IoT (In)Security: Lessons not Learned
The OWASP IoT Security Project

Dr. Vasileios Vlachos

Assistant Professor

University of Thessaly

Emerging Threats

- IoT (In)Security
- Critical Infrastructure / SCADA Systems

Threats can be subtle or overt.

Actor Justus D. Barnes, in *The Great Train Robber*

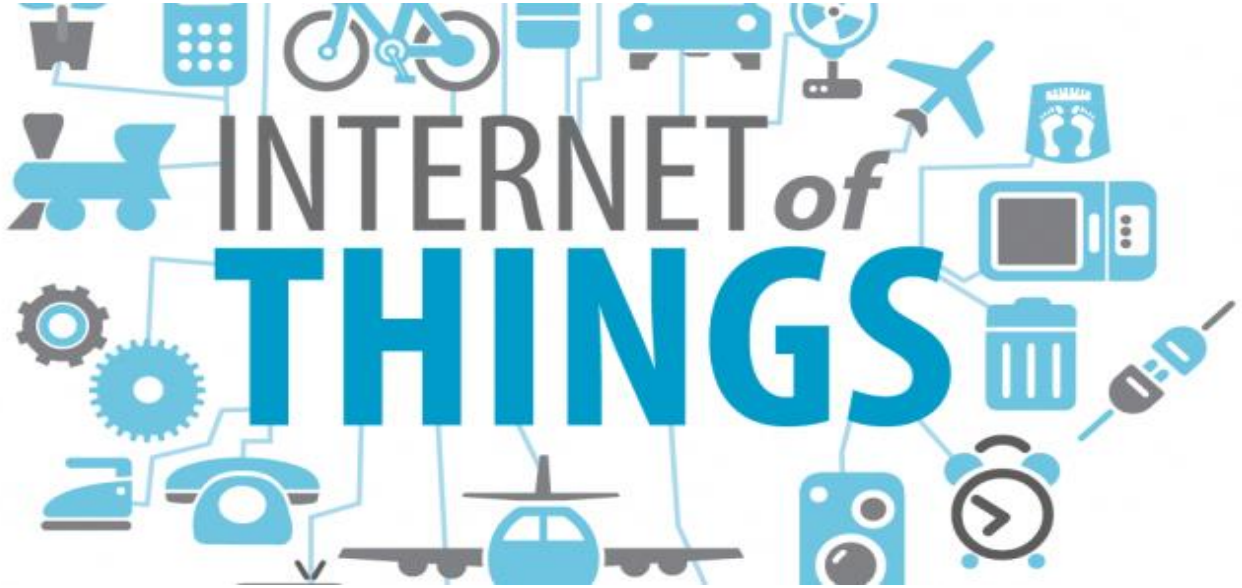
By Edwin S. Porter - The Kobal Collection, Public Domain, https://commons.wikimedia.org/w/index.php?curid=13518

OWASP Internet of Things Project

Internet of Things – IoT ???

"A proposed development of the Internet in which everyday objects have network connectivity, allowing them to send and receive data."

- Oxford Dictionary

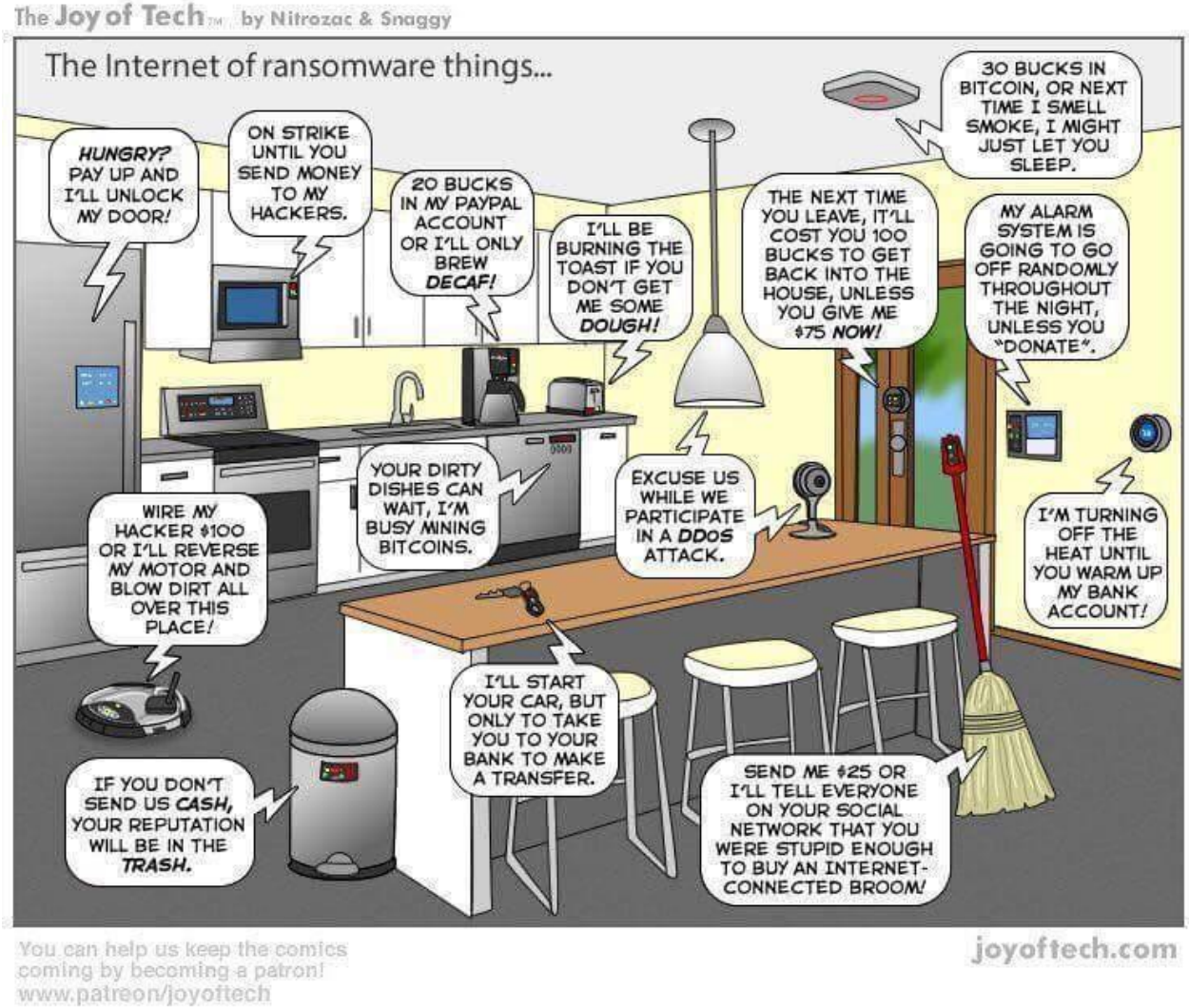


Source: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project *Image Source:* *http://www.itsecurityguru.org/2018/04/10/internet-broken-things-10-key-facts-iot/*

Lessons NOT Learned: IoT (In)Security

Why IoT is important?

- "Internet of things" becomes part of our life
- Animate and inanimate will be interconnected
- Unique identification between each other
- Billion devices are connected already
- More and more devices will be connected in the near future
- The more the devices the largest the **ATTACK** surface



Lessons NOT Learned: IoT (In)Security

IoT: From Internet of Things to Internet of Threats

Forbes

19,305 views | Jul 27, 2017, 05:00pm

Criminals Hacked A Fish Tank To Steal Data From A Casino

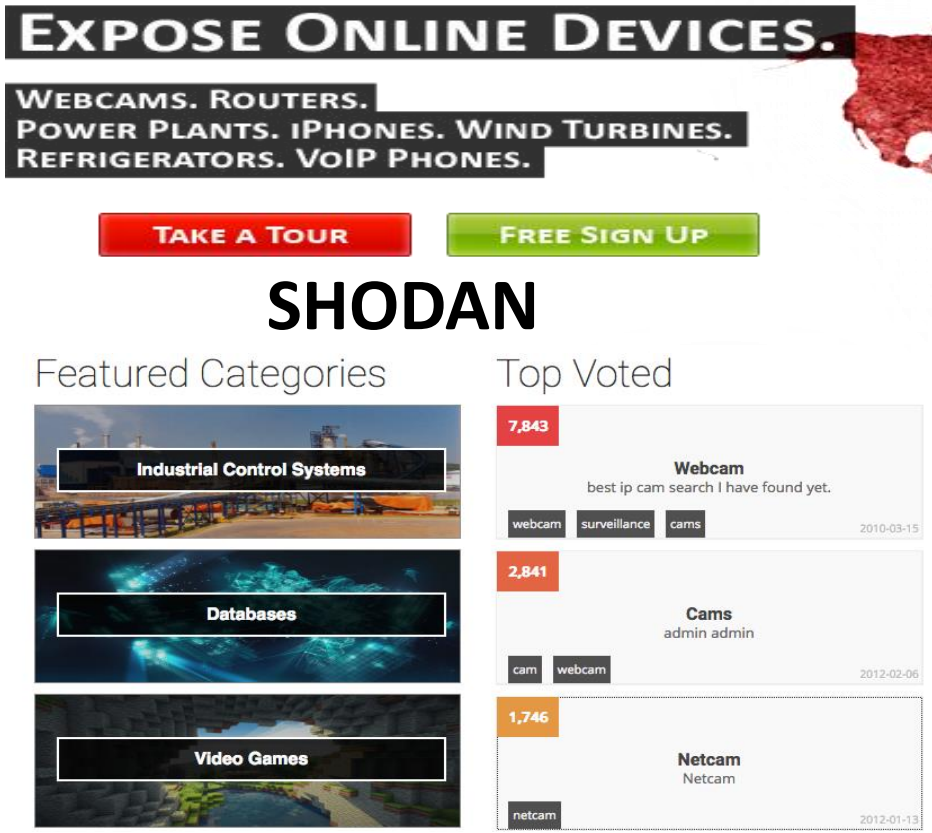
Lee Mathews Senior Contributor ⓘ

Cybersecurity

Observing, pondering, and writing about tech. Generally in that order.

Lessons NOT Learned: IoT (In)Security

Is it just another hype?



Meet the "Mirai" IoT Botnet

Source KrebsOnLine: https://krebsonsecurity.com/2016/10/source-code-for-iot-botnet-mirai-released/

Bashlight + Mirai botnets > 1.400.000 bots

@665 Gbps DDoS

Previous max: 363 Gbs DDoS

Source: http://www.shodanhq.com/

Lessons NOT Learned: IoT (In)Security

Beware: Don't Download It Or Use at your own risk!

[FREE] World's Largest Net:Mirai Botnet, Client, Echo Loader, CNC source code release

Yesterday, 12:50 PM (This post was last modified: Yesterday 04:29 PM by Anna-senpai.)

Anna-senpai

L33t Member

L33T

Preface

Greetz everybody,

When I first go in DDoS industry, I wasn't planning on staying in it long. I made my money, there's lots of eyes looking at IOT now, so it However, I know every skid and their mama, it's their wet dream to have something besides qbot.

So today, I have an amazing release for you. With Mirai, I usually pull max 380k bots from telnet alone. However, after the Kreb DDoS, shutting down and cleaning up their act. Today, max pull is about 300k bots, and dropping.

So, I am your senpai, and I will treat you real nice, my hf-chan.

