Network Security Course | ETH Zurich - Autumn 2020

Internet of Things (IOT)

Dr. Stefan Frei

Security Officer @ SIX Digital Exchange www.sdx.com
frei@techzoom.net | Twitter @stefan_frei

Head of the working group "Supply Chain Security" @ ICT Switzerland

Internet of Things

Cyber Security

Content borrowed from Cyber Security course at D-MTEC

Understanding the key drivers of cyber security

Introduction to the concepts, developments, and the current state of affairs in the cyber security domain. We look at the topic from the attackers, defenders and societies perspective.

Objective

Upon completion of this course students understand the essential developments, principles, challenges as well as the the limitations and the state of practice in cyber security from the technological, economic, legal, and social perspective.

Cyber Security Course

Spring Semester | D-MTEC | 363-1070-00L | 3 ECTS credits | Dr. Stefan Frei | https://bit.ly/2JVpzAg (2019)

Common Ground

SAFETY VS. SECURITY

The English language differentiates **SECURITY** from **SAFETY**, for which there is only one expression **SICHERHEIT** in German.

SAFETY

- Safety is the protection **against random**, unwanted **incidents** - resulting from **coincidences** or driven by the environment
- **THE ENVIRONMENT DOES NOT ADAPT TO BYPASS SAFETY MEASURES.**

Natural Science
Controlled Experiments, Modelling

≠

SECURITY

- Security is the protection **against intended incidents** – resulting from a **deliberate and planned act**
- Driven by targeted attacker.
- **DELIBERATE ACTS DRIVEN BY AN ADAPTIVE ATTACKER.**

Social Science
Ever Changing Environment, Complexity, Chaos

HUMANS ARE NEW TO THE MECHANISMS AND ARTIFACTS OF CYBER RISK

We have no built-in concept to deal with abstract risks

INSTANT
PERCEPTION OF RISKS

No **training needed** to instantly get out of danger

Evolution built us to perceive risks as hunter-gatherer in the wild

LIMITED / NO
PERCEPTION OF RISKS

Security **defects are invisible** without proper testing

Humans are new to technology and abstract risks

NO PERCEPTION OF RISK

People need highly visible incidents before they act

Insecure systems cannot be identified without **extensive testing**

ILLUSION OF CONTROL

We face considerable **difficulty to get resources** (from C-level) to protect **against abstract risks**

ACCUMULATION OF RISKS

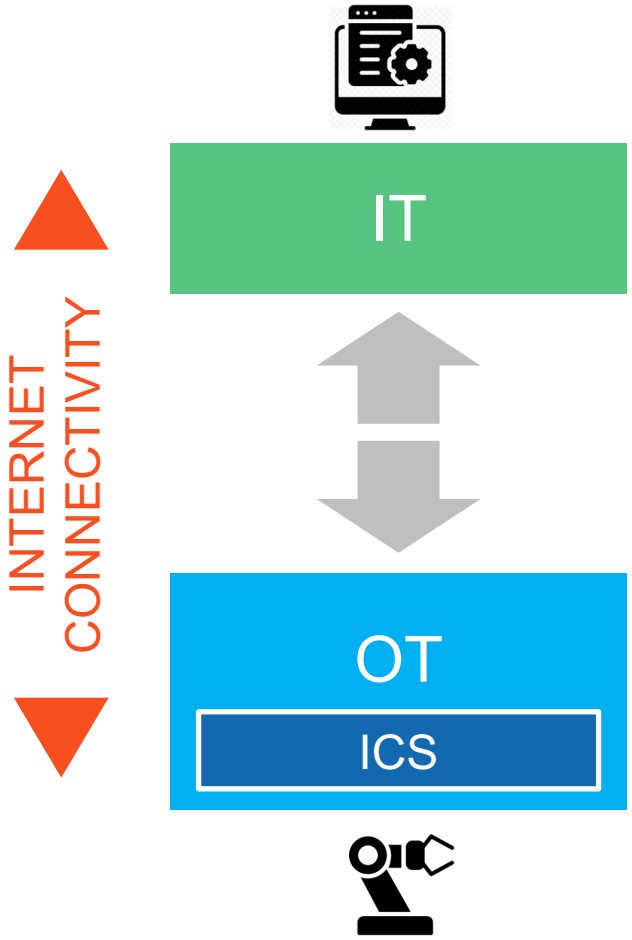
Internet of Things (IOT)

or was it

IOT, IIOT, ICS, SCADA, OT & IT?

Trending Terms ..

In recent years, IT systems have started to permeate the OT landscape



IT
INFORMATION TECHNOLOGY

Entire spectrum of technologies for information processing
- Including software, hardware, communications technologies and related services.

OT
OPERATIONAL TECHNOLOGY

Hardware and software dedicated to detecting or causing changes in physical processes
- E.g. direct monitoring and/or control of physical devices such as valves, pumps, etc.

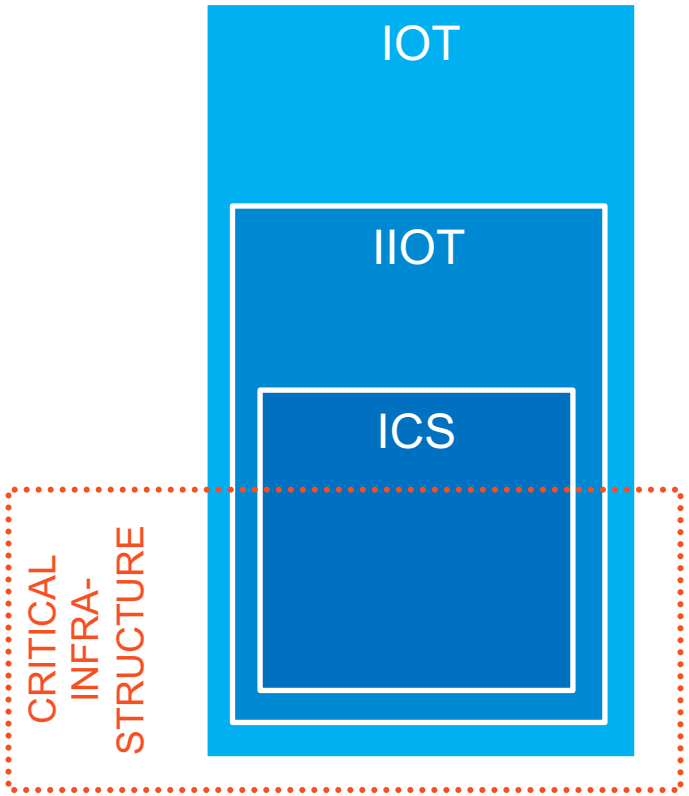
ICS
INDUSTRIAL CONTROL SYSTEMS

Systems used to monitor and control industrial processes
- Focused on automation, computerized monitoring and control of physical industrial processes (e.g. oil refining, electricity grids, building control, ..)
- typically considered to be mission and safety critical applications

IT systems enable OT systems to exchange information with business and user applications

Disruptions of critical infrastructure

Could result in loss of life, adverse economic effects, or significant harm to public confidence.



IOT
INTERNET OF THINGS

System of interrelated and connected computing devices

- Global network of "smart" physical objects of various kinds for monitoring, data gathering, reporting, remote control etc.
- Ability to transfer data without requiring interaction
- E.g. wearables, cars, smartphone, home appliances etc.

IIOT
INDUSTRIAL INTERNET OF THINGS

Subset of IoT specific to industry

- Covers industry as opposed to consumer market
- Varieties of "smart" hardware deployed in transportation, manufacturing, etc.
- E.g. field sensors, GPS asset location, drones, traffic lights, ..

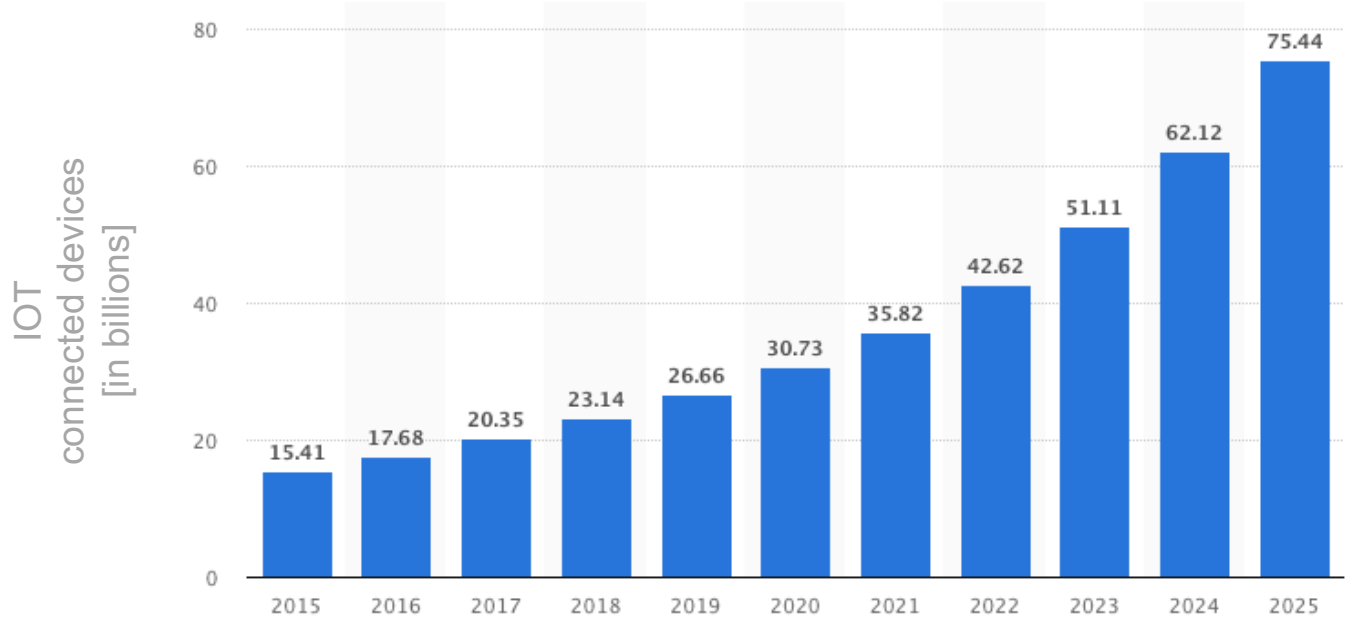
CI
CRITICAL INFRA-STRUCTURE

Processes, facilities, technologies, networks and systems that control and manage essential services (incl. IOT & IIOT)

