Security in IoT Ecosystem

Module 1

Introduction to Security in IoT

Prof.: Joaquín Recas

Table of Contents

1. General introduction and review
2. Introduction to IoT security
    1. IoT problem
    2. OWASP in IoT
    3. Good practices
3. Conclusions

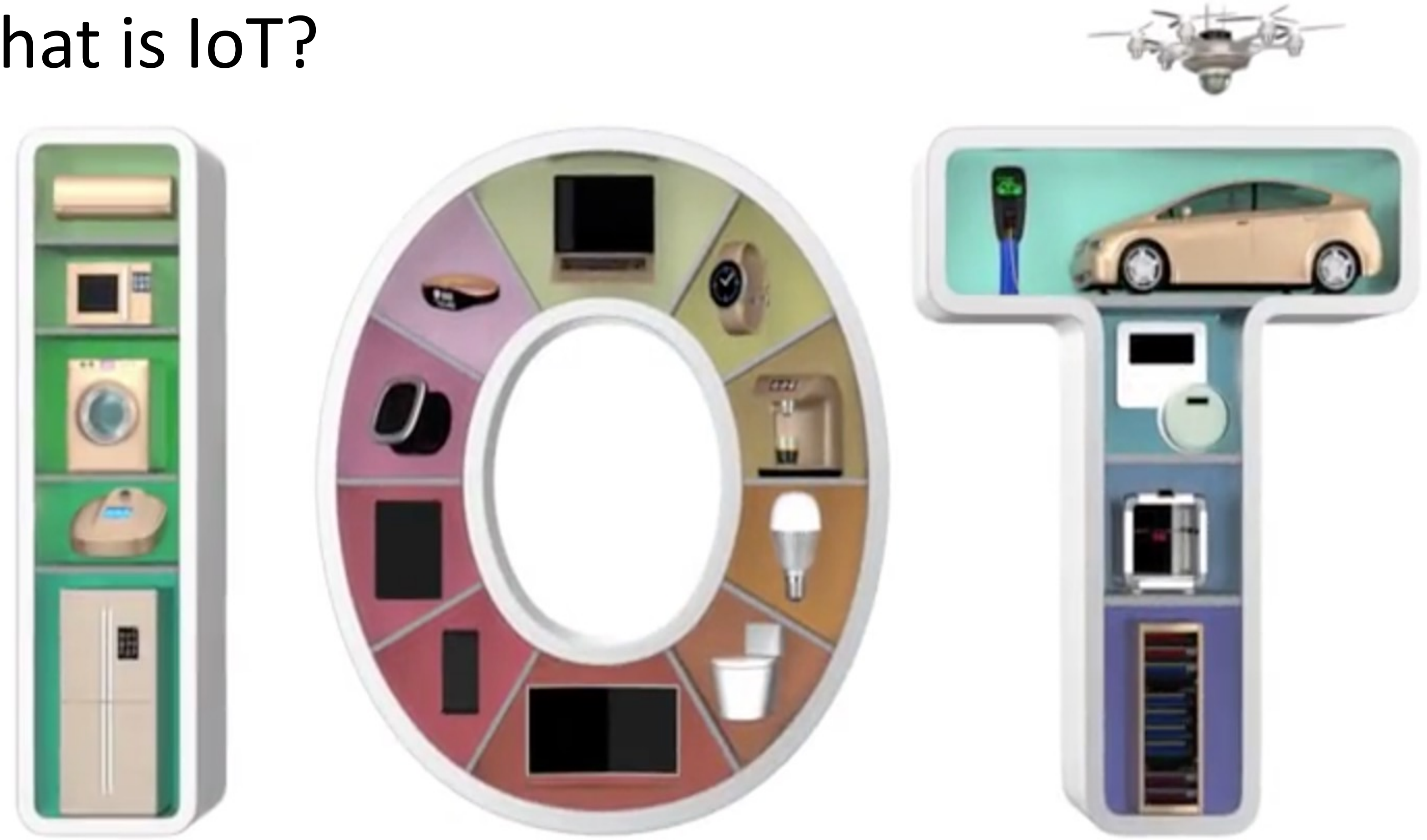
Objective

Take a tour of the main attack vectors and vulnerabilities within the IoT field to carry out a security audit

- Describe what is IoT
- Identify the threats
- How to focus a security audit on IoT
- Good practices

Reviewing Concepts

- What is IoT?



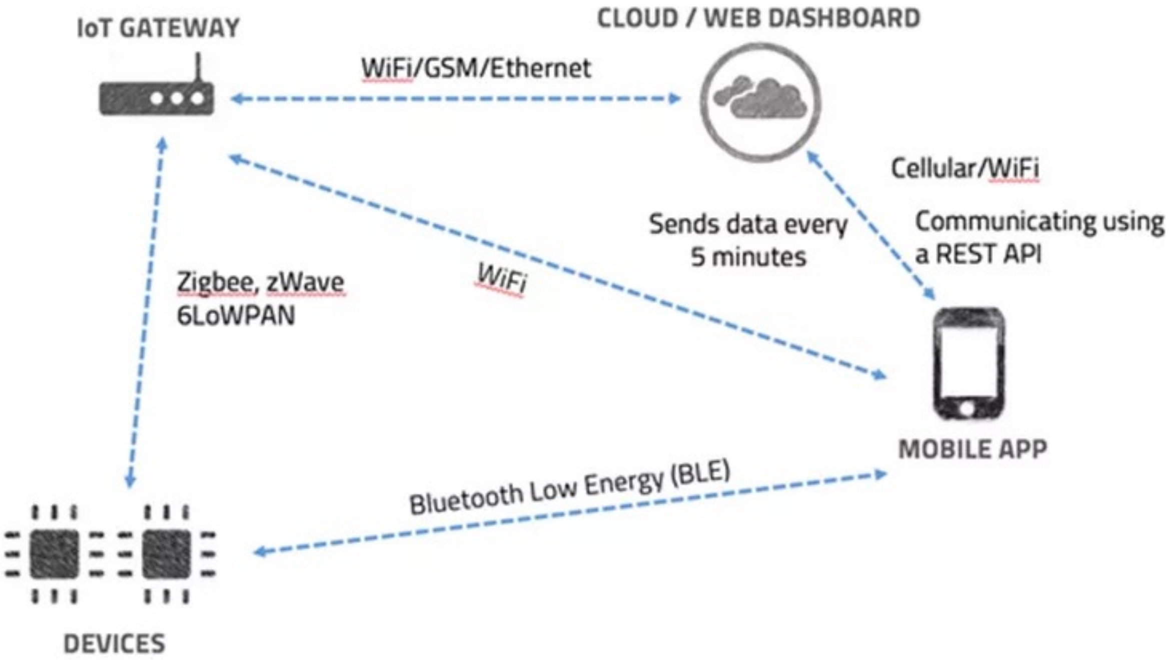
Reviewing Concepts

What is IoT?: Definitions

- International Telecommunication Union (ITU):
  - *Global infrastructure for the **information society**, enabling advanced services by **interconnecting** (physical and virtual) **things** based on existing and **evolving** interoperable information and communication technologies.*
- IoT European Research Cluster (IERC):
  - *A dynamic global network infrastructure with **self-configuring capabilities** based on standard and interoperable communication protocols where physical and virtual “things” have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network.*