BRYAN SCHRODER
United States Attorney

ADAM ALEXANDER
Assistant U.S. Attorney
Federal Building & U.S. Courthouse
222 West Seventh Avenue, #9, Room 253
Anchorage, Alaska 99513-7567
Phone: (907) 271-5071
Fax: (907) 271-1500
Email: adam.alexander@usdoj.gov

KENNETH A. BLANCO
Acting Assistant Attorney General

CATHERINE ALDEN PELKER
Trial Attorney
Computer Crime & Intellectual Property Section
1301 New York Avenue, NW, Suite 600
Washington, DC 20005
Telephone: (202) 514-1026
Facsimile: (202) 514-6113
Email: catherine.pelker@usdoj.gov

IN THE UNITED STATES I
FOR THE DISTRICT (

UNITED STATES OF AMERICA,) No. 3:
Plaintiff,)
vs.) PLEA
PARAS JHA,)
Defendant.)

Unless the parties jointly inform the Court in writing of any additional agreements, this document in its entirety contains the terms of the plea agreement between the defendant and the Prosecuting Offices (the United States Attorney's Office for the District of Alaska and the

Paras Jha 2nd

President at ProTraf Solutions, LLC

Greater New York City Area | Computer & Network Security

Current ProTraf Solutions

Education Rutgers University-New Brunswick

✓ Following 295 followers

https://www.linkedin.com/in/paras-jha-561ba110a

Background

Summary

Paras is a passionate entrepreneur driven by the want to create. Highly self-motivated, in 7th grade he began to teach himself to program in a variety of languages. Today, his skillset for software development includes C#, Java, Golang, C, C++, PHP, x86 ASM, not to mention web "browser languages" such as Javascript and HTML/CSS.

He brings all of these skills to the table at ProTraf Solutions, a DDoS mitigation firm that has a proven track record in mitigating DDoS attacks that competitors cannot.

Source: https://thehackernews.com/

Lessons NOT Learned: IoT (In)Security

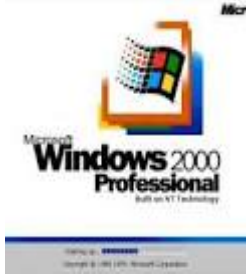
Medical Devices

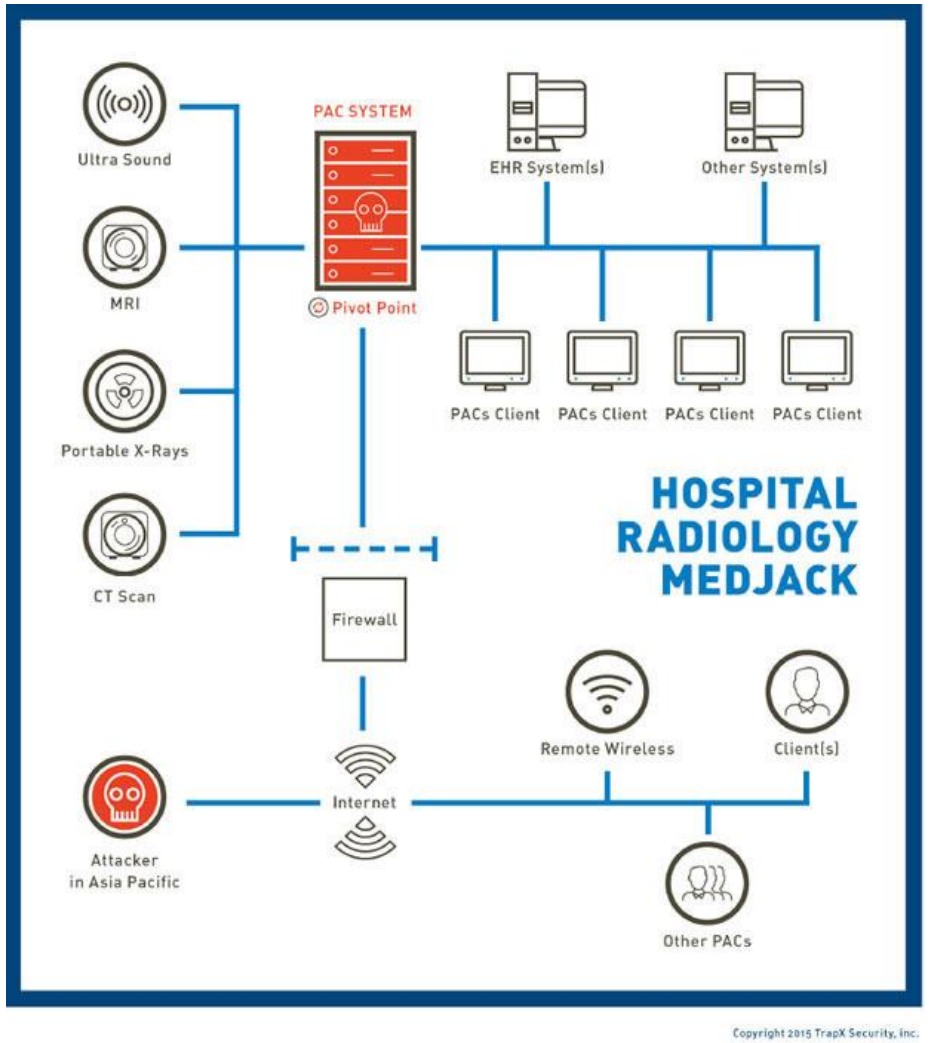
- CT scanners
- MRI scanners
- X-ray machines (c-arms)
- X-ray ultrasound equipment) …

Obsolete OSes / No update policy!

No security applications because of interference with medical device drivers

Orangeworm Group: Kwampirs malware





Source: https://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html#tk.drr_mlt

Lessons NOT Learned: IoT (In)Security

Security Researcher Bill Rios was able to manipulate remotely the device and change the amount of drugs administered to a patient.

"**This is the first time we know we can change the dosage**"

Medical Devices

IBM's security expert Jay Radcliffe exploited an insulin pump to disperse a lethal amount of insulin

Source: https://www.infosecurity-magazine.com/news/barnaby-jack-hacks-diabetes-insulin-pump-live-at/

HACKER CAN SEND FATAL DOSE TO HOSPITAL DRUG PUMPS

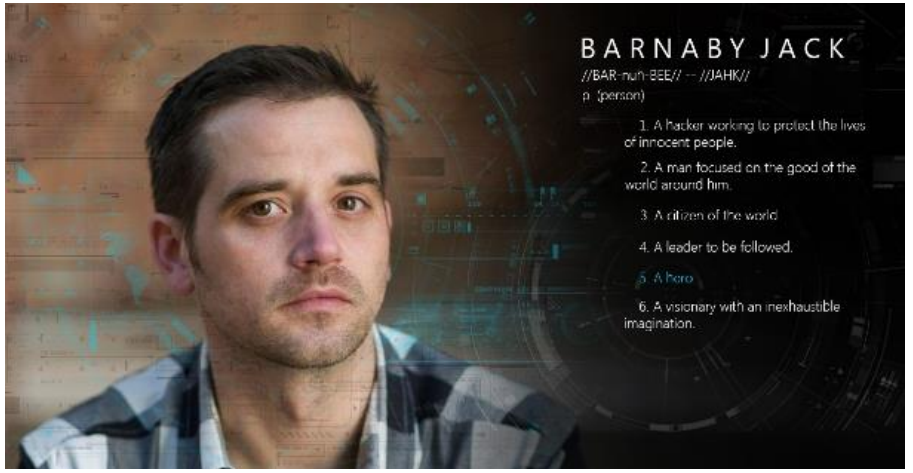
Hospira's drug infusion pumps include a serial cable (the wide grayish-white cable with the single red stripe on one edge) that connects the communications module to the main pump board. BILLY RIOS

Source: https://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/

Lessons NOT Learned: IoT (In)Security

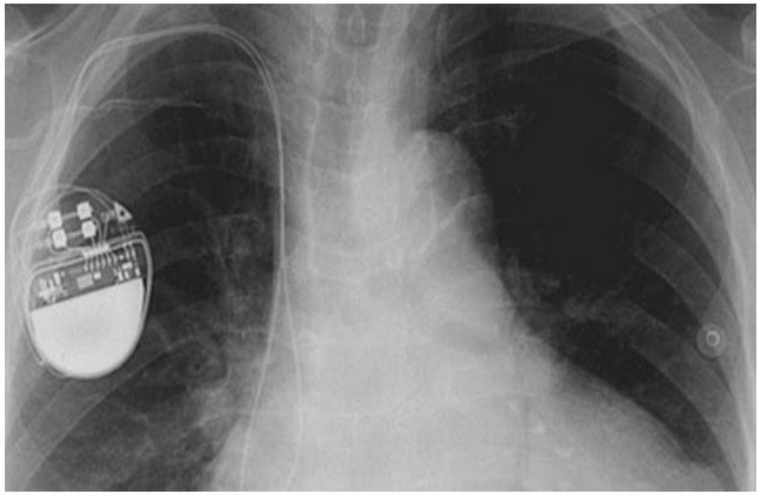
And you found it was possible?

Yeah, the software I developed allows the shutting off of the pacemaker or ICD, reading and writing to the memory of the device and, in the case of ICDs, it allows the delivering of a high voltage shock of up to 830 volts. I wanted to look at these devices with the aim of demonstrating and raising awareness of the issues I found, then hopefully spark the manufacturers into implementing a more secure design.



Medical Devices

William Alexander
Jun 25 2013, 10:00am



Is it difficult to hack into these devices?

It does take a specialised skill, but with more and more security researchers concentrating on embedded devices, the skill set required is becoming more common. It probably took me around six months, from reverse engineering and finding the flaws through to developing software to exploit the vulnerabilities.

If, say, a government official used a pacemaker, would they be vulnerable to assassination from hackers, like in that episode of *Homeland*? Or do they use better defended devices?

I wouldn't feel comfortable speculating about such a scenario, but as far as I'm aware there are no differences in the implantable devices issued to officials as there are to the general public.

Source: https://www.vice.com/en_uk/article/avnx5j/i-worked-out-how-to-remotely-weaponise-a-pacemaker

Source: https://www.infosecurity-magazine.com/news/barnaby-jack-hacks-diabetes-insulin-pump-live-at/

NEWS ANALYSIS

DHS investigates 24 potentially deadly cyber flaws in medical devices

DHS is investigating 24 cases of potentially deadly cybersecurity flaws in medical devices and hospital equipment.

Malware Attack Successfully Alters Radiology Scans, Resulting in Misdiagnoses

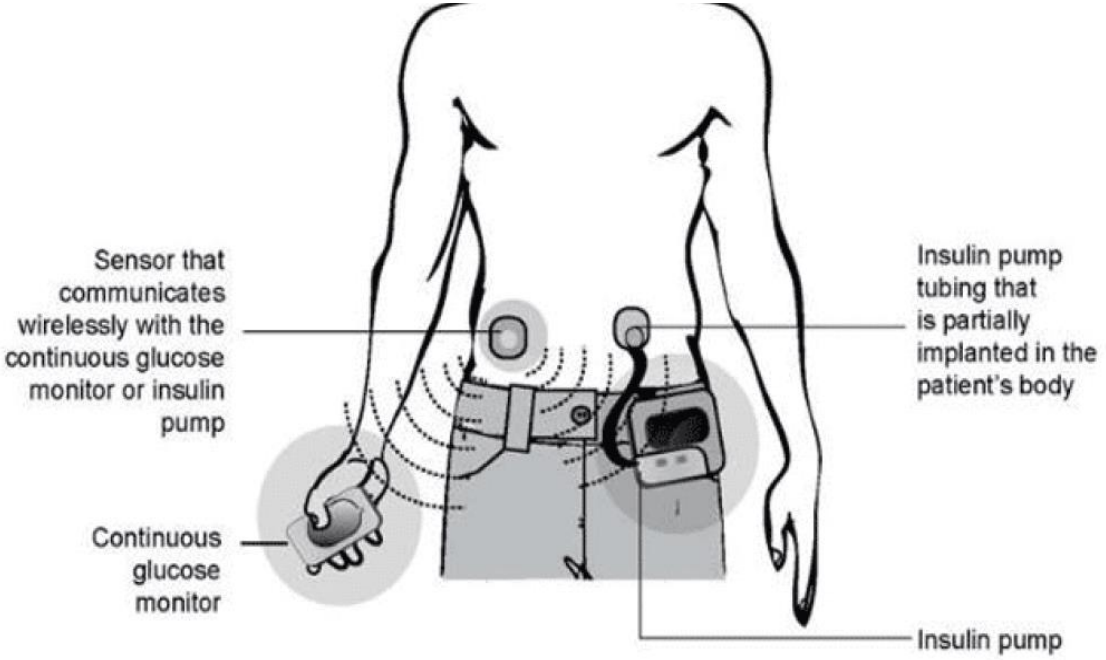
Intelligent Machines

Computer Viruses Are "Rampant" on Medical Devices in Hospitals

A meeting of government officials reveals that medical equipment is becoming riddled with malware.