- Disruptions of critical infrastructure could result in loss of life, adverse economic effect, etc.
- E.g. utilities, transportation and specific industries

IT / OT Convergence

Our world is quickly changing in an irreversible move towards IT/OT convergence…



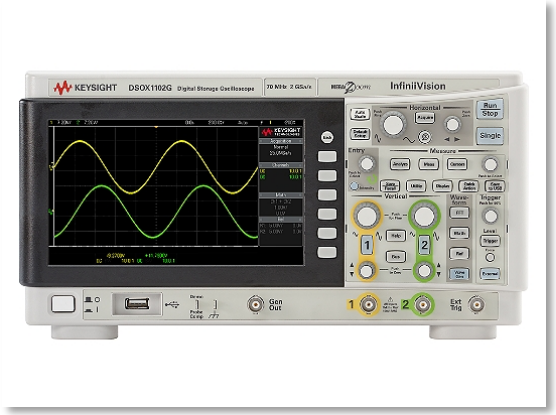
Extending security models to include the OT domain introduces many challenges

- Conventional IT security thinking is relatively mature, but only extends from cloud through to connected IT devices (mobile or fixed).
- OT devices must not be assumed to be ‘just another end point’
- **Security thinking needs to evolve**

Source https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

Embedded Devices Security?

What could possibly go wrong?



Playing Doom on Oscilloscope

or

Minesweeper on ATM

Source https://twitter.com/benschlabs
https://ripitapart.com/2018/10/15/gaining-access-to-the-windows-ce-desktop-and-doom-on-the-keysight-dsox1102g-oscilloscope/

Key Differences between IT and OT

OT and IT systems have different operational requirements which impact their ability to respond and adapt to these threats.

OPERATIONAL TECHNOLOGY (OT)		INFORMATION TECHNOLOGY (IT)
Limited data capacity and computing power	⟷	High data capacity and computing power
Safety Operations is critical	⟷	Few safety critical operations
High availability & integrity are vital with less stringent confidentiality requirements	⟷	**Confidentiality & integrity are vital while availability is important**
Critical operation and systems at edge of network with human operators at the center	⟷	Critical operation and systems at center of network, Human users at edge
Long life resulting in legacy, unsupported infrastructure	⟷	Continuous equipment upgrade with short life cycles
Essential equipment and operations remotely deployed at edge of network	⟷	Essential equipment and operations concentrated at center of network
Slow response to threats – rapid patching might be impossible due to outages	⟷	Rapid response to threats, patching and reboots acceptable

AVAILABILITY **INTEGRITY** **CONFIDENTIALITY**

Example 1

Novel Attacks / Risks

STRAVA - The #1 app for runners and cyclists

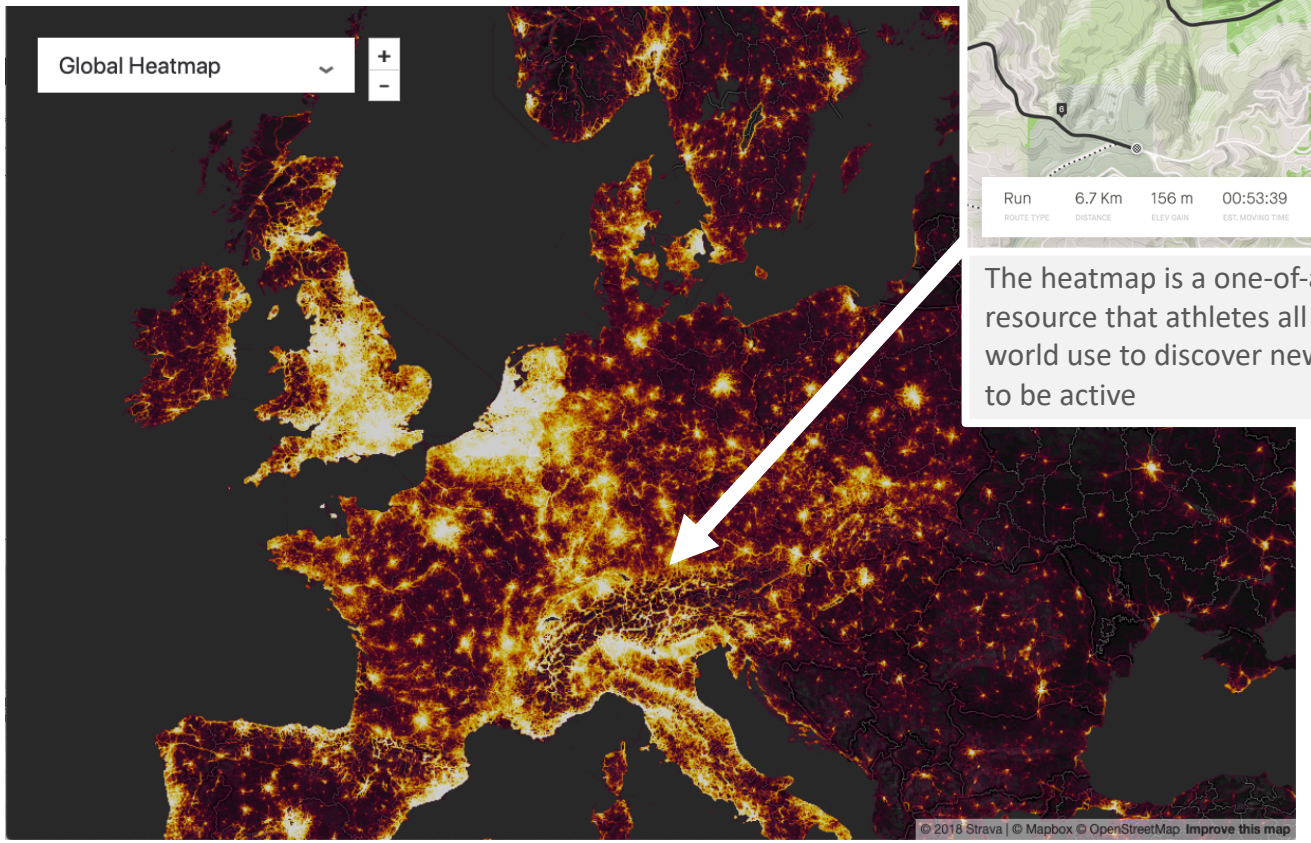
The advantages of IOT and wearable devices

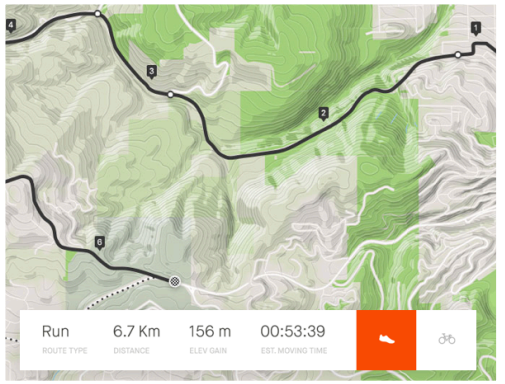
Fitness Tracker IOT

- Connect your fitness tracker with app & cloud
- Track and analyze every aspect of your activity.
- Connect with friends and share your adventure

Unimaginable just a few years ago:

EUROPE





The heatmap is a one-of-a-kind resource that athletes all over the world use to discover new places to be active

