### A Large Scale Analysis of the Security of Embedded Firmwares

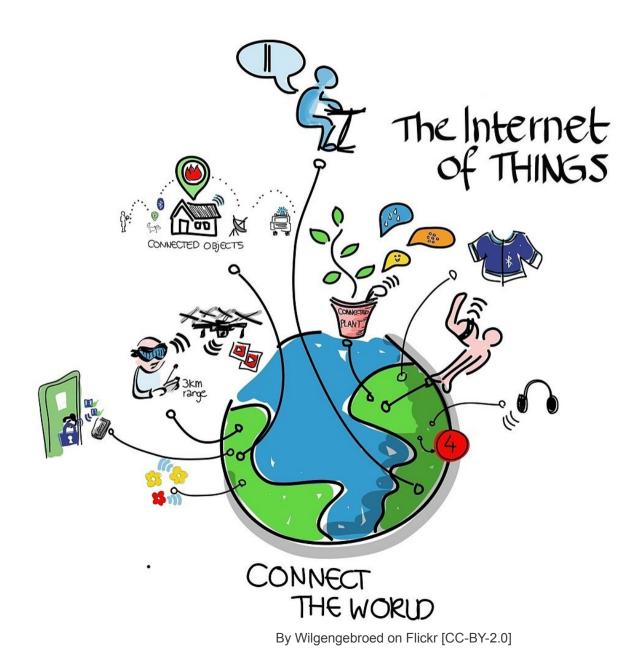
#### <u>A. Costin</u>, J. Zaddach, A. Francillon, D. Balzarotti EURECOM, France

20th August 2014

USENIX Security '14 – San Diego, USA



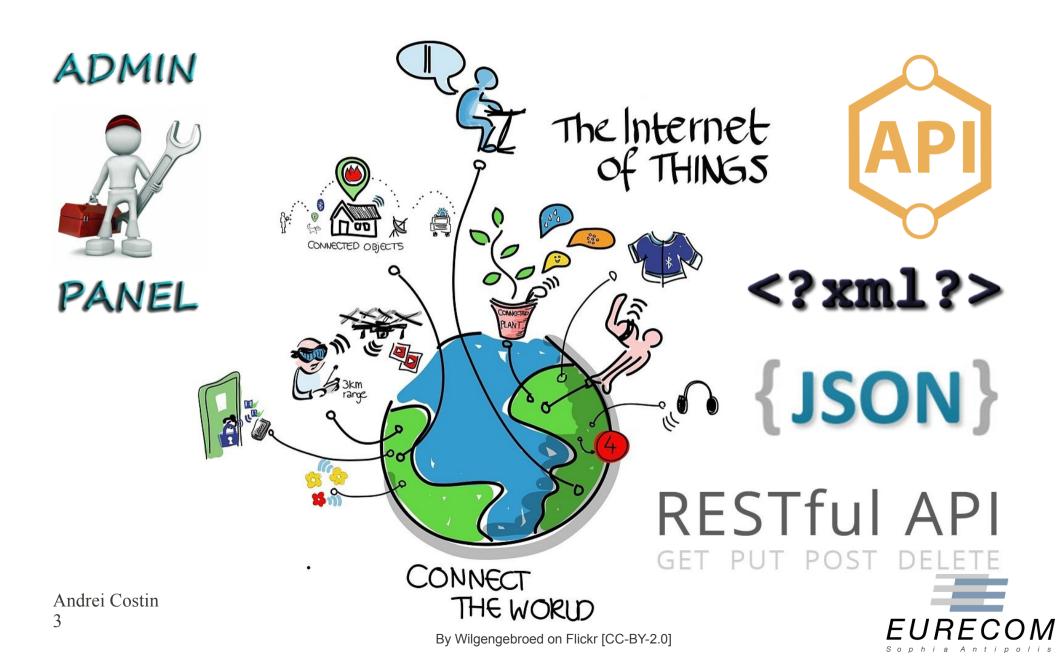
### Embedded Systems Are Everywhere



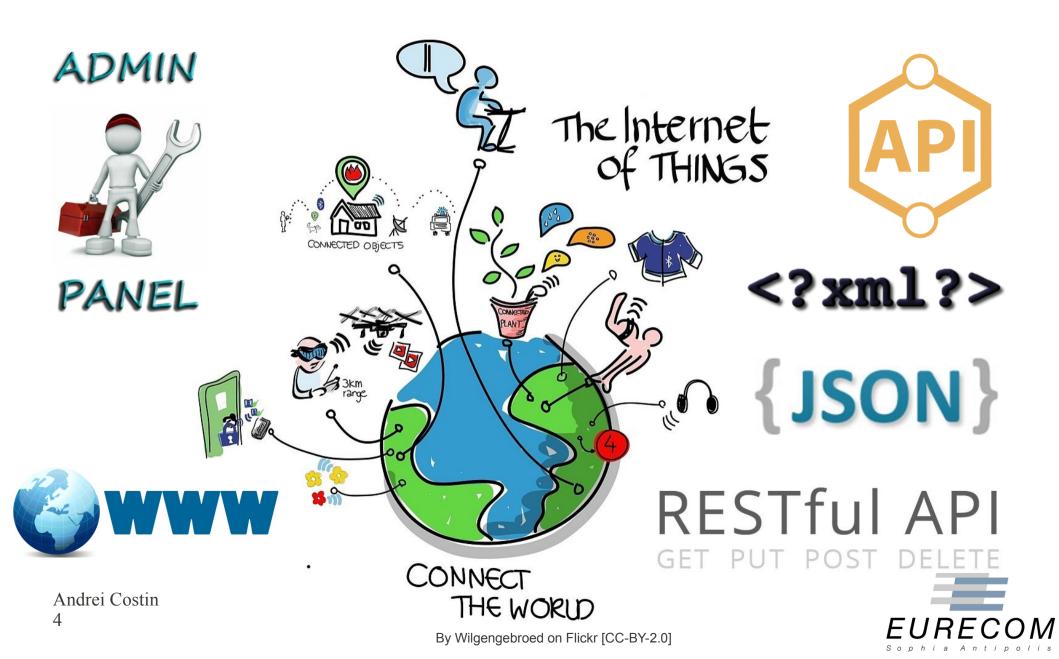


Andrei Costin 2

### **Smarter & More Complex**



### **Heavily Interconnected**



Routers

Firefox 🔻 🎇 Reverse Engineering a D-Link B... 🕂 www.devttys0.com/2013/10/reverse-engineering-a-d-link-backdoor/ Based on the source code of the HTML pages and some Shodan search results D-Link devices are likely affected: DIR-100 DIR-120 DI-624S DI-524UP DI-604S DI-604UP DI-604+ 2 TM-G5240 Additionally, several Planex routers also appear to use the same firmware: BRL-04R BRL-04UR BRL-04CW

You stay classy, D-Link.



