European Organization for Particle Physics

Exploring the frontiers of knowledge

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

Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer

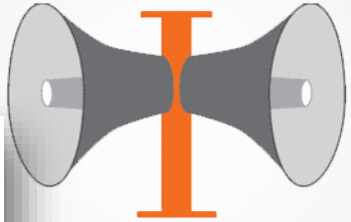
Sunday, April 15, 2018 Wang Wei

Share Share Tweet Share Share Mail Share

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



irenJack

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

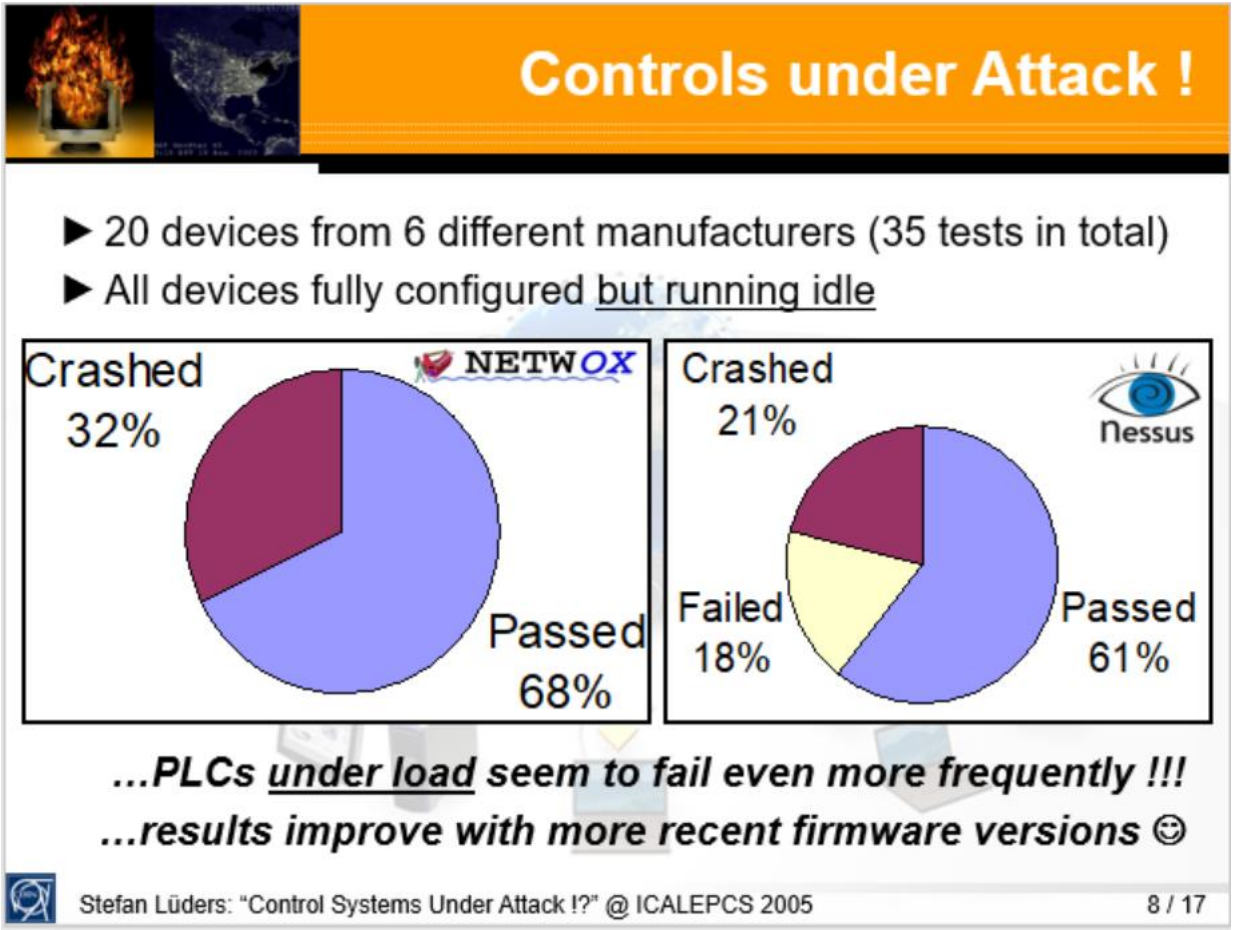
A critical security flaw in popular industrial software put power plants at risk