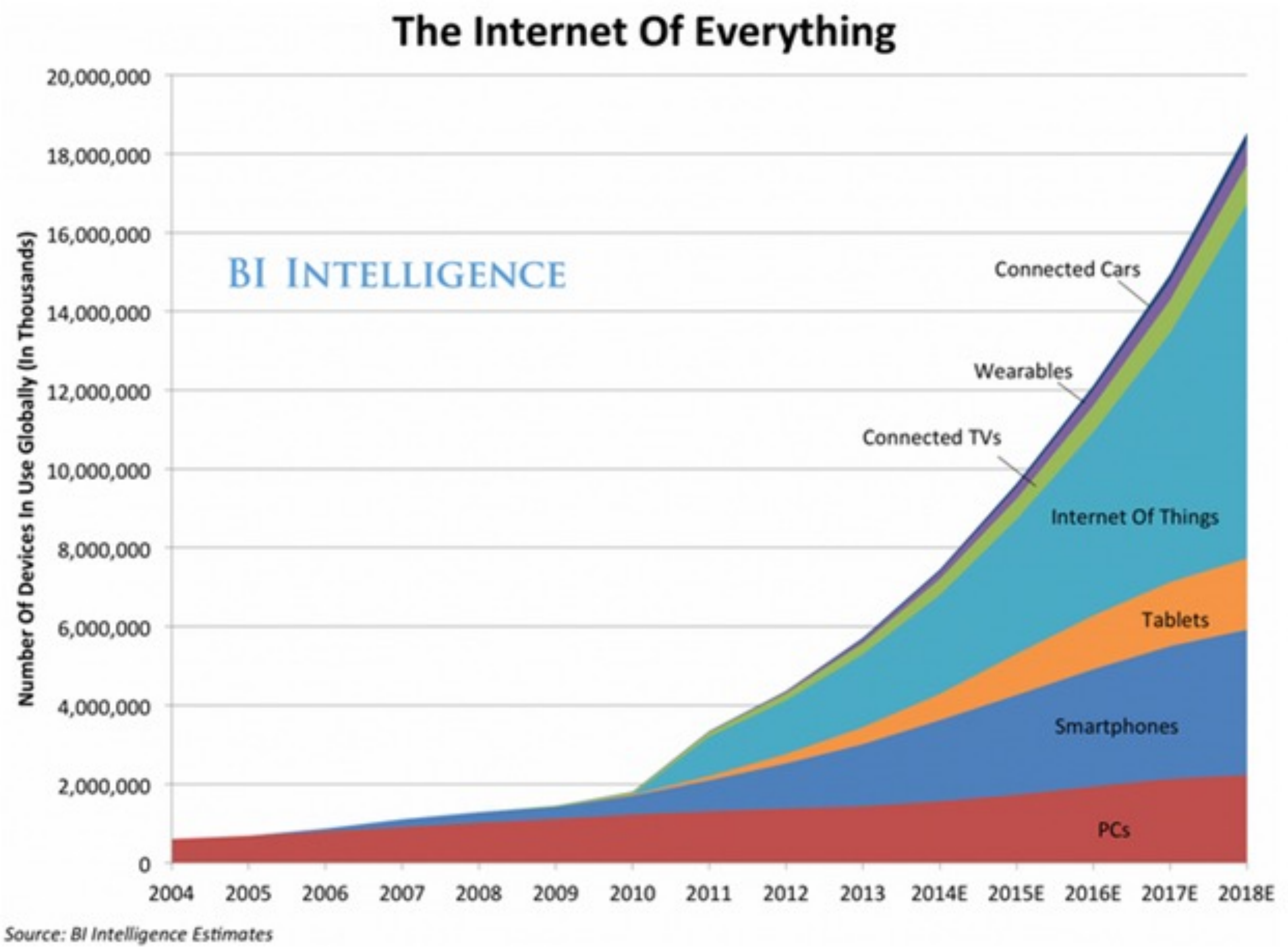
Reviewing Concepts

- What is so special about IoT?
  - It is not just a specific technology
  - Complete paradigm that brings together technologies, protocols, infrastructures and knowledge