- Routers
- Printers

#### Networked Printers at Risk 🟴

By Jimmy Shah on Dec 30, 2011



Multifunction printers (MFPs) have been common in offices for years. They let employees print, scan, and copy documents. Two separate talks at the 28th Chaos Communications Congress (28c3) show how attackers can infect these trusted office devices.

#### Hacking MFPs

In Andrei Costin's presentation "Hacking MFPs," he covered the history of printer and copier hacks from the 1960s to today. The meat of the talk concerned executing remote code on an MFP using crafted PostScript. Just printing a particular document can get code to run on the machine. Previous research proof of concepts have done exactly that, once with a specially designed Word document and once with a Java applet.





- Routers
- Printers
- VoIP

### FBI: Criminals Auto-dialing With Hacked VoIP Systems

By Robert McMillan, IDG News Service

Dec 5, 2008 5:50 PM 🛛 🖾 🖡

Criminals are taking advantage of a bug in the Asterisk Internet telephony system that lets them pump out thousands of scam phone calls in an hour, the U.S. Federal Bureau of Investigation warned Friday.

The FBI didn't say which versions of Asterisk were vulnerable to the bug, but it advised users to upgrade to the latest version of the software. Asterisk is an open-source product that lets users turn a Linux computer into a VoIP (Voice over Internet Protocol) telephone exchange.

In so-called vishing attacks, scammers usually use a VoIP system to set up a phony call center and then use phishing e-mails to trick victims into calling the center. Once there, they are prompted to give private information. But in the scam described by the FBI, they apparently are taking over legitimate Asterisk systems in order to directly dial victims.



- Routers
- Printers
- VoIP
- Cars

RBES 7/24/2013 @ 9:00AM 506,516 views

### Hackers Reveal Nasty New Car Attacks--With Me Behind The Wheel (Video)

This story appears in the August 12, 2013 issue of Forbes.

+ Comment Now + Follow Comments





- Routers
- Printers
- VoIP
- Cars
- Drones

#### Hacker Releases Software to Hijack Commercial Drones

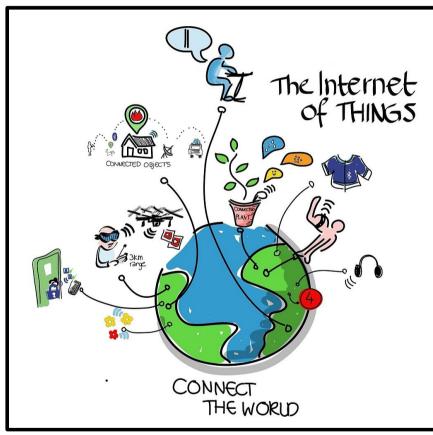
by BRYANT JORDAN on DECEMBER 9, 2013





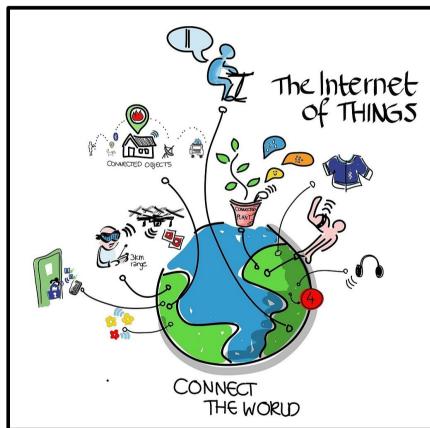


- Routers
- Printers
- VoIP
- Cars
- Drones
- •





- Routers
- Printers
- VoIP
- Cars
- Drones
- ..



- Each of above is a result of an individual analysis
- Manual and tedious efforts, Does not scale

Andrei Costin 11



### The Goal

## Perform a large scale analysis to provide a better undestanding of the problem



Andrei Costin 12

### The Problem With Large Scale Analysis

- Heterogeneity of
  - Hardware, architectures, OSes
  - Users, requirements
  - Security goals



### The Problem With Large Scale Analysis

- Heterogeneity of
  - Hardware, architectures, OSes
  - Users, requirements
  - Security goals
- Manual analysis does not scale, it requires
  - Finding and downloading the firmwares
  - Unpacking and performing initial analysis
  - Re-discovering the same or similar bug in other firmwares



### **Previous Approaches**

- Test on real devices [Bojinov09CCS]
  - Accurate results
  - Does not scale well



### **Previous Approaches**

- Test on real devices [Bojinov09CCS]
  - Accurate results
  - Does not scale well

- Scan devices on the Internet
  - Large scale testing [Cui10ACSAC]
    - Can only test for known vulnerabilities
    - Blackbox approach
  - More is too intrusive [Census2012]



• Collect a large number of firmware images



- Collect a large number of firmware images
- Perform broad but simple static analysis



- Collect a large number of firmware images
- Perform broad but simple static analysis
- Correlate across firmwares



- Collect a large number of firmware images
- Perform broad but simple static analysis
- Correlate across firmwares
- Advantages
  - No intrusive online testing, no devices involved
  - Scalable