Cybersecurity for Networked Medical Devices Shared Responsibility: FDA Safety Reminder

SHARE TWEET LINKEDIN PIN IT EMAIL PRINT



Source: http://resources.infosecinstitute.com/hcking-implantable-medical-devices/

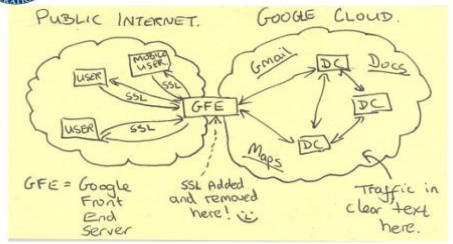
Lessons NOT Learned: IoT (In)Security

The Snowden Files

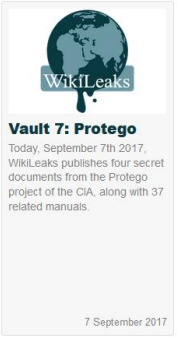
TAO: **T**ailored **A**ccess **O**perations – NSA's Signal Intelligence (SIGINT) Directorate

TOP SECRET//SI//NOFORN

Current Efforts - Google



TOP SECRET//SI//NOFORN



Global surveillance programs		
Program	**International contributors and/or partners**	**Commercial partners**
PRISM	• Australian Signals Directorate (ASD/DSD) of Australia[49] • Government Communications Headquarters (GCHQ) of the UK[50] • Algemene Inlichtingen en Veiligheidsdienst (AIVD) of the Netherlands[51]	• Microsoft[52][52][53]
XKeyscore	• Bundesnachrichtendienst (BND) of Germany[53][54] • Bundesamt für Verfassungsschutz (BfV) of Germany[53][54] • National Defence Radio Establishment (FRA) of Sweden[55][56]	
Tempora	• National Security Agency (NSA)[57][58]	• British Telecommunications (codenamed "Remedy")[59] • Interoute (codenamed "Streetcar")[59] • Level 3 (codenamed "Little")[59] • Global Crossing (codenamed "Pinnage")[59] • Verizon Business (codenamed "Dacron")[59] • Viatel (codenamed "Vitreous")[59] • Vodafone Cable (codenamed "Gerontic")[59]
Muscular	• NSA[60]	
Project 6	• Central Intelligence Agency (CIA)[61]	
Stateroom	• DSD[62][63] • Communications Security Establishment Canada (CSEC)[63][64] • GCHQ[63][65] • Special Collection Service (SCS)[63][65][66]	
Lustre	• NSA[67][68] • Direction Générale de la Sécurité Extérieure (DGSE) of France[67][68]	

GCHQ - **G**overnment **C**ommunications **Headq**uarters

Source: https://en.wikipedia.org/wiki/Edward_Snowden

HELL IS EMPTY
AND
ALL THE DEVILS
ARE HERE.

WILLIAM SHAKESPEARE

Lessons NOT Learned: IoT (In)Security

"Even when technologies are developed inside the NSA, they don't remain exclusive for long. Today's top-secret programs become tomorrow's PhD theses and the next day's hacker tools."

Lessons NOT Learned: IoT (In)Security

Wireless Devices: Router & Access Points

Multiple Backdoors found in D-Link DWR-932 B LTE Router

Wednesday, September 28, 2016 Swati Khandelwal

Tweet Share Share Share Share Share

If you own a D-Link wireless router, especially **DWR-932 B LTE router**, you should get rid of it, rather than wait for a firmware upgrade that never lands soon.

WikiLeaks Leaks News About Partners Search Shop

Vault 7: CIA Hacking Tools Revealed

Releases ▾ Documents ▾

Navigation: » Directory » Embedded Development Branch (EDB) » EDB Home

Owner: User #20873326

Small Routers

Small Routers Research - work in progress

Tools and firmware images:

Stash Repository

Source: https://thehackernews.com/

Lessons NOT Learned: IoT (In)Security

Wireless Devices: Router & Access Points

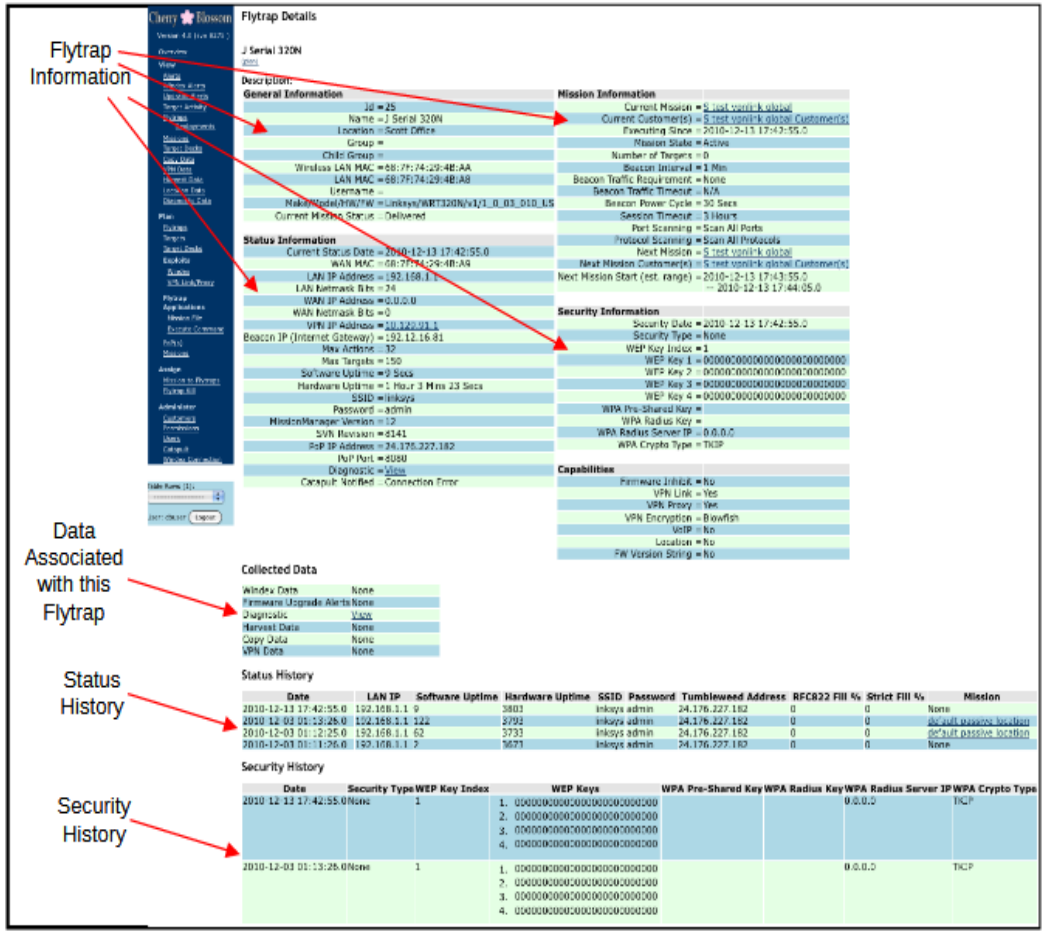


Figure 6: Cherry Web Flytrap Details Page

Cherry Bomb:
Cherry Blossom (CB) Quick Start Guide

For CB Version 5.0
[Corresponds to CB Server Software Version 5.0]

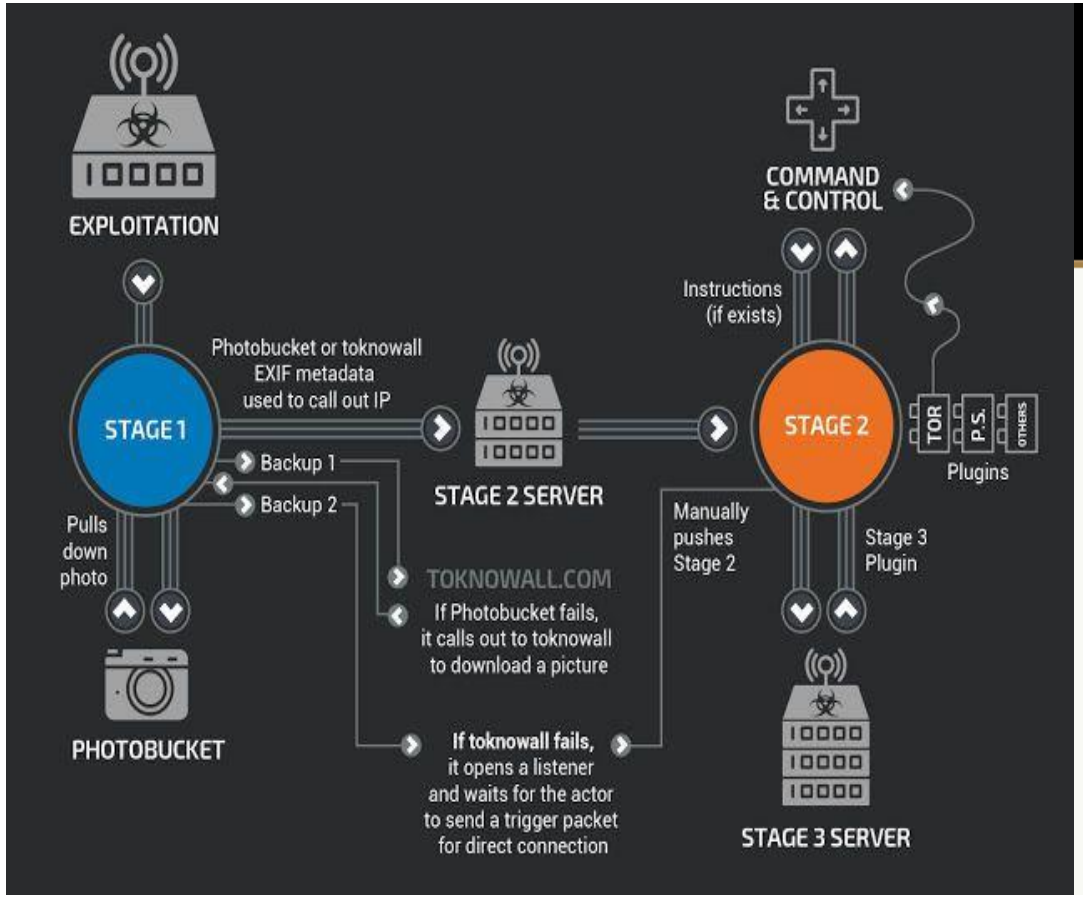
5.1 (S) Implanting a Wireless Device

(S) There are four general methods for getting a Flytrap implant onto a wireless device, some of which are device-specific (the CBUM contains detailed information on device support and upgrade procedures):

- **Use the Device's Firmware Upgrade Web Page over a Wireless (WLAN) Link** – this technique does not require physical access but typically does require an administrator password. Some exploitation tools (for example Tomato and Surfside) have been created to determine passwords for devices of interest. If the device is using wireless security (for example WEP or WPA), then these credentials are required as well.
- **Use a Wireless Upgrade Package** – some devices do not allow a firmware upgrade over the wireless link. To workaround this issue, "Wireless Upgrade Packages" have been created for a few devices of interest. In some cases, the Wireless Upgrade Package also can determine the administrator password.
- **Use the Claymore Tool** – the Claymore tool is a survey, collection, and implant tool for wireless (802.11/WiFi) devices. The survey function attempts to determine device makes/models/versions in a region of interest. The collection function can capture wireless traffic. The implant function can perform wireless firmware upgrades and incorporates the exploitation tools (for determining administrator passwords) and Wireless Upgrade Packages (for devices that don't allow wireless firmware upgrades). Claymore can run in a mobile environment (i.e., on a laptop) or in a fixed environment with a large antenna for longer ranges. See the "Claymore User's Manual" for more information.
- **Use the Device's Firmware Upgrade Web Page over a Wired (LAN) Link** – this technique would likely be used in a supply chain operation.