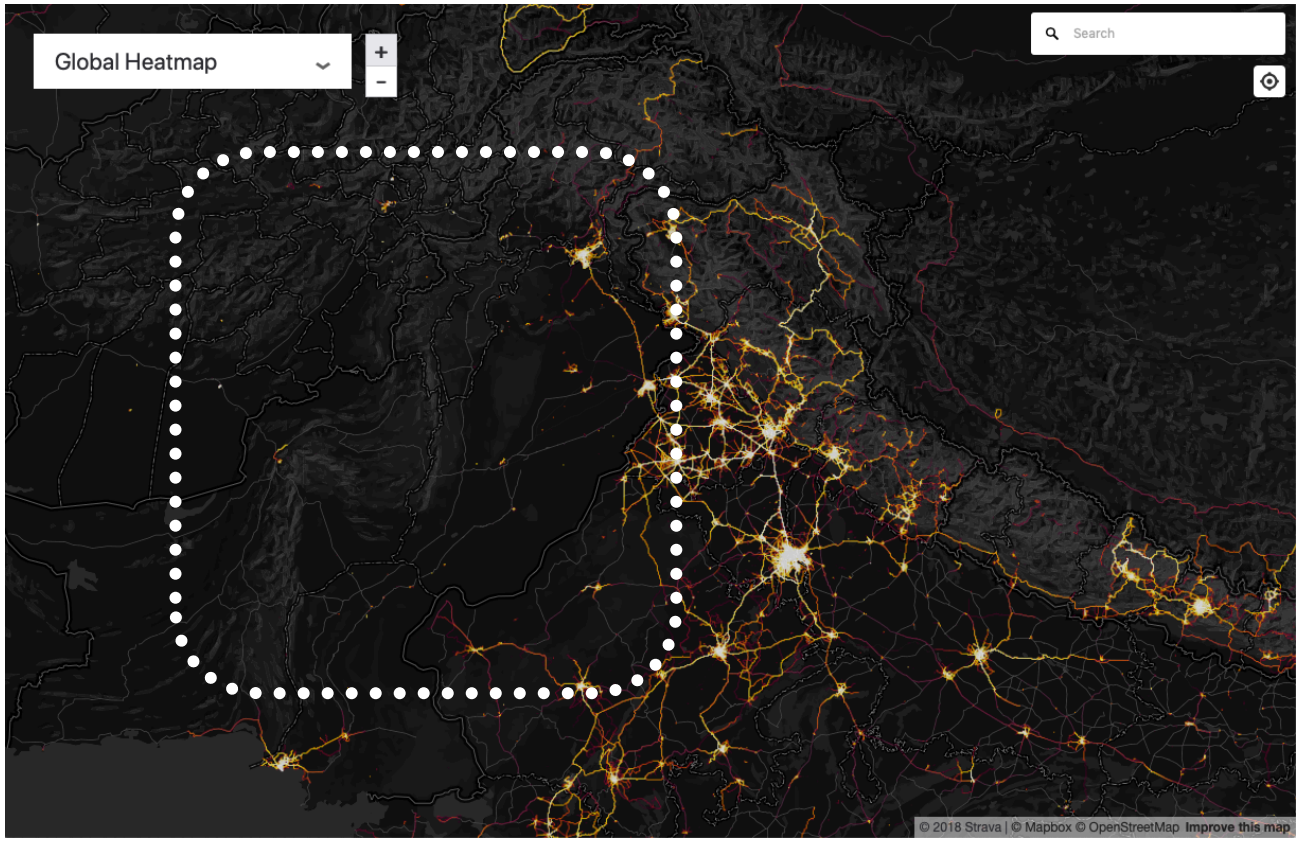
Source: https://www.strava.com/heatmap#4.00/4.41188/51.46564/hot/all

Different location …

Where, and why?

Not a lot going on here ..

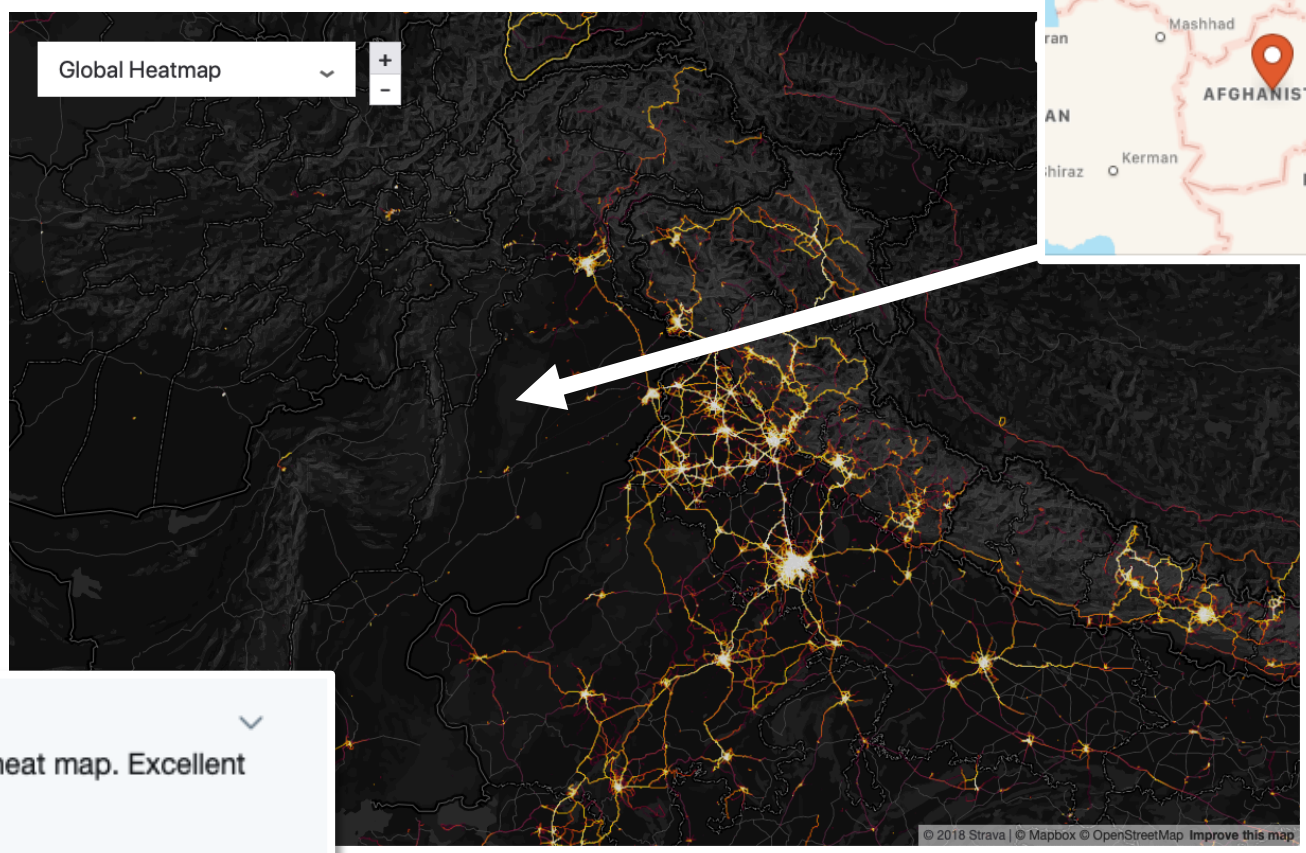
WHERE ARE WE ?

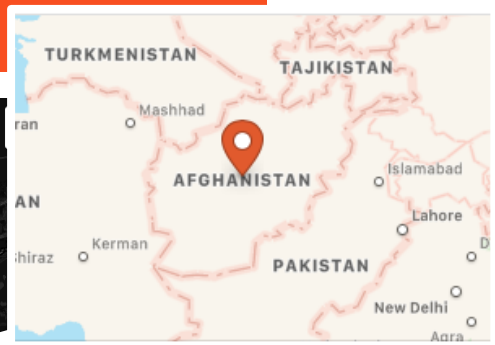


Soldiers use fitness trackers too ..

Data about exercise routes shared online by soldiers can be used to pinpoint overseas facilities

AFGHANISTAN





Fitness tracker reveals location of secret military outposts:

Tobias Schneider @tobiaschneider · 27 Jan 2018

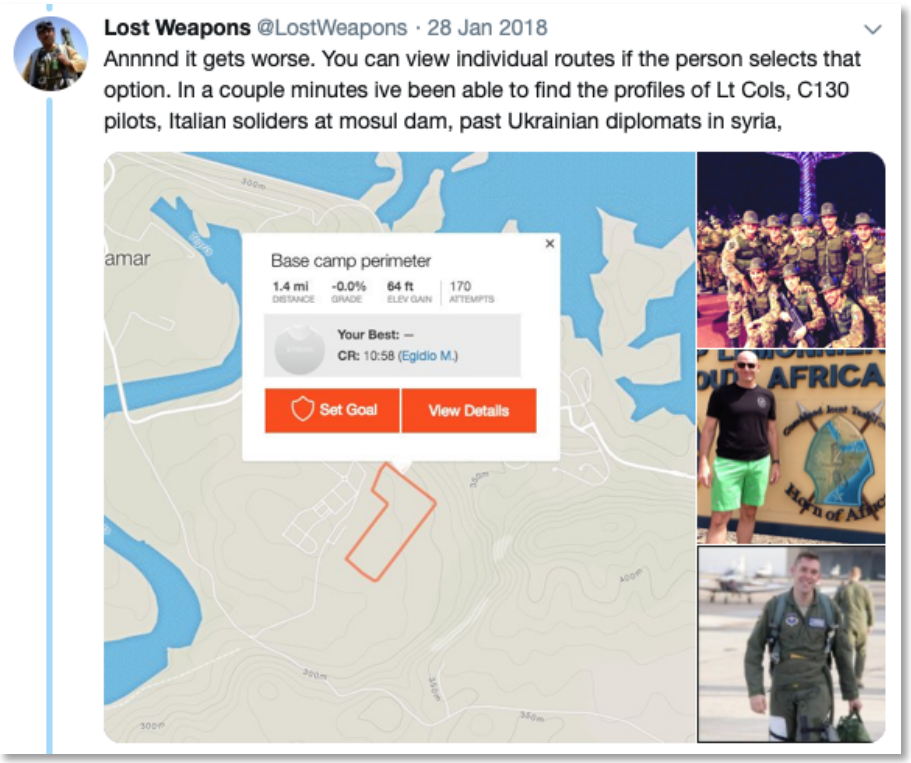
Fitness and social media company Strava releases activity heat map. Excellent for locating military bases (h/t to @Nrg8000).

labs.strava.com/heatmap/#6.06/…

Heatmaps accidentally reveal sensitive military positions

Data about exercise routes shared online by soldiers can be used to pinpoint overseas facilities, and individuals

A military base in Helmand Province, Afghanistan with route taken by joggers highlighted by Strava.



