Internet of Things

Dr. Panagiotis Rizomiliotis

Info-Sec-Lab

Definition IoT

- It is a new buzzword!

"IoT is 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."

IoT

- ENISA defines the Internet of Things (IoT) as a cyber-physical ecosystem of interconnected sensors and actuators, which enable decision making. Information lies at the heart of IoT, feeding into a continuous cycle of sensing, decision making, and actions.

- Cyber-physical systems
  - Internet & comm.
  - Effect on reality

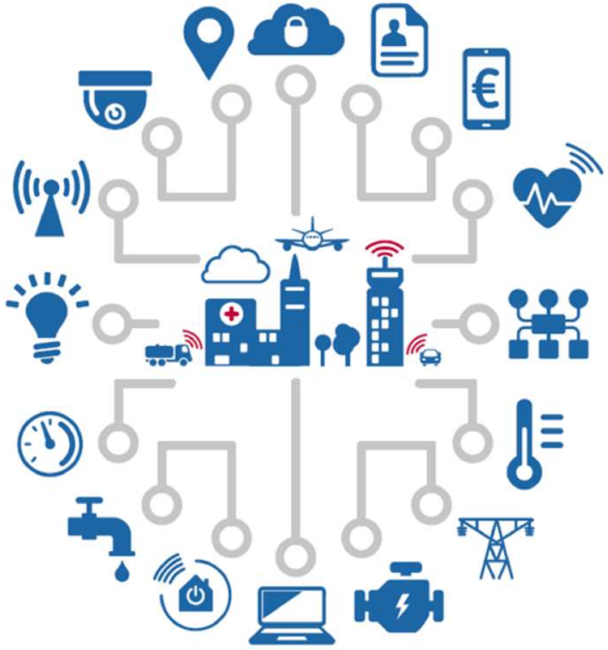
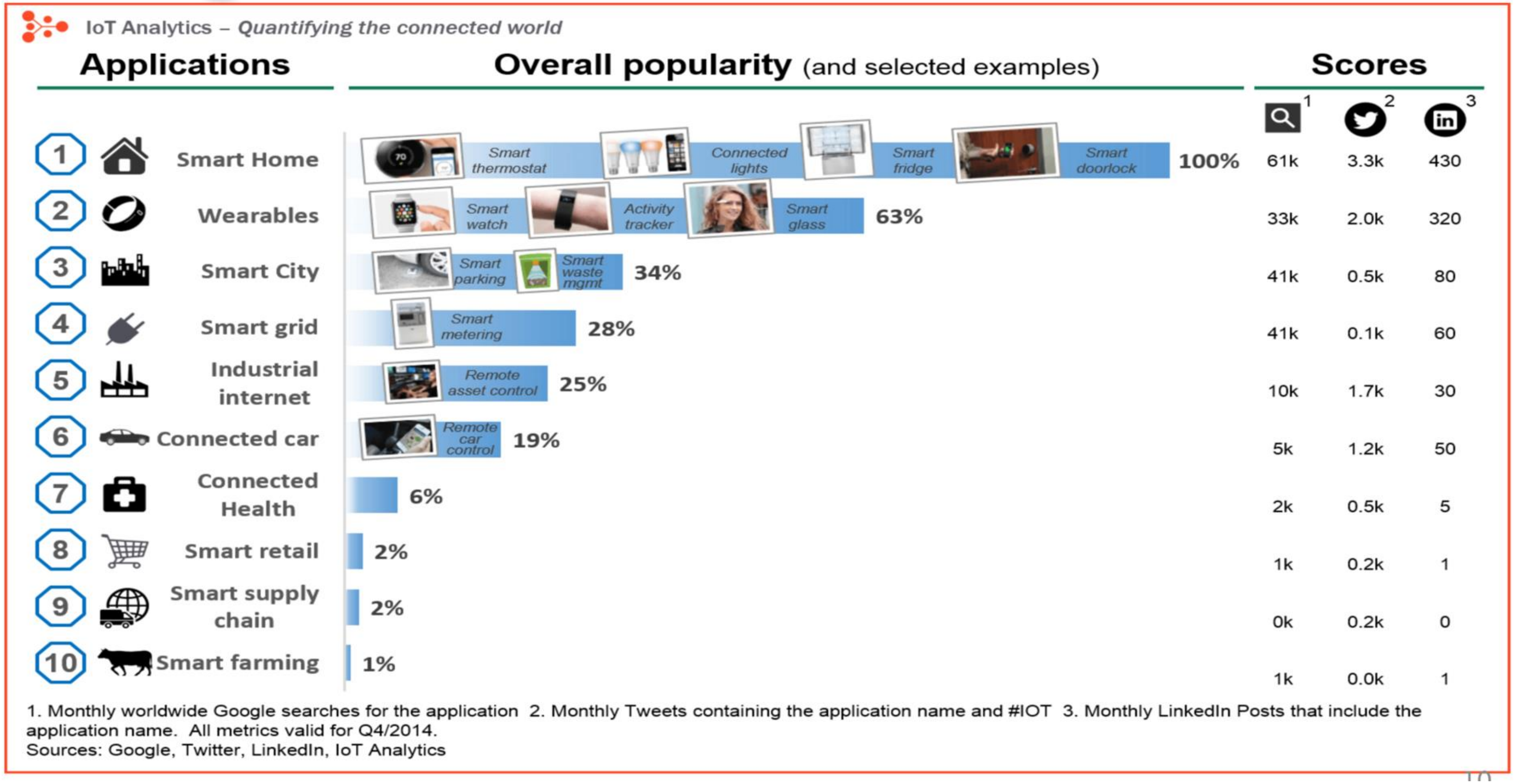