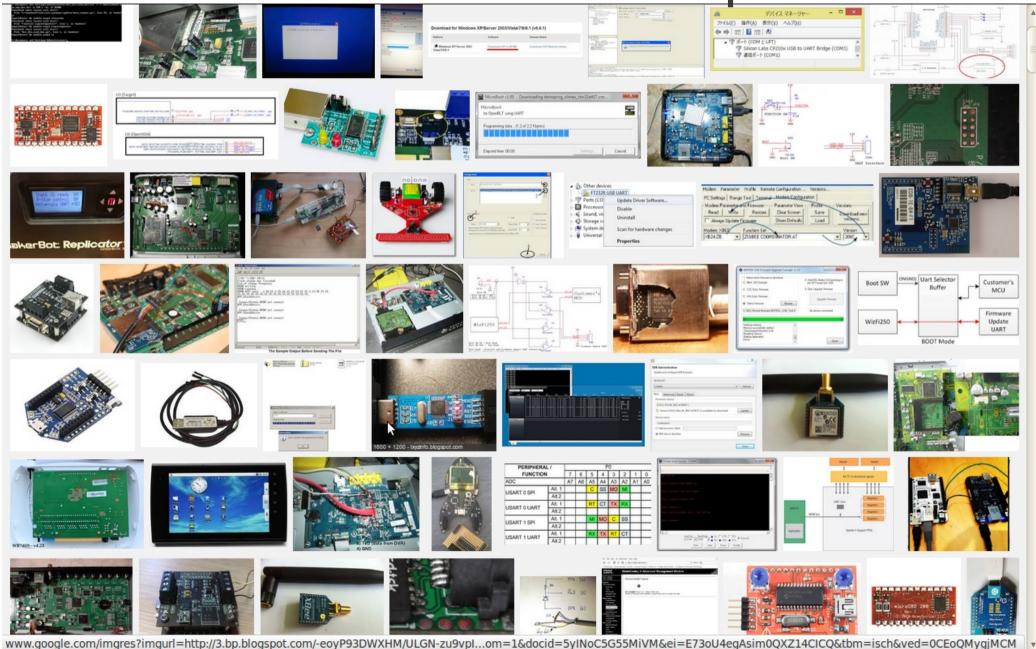
- Collect a large number of firmware images
- Perform broad but simple static analysis
- Correlate across firmwares
- Advantages
  - No intrusive online testing, no devices involved
  - Scalable
- But many challenges



### Mainstream Systems Have Centralized Updates

😣 🔿 🗊 Update Manager		💐 Windows Update			
Welcome to Ubuntu Since this version of Ubuntu was released, these software updates have been		Search Control Panel			Search Control Panel
		File Edit View Tools Help			
issued.    Image: Stribution updates   Image: Daemon which notifies about package updates   Image: Update-notifier (Size: 53 kB)		Control Panel Home Check for updates Change settings View update history Restore hidden updates		Windows Update	
Image: state of the state				1 important updat is available	
2 updates have been selected. 100 kB will be dow	Softw	are Update		8 optional update	7.4 MD
	New software is available for your computer. If you're not ready to install now, you can use the Software Update preference to check for updates later.		are available	Install updates	
	Install Name	Version	Size	Most recent check for updates: T	oday at 8:12 AM
	iDVD Update	7.0.1	20.2 MB	Updates were installed: 3	/15/2010 at 4:05 PM.
	iMovie Update GarageBand Update	7.1	46.1 MB		lew update history
		4.1	47.0 MB		or Windows and other products
	iPhoto Update	7.1	61.8 MB	fr fr	n Microsoft Update
▶ Description of update	iLife Support	8.1	10.3 MB	1	
Settings	This update supports system software components shared by all iLife '08 applications, improves overall stability, addresses a number of other minor issues, and supports general compatibility issues. It is recommended for all users of iLife '08.		Find out more about free softwar Click here for details.	re from Microsoft Update.	
Andrei Costin 22	Note: Use of this software is subject to that accompanied the software being up here: http://www.apple.com/legal/sla/.	pdated. A list of Apple SLAs			FURECOM

### Challenge: Embedded Systems Have No Centralized Updates



- No large scale firmware dataset yet
  - As opposed to existing datasets in security or other CS research areas



- No large scale firmware dataset yet
  - As opposed to existing datasets in security or other CS research areas
- We collected a subset of the firmwares available for download

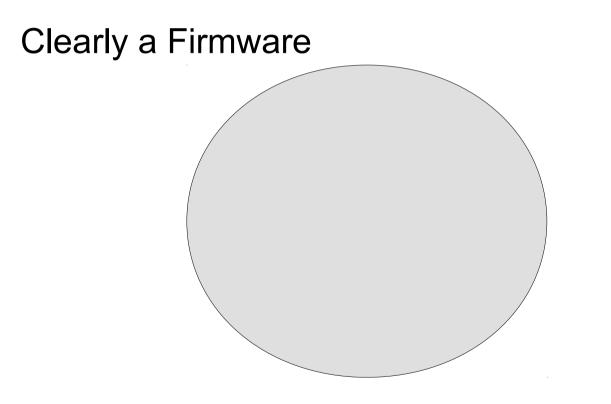


- No large scale firmware dataset yet
  - As opposed to existing datasets in security or other CS research areas
- We collected a subset of the firmwares available for download
- Many firmwares are not publicly available
  - Not intended to have an upgrade
  - Require product purchase and registration



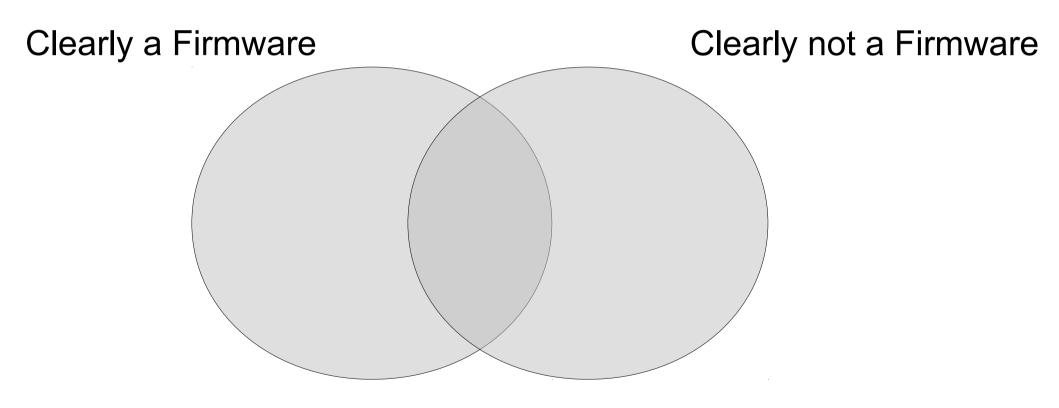
- No large scale firmware dataset yet
  - As opposed to existing datasets in security or other CS research areas
- We collected a subset of the firmwares available for download
- Many firmwares are not publicly available
  - Not intended to have an upgrade
  - Require product purchase and registration
- www.firmware.re project



