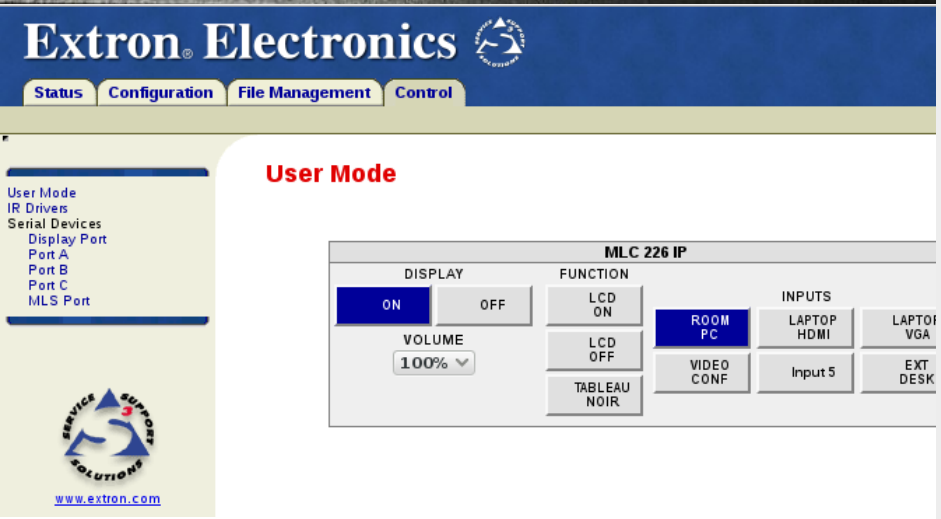


Disable not needed services

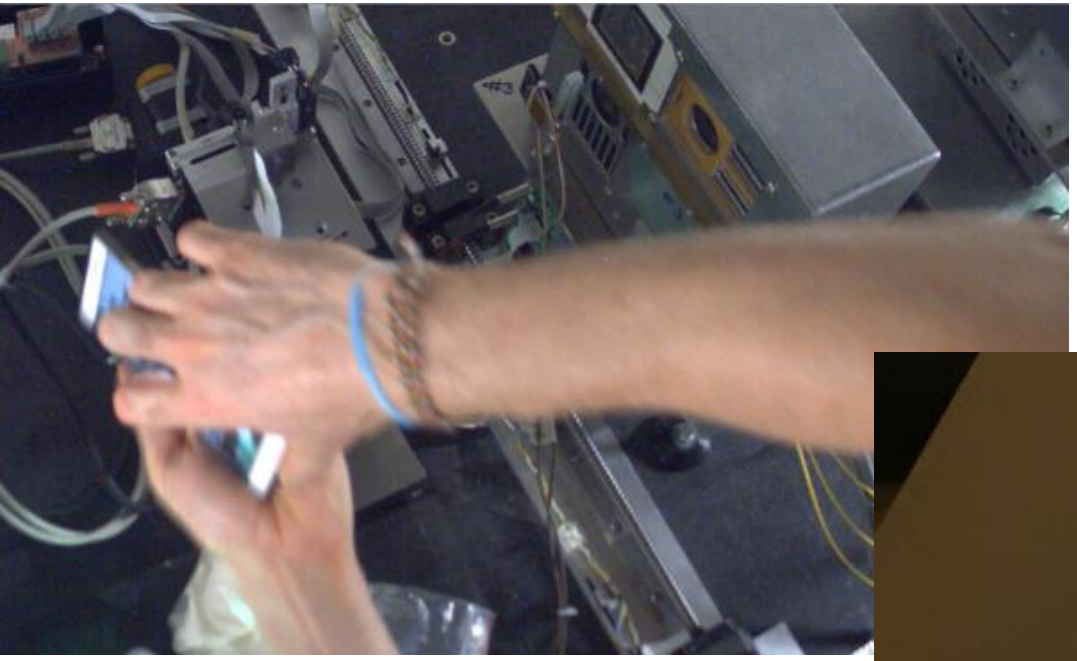
Index of ftp://[redacted]/

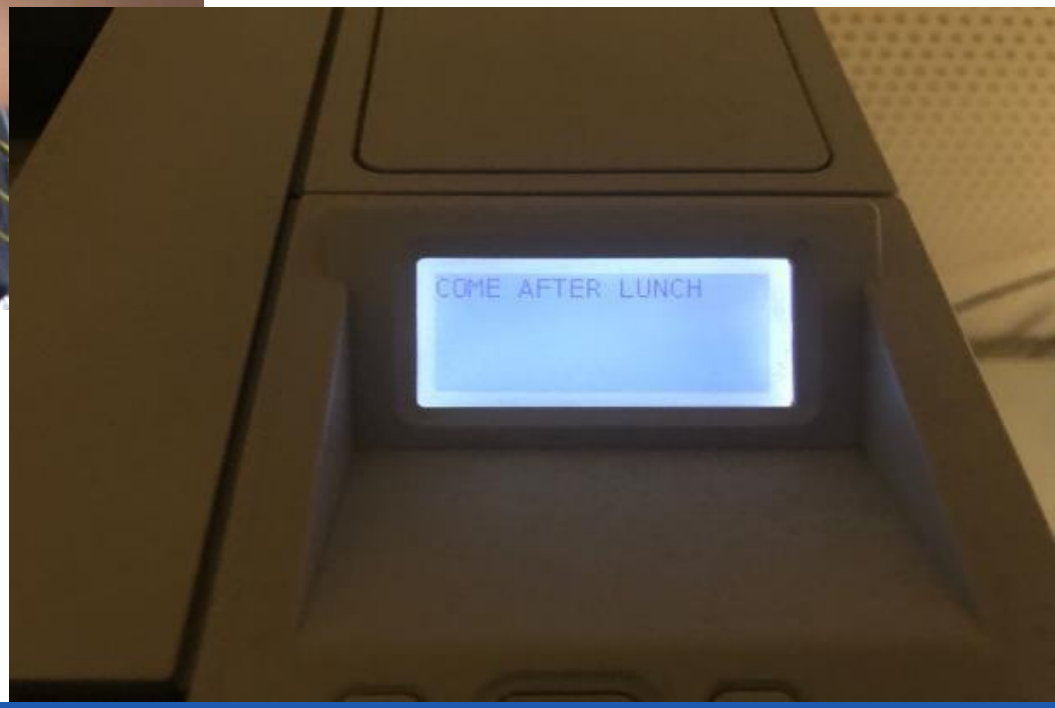
Up to higher level directory

Name	Size	Last Modified
Network		01/01/1998 02:00:00 PM
DSK1		01/01/1998 02:00:00 PM
Tracing		01/01/2006 01:00:00 PM
logs		01/01/2006 01:00:00 PM
devnodeServer.x64P	2643 KB	01/01/2006 02:00:00 PM
My Documents		01/01/2006 02:00:00 PM
Program Files		01/01/2006 02:00:00 PM
Temp		01/01/2006 02:00:00 PM
Windows		01/01/2006 02:00:00 PM