Figure 2: IoT pervasive ecosystem

Top Trends

- Definition
- Market Size (300$ billion)
- Standards (Network)
- Security Considerations
- People & Process Considerations (Smart things)
- Consumer Privacy Considerations
- Data Management Considerations
- Storage Management Considerations
- Server Investment Considerations
- Bandwidth Considerations

Applications

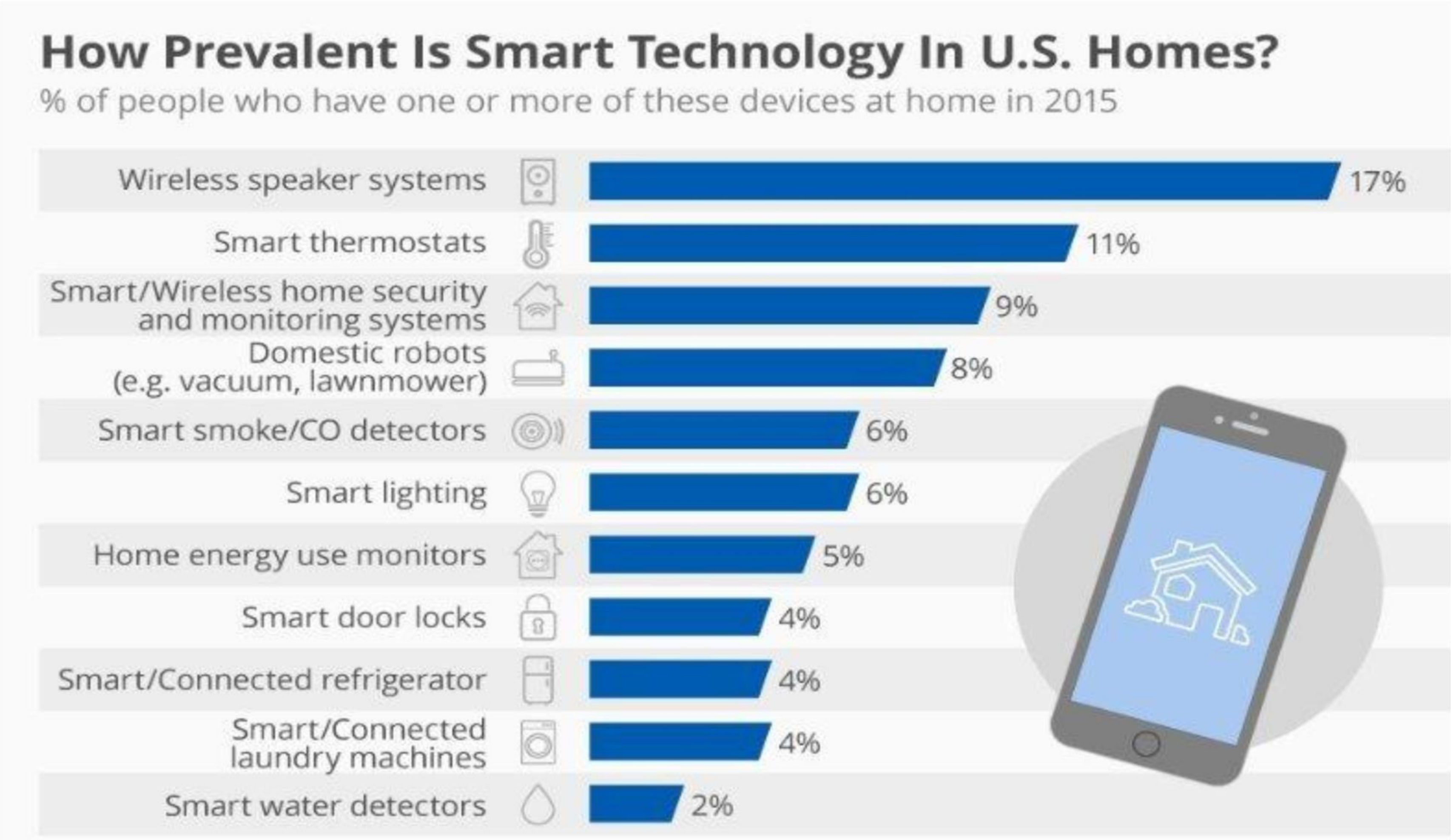


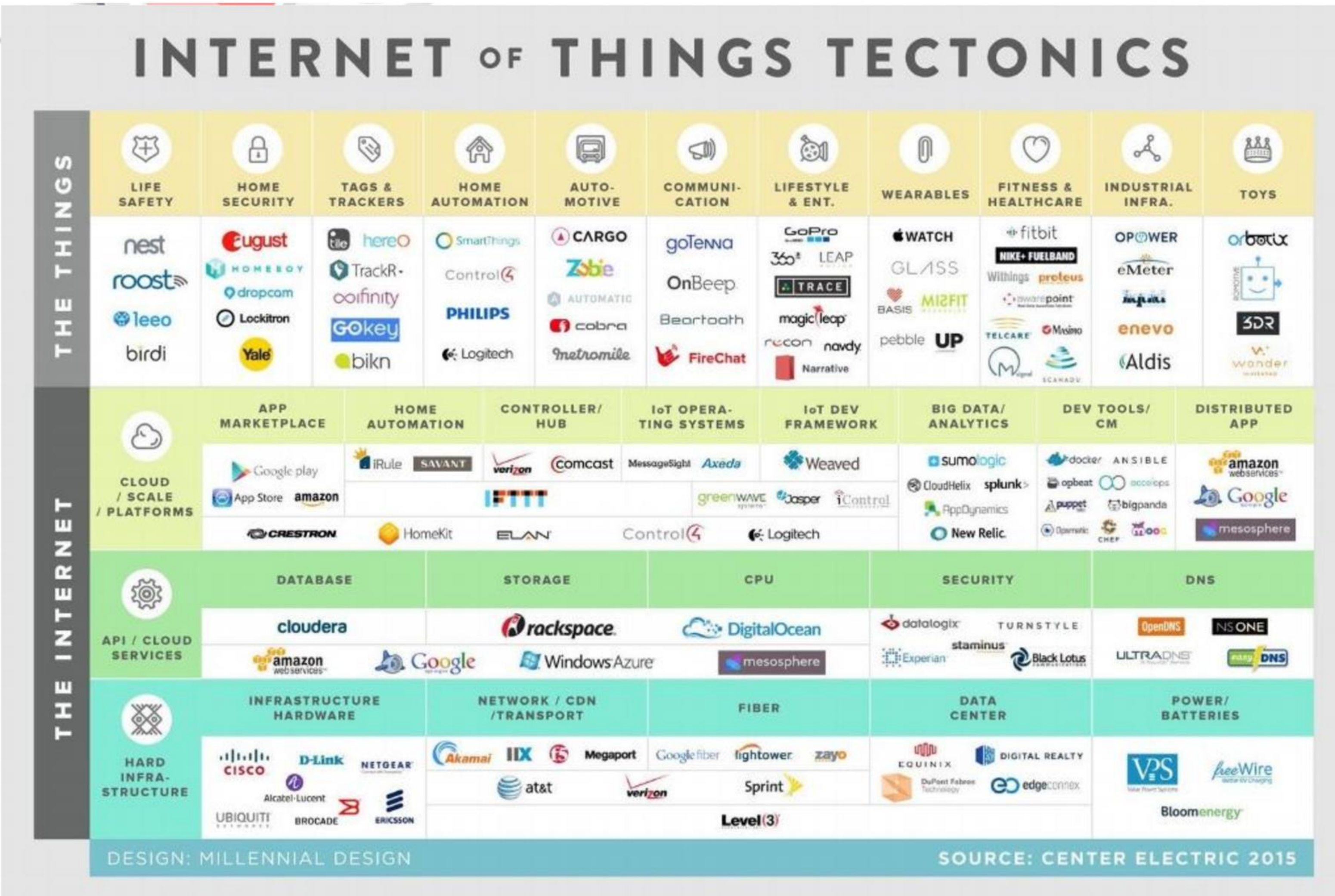
IoT Analytics – *Quantifying the connected world*