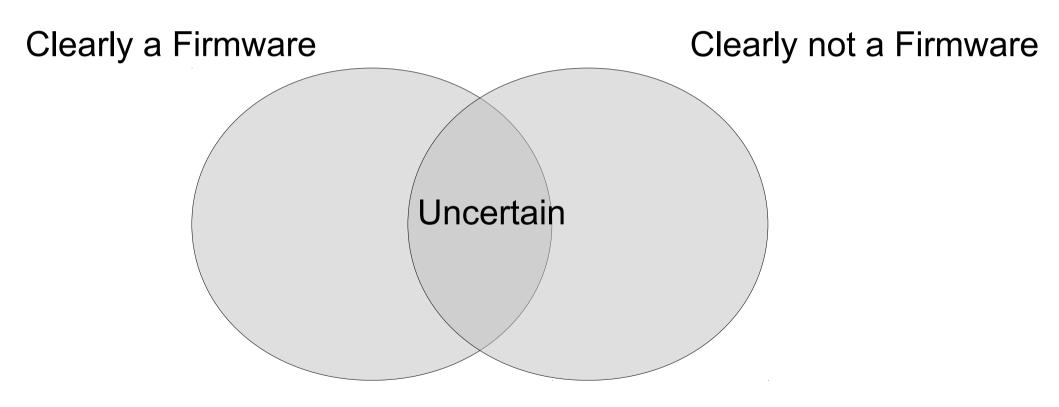




Andrei Costin 28

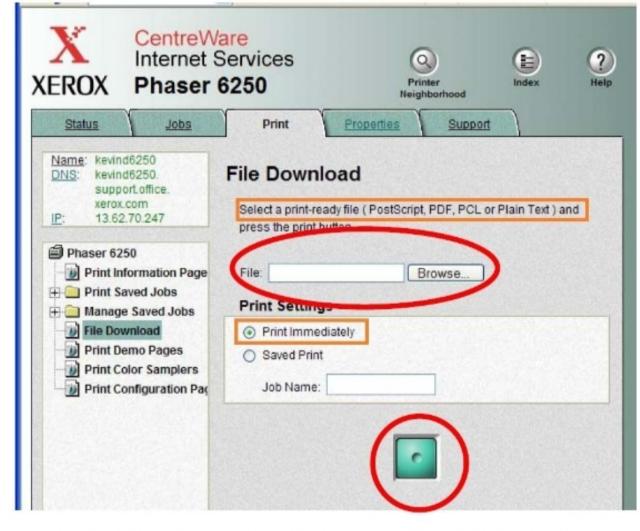








#### • E.g., upgrade by printing a PS document



Andrei Costin 31

Figure 4: Select the firmware update file and press the green button to send it.



How to reliably unpack and learn formats?



- How to reliably unpack and learn formats?
- E.g., vendor provides a .ZIP 'firmware package'
  - .ZIP→.EXE+.PS
    - .EXE $\rightarrow$ self-extracting archive
      - Extract more or not?
      - Turns out to contain a printer driver inside



- How to reliably unpack and learn formats?
- E.g., vendor provides a .ZIP 'firmware package'
  - .ZIP→.EXE+.PS
    - .EXE $\rightarrow$ self-extracting archive
      - Extract more or not?
      - Turns out to contain a printer driver inside
    - .PS $\rightarrow$ ASCII85 stream $\rightarrow$ ELF file that could be:
      - A complete embedded system software
      - An executable performing the firmware upgrade
      - A firmware patch



- How to reliably unpack and learn formats?
- E.g., vendor provides a .ZIP 'firmware package'
  - .ZIP→.EXE+.PS
    - .EXE $\rightarrow$ self-extracting archive
      - Extract more or not?
      - Turns out to contain a printer driver inside
    - .PS $\rightarrow$ ASCII85 stream $\rightarrow$ ELF file that could be:
      - A complete embedded system software
      - An executable performing the firmware upgrade
      - A firmware patch
- Often, a firmware image→just 'data' binary blob



Andrei Costin 35

### Our Approach to Unpacking & Custom Formats

- We compared existing tools
- Used BAT (Binary Analysis Toolkit)
  - Extended it with multiple custom unpackers
  - Continuous development effort



## Our Approach to Unpacking & Custom Formats

- We compared existing tools
- Used BAT (Binary Analysis Toolkit)
  - Extended it with multiple custom unpackers
  - Continuous development effort
- Often, a firmware image→just 'data' binary blob
  - File carving required
  - Bruteforce at every offset with all known unpackers



## Our Approach to Unpacking & Custom Formats

- We compared existing tools
- Used BAT (Binary Analysis Toolkit)
  - Extended it with multiple custom unpackers
  - Continuous development effort
- Often, a firmware image→just 'data' binary blob
  - File carving required
  - Bruteforce at every offset with all known unpackers
- Heuristics for detecting when to stop



### Challenge: Scalability & Computational Limits

Unpacking and file carving is very CPU intensive



### Challenge: Scalability & Computational Limits

Unpacking and file carving is very CPU intensive

- Results in millions of unpacked files
  - Manual analysis infeasible
  - One-to-one fuzzy hash comparison is CPU intensive



### Challenge: Results Confirmation

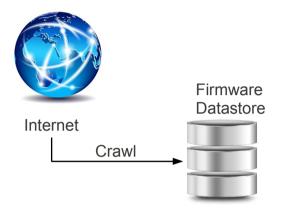
- An issue found statically
  - May not apply to a real-device
  - Cannot guarantee exploitability
  - E.g., vulnerable daemon present but never started



### Challenge: Results Confirmation

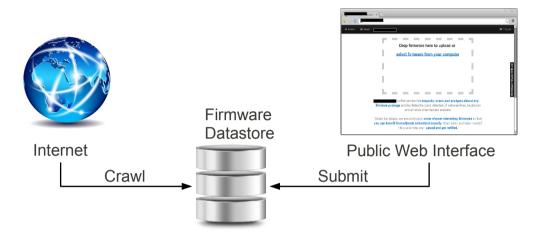
- An issue found statically
  - May not apply to a real-device
  - Cannot guarantee exploitability
  - E.g., vulnerable daemon present but never started
- Issue confirmation is difficult
  - Requires advanced analysis (static & dynamic)
  - Often requires real embedded devices
  - Does not scale well in heterogeneous environments