Lessons NOT Learned: IoT (In)Security

Wireless Devices: Router & Access Points



THE UNITED STATES DEPARTMENT of JUSTICE

en ESPAÑOL

HOME ABOUT AGENCIES RESOURCES

Home » Office of Public Affairs » News

JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE — Wednesday, May 23, 2018

Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices

Additional action necessary worldwide to remediate the botnet.

Source: https://privacy.ellak.gr/2018/06/05/vpnfilter-neo-kakovoulo-logismiko-gia-routers-me-katastreptikes-dinatotites/

Lessons NOT Learned: IoT (In)Security

Hands On

A small experiment:

Hellas OnLine Electronic Communications S.A.

250 IP - port 80

Hellas OnLine Electronic Communications S.A.

522 IP - port 80

TELLAS Telecommunication Services S.A.

583 IP - port 80

FORTHnet SA

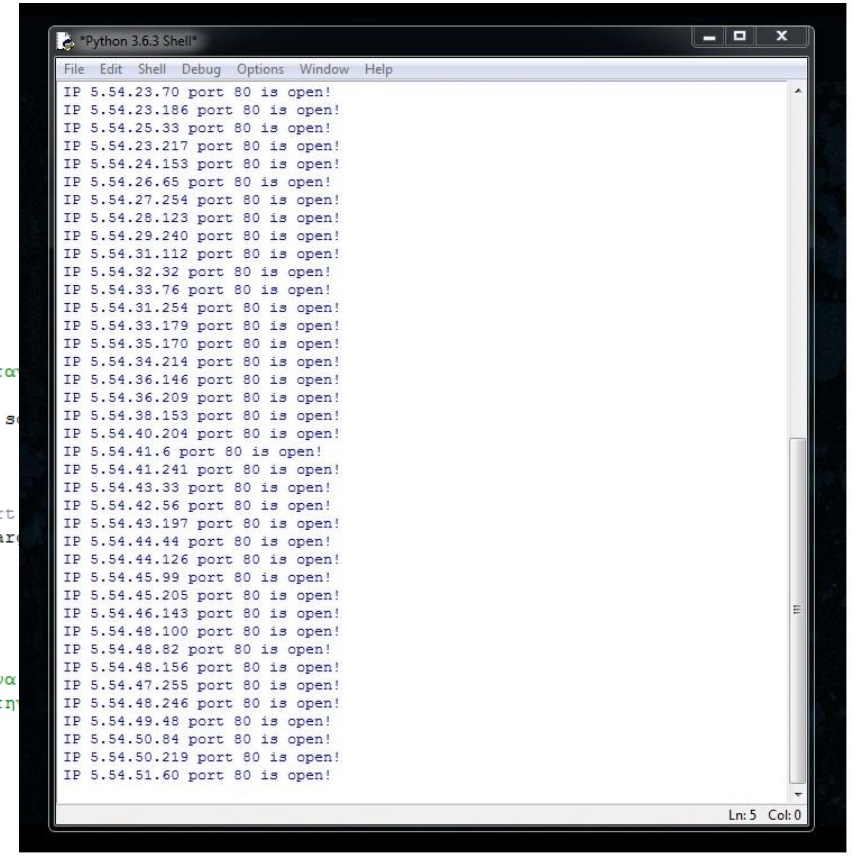
260 IP - port 80

Total: **1615 IP**

```
#Η portscan ελέγχει, εμφανίζει και κατα
def portscan(targ):
    s = socket.socket(socket.AF_INET, s
    try:
        con = s.connect((targ,80))
        with print_lock:
            print('IP ' + targ + ' port
            text_file.write('IP ' + tar
            text_file.flush()
        con.close()
    except:
        pass

#Ο threader είναι το Loop που ξεκινά να
#Κάθε threader, παίρνει απο την ουρά τη
def threader():
    while True:
        worker = q.get()
        portscan(worker)
        q.task_done()


#Εδώ ξεκινώ 650 threads(δηλαδή threaders) απο επιλογή μου. Το 't.deamon = True' θα τερματίσει όλα τα threads,
#σε περίπτωση που main thread τερματίσει.
for x in range(650):
    t = threading.Thread(target=threader)
    t.daemon = True
    t.start()
```

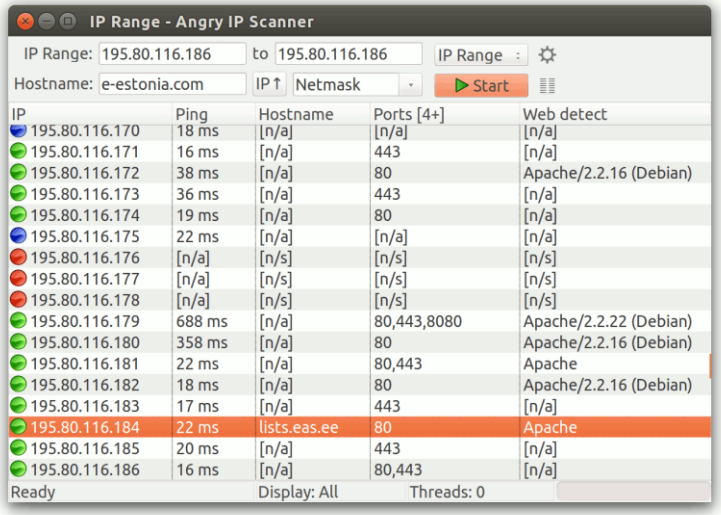


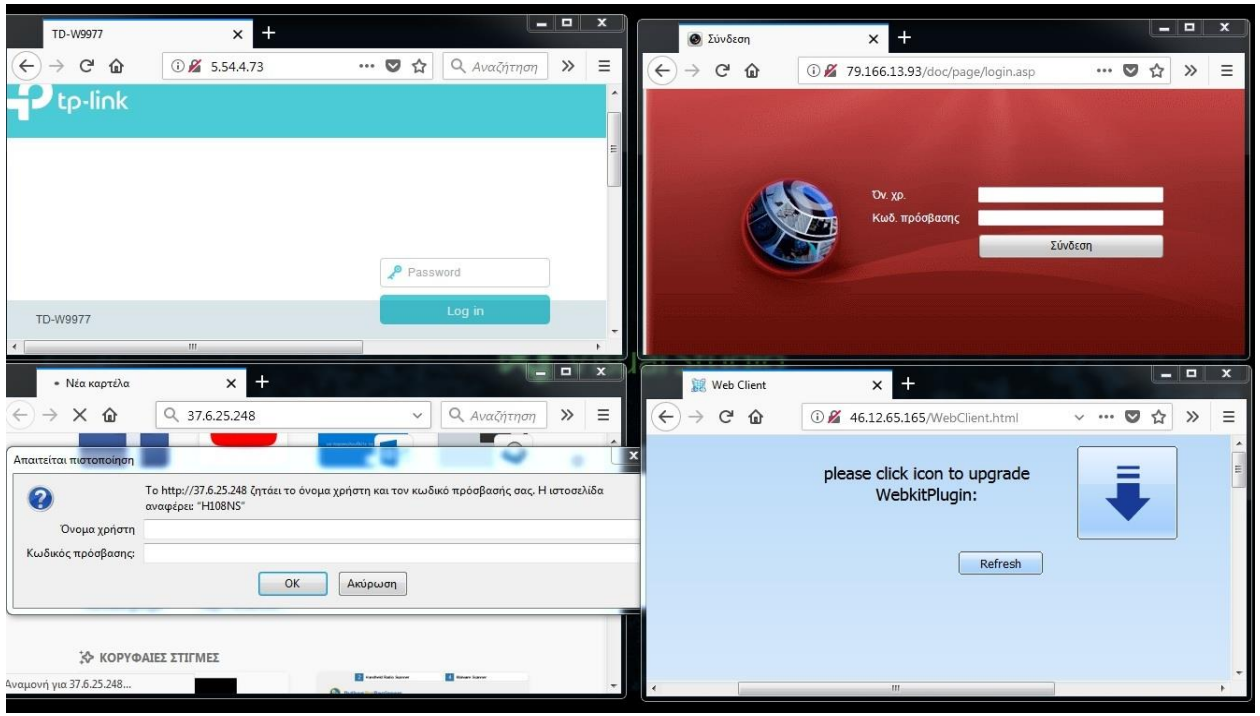
By CS student: Christos Zervas

Lessons NOT Learned: IoT (In)Security

Hands On

After a while: Remotely accessed routers for further evaluation with a decent port scanner