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

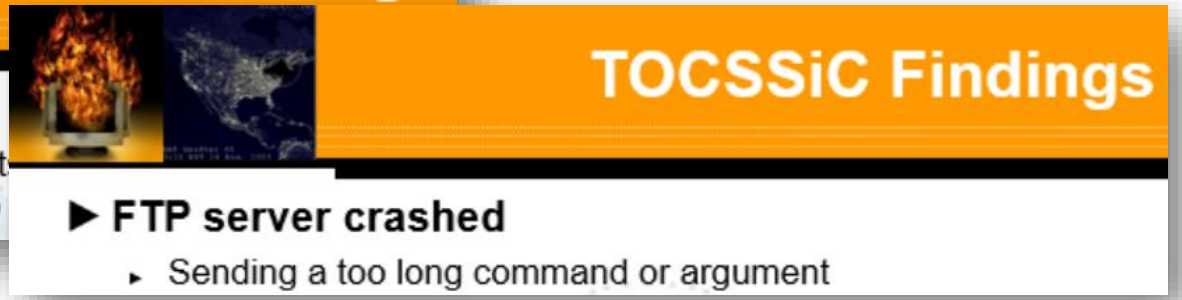
By Zack Whittaker for Zero Day | May 2, 2018 -- 12:00 GMT (13:00 BST) | Topic: Security