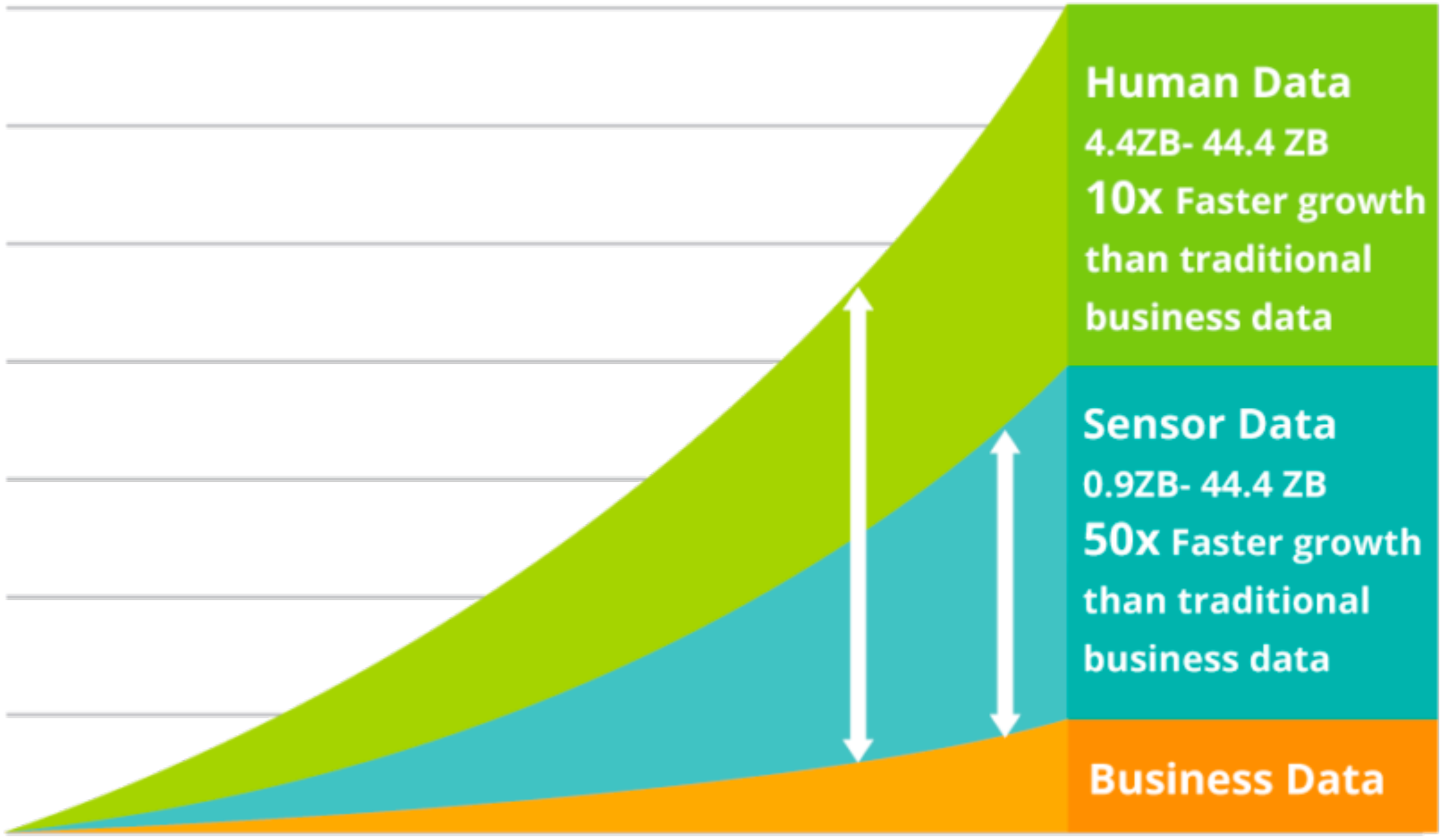
Reviewing Concepts

- IoT Architecture
  - Hardware:
    - ARM, Intel…
    - Arduino, RasPi…
  - Software:
    - Tizen
    - Android Things
    - Windows 10 IoT Core
  - Interconnexion:
    - Wired: SPI, I2C, Ethernet
    - Wirelesss: BLE, ZibBee, MQTT



Source: BI Intelligence Estimates

The growth of human and machine-generated data



Source: Inside big data

Table of Contents

1. General introduction and review
2. Introduction to IoT security
   1. IoT problem
   2. OWASP in IoT
   3. Good practices
3. Conclusions

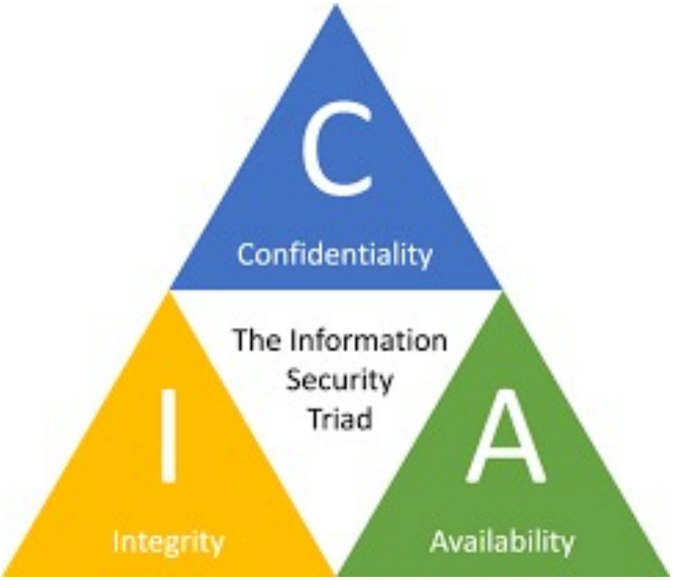
Security in IoT

Are we really aware of the threats that affect IoT devices?

- If we are not, we can fall into a **poor perception of risk**, and overlook some of the attack vectors that can endanger its security.

The IoT problem

- Attributes of *secure* systems (**CIA triad**):
  – **Confidentiality**: the information is not available for unauthorized individuals
  – **Integrity**: data is maintained accurate and complete
  – **Availability**: the data must be available for authorized users
- Recommendation:
  – Non-repudiation: intention to fulfil obligations.



The IoT problem

- Security is not a product, it is a process
- Security restrictions make product development slower and more expensive
- Many bugs are discovered by chance
- The same problems that already existed in traditional systems

The IoT problem

- Auditing the security of an IoT device **is not an easy** (or cheap) **task**.
- Security controls should be evaluated:
  - web/cloud
  - In mobile applications (Android and iOS)
  - In the usual communications (WiFi or Ethernet)
  - In unusual communication protocols (Zigbee, BLE, …)
  - From the device itself (firmware analysis, binary analysis, etc.)
  - Hardware (I/O, reprogramming, power, radiation, etc.)

The IoT problem

- Hardware:
  - Computational and power constraints
    - Computationally expensive anti-malware/cryptographic algorithms
  - Memory restrictions
    - The algorithms designed were not intended for IoT
  - Physical access
    - Remote deployment without physical security
  - Attacks of interference or physical manipulation: Tempest (Video)

The IoT problem

- Software:
  - Embedded software restrictions
    - RTOS: Limited, network protocol stack and no modules for security
  - Dynamic updates
    - Complicated to correct bug or security flaws

The IoT problem

- Network:
  - – Mobility: Variable physical status, may leave and join networks with different security settings
- Scalability
- Device heterogeneity
  - – Variety of devices, difficulty in unifying security
- Heterogeneity protocols and channels
  - – Local or global connections
- Multiprotocol networks
  - – Ex: within the same network, non-IP based devices
- Topologies

The IoT problem

- Cloud
  - Insecure interfaces and APIs
    - Review data authentication and encryption
  - insider threats
    - Credential theft: social engineering, shoulder sniffing or Advanced Persistent Threads
    - Employees of the organization itself
    - Natural or fortuitous disasters
  - Derivatives of shared technologies
    - In IaaS (Infrastructure as a Service) the hardware has not been designed for shared architectures, one hypervisor can see content from another
  - Loss or leak of information
    - Modification or removal attacks
    - Example: a MitM
  - Risks due to ignorance
    - 0-days attack

Module 1: Introduction to IoT Security

Table of Contents

1. General introduction and review
2. Introduction to IoT security
    1. IoT problem
    2. OWASP in IoT
    3. Good practices
3. Conclusions

Sec

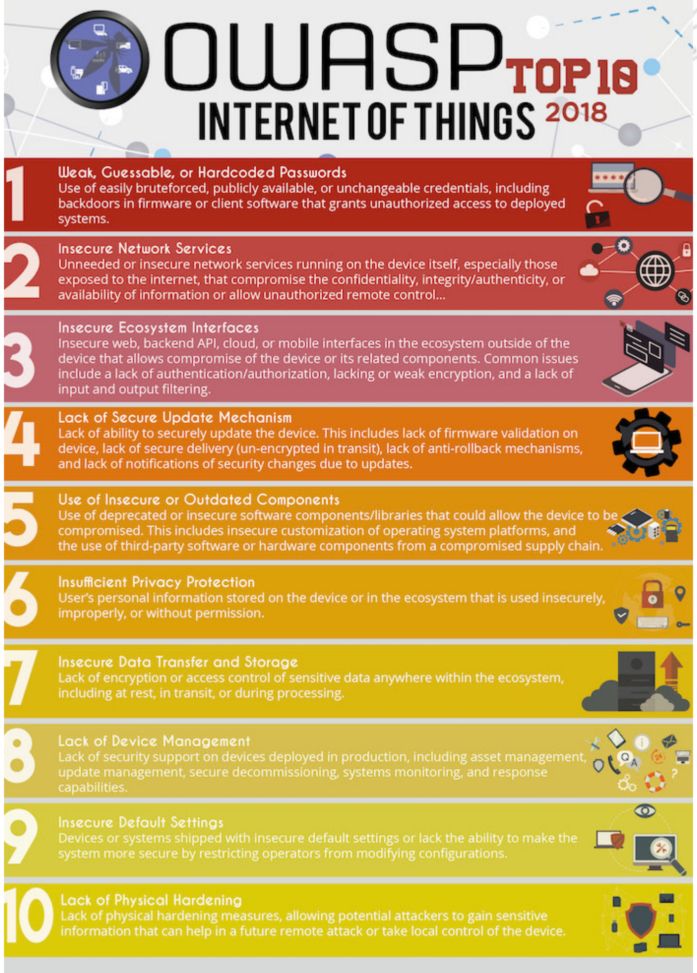
OWASP™

- What is OWASP?
  - *Open Web Application Security Project*

- ***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**, and to enable users in any context to make better **security decisions** when building, deploying, or assessing IoT technologies.*
  - *The project looks to define a **structure for various IoT sub-projects** separated into the following categories - **Seek & Understand, Validate & Test, and Governance.***