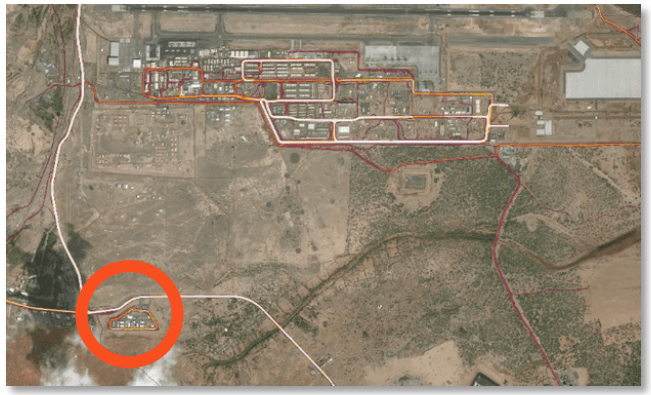
Exploiting App features and OSINT correlation skills to identify individuals

Sources
https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases
https://twitter.com/LostWeapons/status/957342822377472000

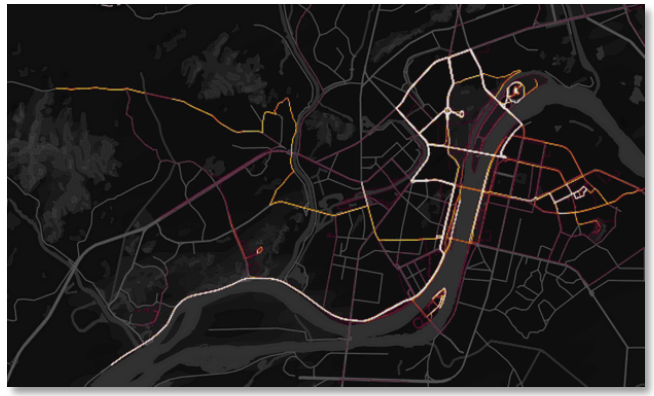
Heatmaps accidentally reveal sensitive military positions

Location of military bases and individual identities exposed

GCHQ in Cheltenham, England



Camp Lemonnier (top right), and a **suspected CIA base** (bottom left) in Djibouti



Heatmap displaying the **center of Pyongyang**, North Korea.

- As well as the location of military bases, the identities of individual service members can also be uncovered
- Such information can be extremely sensitive.
- The leaderboard for one 600m stretch outside an airbase in Afghanistan, for instance, reveals the full names of more than 50 service members who were stationed there, and the date they ran that stretch.

THE DEFAULT PRIVACY SETTINGS ALLOWED FOR THIS MASSIVE ACCIDENT.

Source https://www.theguardian.com/technology/2018/Jan/29/strava-secret-army-base-locations-heatmap-public-users-military-ban

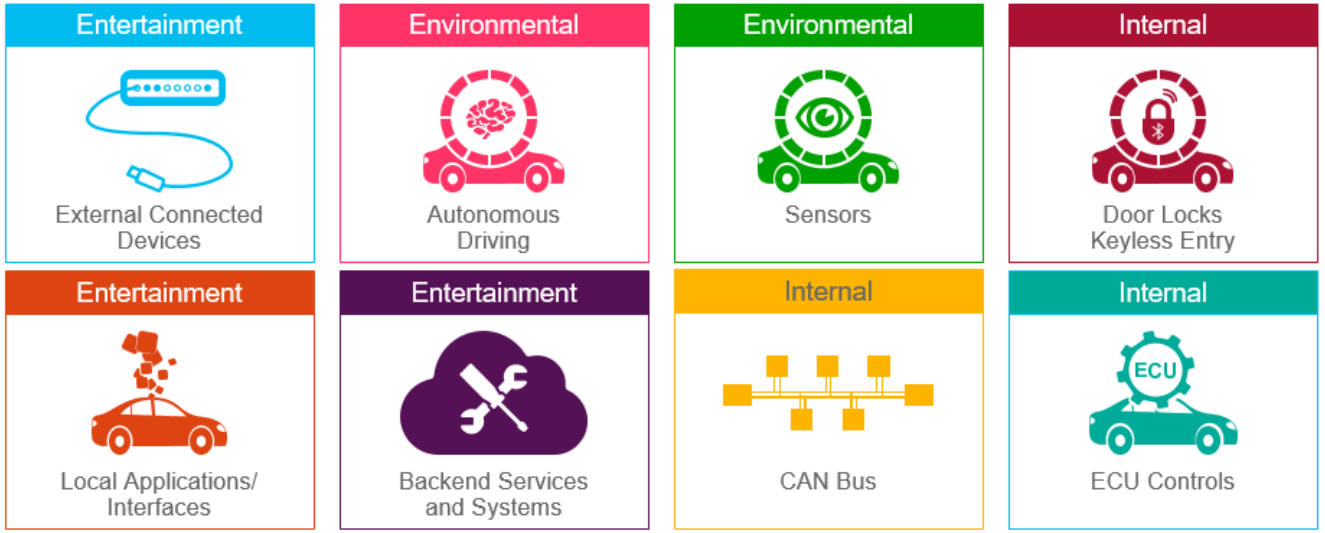
Example 2

Ignoring Known Security Best Practice

Connected vehicle attack surface

Ubiquitous networking within the vehicle, its environment, cloud services, and multiple user applications will become the new norm.

- Built on top of by-nature and by-default insecure transport channels) (Ethernet, CAN)
- Lifetime of user comfort and interactive components is far shorter than the car itself
- Insufficient protection against reverse engineering of both software and hardware
- “Gadgetizing” cars with mobility, connectivity and productivity while doing alterations to proven software to meet automotive standards
- “Cloudification” of automotive data with insufficient protection



See also: https://www.accenture.com/t20160719T011940__w__/us-en/_acnmedia/Accenture/Conversion-Assets/Microsites/Documents22/Accenture-Security-Call-to-Action-IOT.pdf

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY

Researchers exploit vulnerabilities in the car infotainment system to take control of critical vehicle functionality.

PHASE 1

- **Hack the Wi-Fi entertainment system connection** either by brute-forcing the Wi-Fi password or use the open port 6667 for Inter Process Communication and Remote Procedure Calls
- Reprogram the CAN Controller firmware used to interact with CAN-C and CAN-HS buses

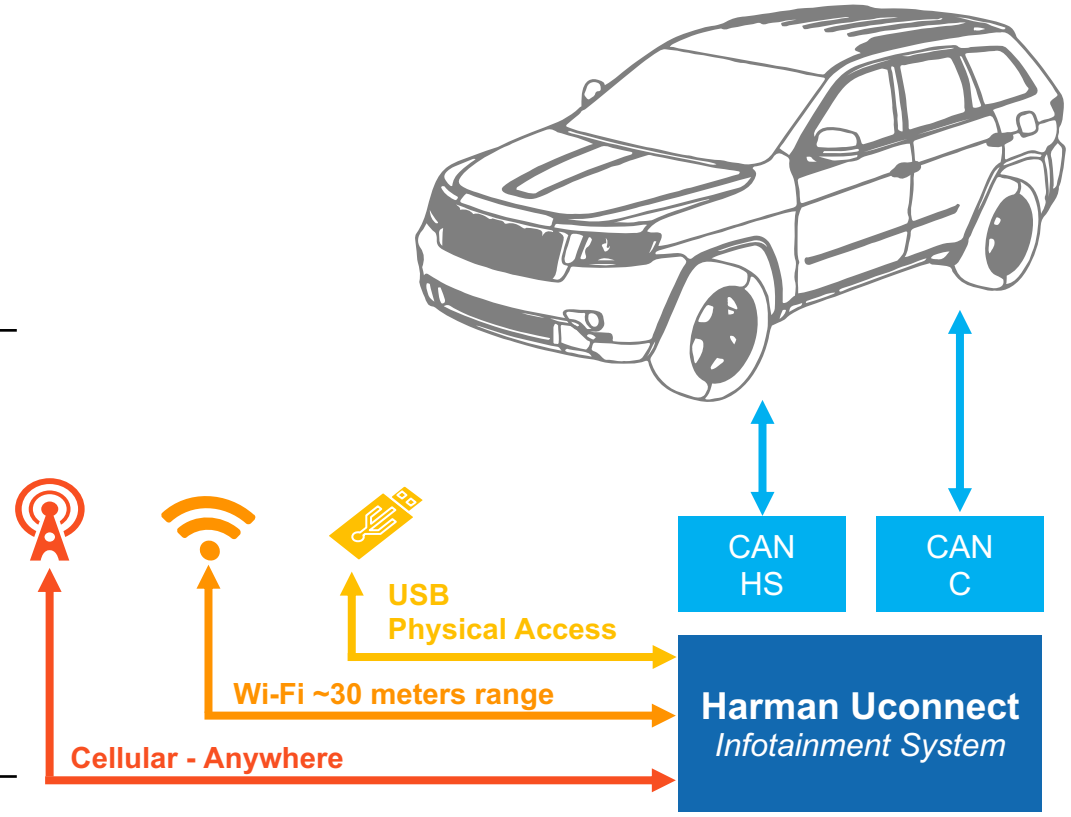
IMPACT The researchers were able to control the following control units (ECU): HVAC, Radio Volume, Bass, Display