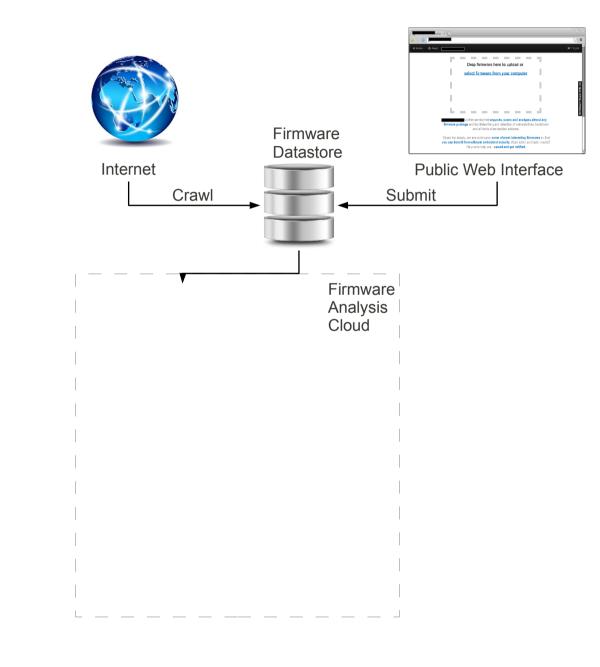




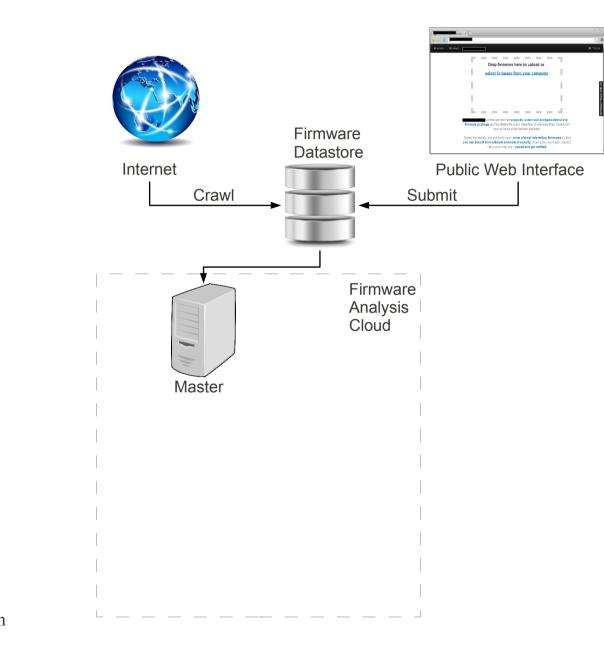
Andrei Costin 43





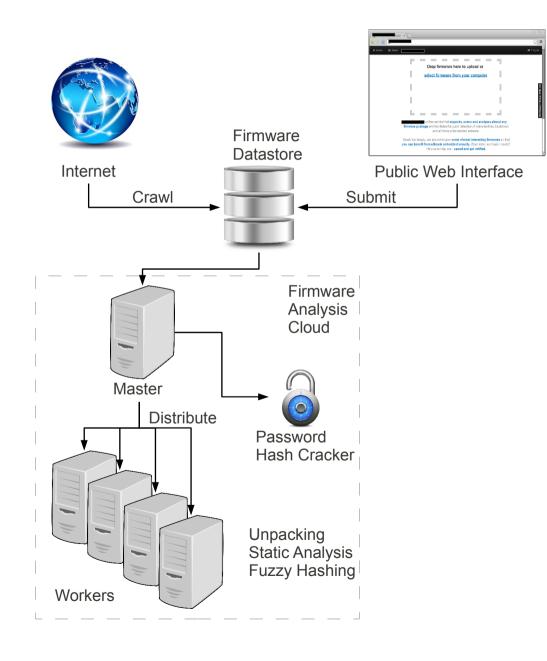






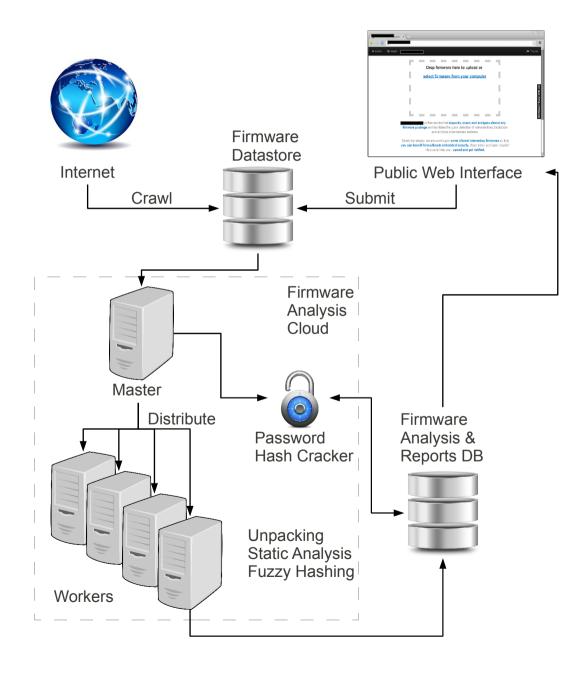


Andrei Costin 46



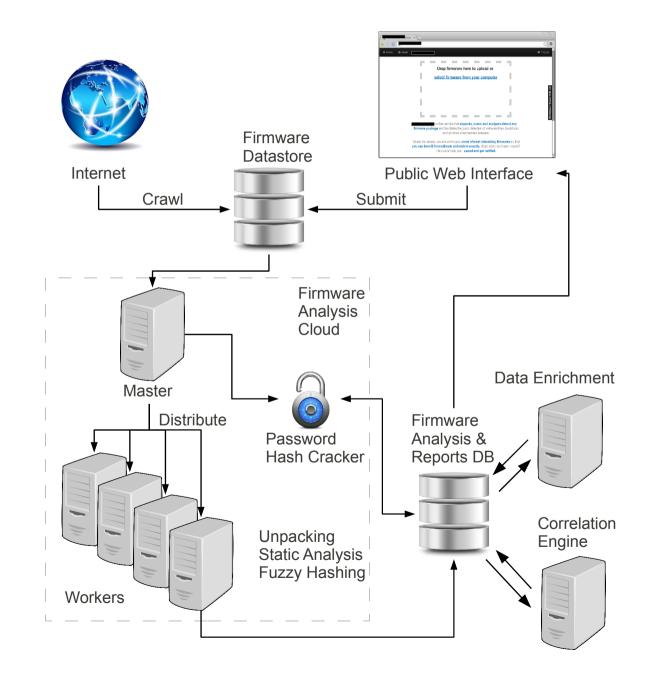


Andrei Costin 47





Andrei Costin 48



EURECOM

Andrei Costin 49

### Crawler

• 759 K collected files, 1.8 TB of disk space



### Crawler

• 759 K collected files, 1.8 TB of disk space

### • FTP-index engines

www.**mmnt.net**/get?cx=partner-pub-7093288927147322%3Asqzu2pvo68m&cof=FORID%3

#### **Mamont's open FTP Index**

firmware	download	

MMNT.net search

About 1,260 results (0.31 seconds)