OWASP IoT Top 10

- IoT Top 10 2018
  - **Top ten things to avoid** when building, deploying or managing IoT systems.
- IoT Top 10 Mapping Project
  - Provides mappings of the OWASP IoT Top 10 2018 to industry publications and sister projects (2014 project).
- IoTGoat
  - Deliberately insecure firmware based on OpenWrt. The project’s goal is to teach users about the most common vulnerabilities typically found in IoT devices



OWASP TOP 10
INTERNET OF THINGS 2018

1 **Weak, Guessable, or Hardcoded Passwords**
Use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.

2 **Insecure Network Services**
Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control...

3 **Insecure Ecosystem Interfaces**
Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.

4 **Lack of Secure Update Mechanism**
Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.

5 **Use of Insecure or Outdated Components**
Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.

6 **Insufficient Privacy Protection**
User’s personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.

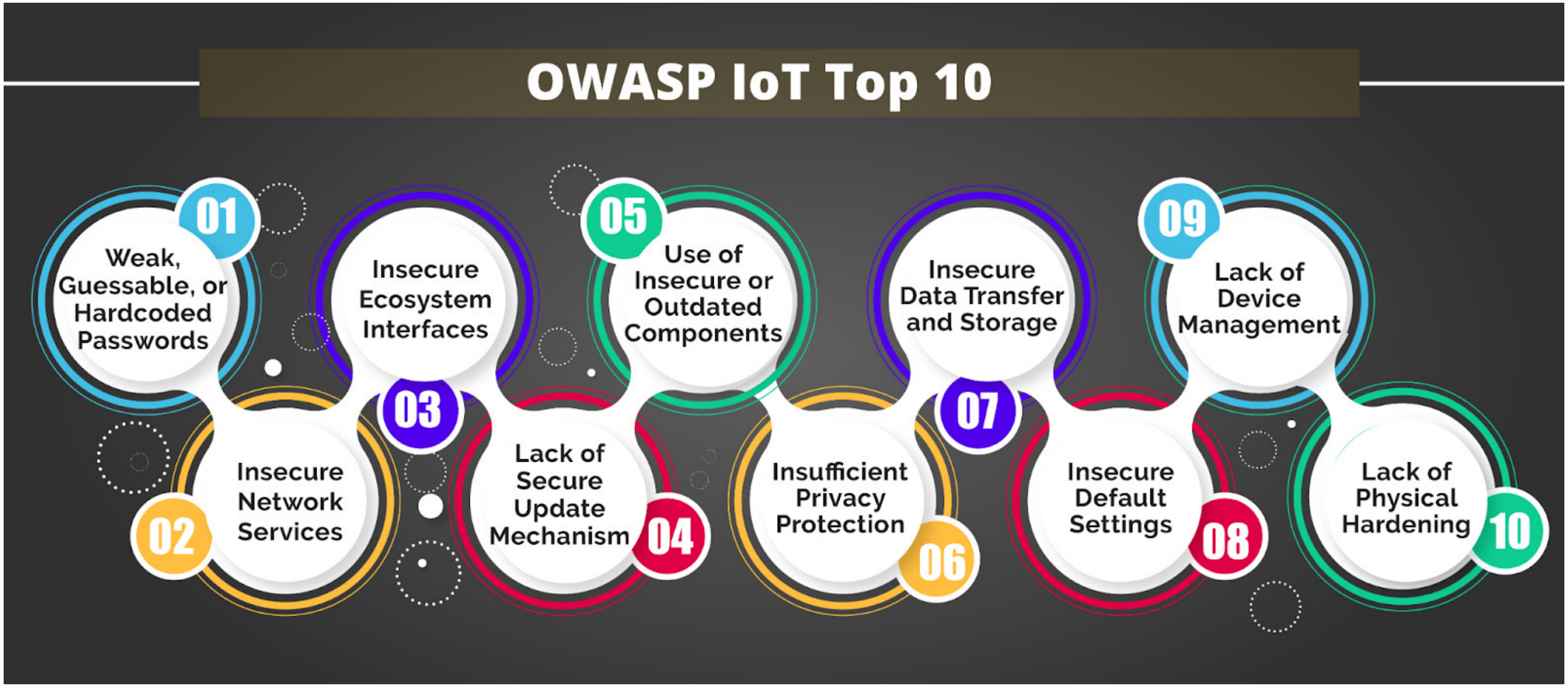
7 **Insecure Data Transfer and Storage**
Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.

8 **Lack of Device Management**
Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.

9 **Insecure Default Settings**
Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.

10 **Lack of Physical Hardening**
Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

