



European Organization for Particle Physics
Exploring the frontiers of knowledge



DIY.DESPAIR.COM

Emerging IoT Threats... ...a not-so-new pain!



Emerging IoT Threats...
Dr. Stefan.Lueders@cern.ch
IoT Week, June 4th-8th 2018, Bilbao (E)

Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer

Sunday, April 15, 2018 Wang Wei

Share Share Tweet Share Share Mail Share



KRACK Wi-Fi vulnerability can expose medical devices, patient records

The Wi-Fi vulnerability can be used to steal and tamper with patient records.



By Charlie Osborne for Zero Day | May 1, 2018 -- 09:11 GMT (10:11 BST) | Topic: Security

Flaw in Emergency Alert Systems Could Allow Hackers to Trigger False Alarms

Tuesday, April 10, 2018 Swati Khandelwal

Share Share Tweet Share Share Mail Share



A critical security flaw in popular industrial software put power plants at risk

The bug in the industrial control software could leave power and manufacturing plants exposed.



By Zack Whittaker for Zero Day | May 2, 2018 -- 12:00 GMT (13:00 BST) | Topic: Security



Emerging IoT Threats...

Dr. Stefan.Lueders@cern.ch

IoT Week, June 4th-8th 2018, Bilbao (E)

Threats? Yes



C3 ~ RET

@c3retc3

#CERN discloses pass
and tickets to Web sp

6:03 a.m. - 29 Sep 2015

Telegraph.co.uk



Home

News

Sport

Business

Travel

Jobs

Motoring

Telegraph TV

Earth home

Earth news

Earth watch

Comment

Charles Clover



Hackers infiltrate Large Hadron Collider systems and mock IT security

By Roger Highfield, Science Editor

4:01pm BST 12/09/2008

anonymous Coward
ser ID: 9578086
United States
5/25/2015 10:42 PM
[Report Abusive Post](#)
[Report Copyright Violation](#)

Do you think it's possible for the CERN LHC to be hacked?

Shouldn't it have the same level of protections as a nuclear power plant? Yet I feel it probably does not...

ZDNet Government

Richard Koman

Get ZDNet Government via:

[Mobile](#)

[RSS](#)

[Email Alerts](#)

Bios:

Pick a blog category

view

September 12th, 2008

Hackers deface LHC site, came close to turning off particle detector

Posted by Richard Koman @ September 12, 2008 @ 8:35 AM

COMPUTERWORLD
Security

SEARCH Google

Budgets In
c Times

BigFix & PCI - Bringing Retail
Endpoints into Compliance

The Power of One - Global Visibility &
Control at the Velocity of Business Change

Hackers hit Large Hadron Collider Web site

Greek group says it defaced site of one of the project's main experiments

YOU D

Skyrocket 30%...
Again
GOOGLE TONE
SHARES LINKS TO
COMPUTERS WITHIN
EARSHOT USING



Emerging IoT Threats...

Dr. Stefan.Lueders@cern.ch

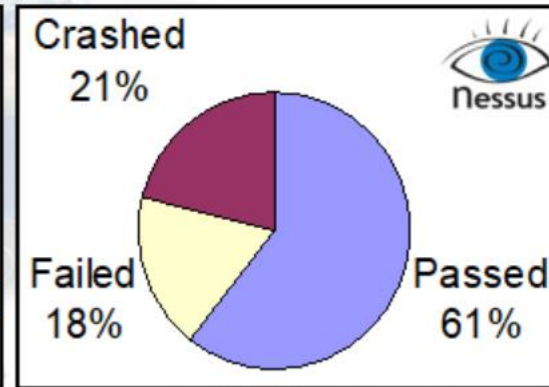
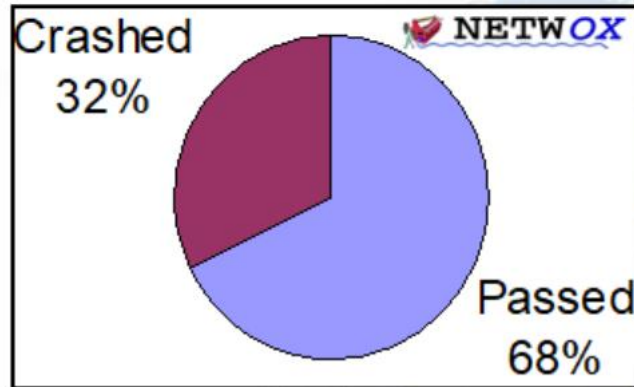
IoT Week, June 4th-8th 2018, Bilbao (E)

CERN: Under attack like everyone else



Controls under Attack !