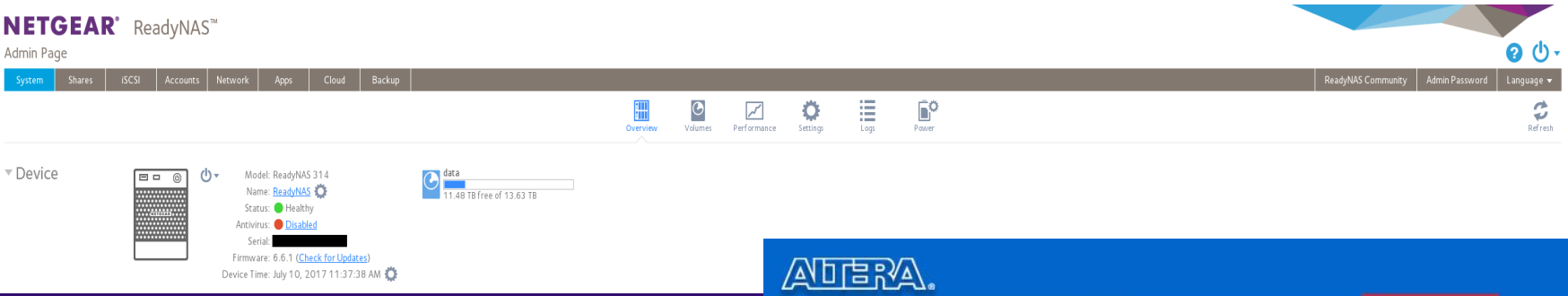


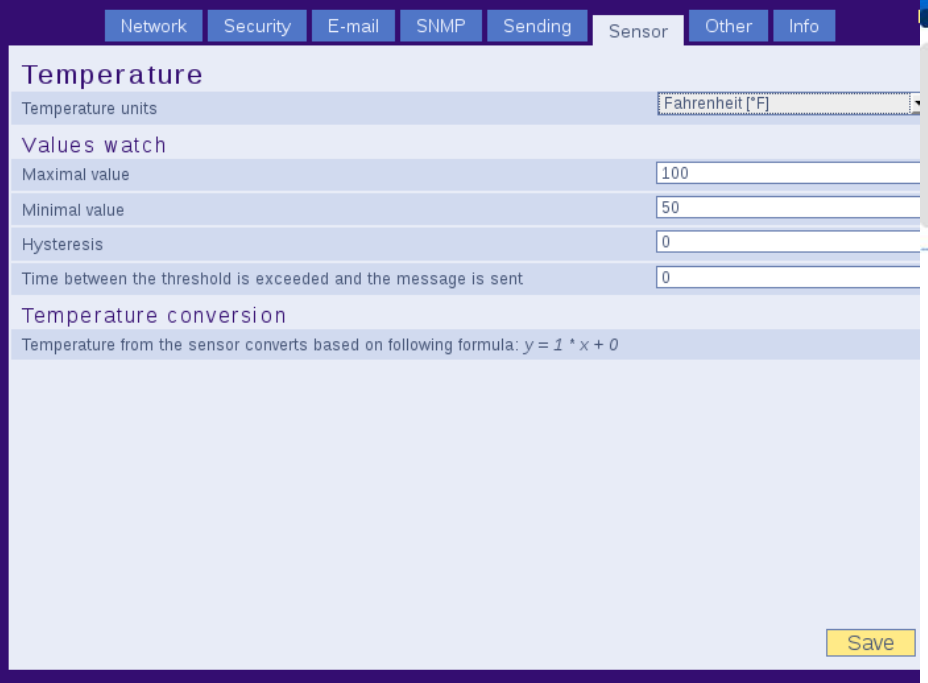
Be aware of authentication bypass

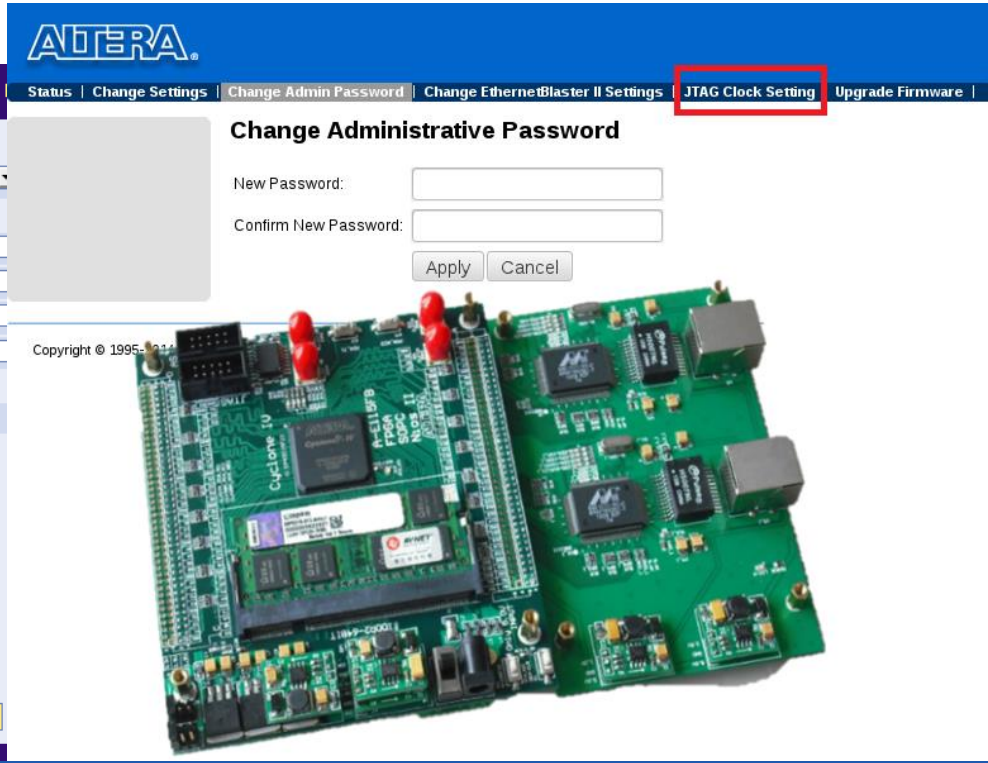




Don’t use guessable passwords







Keep your Firmware up-to-date

How we do improve IoT security

Which IoT is “*secure*“?

Estimating the security level of the IoT devices you run

You see the vulnerable IoT devices in your network

```
06:44 mktemp -> busybox
06:44 more -> busybox
06:44 mount -> busybox
06:44 mountpoint -> busybox
06:44 mv -> busybox
06:44 nice -> busybox
06:44 pidof -> busybox
06:44 ping -> busybox
06:44 pipe_progress -> busybox
06:44 printenv -> busybox
06:44 ps -> busybox