OWASP IoT Top 10

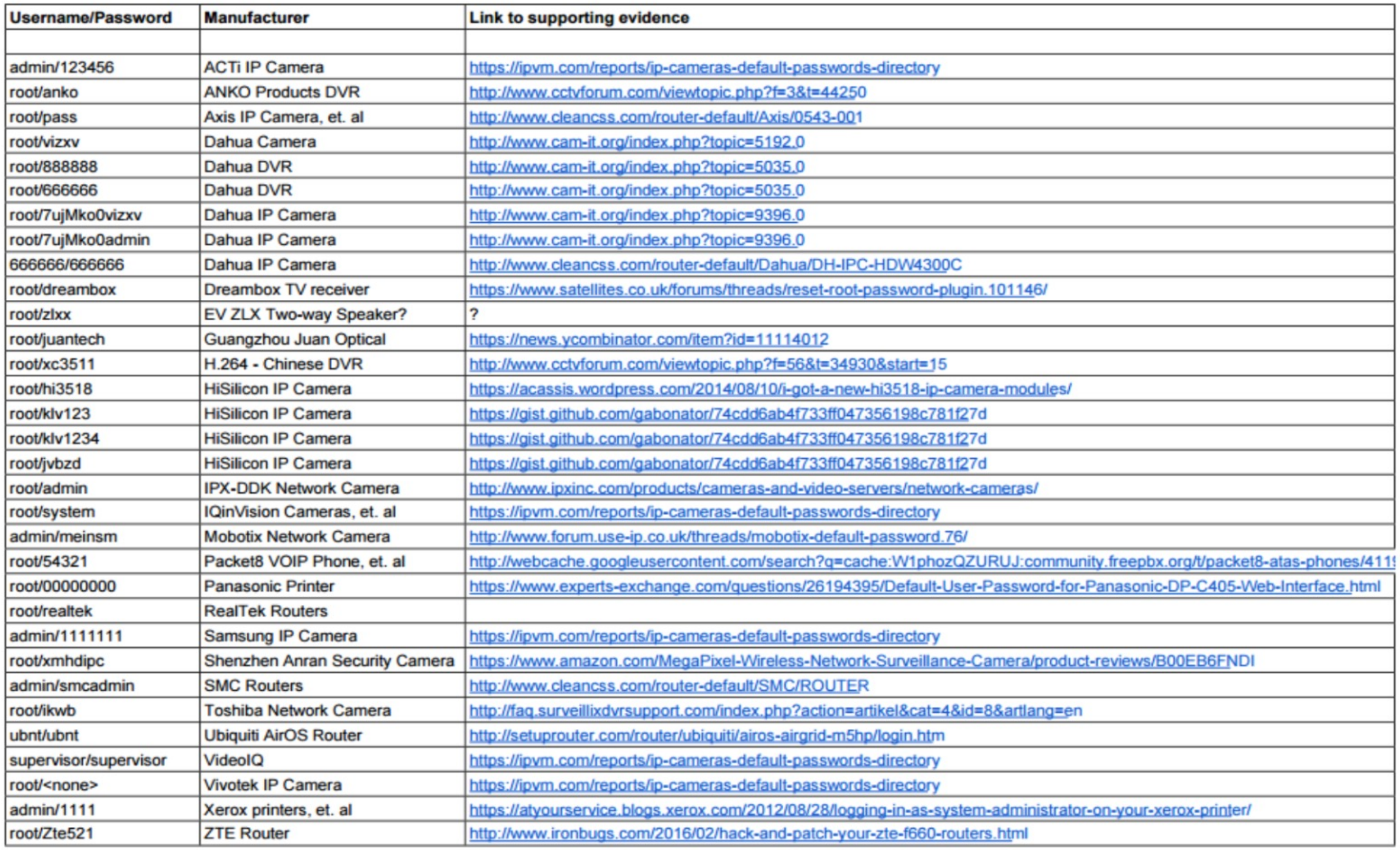

OWASP IoT Top 10
01
Weak, Guessable, or Hardcoded Passwords
02
Insecure Network Services
03
Insecure Ecosystem Interfaces
04
Lack of Secure Update Mechanism
05
Use of Insecure or Outdated Components
06
Insufficient Privacy Protection
07
Insecure Data Transfer and Storage
08
Insecure Default Settings
09
Lack of Device Management
10
Lack of Physical Hardening

https://www.appsealing.com/owasp-iot-top-10/

TOP 1:
Weak, Guessable, or Hardcoded Pass.

- *“Use of easily bruteforced, publicly available (defpass) or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.”*
- To combat the first vulnerability, manufacturers must take the following steps:
  - Every device must have a unique set of credentials
  - Disable weak passwords
  - Removing backdoors created during debugging

OWASP IoT



Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

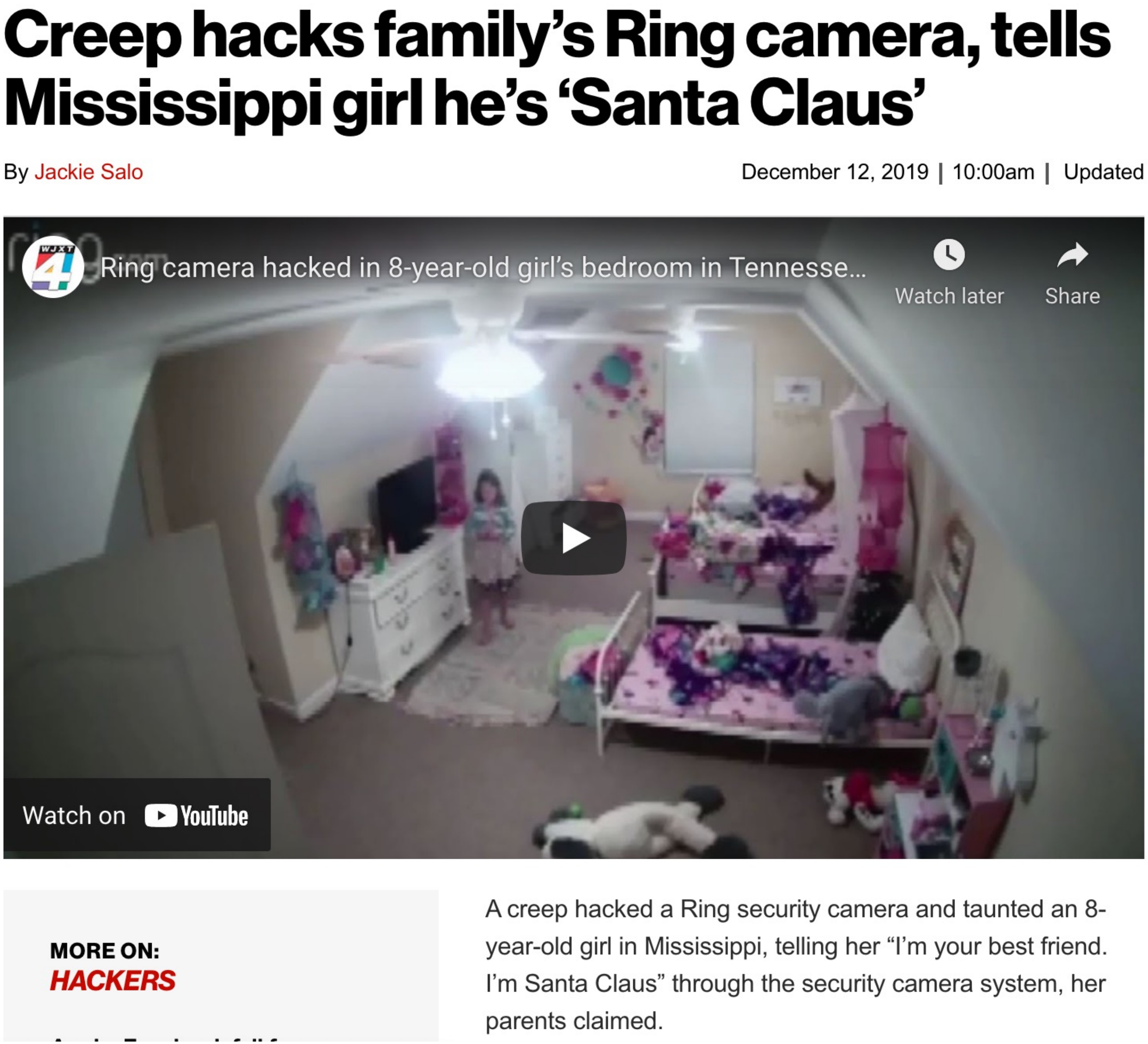
https://github.com/jgamblin/Mirai-Source-Code

TOP 2:
Insecure Network Services

- *"Unneeded or insecure network services running on the device itself (ftp, mqtt), especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control"*
- To prevent threats arising from insecure network services, manufacturers should:
  - Use secure protocols like HTTPS, sFTP, and SSH
  - Disable non-essential ports and services that provide remote access
  - Keep IoT devices on a separate network
  - Installation of regular updates

TOP 3:
Insecure Ecosystem Interfaces

- *“Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include: a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.”*
- To address insecure interfaces, the following tips are useful:
  - Adhering to the principle of least privilege
  - Block public access to private resources (S3 bucket AWS)
  - Strong authentication of IoT endpoints



Creep hacks family's Ring camera, tells Mississippi girl he's 'Santa Claus'

By Jackie Salo

December 12, 2019 | 10:00am | Updated

Ring camera hacked in 8-year-old girl's bedroom in Tennesse...