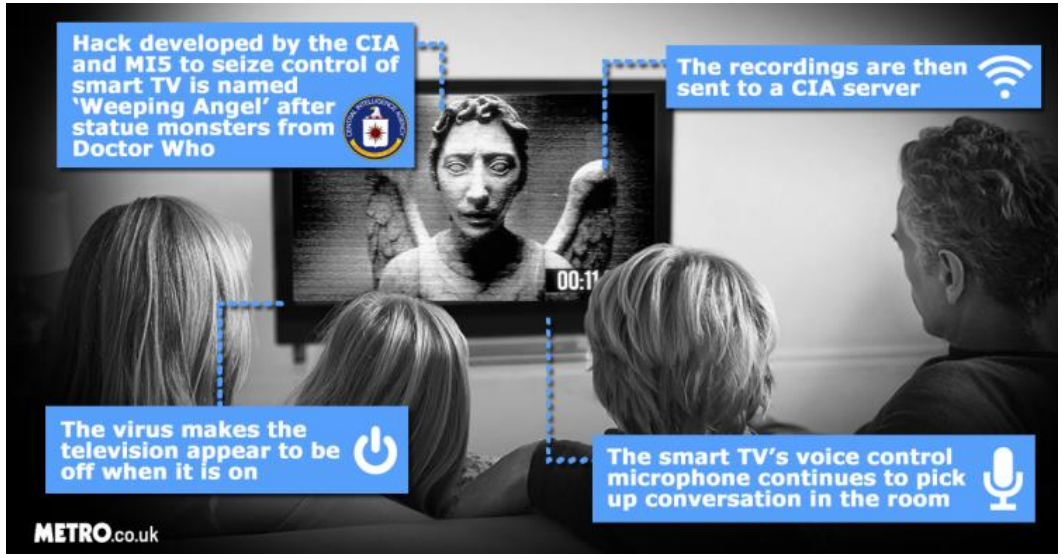
By CS student: Christos Zervas

ICT Security World 2019

Lessons NOT Learned: IoT (In)Security

Smart TVs

Weeping Angel



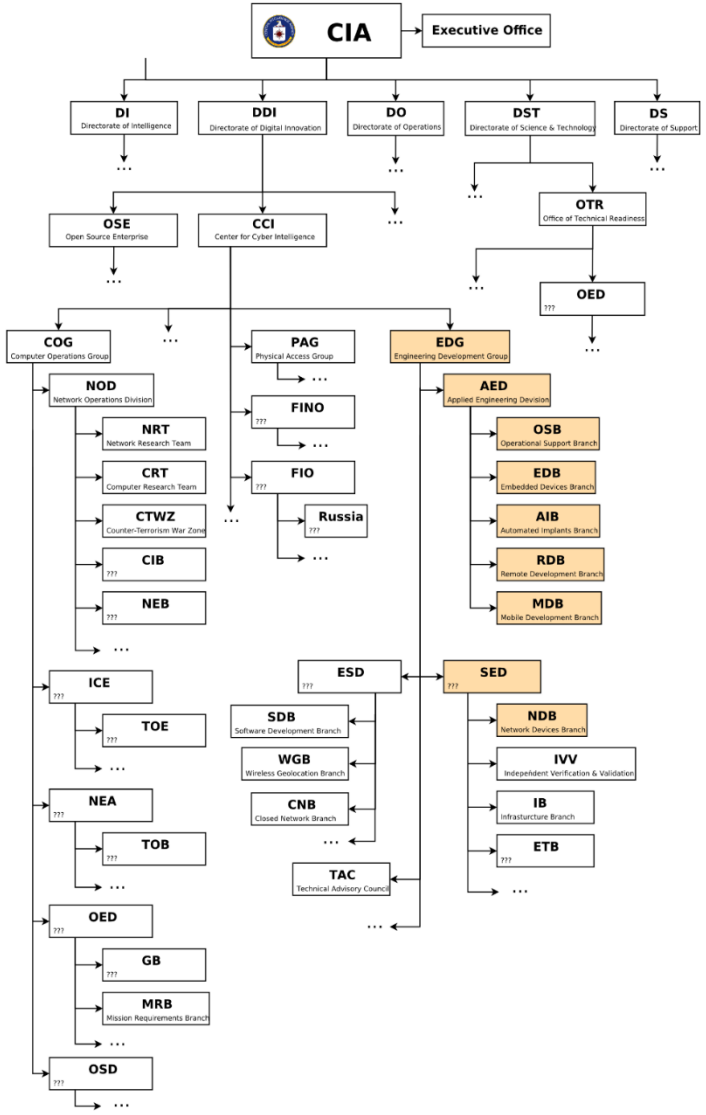


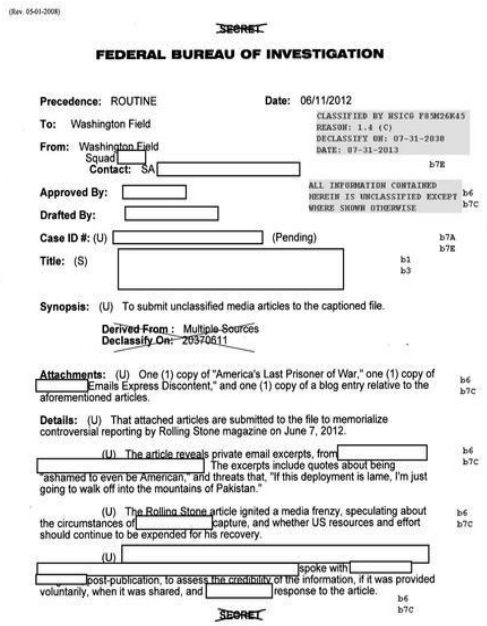
Image source: http://metro.co.uk/2017/03/09/mi5-and-cia-have-been-spying-on-us-through-our-tvs-6497867/

Lessons NOT Learned: IoT (In)Security

Autonomous Cars

NSA - Vehicle Systems (e.g. VSEP)

By Lord Jim - flickr, CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=36943733



~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: ROUTINE **Date:** 06/11/2012

To: Washington Field

From: Washington Field
Squad
Contact: SA

CLASSIFIED BY NSICG F85M26K45
REASON: 1.4 (C)
DECLASSIFY ON: 07-31-2038
DATE: 07-31-2013

ALL INFORMATION CONTAINED HEREIN IS UNCLASSIFIED EXCEPT WHERE SHOWN OTHERWISE

Approved By:

Drafted By:

Case ID #: (U) (Pending)

Title: (S)

Synopsis: (U) To submit unclassified media articles to the captioned file.

~~Derived From:~~ Multiple Sources
~~Declassify On:~~ 20370611

Attachments: (U) One (1) copy of "America's Last Prisoner of War," one (1) copy of Emails Express Discontent," and one (1) copy of a blog entry relative to the aforementioned articles.

Details: (U) That attached articles are submitted to the file to memorialize controversial reporting by Rolling Stone magazine on June 7, 2012.

(U) The article reveals private email excerpts, from The excerpts include quotes about being "ashamed to even be American," and threats that, "If this deployment is lame, I'm just going to walk off into the mountains of Pakistan."

(U) The Rolling Stone article ignited a media frenzy, speculating about the circumstances of capture, and whether US resources and effort should continue to be expended for his recovery.

(U) spoke with post-publication, to assess the credibility of the information, if it was provided voluntarily, when it was shared, and response to the article.

~~SECRET~~

Image: By Aude - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=299

Richard A. Clarke former National Coordinator for Security, Infrastructure Protection and Counter-terrorism for the United States **"There is reason to believe that intelligence agencies for major powers—including the United States—know how to remotely seize control of a car. So if there were a cyber attack on the car—and I'm not saying there was, I think whoever did it would probably get away with it."**

Source: http://www.huffingtonpost.com/2013/06/24/michael-hastings-car-hacked_n_3492339.html

Lessons NOT Learned: IoT (In)Security

Air Transportation

Having Fun with In-Flight Entertainment System

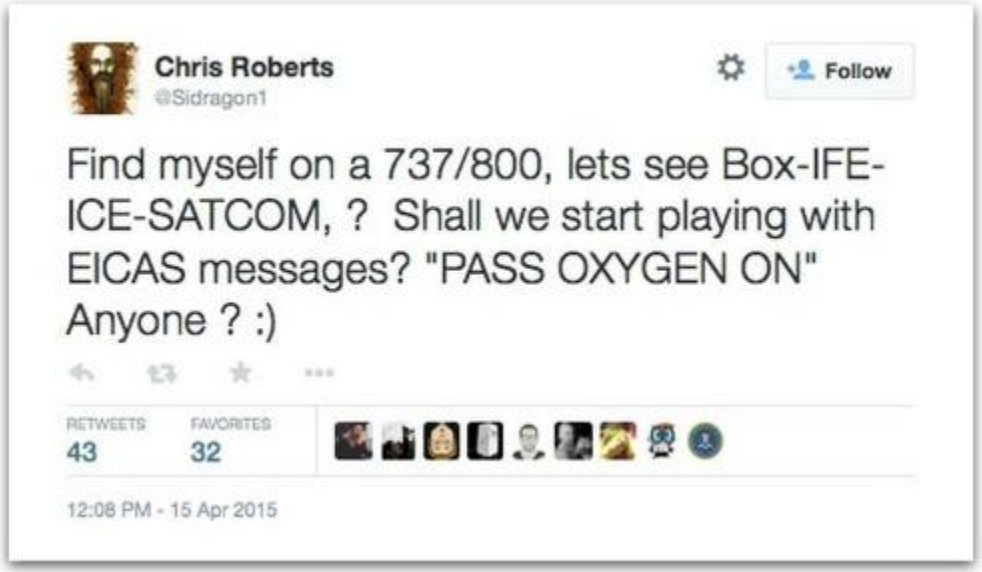


Image source: http://www.modernreaders.com/wp-content/uploads/2015/05/0517-Chris-Roberts.jpg

Lessons NOT Learned: IoT (In)Security

Air Transportation

"We got the airplane on Sept. 19, 2016. Two days later, I was successful in accomplishing a remote, non-cooperative, penetration. [Which] means I didn't have anybody touching the airplane, I didn't have an insider threat. I stood off using typical stuff that could get through security and we were able to establish a presence on the systems of the aircraft."

Robert Hickey, aviation program manager within the Cyber Security Division of the DHS Science and Technology (S&T) Directorate

Source: http://www.aviationtoday.com/2017/11/08/boeing-757-testing-shows-airplanes-vulnerable-hacking-dhs-says/

Lessons NOT Learned: IoT (In)Security

SCADA Systems: Dams

The Dam Busters
Operation Chastise revised

Rye Brook, New York Dam Attack

Source: http://time.com/4270728/iran-cyber-attack-dam-fbi/

SOUTHERN DISTRICT OF NEW YORK
- - - - - - - - - - - - - - - - - - - -X

UNITED STATES OF AMERICA : SEALED INDICTMENT

- v. - : 16 Cr.

AHMAD FATHI, :
HAMID FIROOZI, :
AMIN SHOKOHI, :
SADEGH AHMADZADEGAN, :
a/k/a "Nitr0jen26," :
OMID GHAFFARINIA, :
a/k/a "PLuS," :
SINA KEISSAR, and :
NADER SAEDI, :
a/k/a "Turk Server," :
: 16 CRIM 548
Defendants. :

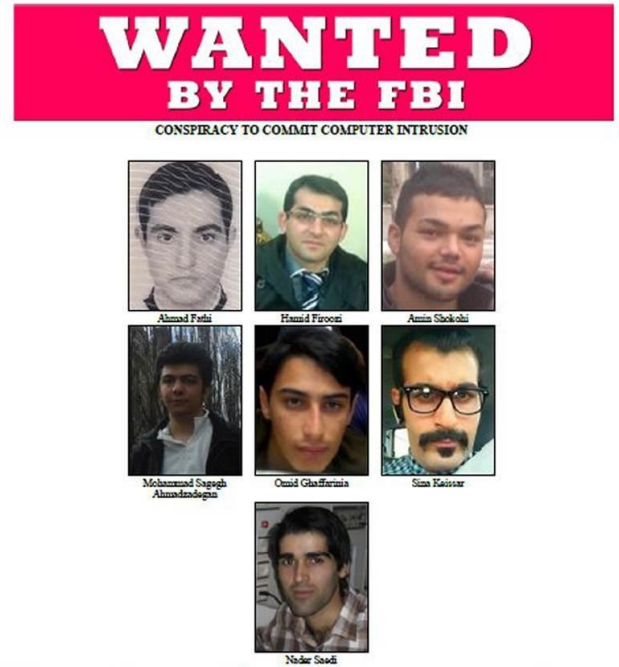
- - - - - - - - - - - - - - - - - - - -X

COUNT ONE

(CONSPIRACY TO COMMIT COMPUTER HACKING -

The Grand Jury charges:

BACKROUND ON THE DEFENDANTS AND RELATED



"Although access to the SCADA typically would have also permitted FIROOZI to remotely operate and manipulate the sluice gate did not have that capability because the sluice gate had been manually disconnected for maintenance at the time of the intrusion," U.S. government

By unknown Official RAF photograph - National Archives (AIR 14/840) and IWM HU 69915, Public Domain, https://commons.wikimedia.org/w/index.php?curid=11152059

Lessons NOT Learned: IoT (In)Security

SCADA Systems: Power Stations

Aurora Project Review

- A vulnerability was discovered and an Interagency Tiger Team was formed
- Initial concerns and modeling results were confirmed by a physical test March 4 2007
- Test resulted in a total loss of generating capability with extensive damage in about 3 minutes
- A strong example of interagency cooperation and public-private partnership

Homeland Security

UNCLASSIFIED/FOR OFFICIAL USE ONLY

3

Source: https://youtu.be/fJyWngDco3g

21 lines of code

Aurora Generator Test – Idaho National Labs

Source: https://s3.amazonaws.com/s3.documentcloud.org/documents/1212530/1450304-documents.pdf