06:44 pwd -> busybox
06:44 rm -> busybox
06:44 rmdir -> busybox
06:44 sed -> busybox
06:44 sh -> busybox
06:44 sleep -> busybox
06:44 stat -> busybox
06:44 su -> busybox
06:44 sync -> busybox
06:44 tar -> busybox
06:44 touch -> busybox
06:44 true -> busybox
06:44 umount -> busybox
06:44 uname -> busybox
06:44 usleep -> busybox
06:44 vi -> busybox
06:44 watch -> busybox
06:44 zcat -> busybox
```

Remotely detecting IoT devices

- Clock skew
  - Remote measuring the internal Quartz

Estimating the security level of IoT devices

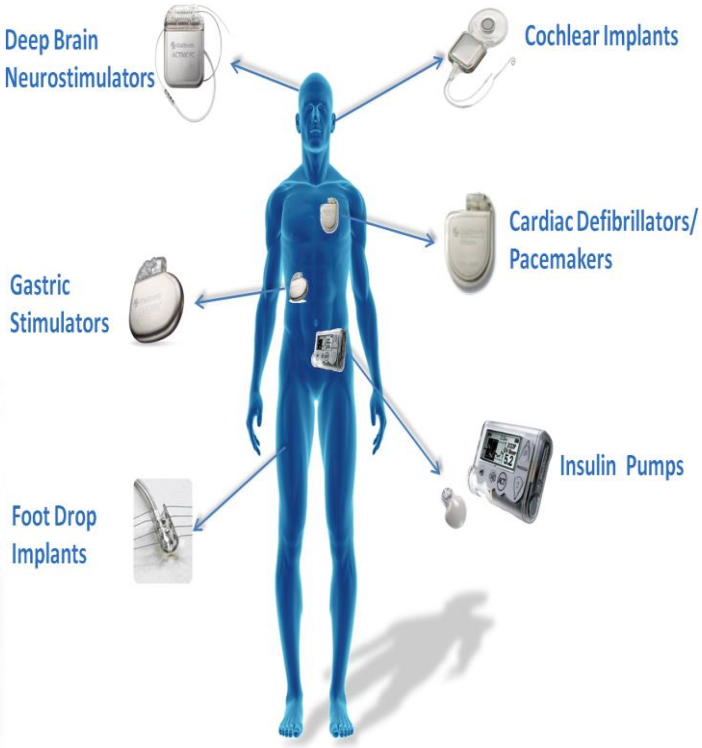
- Firmware analysis
  - Certificates, web server, libraries, code patterns, strings …