PHASE 2

- **Identify the IP Address of the vehicle (pick a** random IP address within a specific range)
- Use port 6667 to get access to the main SOC remotely
- Reprogram (no need for USB) the CAN Controller Firmware

Cellular

IMPACT The researchers were able to control the following control units (ECU): Locks, RPMS, Engine, Brakes, Steering

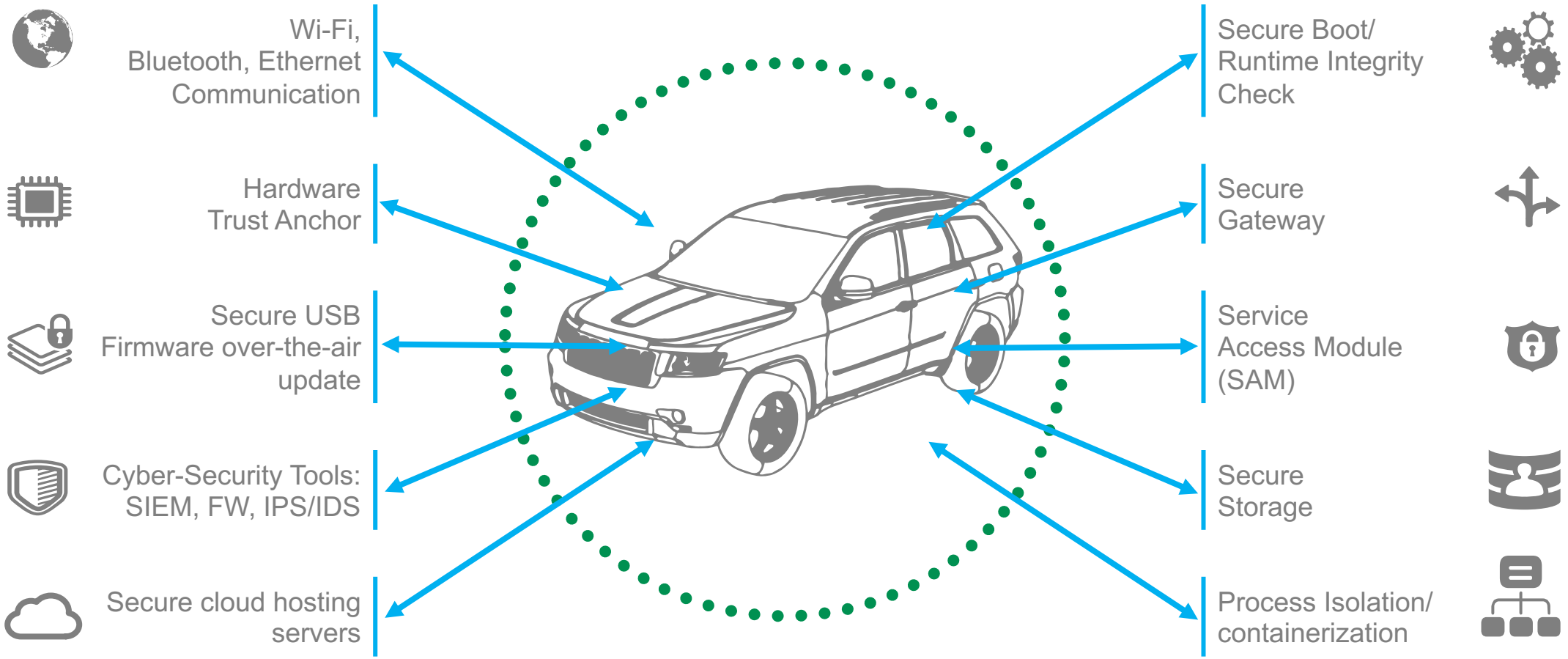


HVAC Heating Ventilation and Air Conditioning
CAN Controller Area Network

Source: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/
https://hackaday.com/2018/08/11/car-hacking-at-def-con-26/

CONNECTED VEHICLE ATTACK SURFACE

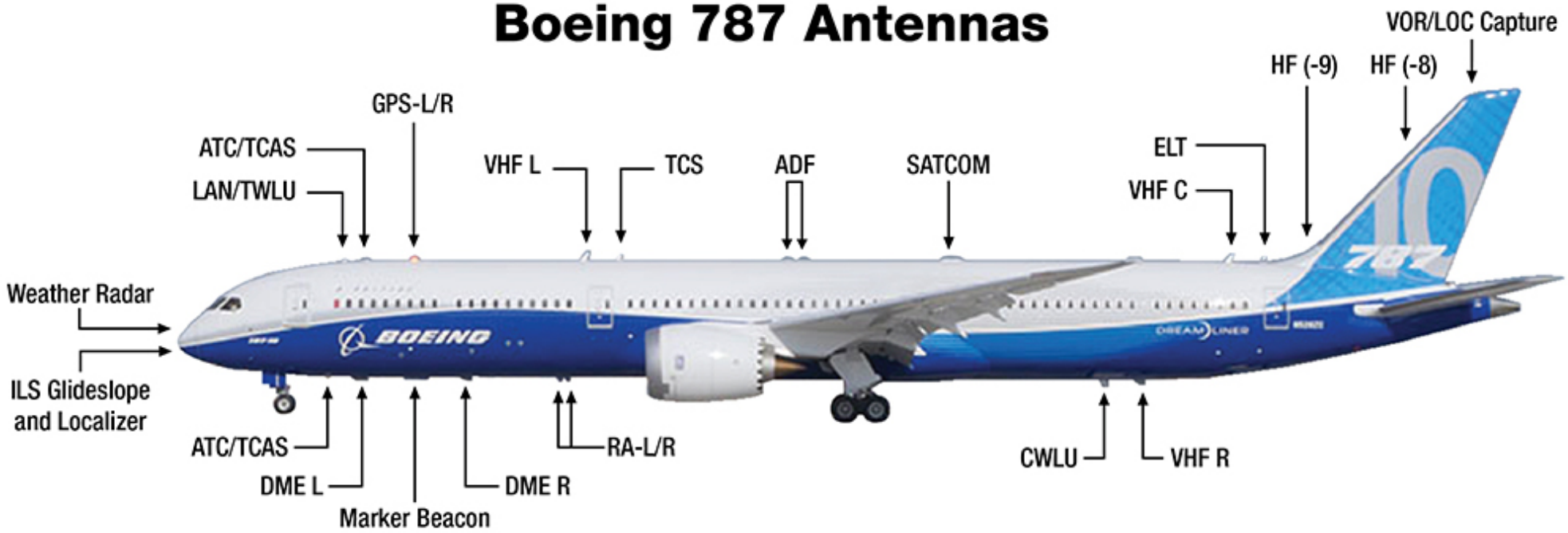
Major mechanisms to address to secure a connected vehicle



Example 3
Modern Product – Legacy Communications

MODERN AIRPLANES – LEGACY COMMUNICATIONS

Increasing number of poorly or not at all protected communication channels in modern aircraft



- **LAN/TWLU** Terminal wireless local area network (LAN) unit
- **ATC/TCAS** Air traffic control/traffic collision and avoidance system
- **DME** Distance measuring equipment
- **RA** Radio altimeter
- **GPS** Global positioning system
- **TCS** Terminal cellular system
- **ADF** Automatic direction finder
- **CWLU** Crew wireless LAN unit
- **ELT** Emergency locator transmitter
- **HF** High-frequency radio
- **VOR** VHF omni-directional ranging