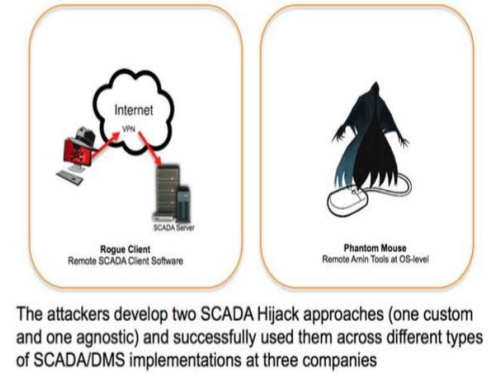
Lessons NOT Learned: IoT (In)Security

SCADA Systems: Power Stations

SandWorm

Prykarpattyaoblenergo 5:00 p.m. on Dec. 23 2016 – breach began 9 months earlier

- 230.000 customers impacted for 1 to 6 hours
- More companies infected (2 to 6)
- 30 intruders disconnected breakers for 30 of its substation
- DDoS against the Prykarpattyaoblenergo telephone network / call center
- Destructive payload (killDisk)
- Mainstream malware (BlackEnergy2, BlackEnergy3)



The attackers develop two SCADA Hijack approaches (one custom and one agnostic) and successfully used them across different types of SCADA/DMS implementations at three companies

Figure 6: A Sample of a BlackEnergy 3 Infected Microsoft Office Document[27]

Source: E-ISAC | Analysis of the Cyber Attack on the Ukrainian Power Grid | March 18, 2016

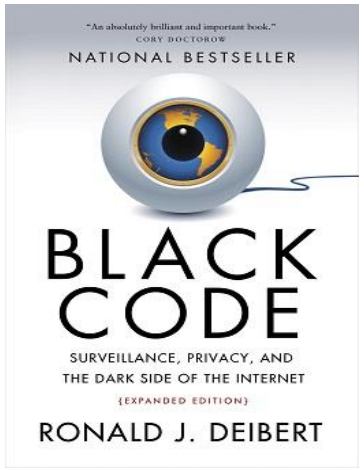
Lessons NOT Learned: IoT (In)Security

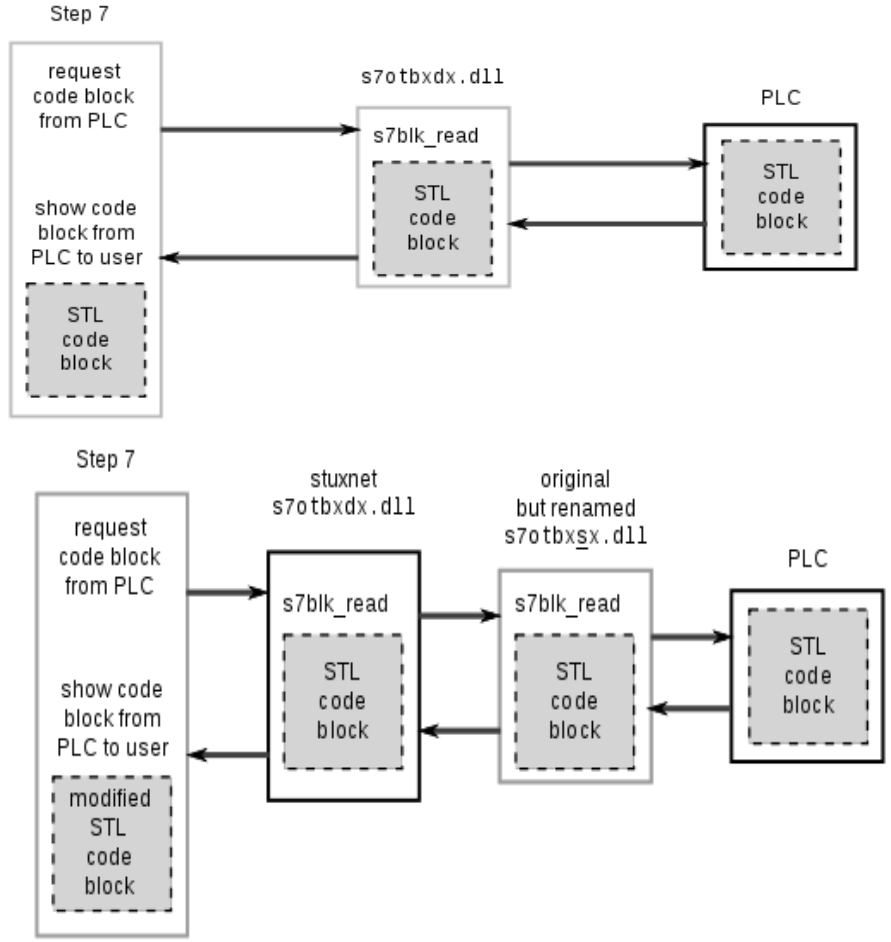
SCADA Systems: Nuclear Power Stations

Stuxnet (2010 – 2011)

- **Target:** Simen's SIMATIC WinCC/Step 7 software for Programmable Logic Controller (PLC) which are used in coal power plants, nuclear power plants, pumping stations etc.
- **Analysis:** 4 zero day exploits, valid stolen certificates, sophisticated obfuscation techniques, multiple levels of encryption. Estimated effort to develop it: 50-60 mon-months. Issues conflicting instructions to cause fast-spinning centrifuges to tear themselves apart. Disables monitoring services on supervisors systems to avoid detection.
- **Motives:** Iran's nuclear program.

Source: Wired





By Grixlkraxl - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=12200863

Lessons NOT Learned: IoT (In)Security

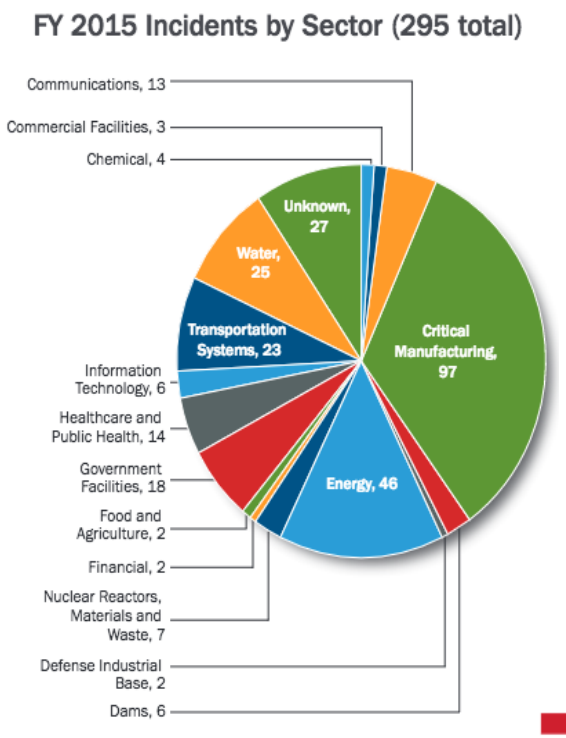
SCADA Systems: Nuclear Power Stations

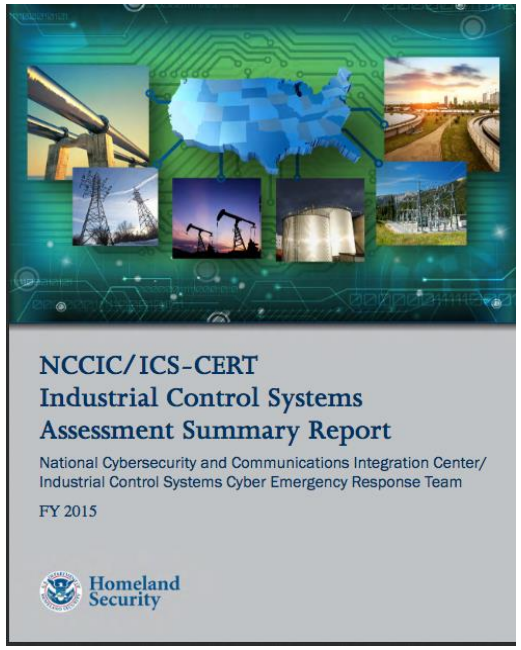
Disruptive, not destructive**:**

- **Gundremmingen NPP (2014 or 2015): Conficker** (2008) and **W32 Ramnit** (2010)
- **Monju Nuclear Power Plant (2014)** accessed over 30 times, over 40.000 emails and documents available at the compromised system
- **The Korea Hydro and Nuclear Power Co Ltd (KHNP):** hactivism? Stolen data?
- **The Wolf Creek Nuclear Power Plant in Kansas (2017)** according to joint report of the Department of Homeland Security obtained by The New York Times

Lessons NOT Learned: IoT (In)Security

SCADA Systems: Status Report





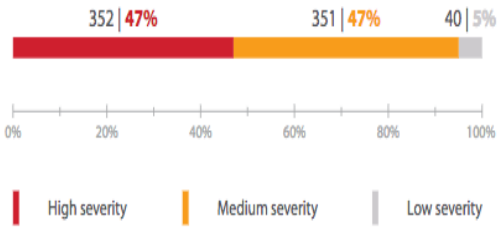
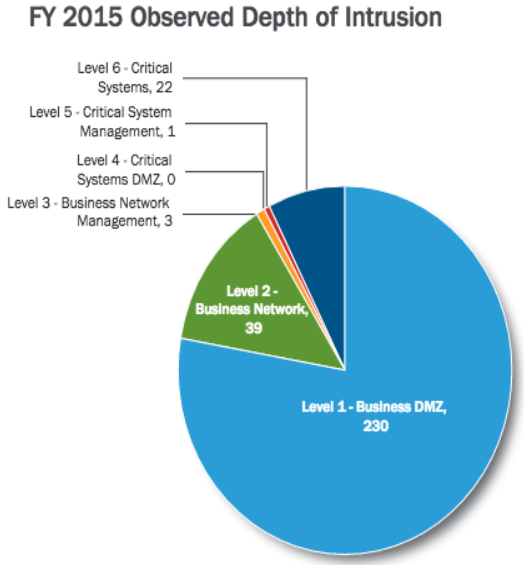


Figure 4. Distribution of vulnerabilities (by risk)



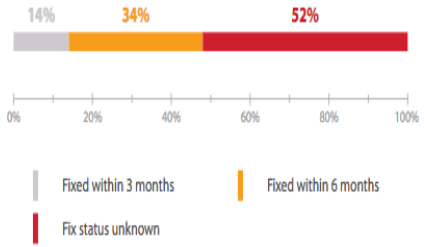
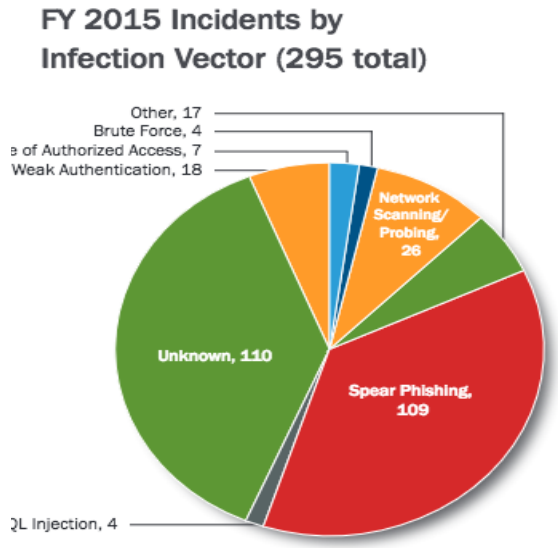