MORE ON:

HACKERS

A creep hacked a Ring security camera and taunted an 8-year-old girl in Mississippi, telling her "I'm your best friend. I'm Santa Claus" through the security camera system, her parents claimed.

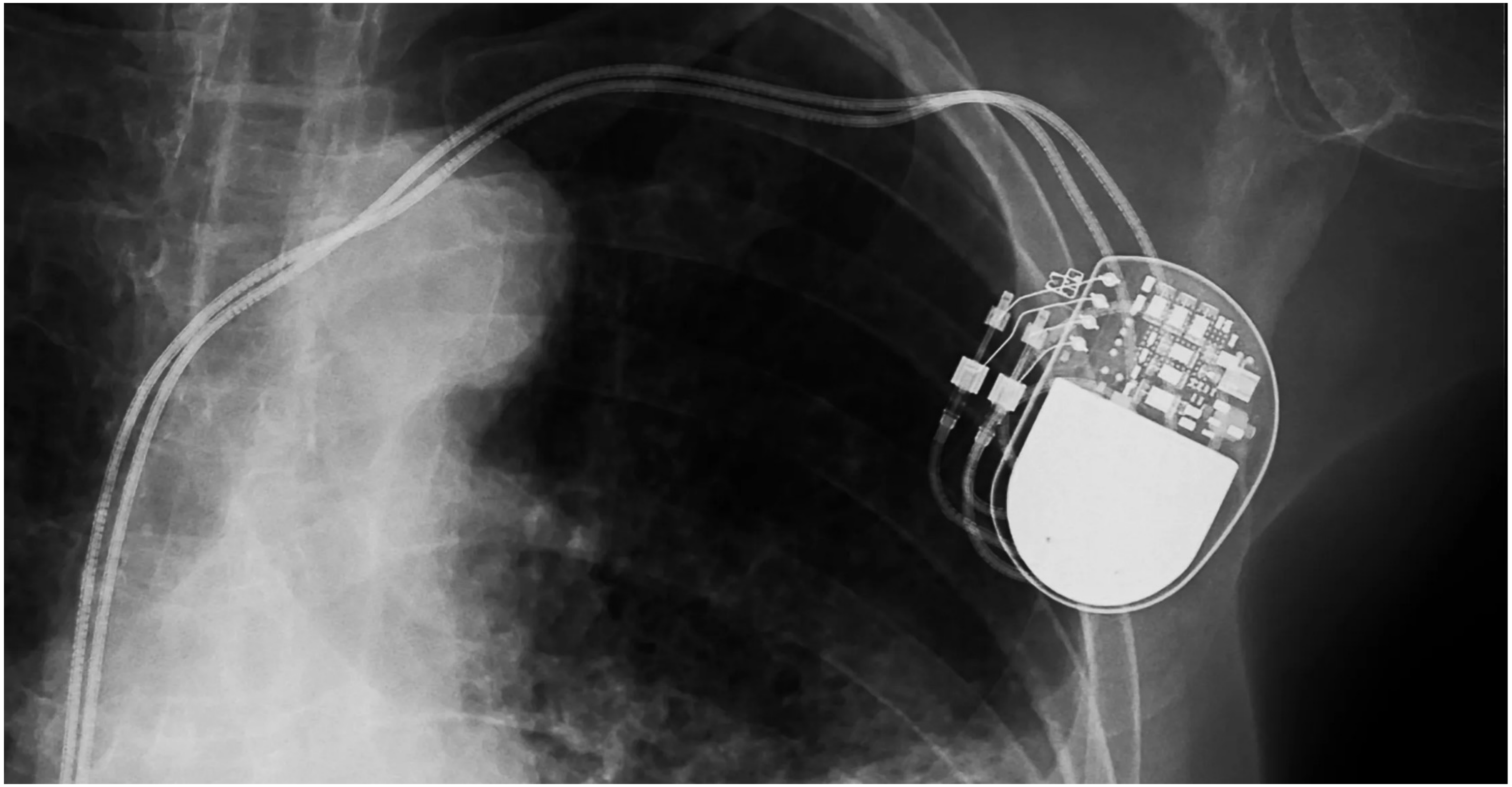
Link

TOP 4:

Lack of Secure Update Mechanism

- *“Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.”*
- For secure delivery of updates to IoT devices, manufacturers must:
  - – Only implement updates that are digitally signed
  - – Implement anti-rollback mechanisms
  - – Secure and verify access to updates

Pacemaker Hack Puts Malware on the Device



Link

TOP 5:

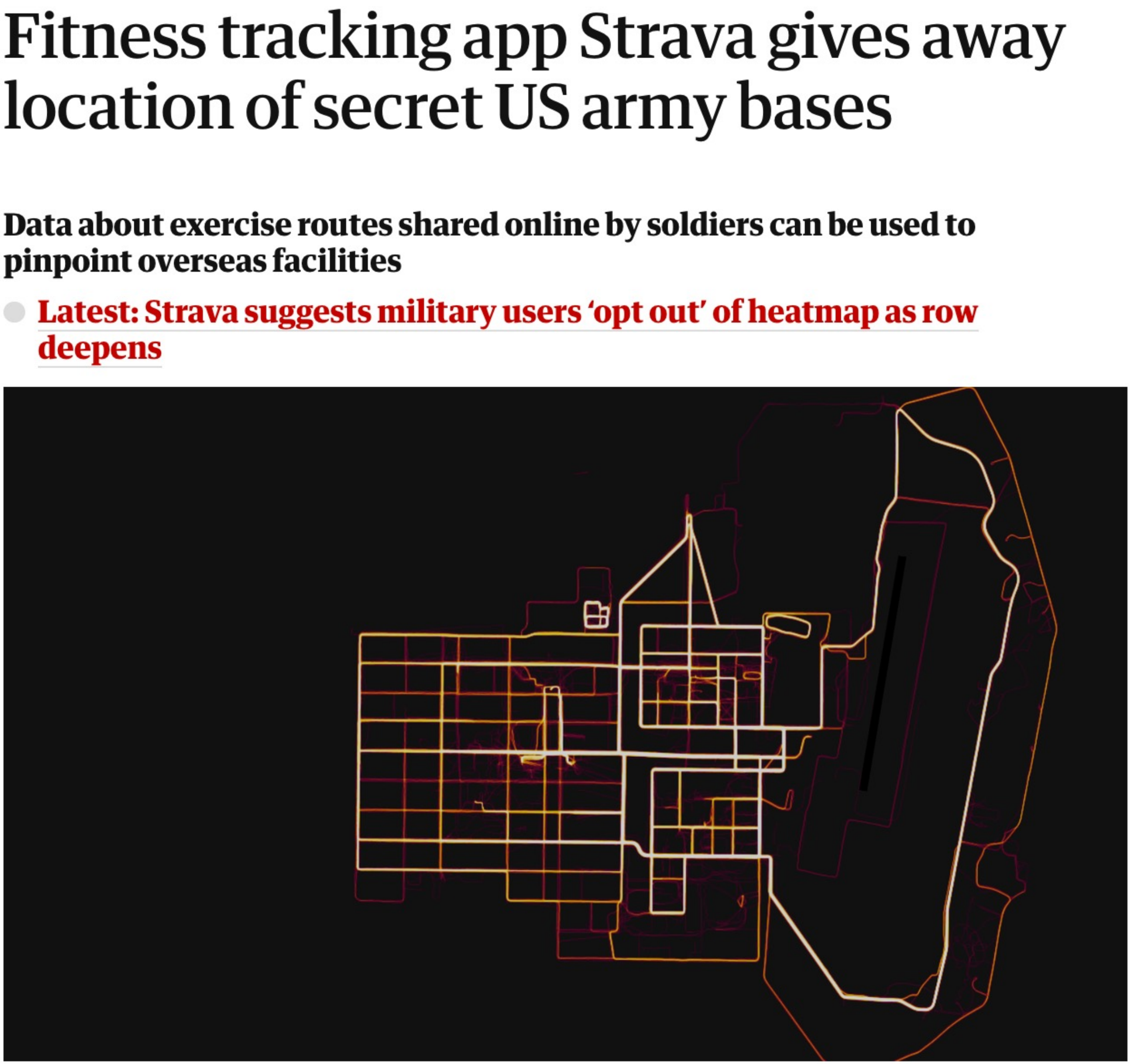
Use of Insecure or Outdated Components

- *“Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.”*
- IoT manufacturers are advised to :
  - Refrain from legacy technologies
  - Ensure continuous tracking of hardware and software components
  - Immediately replace any of the components that turn obsolete

TOP 6:

Insufficient Privacy Protection

- *“User’s personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.”*
- Consumer privacy is one of the key concerns that need to be addressed with the following measures:
  - Limit the storage of personal data on devices
  - Frame a data protection policy for your organization
  - Prepare an incident response plan to combat any breach of security in the future



Fitness tracking app Strava gives away location of secret US army bases

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

- **Latest: Strava suggests military users 'opt out' of heatmap as row deepens**

TOP 7:
Insecure Data Transfer and Storage

- *“Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.”*
- To ensure maximum protection of data, IoT manufacturers need to implement the following for complete security:
  - Ensure encryption at all levels
  - Strictly utilize secure channels like HTTPS, sFTP and SSH
  - Opt for one-time-use keys that aren’t stored in the device

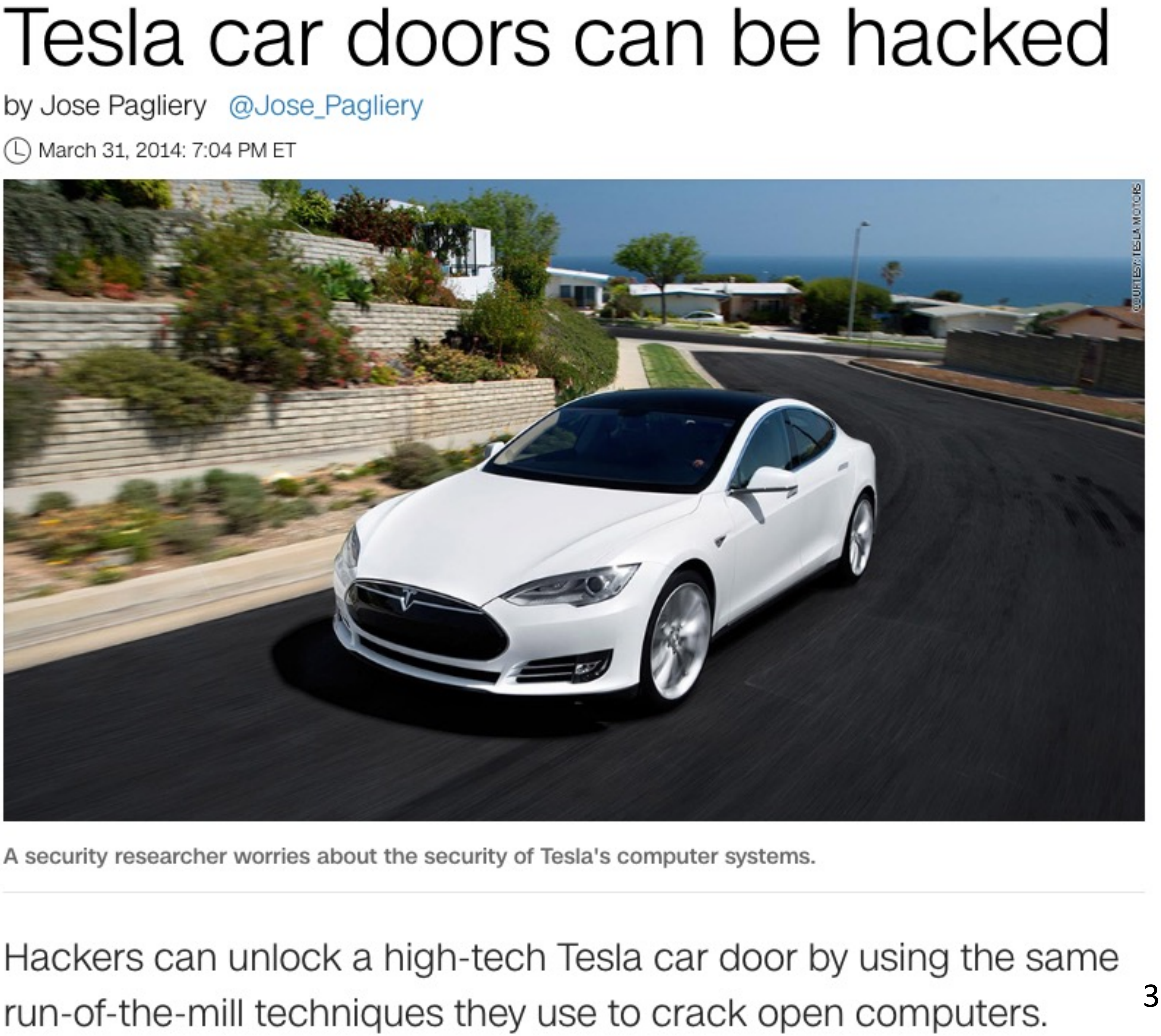
Sony admitted a great PSN hack

- 77m users' personal details were put at risk:
  - *“It was the largest security breach of its kind to ever hit console gamers, and an event with huge repercussions for PlayStation - both in the short term for its users, left for weeks without access to online services, and longer term as Sony sought to win back customer trust.”*

Link

TOP 8:
Lack of Device Management

- *“Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.”*
- There is an increased risk of attacks if there are several devices with weak security functioning within the same system. The following steps must be implemented for flawless device management.
  - Secure decommissioning, endpoint quarantine and blacklisting
  - Integrate devices with asset management, bug tracking and patch management systems
  - Build an interface that is flexible and seamlessly integrates with other systems



Tesla car doors can be hacked

by Jose Pagliery @Jose_Pagliery

March 31, 2014: 7:04 PM ET

COURTESY: TESLA MOTORS

A security researcher worries about the security of Tesla's computer systems.