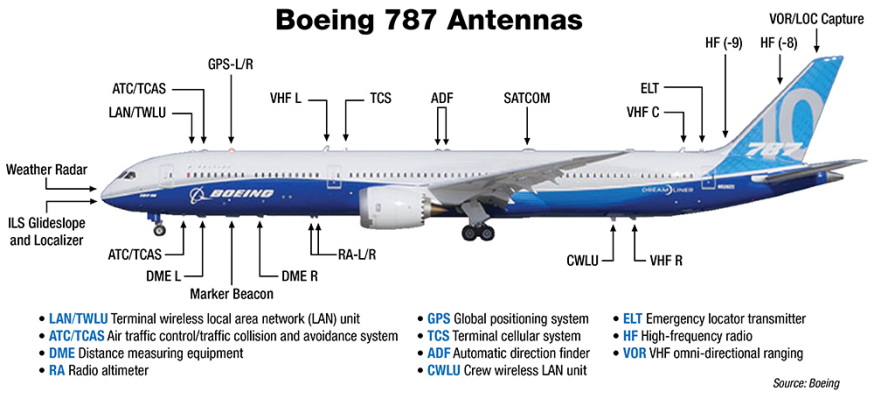
Source: Boeing

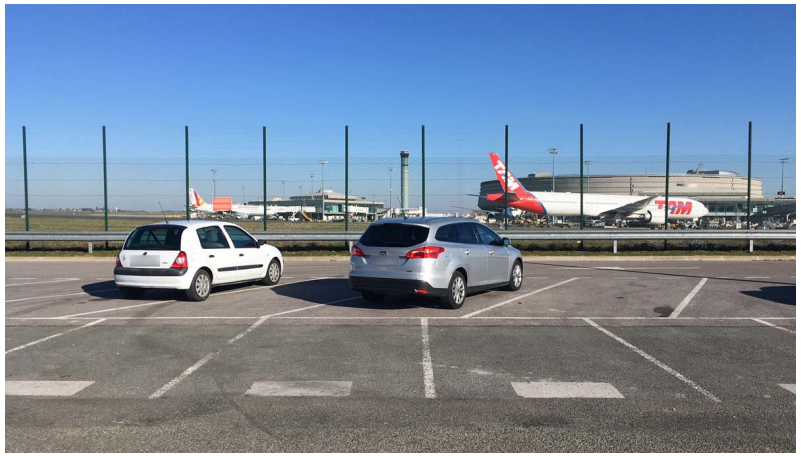
See also: "Data communications between an airplane Airbus A350 and the ground infrastructure" https://fenix.tecnico.ulisboa.pt/downloadFile/395146456513/Extended%20Abstract.pdf

MODERN AIRPLANES – LEGACY COMMUNICATIONS

Hacking into wireless communication with software defined radios

Legacy flight critical communication and navigation systems are not protected.
Modern airplanes use wireless (802.11 b/g) technology while at the gate transferring maintenance and reliability data (engine health management, replacement parts, software updates).





1. Intercept wireless communication between aircraft and airport terminal.
2. Team **sits in parked car**, connecting to target aircraft with **software defined radio**.
3. Accessed flight/cabin systems, modified code for specific flight plan.
4. **KNOCKING AT THE DOOR OF THE FLIGHT MANAGEMENT SYSTEM (FMS)**

Example 3

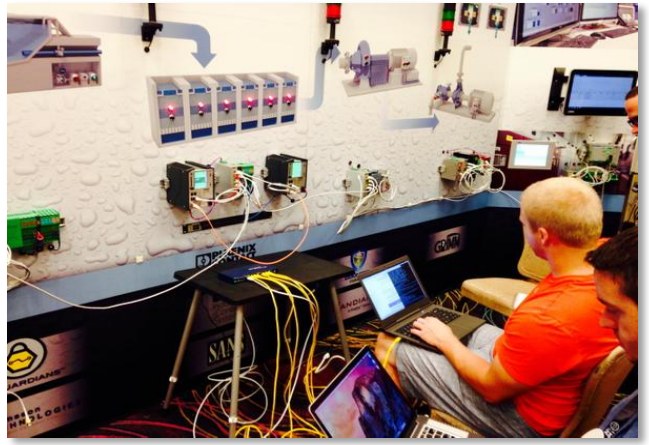
Security Through Obscurity

Attackers having fun with hardware

Security through obscurity does not work

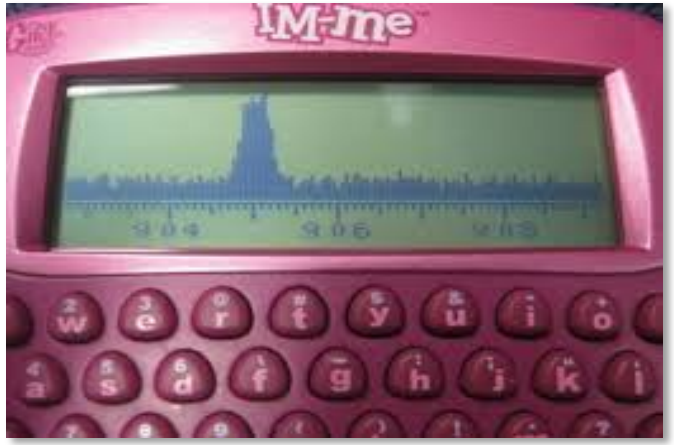
IOT Village @ Defcon

- DefCon 2015 hosted the IoT Village
- Participants examined 15+ off-the-shelf SOHO routers and IoT devices
- Result: **15 new zero-day exploits**
- The firmware of embedded devices is often found insecure or even containing backdoors



Garage Door Opener

- Prevalent garage door openers can be exploited over radio
- Design flaws allowed researcher to try all possible keys **in under 10 sec**.
- A kids toy from Mattel (USD 30.-) can be used to open any garage door after a firmware update



IOT
Attack Surface

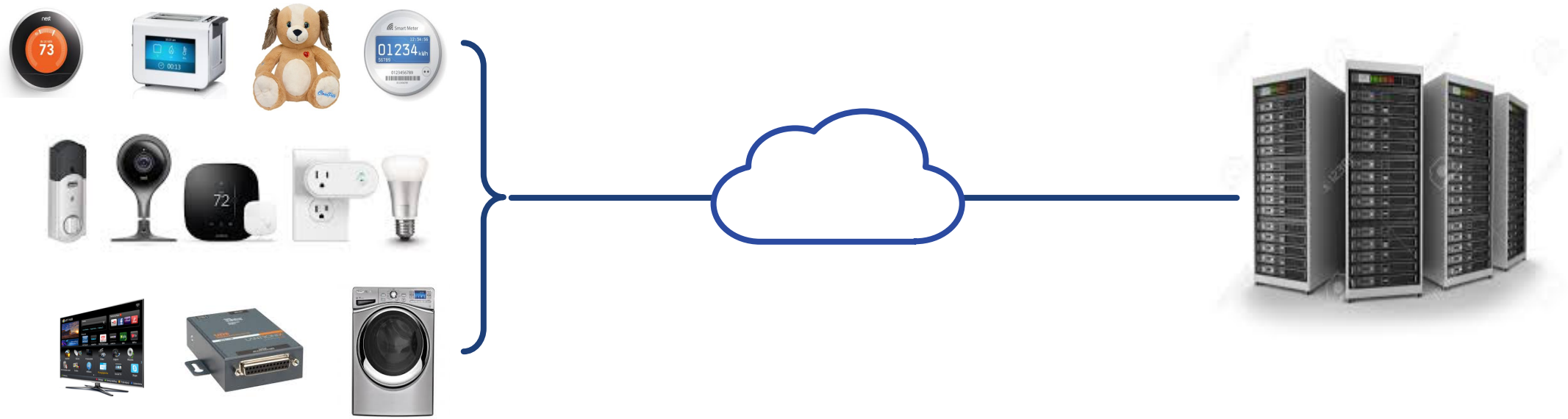
Internet of Things (IOT) Attack Surface

IOT connects innumerable everyday devices and systems

DEVICE
- Insecure software & defaults
- Lacking update mechanism
- Vulnerabilities

COMMUNICATION
- Insecure communication
- Weak or no cryptography
- Lack of authentication

BACKEND SERVICE
- Central control
- Erosion of privacy
- Data breaches



Previously closed systems are opened up to remote access and control

Risk Perception – User Perspective

COMPUTER	THERMOSTAT	TOASTER	SMART BEAR	SMART METER	SMART-TV
dangerous	great	cool	cute	nice	cool
					

TRADITIONAL IT

IOT & IIOT DEVICES

Risk Perception – Attacker Perspective

COMPUTER	THERMOSTAT	TOASTER	SMART BEAR	SMART METER	SMART-TV
antivirus, exploit mitigation patching	not patchable	easily exploitable	default password	outdated firmware	app vulnerabilities



DEVICE PROTECTED

DEVICES ARE BADLY PREPARED OR PROTECTED

ATTACKERS PERSPECTIVE

IOT and IIOT devices are just poorly protected networked computers

- built form cheapest components
- running complex, often outdated software
- suffer the same vulnerabilities as any software

NUMEROUS **EASY TARGETS**

Known and Proven Security Practice

.. mostly ignored in the IOT world

PERSONAL COMPUTER

- Networked and continuously hardened in battle
- Designed to withstand external threats
- Secure defaults

- Exploit mitigation, antivirus
- Frequent security updates

IOT, IIOT & ICS DEVICES

- Ran isolated for decades
- Designed for high availability and safety, not security
- Insecure defaults

- Old code, no protection
- No security updates

Most IOT, IIOT and ICS systems are not fit for todays harsh threat environment: When deployed, or when being connected.

Attacking Embedded Devices – 1/2

Extract data from a device‘s internals (hardware, firmware, and software)

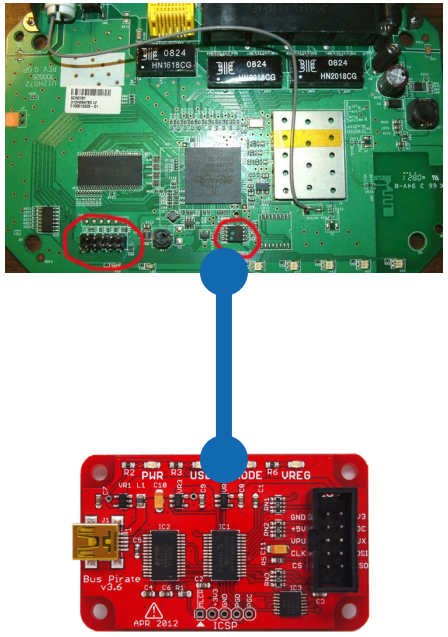
OSINT

Open Source Intelligence
- Retrieve firmware from vendor website
- Get devices from e-bay (e.g. avionics)

ACCESS
DEBUG
INTERFACES

Connect to device bus or debug ports
- Retrieve firmware, configurations, secrets
- Extract non-protected “secrets”

TARGET DEVICE
EXPOSED DEBUG
PORTS



BUS PIRATE
SNIFF DEBUG
PORTS

Assume attacker has full access to device.