Threats? Yes

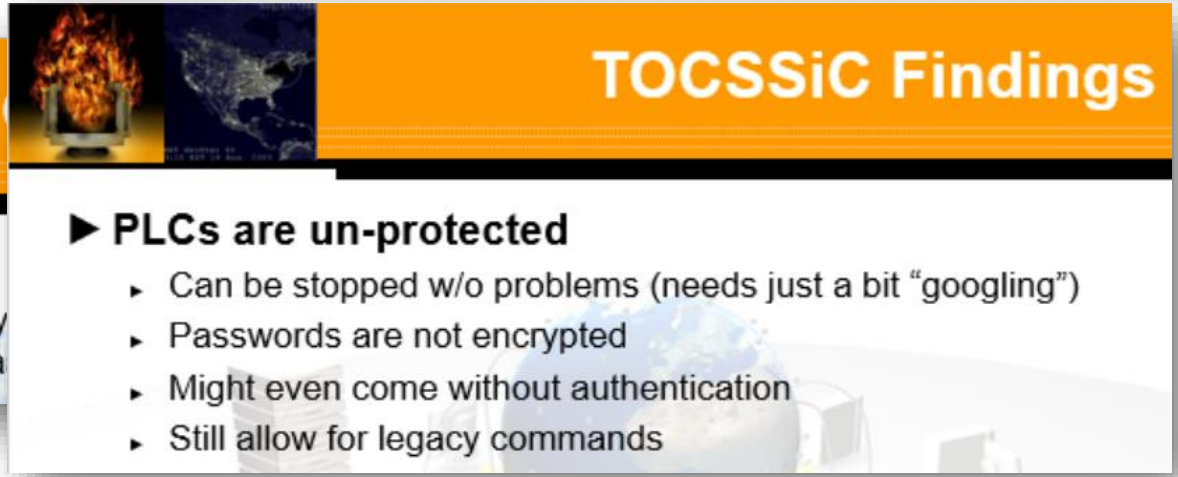
CERN: Under attack like everyone else

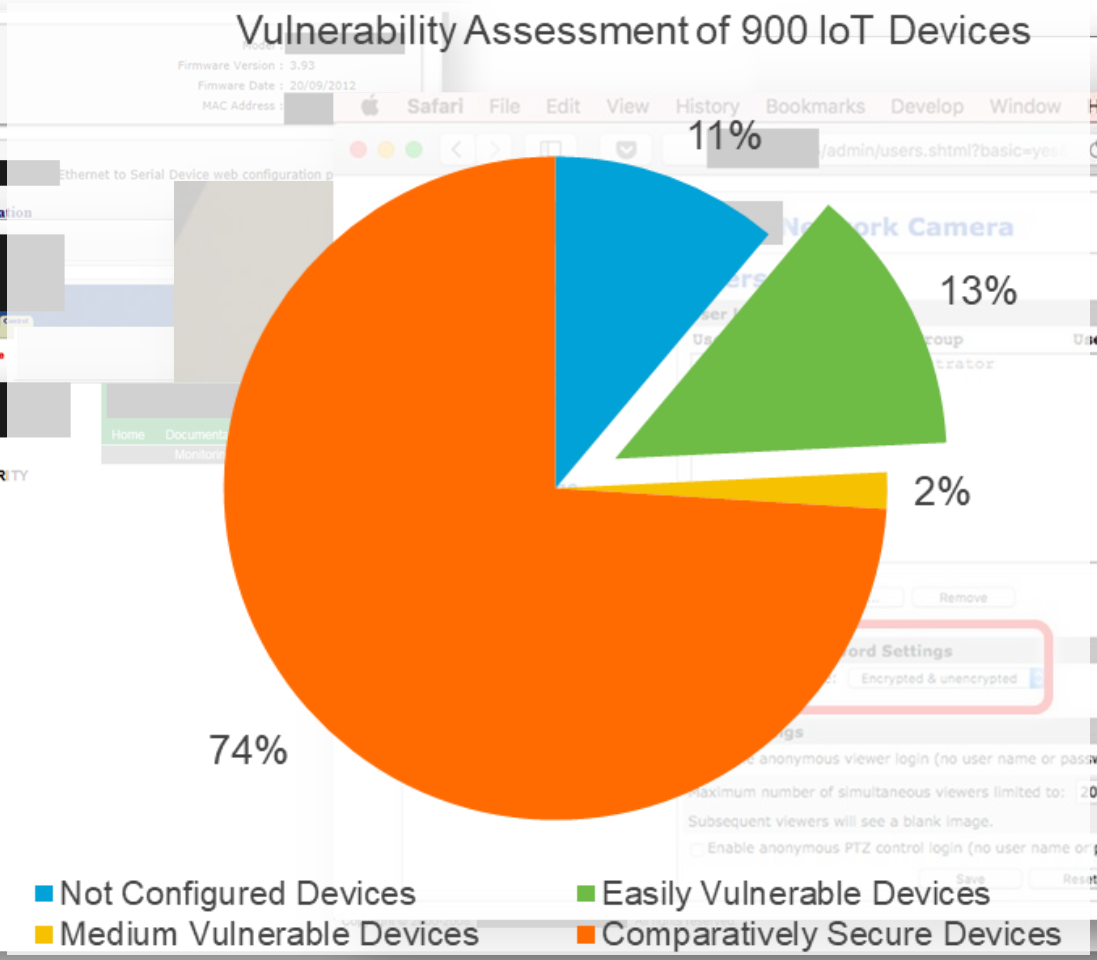

Controls under Attack !
▶ 20 devices from 6 different manufacturers (35 tests in total)
▶ All devices fully configured but running idle
Crashed
32%
NETWOX
Passed
68%
Crashed
21%
Nessus
Failed
18%
Passed
61%
...PLCs under load seem to fail even more frequently !!!
...results improve with more recent firmware versions ☺
Stefan Lüders: "Control Systems Under Attack !?" @ ICALEPCS 2005
8 / 17


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



The Internet of Stupid Things

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