Summing-up

Internet of insecure Things

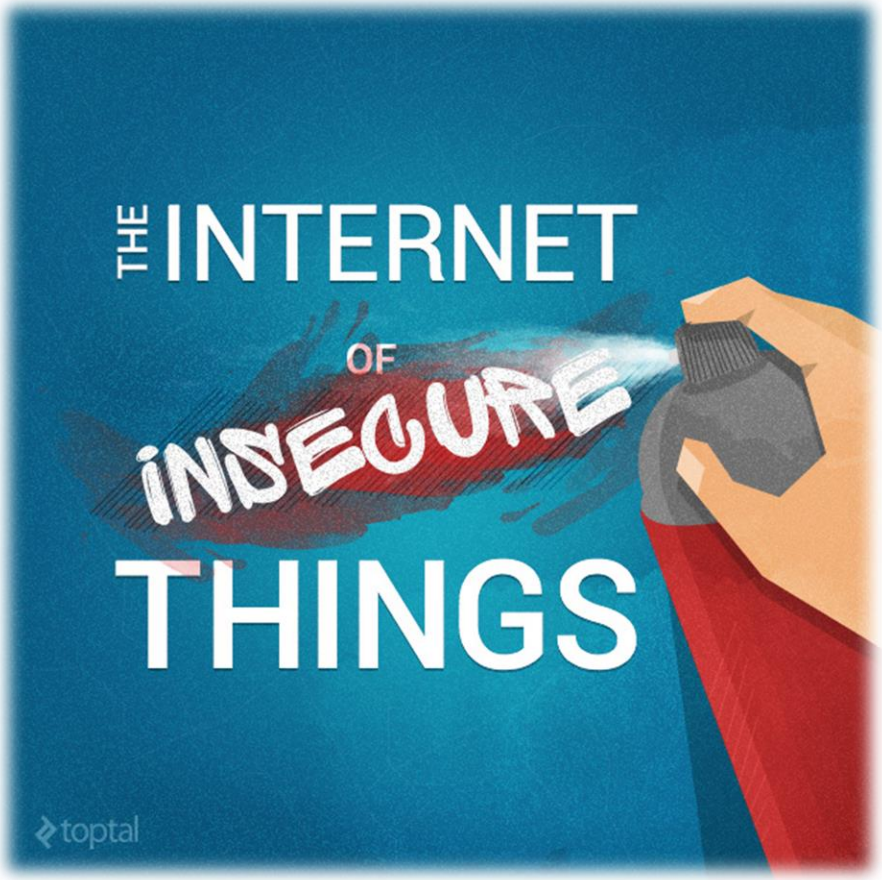
- Care about a secure product
- Configure your devices properly
- Choose strong credentials
- Don’t forget to update them
- Limit the access

- And be aware…



IoT don’t look always like IoT

Questions?



p.oser@cern.ch

Backup

IoT war flying

Resources

- Oscilloscope: http://www.conrad.com/medias/global/ce/2000_2999/2700/2780/2786/123467_BB_01_FB.EPS_1000.jpg
- Mirai: https://4.bp.blogspot.com/-p8D76bMmh38/WXcXv6OMDII/AAAAAAAAtw8/jJiK0rQiWIED4UqW6cCu2WW6mEaPGrqOwCLcBGAs/s1600/Mirai-Botnet-ddos-attack.png
- Jeep: https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix
- Smart meter: https://images.futurezone.at/smart-meter-neu-1.jpg/24.490.046
- Smart meter: http://www.bbc.com/news/technology-29643276
- Unsecure things: https://static1.squarespace.com/static/52b489ede4b01176ccb429a3/t/570fa14e07eaa02ef84be726/1460642254897/
- Medical: ww2.kqed.org/futureofyou/wp-content/uploads/sites/13/2015/07/Implantable-medical-devices_graphic_WHITE.jpg
- Busybox: https://i.ytimg.com/vi/GuXcdopoJII/maxresdefault.jpg
- Clock: https://www.microsemi.com/images/gallery/Chip%20Scale%20Atomic%20Clock-CSAC-300dpi.jpg
- Thermometer: https://static.webshopapp.com/shops/097528/files/044833734/papouch-tme-ethernet-thermometer.jpg
- SmartDuvet: https://www.smartduvet.com/
- Hair coach: https://health.nokia.com/us/en/hair-coach?btmsg&
- BBQ: http://www.wired.co.uk/topic/ces-2017
- Barbie: https://www.nytimes.com/2015/09/20/magazine/barbie-wants-to-get-to-know-your-child.html?_r=0
- Smart TV: http://www.bbc.com/news/technology-31296188
- Alexa: https://www.technologyreview.com/s/604284/amazons-echo-look-rates-your-outfits-and-slurps-up-revealing-data/#
- War flying: https://www.youtube.com/watch?v=Ed1OjAuRARU