#### Index of ftp://ftp2.zyxel.com/NSA310/firmware 450AFK1C0.bin, 41.63Mb, August 14 2012 at 10:58. [ZIP] NSA310 4.22(AFK.0) C0.zip,

36.07Mb, August 24 2011, [ZIP] NSA310\_4.22(AFK.1)C0.zip, 36.24Mb ... www.mmnt.net/db/0/0/ftp2.zyxel.com/NSA310/firmware

2

#### Index of ftp://ftp.d-link.co.za/dwr512/Firmware

DWR-512 V1.01b06, 0.00b, October 9 2013 at 09:55. [DIR] Latest DWR-512 V1. 06b01.BIN, 0.00b, October 9 2013 at 09:55. [DIR] V 1.01b05 dwr512, 0.00b ... www.mmnt.net/db/0/0/ftp.d-link.co.za/dwr512/FIrmware

Index of ftp://www.scansourcela.us/Bixolon/Firmware Download Utility 350plus 352plus 500 370 372 275, 0.00b, January 18 2008. [TXT] Firmware Download,selftest,Hexdump manual for SRP-350, SRP-770 STP-103.pdf, 214.76 ... www.mmnt.net/db/0/0/www../Firmware%20Download%20Utility

Index of ftp://ftp.zyxeltech.de/SP-300E/firmware SP-300E Upgrade Utility ReleaseNote v1.00.00.txt, 516.00b, March 1 2012 at 18: 33. [TXT] SP300E V1.03.txt, 1.52Kb, March 1 2012 at 18:33. [ZIP] ... www.mmt.net/db/0/0/ftp.zyxeltech.de/SP-300E/firmware

Index of ftp://ftp2.zyxel.com/WAP3205/firmware 100BFR7C0.bin, 3.31Mb, November 27 2012 at 05:11. [ZIP] WAP3205\_1.00(BFR .0)C0.zip, 3.37Mb, July 27 2009. [ZIP] WAP3205\_1.00(BFR.1)C0.zip, 3.38Mb ... www.mmt.net/db/0//ftp2.zyxel.com/WAP3205/firmware

Index of ftp://ftp2.zyxel.com/NSA325/firmware 450AFO1C1.rar, 41.22Mb, January 4 2013 at 01:46. [ZIP] NSA325\_4.30(AAAJ.0) C0.zip,

Andrei Costin 51



### Crawler

759 K collected files, 1.8 TB of disk space

MMNT.net search

### FTP-index engines and GCSE

www.mmnt.net/get?cx=partner-pub-7093288927147322%3Asgzu2pvo68m&cof=FORID%3

#### Mamont's open FTP Index

firmware download		
About 1.060 requite (0.21 accords)	2	

About 1,260 results (0.31 seconds)

#### Index of ftp://ftp2.zyxel.com/NSA310/firmware

www.mmnt.net/db/0/0/ftp.d-link.co.za/dwr512/Firmware

450AFK1C0.bin, 41.63Mb, August 14 2012 at 10:58. [ZIP] NSA310 4.22(AFK.0) C0.zip, 36.07Mb, August 24 2011. [ZIP] NSA310 4.22(AFK.1)C0.zip, 36.24Mb ... www.mmnt.net/db/0/0/ftp2.zyxel.com/NSA310/firmware

Index of ftp://ftp.d-link.co.za/dwr512/Firmware DWR-512 V1.01b06, 0.00b, October 9 2013 at 09:55. [DIR] Latest DWR-512 V1. 06b01.BIN, 0.00b, October 9 2013 at 09:55. [DIR] V 1.01b05 dwr512, 0.00b ...

Index of ftp://www.scansourcela.us/Bixolon/Firmware Download Utility 350plus 352plus 500 370 372 275, 0.00b, January 18 2008. [TXT] Firmware Download, selftest, Hexdump manual for SRP-350, SRP-770 STP-103.pdf, 214.76 ... www.mmnt.net/db/0/0/www.../Firmware%20Download%20Utility

Index of ftp://ftp.zyxeltech.de/SP-300E/firmware SP-300E Upgrade Utility ReleaseNote v1.00.00.txt, 516.00b, March 1 2012 at 18: 33. [TXT] SP300E V1.03.txt, 1.52Kb, March 1 2012 at 18:33. [ZIP] ... www.mmnt.net/db/0/0/ftp.zyxeltech.de/SP-300E/firmware

#### Index of ftp://ftp2.zyxel.com/WAP3205/firmware

100BFR7C0.bin, 3.31Mb, November 27 2012 at 05:11. [ZIP] WAP3205 1.00(BFR .0)C0.zip, 3.37Mb, July 27 2009. [ZIP] WAP3205 1.00(BFR.1)C0.zip, 3.38Mb ... www.mmnt.net/db/0/0/ftp2.zyxel.com/WAP3205/firmware

Index of ftp://ftp2.zvxel.com/NSA325/firmware 450AFO1C1.rar, 41.22Mb, January 4 2013 at 01:46. [ZIP] NSA325 4.30(AAAJ.0) C0.zip, About 2,160 results (0.19 seconds)

Sort by:

Relevance

powered by Google " Custom Search

#### Current Firmware

https://support.nikonusa.com/.../cu rrent-firmware-downloads-availabl e-for- nikon-products

Current Firmware downloads available for Nikon products. Answer ID 13783 Published 12/06/2005 03:04 PM/Updated 07/16/2014 01:19 PM ...