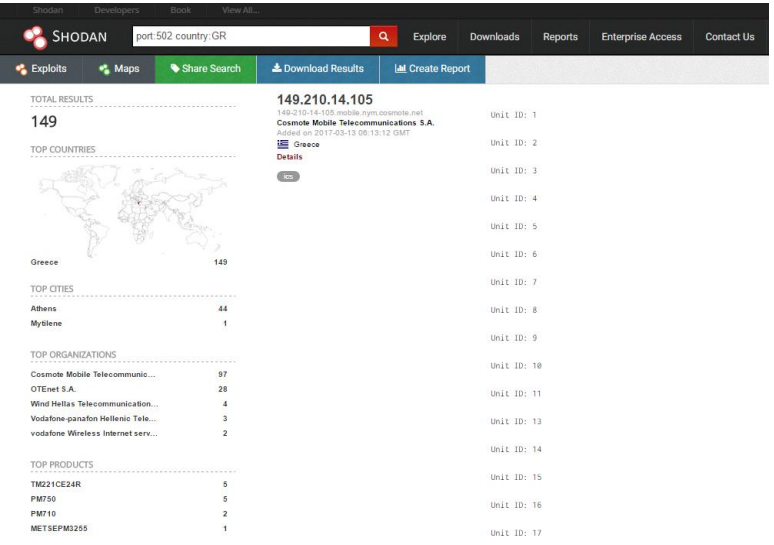
Figure 7. Repair timeline for vulnerabilities identified in ICS components



Source: https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/Year_in_Review_FY2015_Final_S508C.pdf

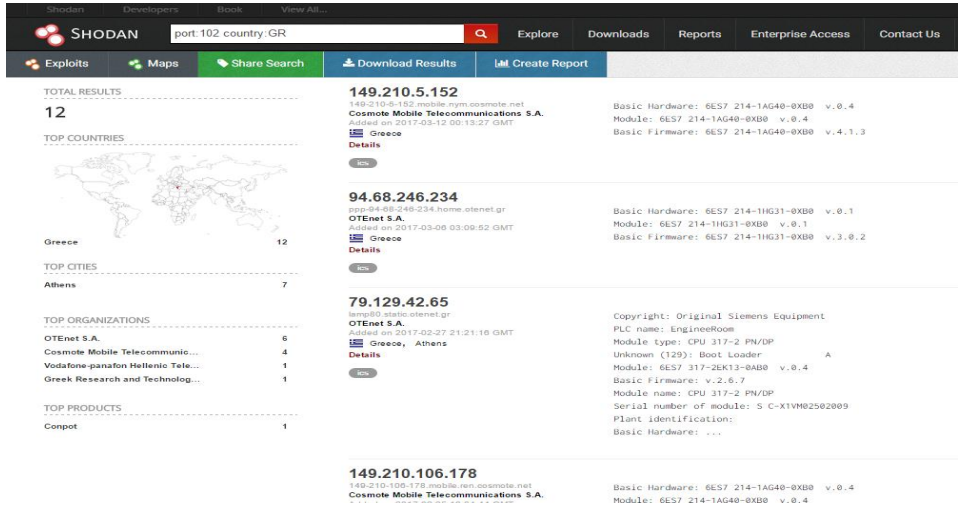
SCADA Systems: Status Report

MODBUS

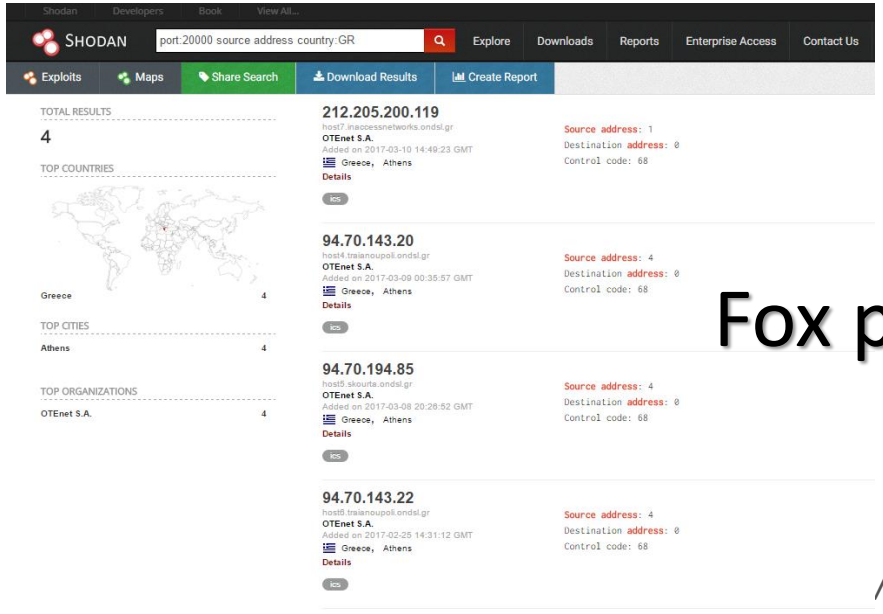


Hands On

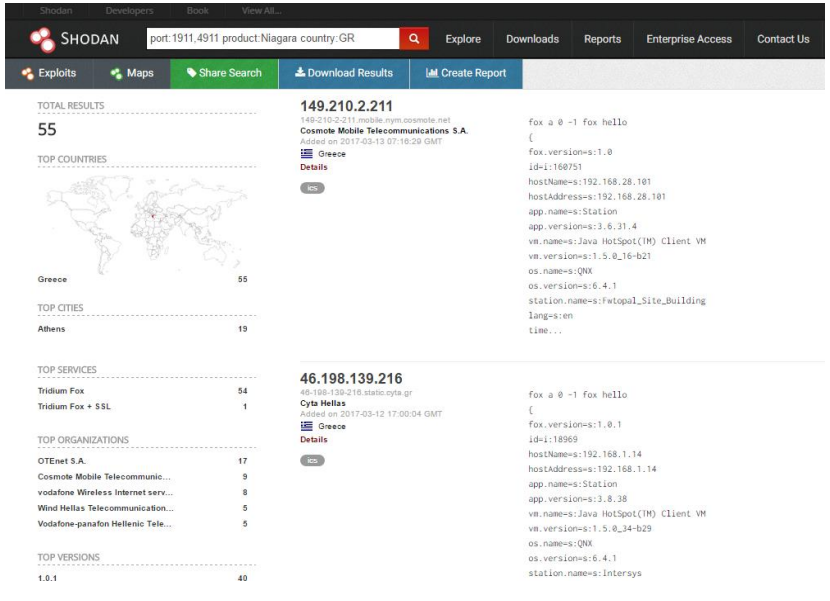
S7 Communication



DNP3



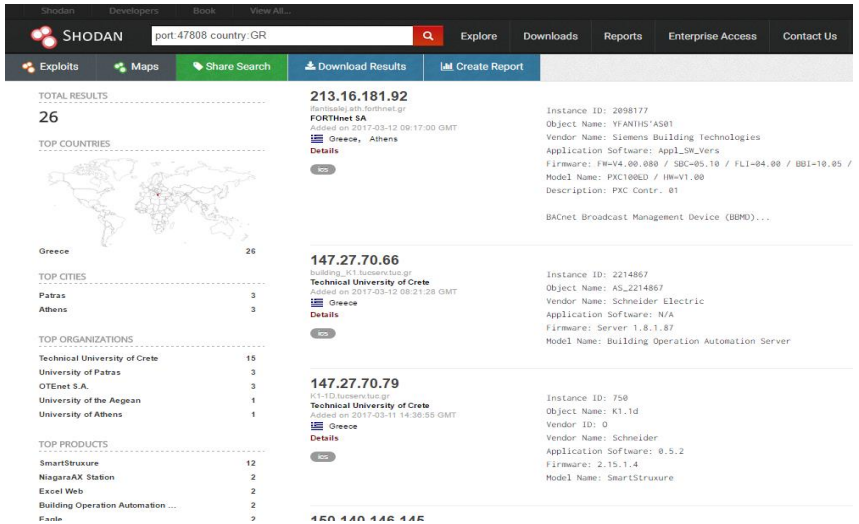
Fox protocol



/orld 2019

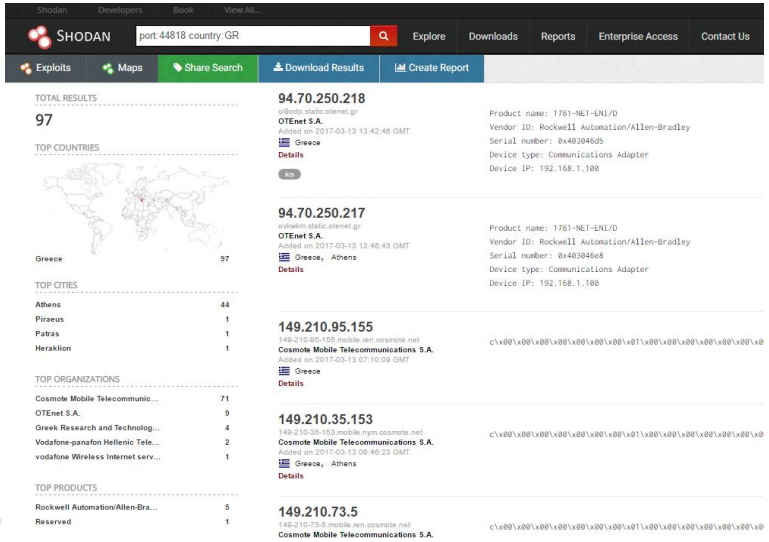
SCADA Systems: Status Report

FINS

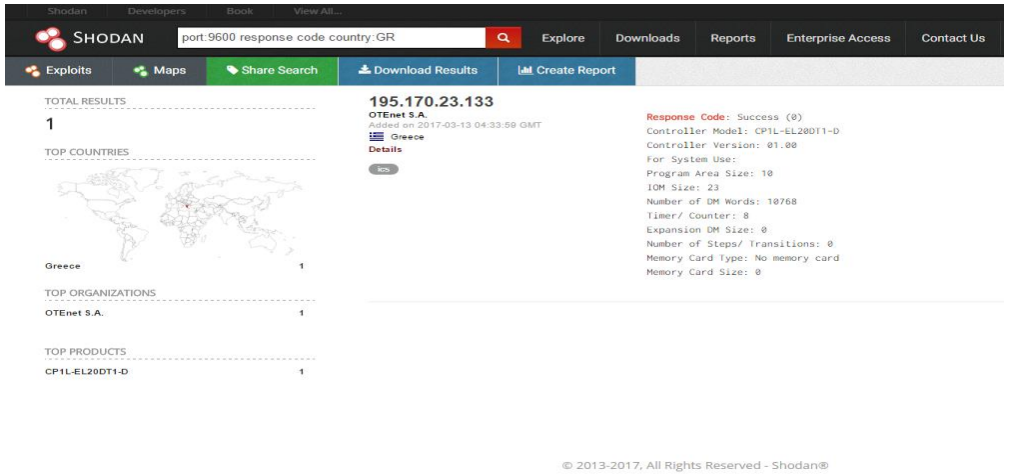


Hands On

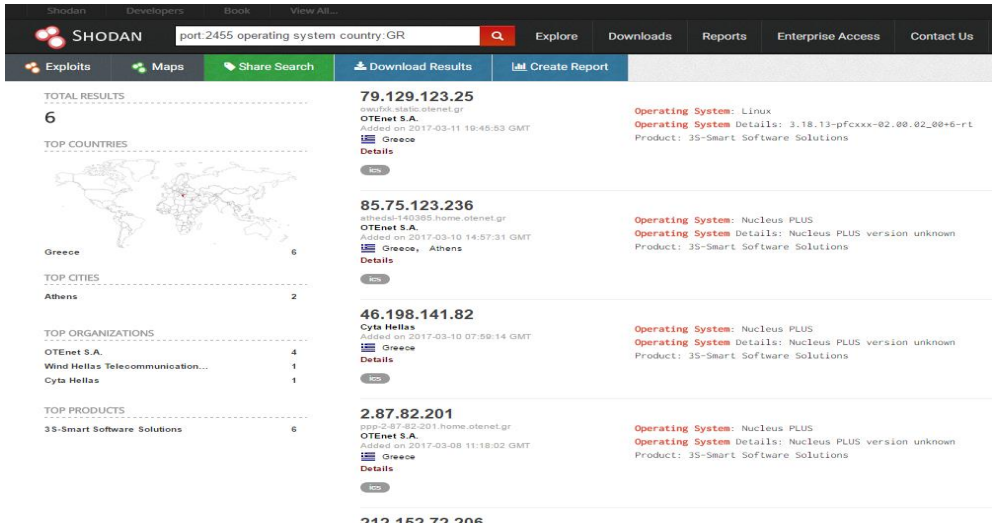
EtherNet/IP



BACnet



CODESYS



OWASP Internet of Things Project

The OWASP Internet of Things Project is designed to:

- Help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things
- Enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies.
- Define structure for various IoT sub-projects such as Attack Surface Areas, Testing Guides and Top Vulnerabilities.
- It is licensed under the Creative Commons Attribution-ShareAlike 3.0 license (http://creativecommons.org/licenses/by-sa/3.0/)

OWASP
Open Web Application Security Project

Image Source: https://www.secplicity.org/2017/04/12/owasp-top-10-web-application-security-update/owasp-logo/

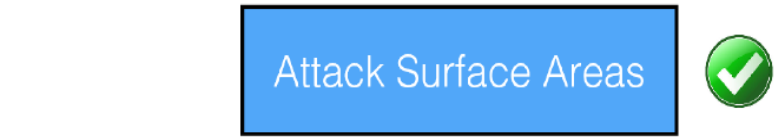


Image Source: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

Source: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

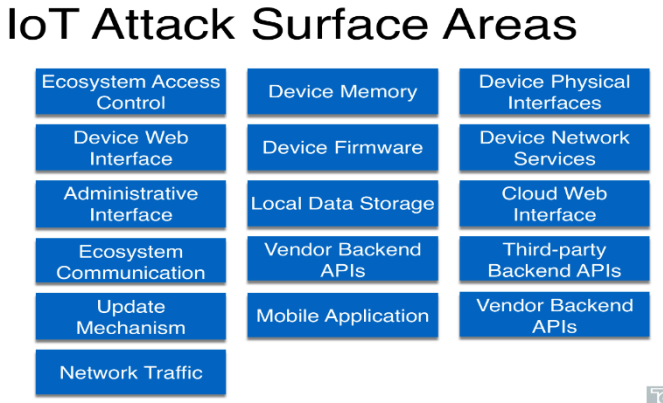
OWASP Internet of Things Project

Provides information on:

- IoT Attack Surface Areas
- IoT Vulnerabilities
- Firmware Analysis
- ICS/SCADA Software Weaknesses
- Community Information
- IoT Testing Guides
- IoT Security Guidance
- Principles of IoT Security
- IoT Framework Assessment
- Developer, Consumer and Manufacturer Guidance
- Design Principles

OWASP IoT Top Ten	Maturity	Builds on Existing Knowledge of	
List Item	of List Item	Application Security	Network Security
I1 - Insecure Web Interface	Mature	Yes	Some
I2 - Insufficient Authentication/Authorization	Mature	Yes	Yes
I3 - Insecure Network Services	Mature	Some	Yes
I4 - Lack of Transport Encryption	Mature	Yes	Yes
I5 - Privacy Concerns	Emerging	Some	Some
I6 - Insecure Cloud Interface	Mature	Yes	Some
I7 - Insecure Mobile Interface	Emerging	No	Yes
I8 - Insufficient Security Configurability	Mature	Yes	Yes
I9 - Insecure Software/Firmware	Mature	Some	Some
I10 - Poor Physical Security	Emerging	No	Some

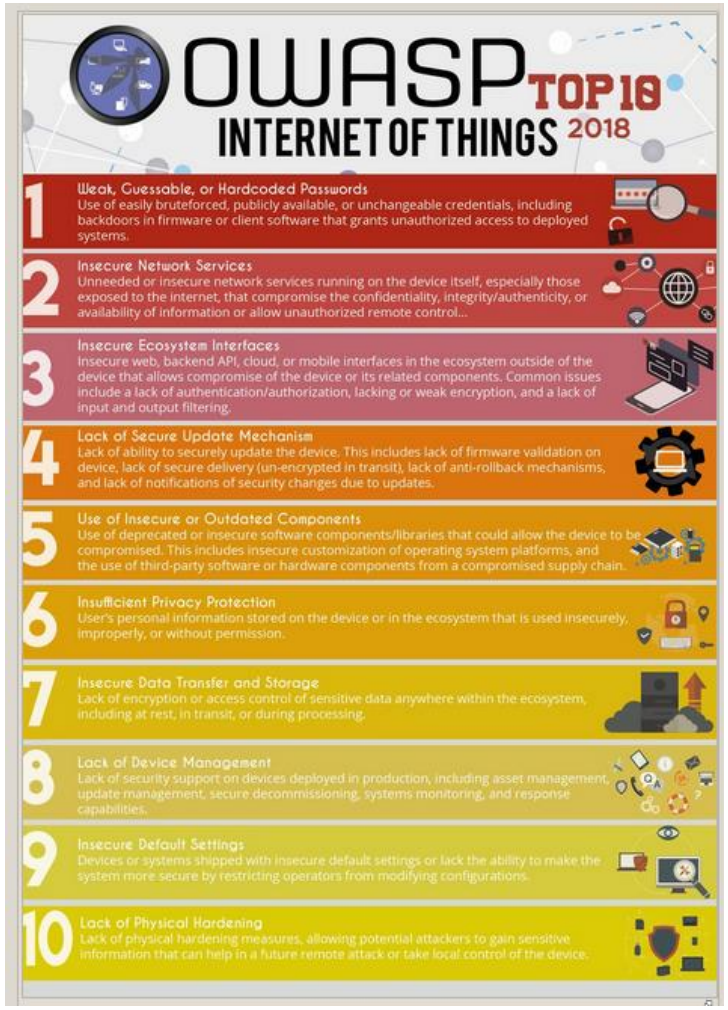
Image Source: http://resources.infosecinstitute.com/test-security-iot-smart-devices/



Source: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

Image Source: https://hackaday.com/2016/06/13/iot-security-is-an-empty-buzzword/

OWASP Top 10 IoT - OWASP Top 10



Top 10 2013	Top 10 2017
A1 – Injection	A1 – Injection
A2 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A3 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting
A4 – Insecure Direct Object References	A4 – Broken Access Control
A5 – Security Misconfiguration	A5 – Security Misconfiguration
A6 – Sensitive Data Exposure	A6 – Sensitive Data Exposure
A7 – Missing Function Level Access Control	A7 – Insufficient Attack Protection
A8 – Cross-site Request Forgery (CSRF)	A8 - Cross-site Request Forgery (CSRF)
A9 – Using Components with Known Vulnerabilities	A9 – Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	A10 – Unprotected APIs

Image Source: http://resources.infosecinstitute.com/owasp-2017-top-10-vs-2013-top-10/

Recommendations (the usual stuff):

- Isolate critical systems from public internet (but that not enough)
- Operating system hardening (disable non critical services, regular updates, rigid auditing, minimize remote access)
- Avoid the “if it ain't broke, don't fix it” approach
- Security appliances (Firewalls, IPS/IDS, AV)
- Raising awareness to all involved actors and training
- Redundancy and (tested to work) backups

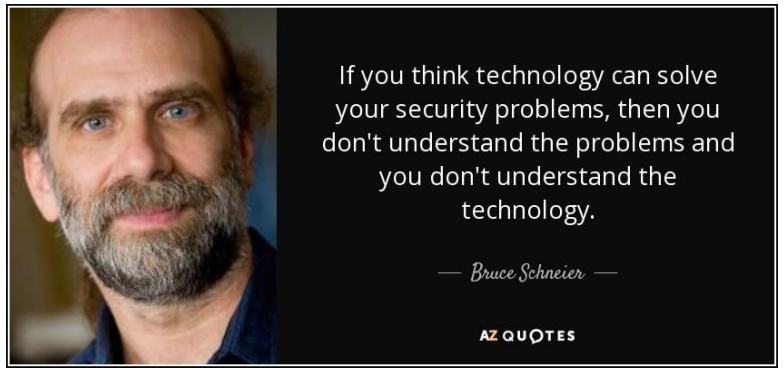
“I’m no expert, but I think it’s some kind of cyber attack!”

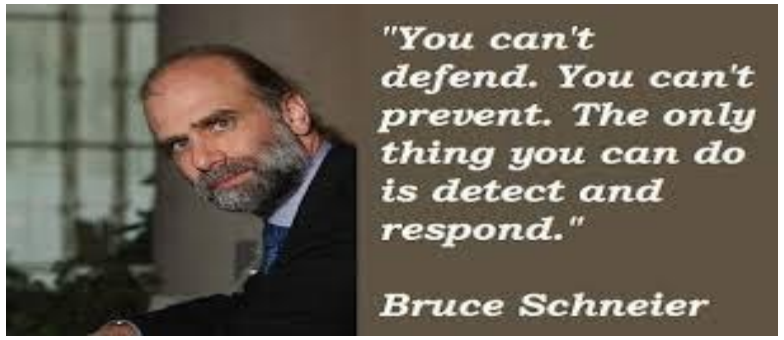
Recommendations (FBI stuff):

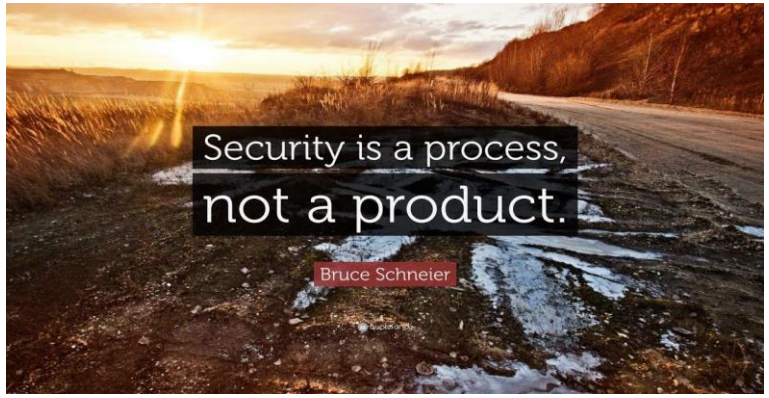
- Change default usernames and passwords. Many default passwords are collected and posted on the Internet. Do not use common words and simple phrases or passwords containing easily obtainable personal information, such as important dates or names of children or pets.
- If you can't change the password on the device, make sure your wireless Internet service has a strong password and encryption.
- Invest in a secure router with robust security and authentication. Most routers will allow users to whitelist, or specify, which devices are authorized to connect to a local network.
- Isolate “IoT” devices on their own protected networks.
- Turn devices off when not in use.
- Research your options when shopping for new “IoT” devices. When conducting research, use reputable Web sites that specialize in cyber security analysis and provide reviews on consumer products.
- Look for companies that offer firmware and software updates, and identify how and when these updates are provided.
- Identify what data is collected and stored by the devices, including whether you can opt out of this collection, how long the data is stored, whether it is encrypted, and if the data is shared with a third party.
- Ensure all “IoT” devices are up to date and security patches are incorporated when available.

Source: https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/fbi-tech-tuesday---building-a-digital-defense-against-the-internet-of-things-iot

Conclusions







Q&A

"Plans are worthless, but planning is everything."
- Dwight D. Eisenhower

Thank you!