The Bus Pirate is an open source hacker multi-tool that talks to electronic stuff - http://dangerousprototypes.com/docs/Bus_Pirate
Binwalk is a fast, easy to use tool for analyzing, reverse engineering, and extracting firmware images - https://github.com/ReFirmLabs/binwalk

Attacking Embedded Devices – 2/2

Extract data from a device‘s internals (hardware, firmware, and software)

Manufacturers and engineers have long assumed that embedded devices are not targets for hackers. These assumptions are outdated, including the belief in security by obscurity.

IMPACT OF A HACKED EMBEDDED DEVICE

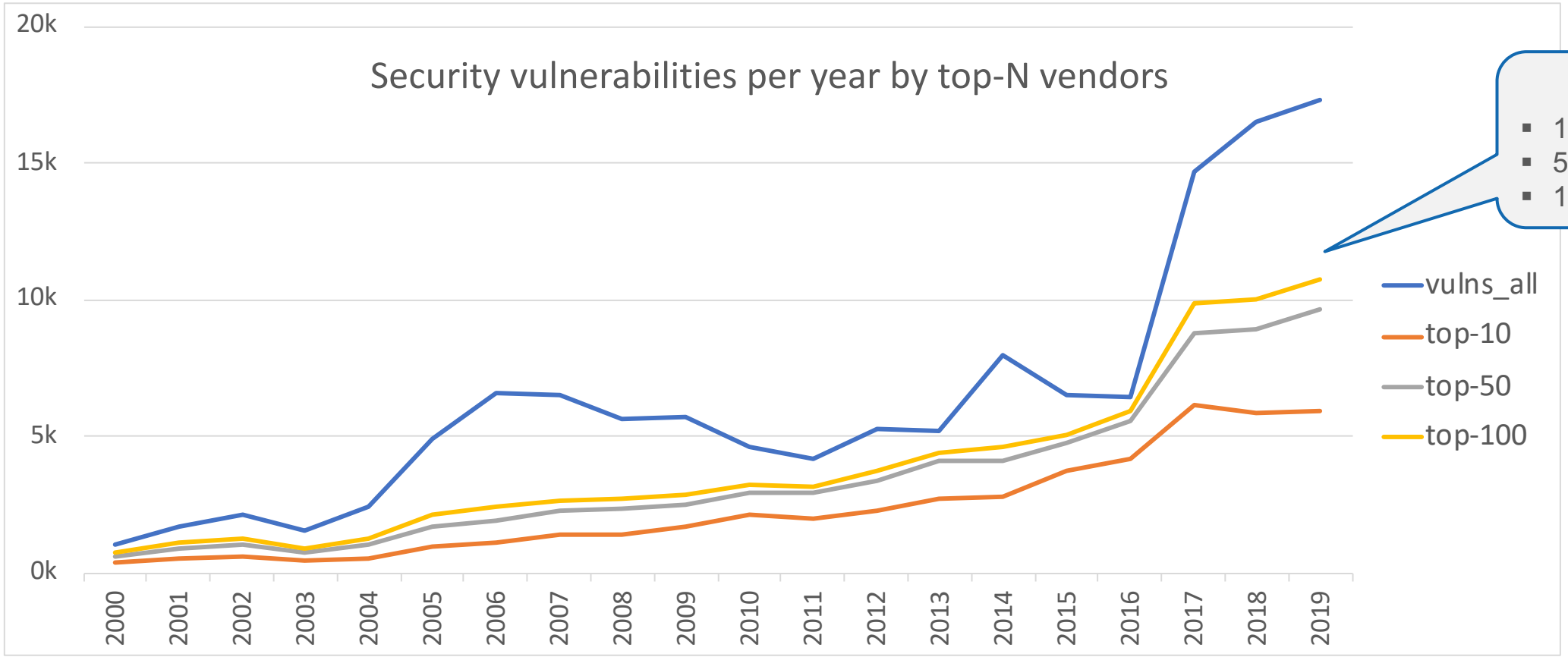
- Once designed and built, embedded devices are mass produced
- There may be thousands to millions of identical devices
- If a hacker is able to build a successful attack against one of these devices, the attack can be replicated across all devices

Root level access to the device (default accounts or secrets), certificates, device fleet passwords

Secure and harden embedded devices. Create unique identity & default passwords for devices in the field.

Software Vulnerabilities

20 Years of History / Experience with Vulnerabilities



>17k VULNERABILITIES PUBLISHED IN 2019

>30% MORE THAN 30% OF THE VULNERABILITIES IN PRODUCTS OF 10 VENDORS

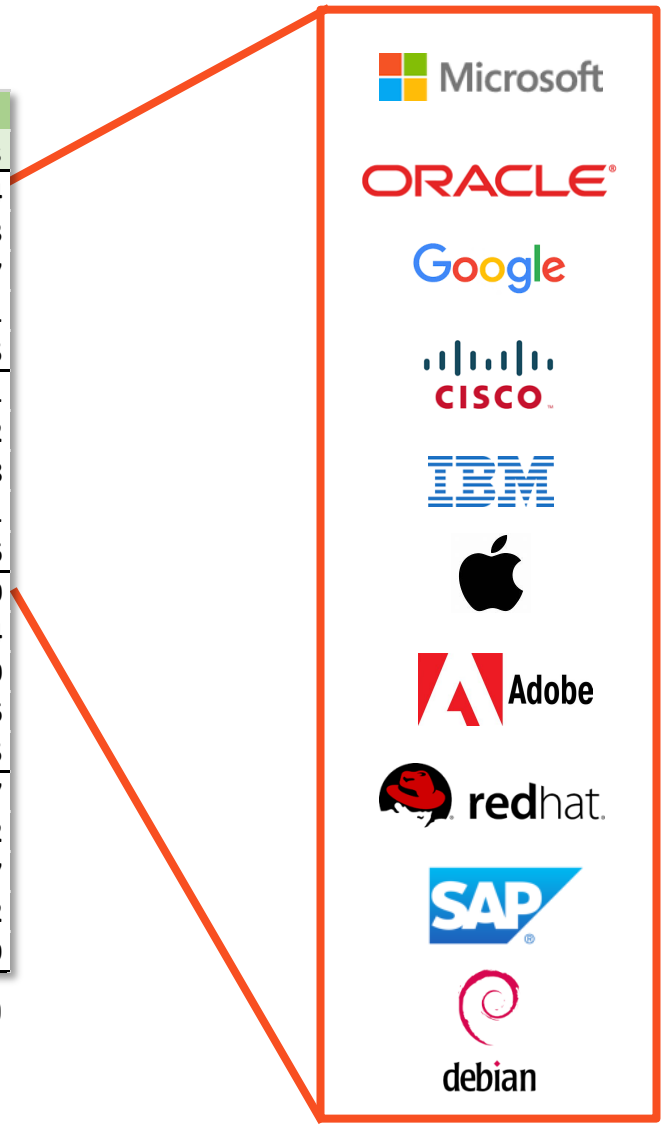
Source: National Vulnerability Database (NVD) | Nov 2020

Software Vulnerabilities

A few vendors account for majority of vulnerabilities

	Period 2017		Period 2018		Period 2019		Period 2020 Jan-Oct	
Rank	Vendor	CVEs	Vendor	CVEs	Vendor	CVEs	Vendor	CVEs
1	microsoft	**1'287**	microsoft	**1'350**	microsoft	**1'845**	microsoft	**1'374**
2	google	**1'084**	debian	**1'339**	apple	**1'101**	oracle	**663**
3	apple	**896**	redhat	**867**	google	**901**	google	**527**
4	oracle	**893**	google	**845**	debian	**678**	cisco	**361**
5	ibm	**686**	canonical	**825**	oracle	**644**	ibm	**325**
6	linux	**631**	oracle	**770**	adobe	**569**	apple	**301**
7	debian	**564**	ibm	**643**	cisco	**560**	adobe	**262**
8	cisco	**491**	apple	**508**	redhat	**491**	redhat	**178**
9	imagemagick	**357**	cisco	**457**	ibm	**478**	sap	**171**
10	adobe	**353**	adobe	**387**	linux	**385**	debian	**166**
11	huawei	**252**	qualcomm	**376**	jenkins	**344**	jenkins	**160**
12	apache	**223**	mozilla	**361**	fedoraproject	**328**	opensuse	**144**
13	redhat	**199**	hp	**301**	cpanel	**321**	huawei	**140**
14	gnu	**198**	linux	**279**	canonical	**299**	gitlab	**136**
15	canonical	**197**	foxitsoftware	**251**	qualcomm	**298**	linux	**135**
16	tcpdump	**133**	huawei	**226**	intel	**236**	mozilla	**127**
17	irfanview	**115**	apache	**176**	opensuse	**232**	intel	**122**
18	xnview	**114**	jenkins	**161**	foxitsoftware	**176**	chadhaajay	**117**
19	opensuse	**110**	netapp	**143**	hp	**170**	fedoraproject	**112**
20	fedoraproject	**101**	sap	**127**	gitlab	**165**	qualcomm	**99**

Source: National Vulnerability Database (NVD) | Nov 2020



In spite of increased investment,

there will never be secure code, given the 'special' business model of software.