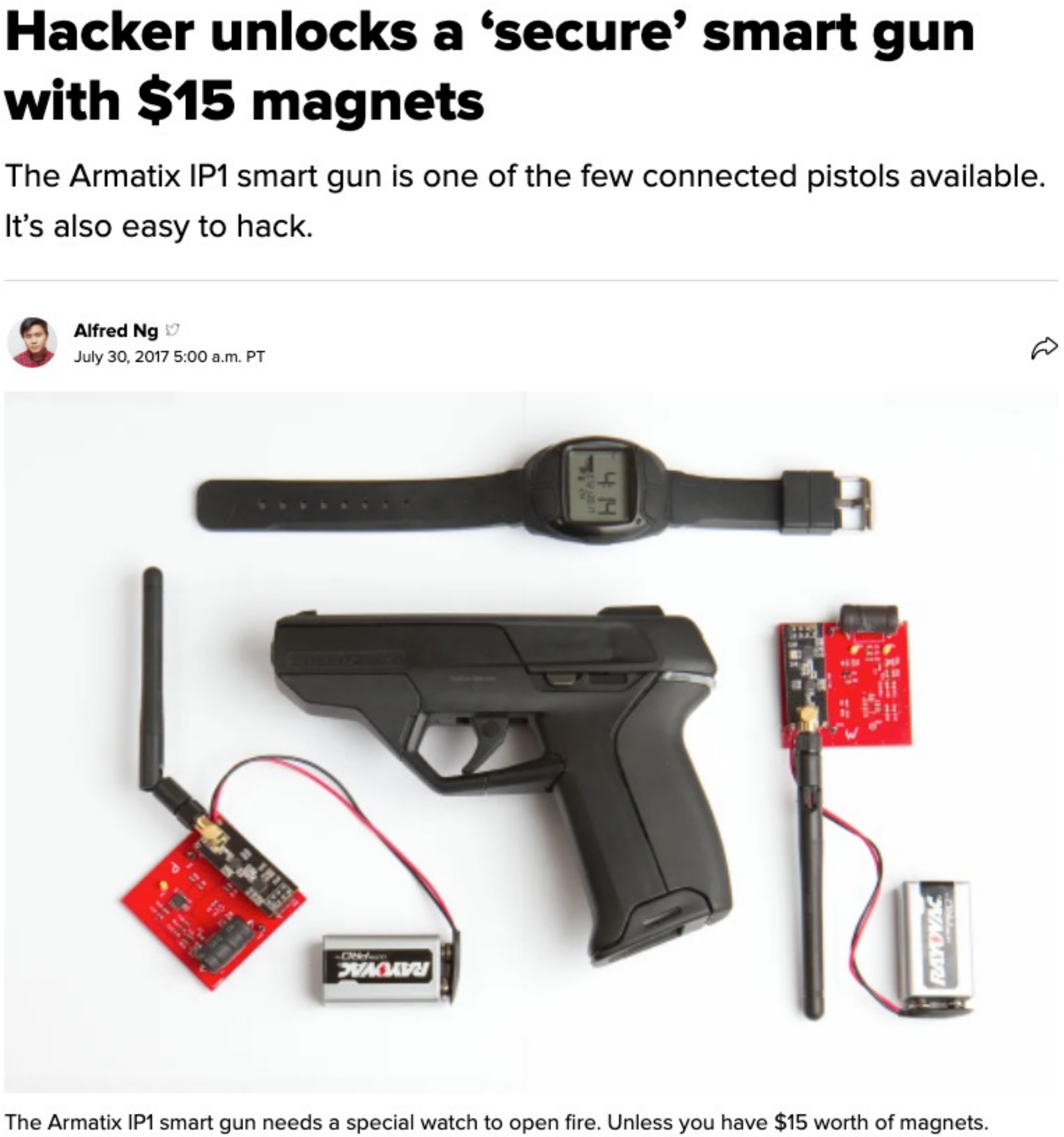
Hackers can unlock a high-tech Tesla car door by using the same run-of-the-mill techniques they use to crack open computers.

TOP 9:
Insecure Default Settings

- *"Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations."*
- The following 3 tips can enable IoT manufacturers to thwart the risks associated with weak default settings:
  - Use only secure default settings
  - Grant users permission to change default passwords
  - Prompt users to change their default passwords compulsorily

TOP 10:
Lack of Physical Hardening

- *"Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device."*
- To counter physical threats to IoT devices, manufacturers should:
  - Understand how a user may modify the device
  - Proactively anticipate what damages any user may inflict on the device
  - Devise solutions and build an IoT device that can withstand all the possible attacks



Hacker unlocks a 'secure' smart gun with $15 magnets

The Armatix IP1 smart gun is one of the few connected pistols available. It's also easy to hack.

Alfred Ng
July 30, 2017 5:00 a.m. PT

The Armatix IP1 smart gun needs a special watch to open fire. Unless you have $15 worth of magnets.

Table of Contents

1. General introduction and review
2. Introduction to IoT security
   1. IoT problem
   2. OWASP in IoT
   3. Good practices
3. Conclusions

Protection of an IoT infrastructure

- From 4 perspectives:
  - IoT Hardware Manufacturer/Integrator
  - IoT Solution Developer
  - IoT solution implementer
  - IoT Solution Developer

Protection of an IoT infrastructure

- IoT Hardware Manufacturer/Integrator
  - Limit the hardware to a few minimum requirements:
    - If I don't need USB port, don't put it
  - Create tamper-proof hardware:
    - HW capable of detecting physical tampering
  - Rely on secure hardware:
    - Secure/encrypted storage
    - Secure Boot with Trusted Platform Module
  - Apply updates safely
    - Secure paths
    - Crypto Assurance
    - evil grade

Protection of an IoT infrastructure

- IoT Solution Developer
  - Follow a secure software development methodology:
    - From conception to implementation
  - Choose open source software carefully
    - Review introduced components
    - activity level
  - Integrate carefully:
    - Monitor the functionalities offered by the APIs that we do not use

Protection of an IoT infrastructure

- IoT solution implementer
  - Deploy hardware safely:
    - Unsecured deployment locations
  - Keep authentication keys secure:
    - Device ID and authentication keys physically secured for communication with the cloud

Protection of an IoT infrastructure

- IoT Solution Operator
  - Keep the system updated:
    - SSOO and updated drivers
  - Protect against malicious activity:
    - AVS (address verification service)
    - IDS (intrusion detection system)
  - audit often
    - Audit as a response measure to incidents
    - Logs, logs, etc.
  - Protect credentials in the cloud
    - The input vector to the IoT infrastructure can be from the cloud
    - Strong passwords, periodic change and avoid access in public places

Table of Contents

1. General introduction and review
2. Introduction to IoT security
    1. IoT problem
    2. OWASP in IoT
    3. Good practices
3. Conclusions

Conclusions

- The deficiencies are not new, they are inherited from traditional computer systems
- Security in IoT addresses
  - Devices (HW & SW)
  - Network / Infrastructure
  - Mobile
  - Cloud
- OWASP as a reference guide against audits
- Good practices and … common sense!