- ▶ 20 devices from 6 different manufacturers (35 tests in total)
- ▶ All devices fully configured but running idle



...PLCs under load seem to fail even more frequently !!!
...results improve with more recent firmware versions ☺





TOCSSiC Findings

► Device crashed

- Sending specially crafted IP packet fragmentation re-assembly code to



TOCSSiC Findings

► FTP server crashed

- Sending a too long command or argument



TO

► HTTP server crashed

- Requesting a URL with too many (e.g. "http://<IP>/cgi-bin/aaa...aa



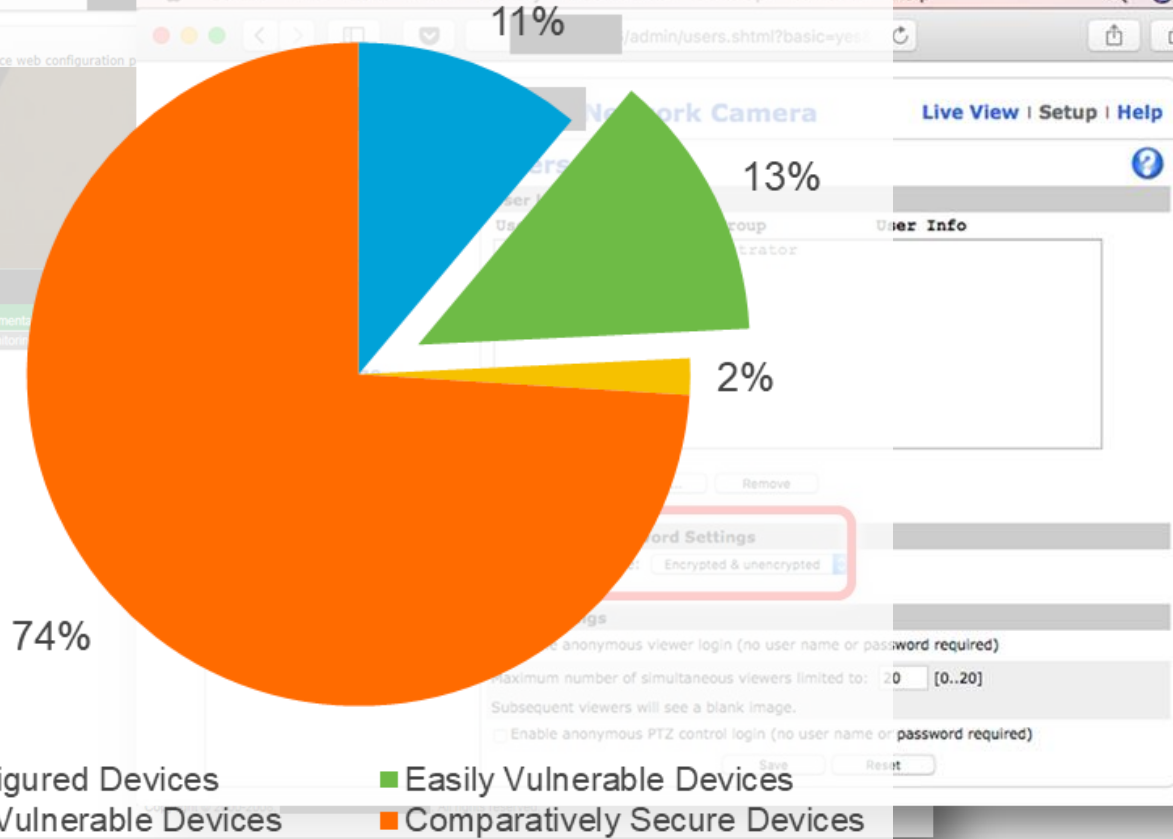
TOCSSiC Findings

► PLCs are un-protected

- Can be stopped w/o problems (needs just a bit "googling")
- Passwords are not encrypted
- Might even come without authentication
- Still allow for legacy commands

Vulnerability Assessment of 900 IoT Devices

Firmware Version : 3.93
Firmware Date : 20/09/2012
MAC Address : [REDACTED]



- Not Configured Devices
- Easily Vulnerable Devices
- Medium Vulnerable Devices
- Comparatively Secure Devices



**Exposure
Threats**

**Complexity
Vulnerabilities**

**Dependencies
Consequences**



Emerging IoT Threats...
...a permanent pain



Bye, Bill. Welcome RasPI & Arduino

Core-ICS apart, interconnections will grow

ICS and IoT will merge in some way

Wireless is already on the plant-floor

Internet & cloud access will become normal

Incentives for secure ICS lacks business case





www.cern.ch