Software Vulnerabilities | Industrial Control Systems Exposure

September 2018 to August 2019

PWN2OWN

31

Successful exploitations at Pwn2Own Contest 2019

- Desktop OS: **Apple** MacOS (4), **Microsoft** Windows (1)
- Mobile: **Xiaomi** Mi6 (8), **Samsung** Galaxy (5), **Apple** iOS (2), **Google** Android (1)
- Browser: **Apple** Safari (3), **Mozilla** Firefox (2)
- Virtualization: **VMWare** Workstation (2), **Oracle** VirtualBox (4)

BUG BOUNTY

1,251

Vulnerabilities reported to Zero Day Initiative (ZDI)

- 1,251 vulnerabilities affecting 51 vendors **reported to ZDI** bug bounty program
- Top 5 vendors: **Adobe (200), Microsoft (178), Foxit (140), Advantech (92), HPE (92)**

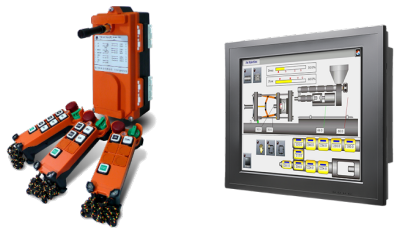
ICS / SCADA

278 | 22%

Industrial Control Systems ICS / SCADA

- **278 or 22%** of these affect Industrial Control Systems (ICS)
- Top 5 vendors: **Advantech (92), Delta Industrial Automation (56), LAquis SCADA (55), Fuji Electric (23), Schneider Electric (20)**

Devices

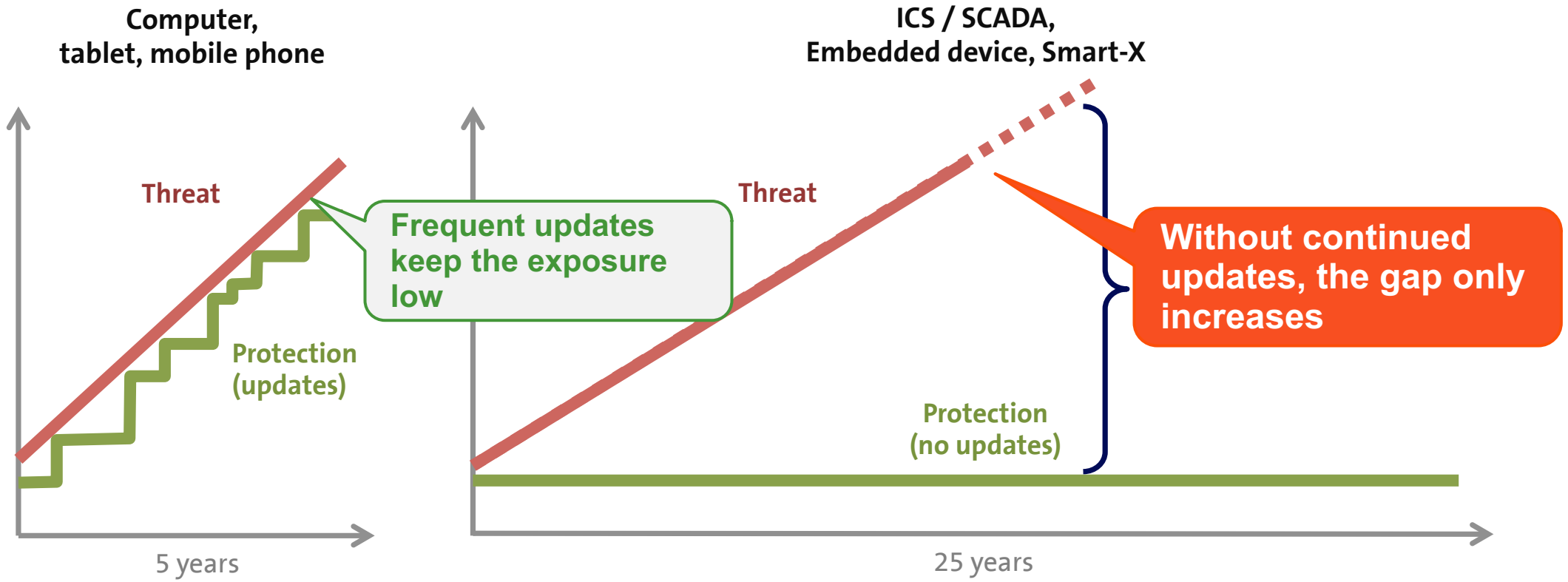


Local Controller

Simulation & Central Control

MANAGE AND PATCH VULNERABILITIES

Cyber devices require continued "security maintenance"



We rapidly create a huge future liability with devices lacking and automated and robust update functionality

VULNERABILITY MANAGEMENT - STILL A LONG WAY TO GO

IOT industry re-discovers the full disclosure debate

2013

Researchers informed Volkswagen in May 2013 of critical issues in the keyless car access system (also used by Porsche, Audi, Bentley, and Lamborghini, Audi, Fiat, Honda, Volvo, ..)

Volkswagen sued researchers and universities in order to prevent publication.

> Volkswagen acknowledged the technological flaw in its cars. But the company stressed that the hack takes "**considerable, complex effort**" that's **unlikely** to be used except by tech-savvy, **organized crime syndicates**. It didn't comment on its attempt to silence researchers, though.

2015

News Reports: **42% of top-end cars stolen by keyless entry systems**.

14 AUGUST 2015 - 9:35PM | POSTED BY NOEL YOUNG

Electronic car thieves carry out 42 per cent of top-end car grabs in London; the story VW kept quiet

11 Shares

Keyless car theft, in which hackers worm their way into electronic locks and immobilizers, now accounts for 42 percent of stolen vehicles in London.

BMWs and Range Rovers are particularly at risk, police say, and can be in the hands of a technically minded criminal within 60 seconds.

Source: http://www.thedrum.com/news/2015/08/14/electronic-car-thieves-carry-out-42-cent-top-end-car-grabs-london-story-vw-kept
http://bit.ly/VWHack2015 | https://money.cnn.com/2015/08/14/technology/volkswagen-car-hacking/index.html

Traditional Products vs. Digital Products

Traditional products rarely change after delivery,
whereas digital products constantly require security updates.

PURCHASE AND DEPLOYMENT
e.g. smart meter, IOT device

VENDOR EXITS MARKET
e.g. bankrupt
Product discontinued

CRITICAL VULNERABILITY
- *devices left exposed*
- *no more security updates*
- *loss of control for years or decades*

product supported | product no longer supported → *time*

Lifespan of decades for embedded or IoT devices
Replacement of devices is very difficult or prohibitively expensive

OPTIONS **BEFORE PURCHASE**

Code Escrow
- Agree to have a copy of source code deposited with trusted third party

Open Source
- Mandate to open source code in case of manufacturer exiting market

Certification vs. Security

Digital products constantly require security updates

Digital products may have a lifetime of decades.

Many digital devices have to be certified to be used

- By applying a security patch the certification is lost, further use of the device is illegal
- Current (re)certification cannot keep up with dynamic security requirements

Certification timeline is outpaced by cyber security, an industry wide challenge.

Aviation

Medical

Power

You're doomed if you patch – you're doomed if you don't.

Conclusions

NEW ‘CYBER-RISKS’ ARISE AS WE BECOME ENORMOUSLY DEPENDENT IOT.

The digital and real world cannot be divided any more - they form a single connected system > Digital information drives real events

This includes threats to:

- Individuals, such as privacy intrusion, identity theft, manipulation by personalized information
- Companies, such as cyber crime, cyber espionage & sabotage
- Societies, such as cyberwar, erosion of privacy, fake news, or totalitarian control

Today’s strongly connected, global networks have produced highly interdependent systems that we do not understand and cannot control well

Security beyond pure Technology

IOT security is part of a complex and evolving ecosystem of diverse domains

Challenges	What is needed
The security of individual components (e.g. technologies) **does not imply the security of the complete system** (connected vehicle ecosystem).	▪ Design systems with **redundancy and resiliency** (fail safe, fail secure) ▪ Realistic testing plans for the **complete system (end-to-end)**
The continued innovation of attackers, threats, technologies, society, and use-cases creates **a dynamic and adaptive threat** landscape.	▪ Prepare **for continued adaptation** to new threats, no matter what the driver or domain behind the attacker or threat. ▪ Comprehensive and continued security monitoring
Software drives everything, and there is no such thing as secure software. Prepare for the continued **discovery and publication of vulnerabilities in software and hardware**.	▪ Active **management of vulnerabilities** (coordinated disclosure, bug bounty) ▪ Robust and **scalable process to deploy security updates** timely and efficiently – on **any connected device**
We depend on a **complex supply chain of hardware and software** components, which **can not be fully controlled**. Assume that some components are already compromised.	▪ Systematic **security and integrity testing** of all critical components (reverse engineering of software & hardware). ▪ Comprehensive security appendix in supplier contracts

Technology based security solutions have to complement other domains to achieve the desired security level.