	Applications	Overall popularity (and selected examples)		Scores		
				🔍[1]	[2]	in[3]
1	Smart Home	*Smart thermostat*, *Connected lights*, *Smart fridge*, *Smart doorlock*	100%	61k	3.3k	430
2	Wearables	*Smart watch*, *Activity tracker*, *Smart glass*	63%	33k	2.0k	320
3	Smart City	*Smart parking*, *Smart waste mgmt*	34%	41k	0.5k	80
4	Smart grid	*Smart metering*	28%	41k	0.1k	60
5	Industrial internet	*Remote asset control*	25%	10k	1.7k	30
6	Connected car	*Remote car control*	19%	5k	1.2k	50
7	Connected Health		6%	2k	0.5k	5
8	Smart retail		2%	1k	0.2k	1
9	Smart supply chain		2%	0k	0.2k	0
10	Smart farming		1%	1k	0.0k	1

1. Monthly worldwide Google searches for the application 2. Monthly Tweets containing the application name and #IOT 3. Monthly LinkedIn Posts that include the application name. All metrics valid for Q4/2014.
Sources: Google, Twitter, LinkedIn, IoT Analytics

Smart Homes


How Prevalent Is Smart Technology In U.S. Homes?
% of people who have one or more of these devices at home in 2015
Wireless speaker systems 17%
Smart thermostats 11%
Smart/Wireless home security and monitoring systems 9%
Domestic robots (e.g. vacuum, lawnmower) 8%
Smart smoke/CO detectors 6%
Smart lighting 6%
Home energy use monitors 5%
Smart door locks 4%
Smart/Connected refrigerator 4%
Smart/Connected laundry machines 4%
Smart water detectors 2%