#### D5200 firmware: C: 1.02

https://support.nikonusa.com/.../d5 200-firmware%3A-c%3A-1.02-upgr ade

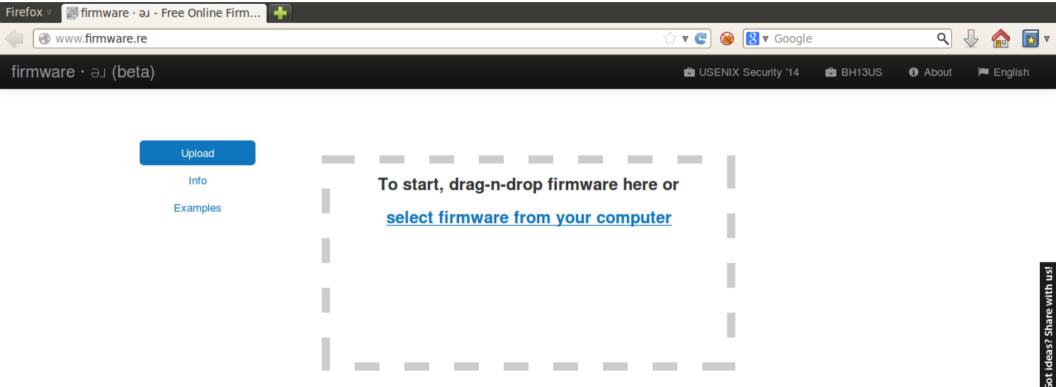
Jan 14, 2014 ... This is the D5200 firmware upgrade download -Please review the information provided, and click the appropriate download at the bottom of ...

#### Update Firmware

support.nikonusa.com/fagid=14187 Nikon USA Support · My Account ·



### www.Firmware.RE (beta) Will provide Unpacking and Analysis



## Unpacking

 759 K total files collected Filter non firmware 172 K filtered interesting files Random selection 32 K analyzed Successful unpack • 26 K unpacked (fully or partially)

Unpacked files

• 1.7 M resulted files after unpacking

Andrei Costin 54

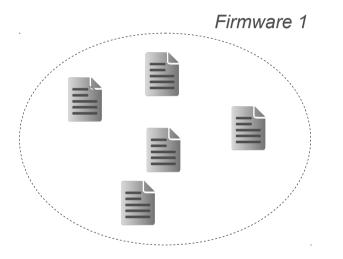


### Static Analysis

- Correlation/clustering
  - Fuzzy hashes, Private SSL keys, Credentials
- Misconfigurations
  - Web-server configs, Credentials, Code repositories
- Data enrichment
  - Version banners
  - Keywords (e.g., telnet, shell, UART, backdoor)

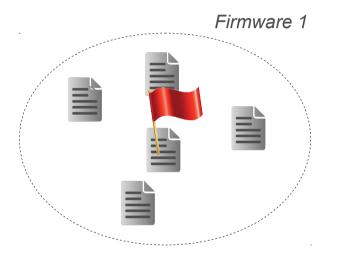


- Correlation via fuzzy-hashes (ssdeep, sdhash)
  - E.g., Vulnerability Propagation





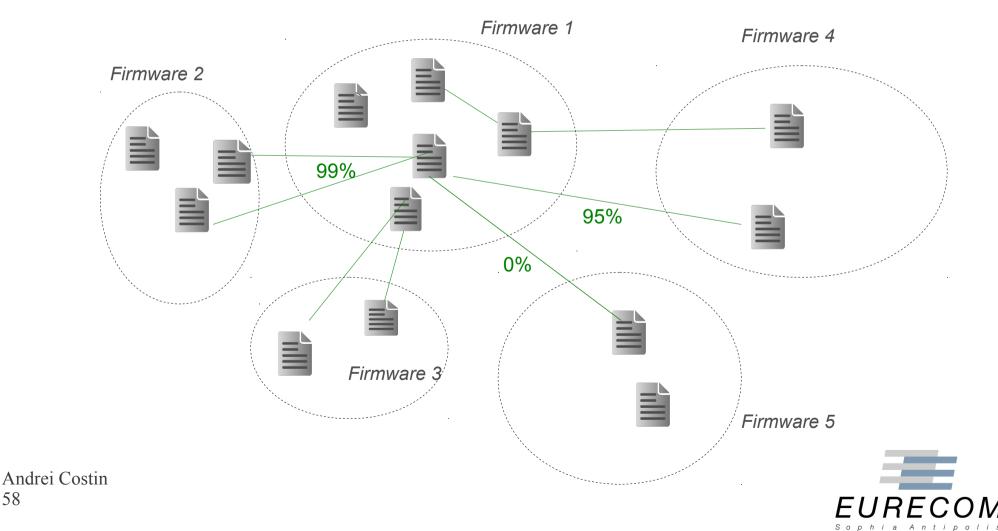
- Correlation via fuzzy-hashes (ssdeep, sdhash)
  - E.g., Vulnerability Propagation



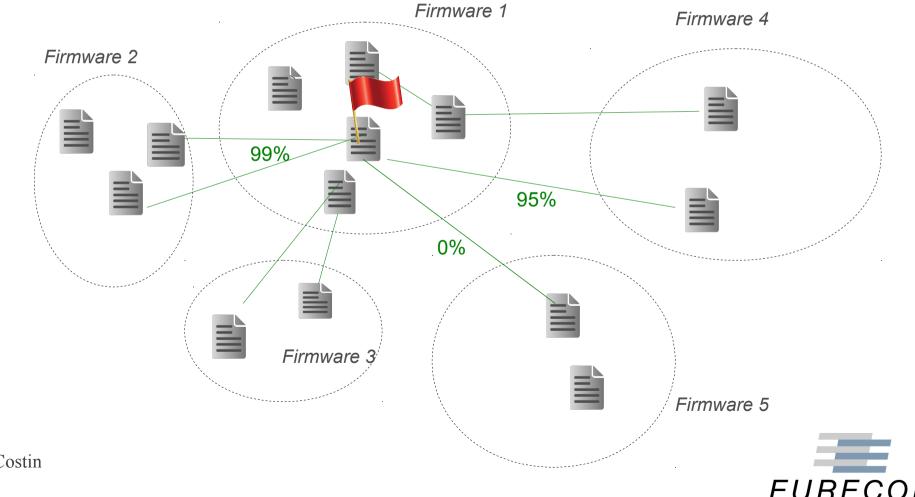


- Correlation via fuzzy-hashes (ssdeep, sdhash)
  - E.g., Vulnerability Propagation