INTERNET OF THINGS TECTONICS

THE THINGS

- LIFE SAFETY: nest, roost, leeo, birdi
- HOME SECURITY: august, HOMEBOY, dropcam, Lockitron, Yale
- TAGS & TRACKERS: tile, hereO, TrackR, oofinity, GOkey, bikn
- HOME AUTOMATION: SmartThings, Control4, PHILIPS, Logitech
- AUTO-MOTIVE: CARGO, Zubie, AUTOMATIC, cobra, metromile
- COMMUNI-CATION: goTenna, OnBeep, Beartooth, FireChat
- LIFESTYLE & ENT.: GoPro, 360fly, LEAP, TRACE, magic leap, recon, navdy, Narrative
- WEARABLES: WATCH, GLASS, BASIS, MISFIT, pebble, UP
- FITNESS & HEALTHCARE: fitbit, NIKE+ FUELBAND, Withings, proteus, swarmpoint, TELCARE, Masimo, SCANADU
- INDUSTRIAL INFRA.: OPOWER, eMeter, enevo, Aldis
- TOYS: orbotix, 3DR, wonder

THE INTERNET

CLOUD / SCALE / PLATFORMS

- APP MARKETPLACE: Google play, App Store, amazon
- HOME AUTOMATION: iRule, SAVANT
- CONTROLLER/ HUB: verizon, comcast
- IoT OPERA-TING SYSTEMS: MessageSight, Axeda
- IoT DEV FRAMEWORK: Weaved, greenwave, Jasper, iControl
- IFTTT
- CRESTRON, HomeKit, ELAN, Control4, Logitech
- BIG DATA/ ANALYTICS: sumologic, CloudHelix, splunk, AppDynamics, New Relic
- DEV TOOLS/ CM: docker, ANSIBLE, opbeat, accelops, puppet, bigpanda, Opsmatic, CHEF
- DISTRIBUTED APP: amazon web services, Google, mesosphere

API / CLOUD SERVICES

- DATABASE: cloudera, amazon web services, Google
- STORAGE: rackspace, Windows Azure
- CPU: DigitalOcean, mesosphere
- SECURITY: datalogix, TURNSTYLE, staminus, Experian, Black Lotus
- DNS: OpenDNS, NS ONE, ULTRADNS, easyDNS