58

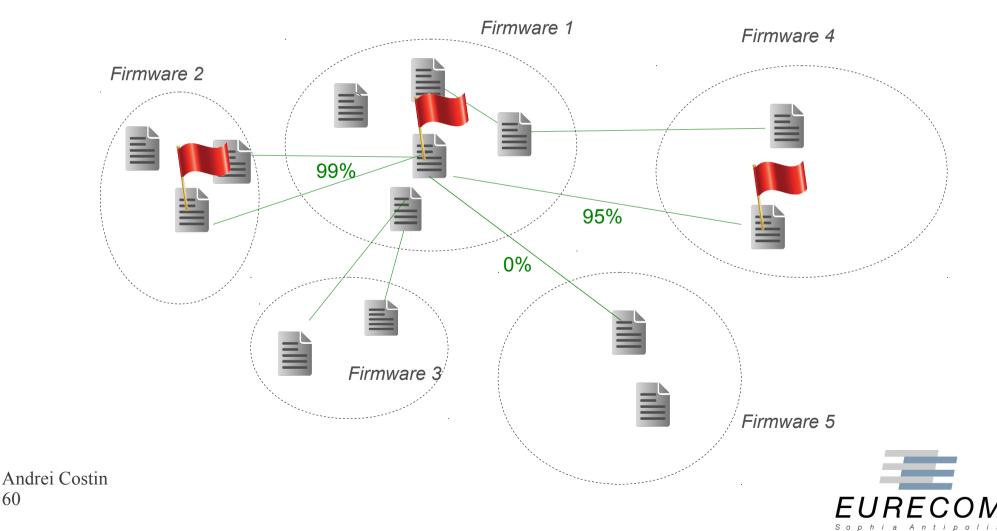


- Correlation via fuzzy-hashes (ssdeep, sdhash)
  - E.g., Vulnerability Propagation



- Correlation via fuzzy-hashes (ssdeep, sdhash)
  - E.g., Vulnerability Propagation

60



• SSL keys correlation + vulnerability propagation

Private RSA keys





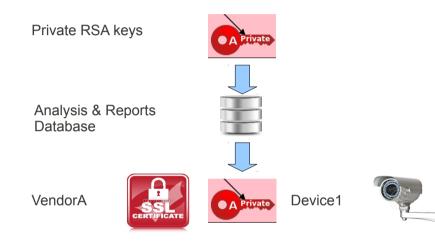
SSL keys correlation + vulnerability propagation

Private RSA keys

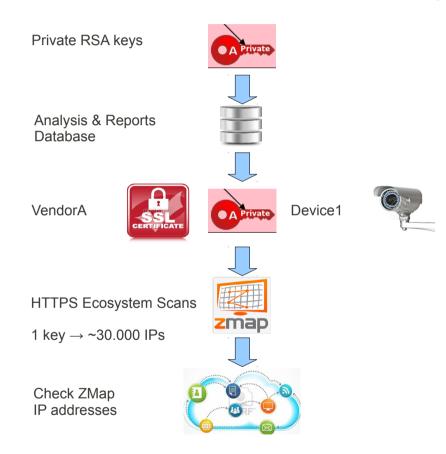


Analysis & Reports Database

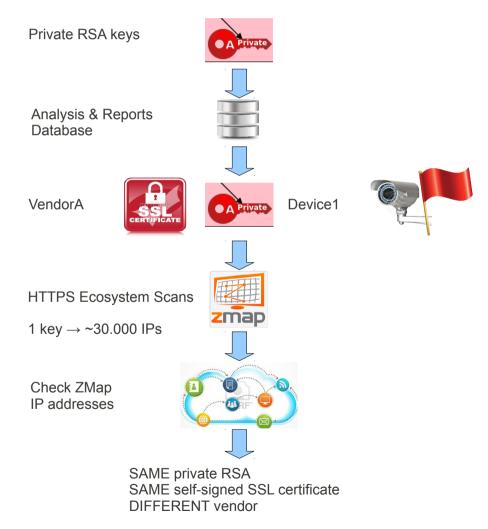










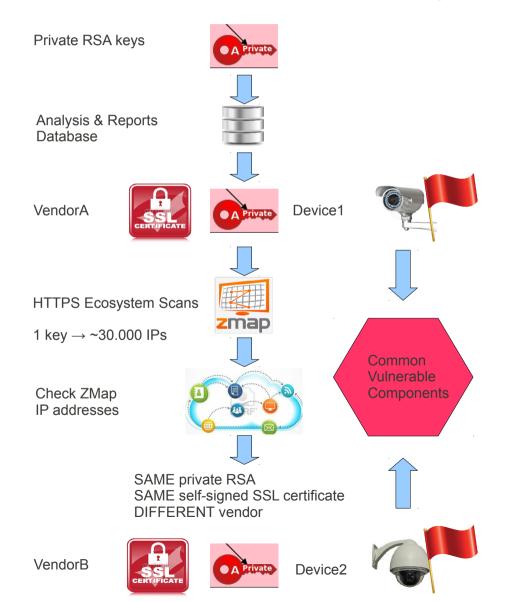














### **Results: Summary**

• 38 new vulnerabilities (CVE)

• Correlated them to 140 K online devices

• Affected 693 firmware files by at least one vuln



### **Contributions Summary**

- First large-scale static analysis of firmwares
- Described the main challenges associated
- Shown the advantages of performing a largescale analysis of firmware images
- Implemented a framework and several efficient static techniques



### Conclusions

- A broader view on firmwares
  - Not only beneficial
  - But necessary for discovery and analysis of vulnerabilities
- Correlation reveals firmware relatioship
  - Shows how vulnerabilities reappear across different products
  - Could allow seeing how firmwares evolve/get fixed



### Conclusions

• There are plenty of latent vulnerabilities

- Security
  - Tradeoff with cost and time-to-market
  - Clearly not a priority for some vendors



# Thank You! Questions?

### {name.surname}@eurecom.fr



Andrei Costin 71

### References

- [1] A. Costin, J. Zaddach, A. Francillon, D. Balzarotti, "A Large-Scale Analysis of the Security of Embedded Firmwares", In Proceedings of the 23<sup>rd</sup> USENIX Conference on Security (to appear)
- [2] A. Costin, J. Zaddach, "Poster: Firmware.RE: Firmware Unpacking and Analysis as a Service", In Proceedings of the ACM Conference on Security and Privacy in Wireless Mobile Networks (WiSec) '14
- [3] A. Costin, A. Francillon, "Short paper: A Dangerous 'Pyrotechnic Composition': Fireworks, Embedded Wireless and Insecurity-by-Design", In Proceedings of the ACM Conference on Security and Privacy in Wireless Mobile Networks (WiSec) '14