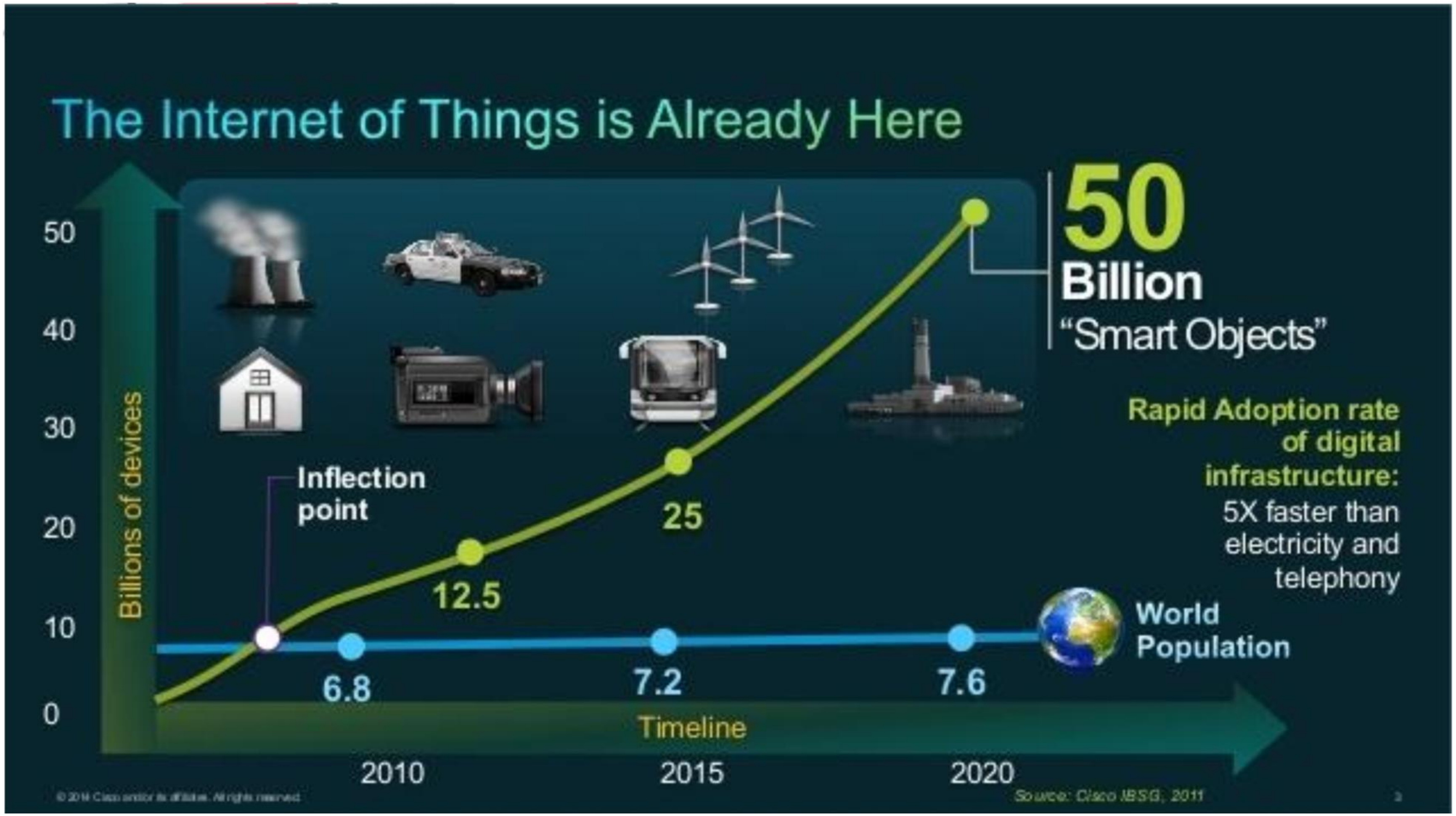
HARD INFRA-STRUCTURE

- INFRASTRUCTURE HARDWARE: cisco, D-Link, NETGEAR, Alcatel-Lucent, UBIQUITI, BROCADE, ERICSSON
- NETWORK / CDN /TRANSPORT: Akamai, IIX, F5, Megaport, at&t, verizon
- FIBER: Google fiber, lightower, zayo, Sprint, Level(3)
- DATA CENTER: EQUINIX, DIGITAL REALTY, DuPont Fabros Technology, edgeconnex
- POWER/ BATTERIES: VPS, freeWire, Bloomenergy

DESIGN: MILLENNIAL DESIGN

SOURCE: CENTER ELECTRIC 2015

Future of IoT

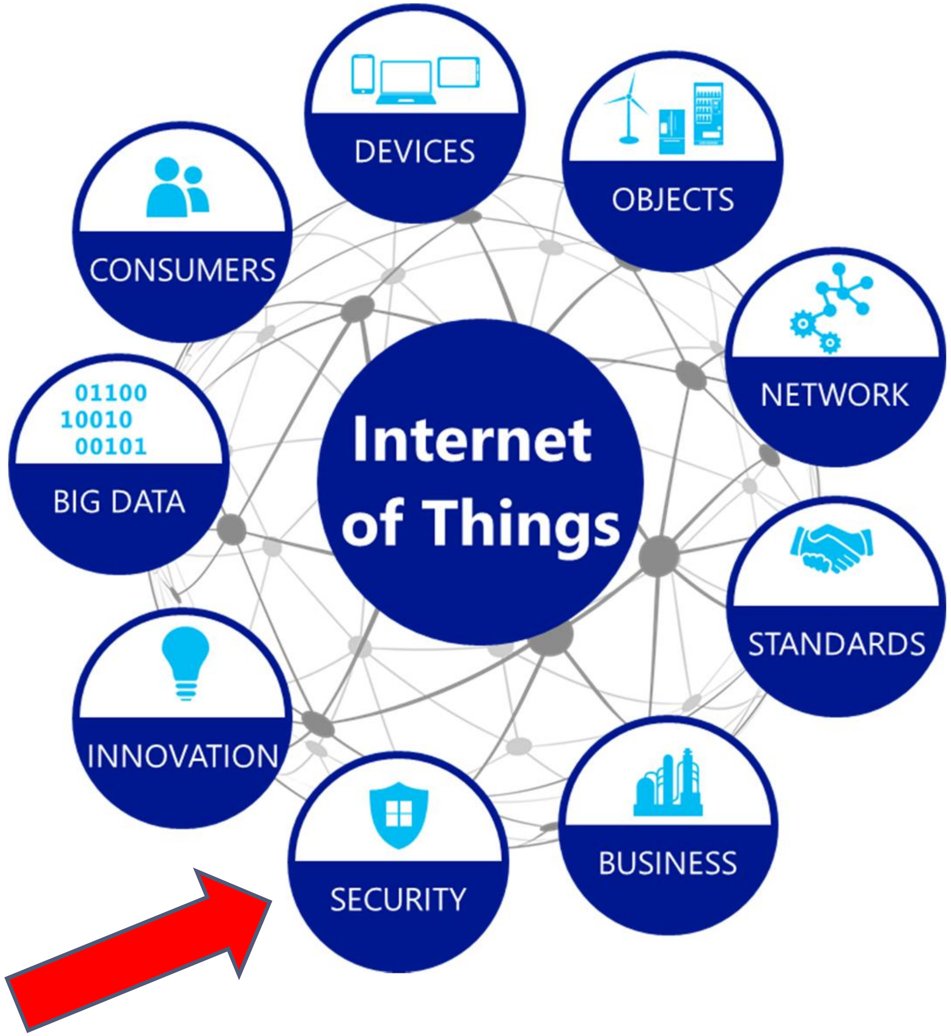

The Internet of Things is Already Here

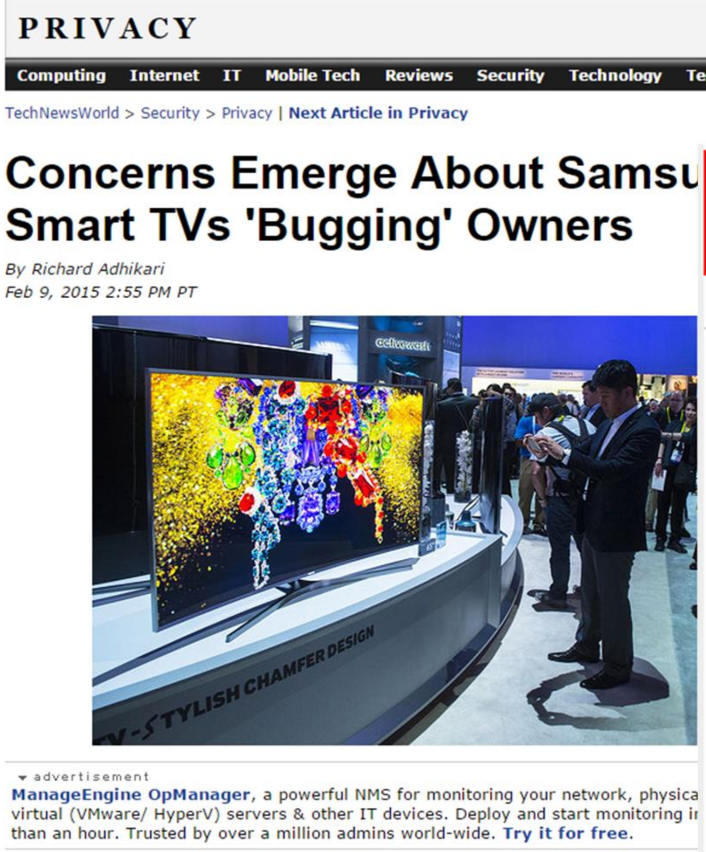
50 Billion "Smart Objects"

Rapid Adoption rate of digital infrastructure: 5X faster than electricity and telephony

Source: Cisco IBSG, 2011

Emerging Challenges





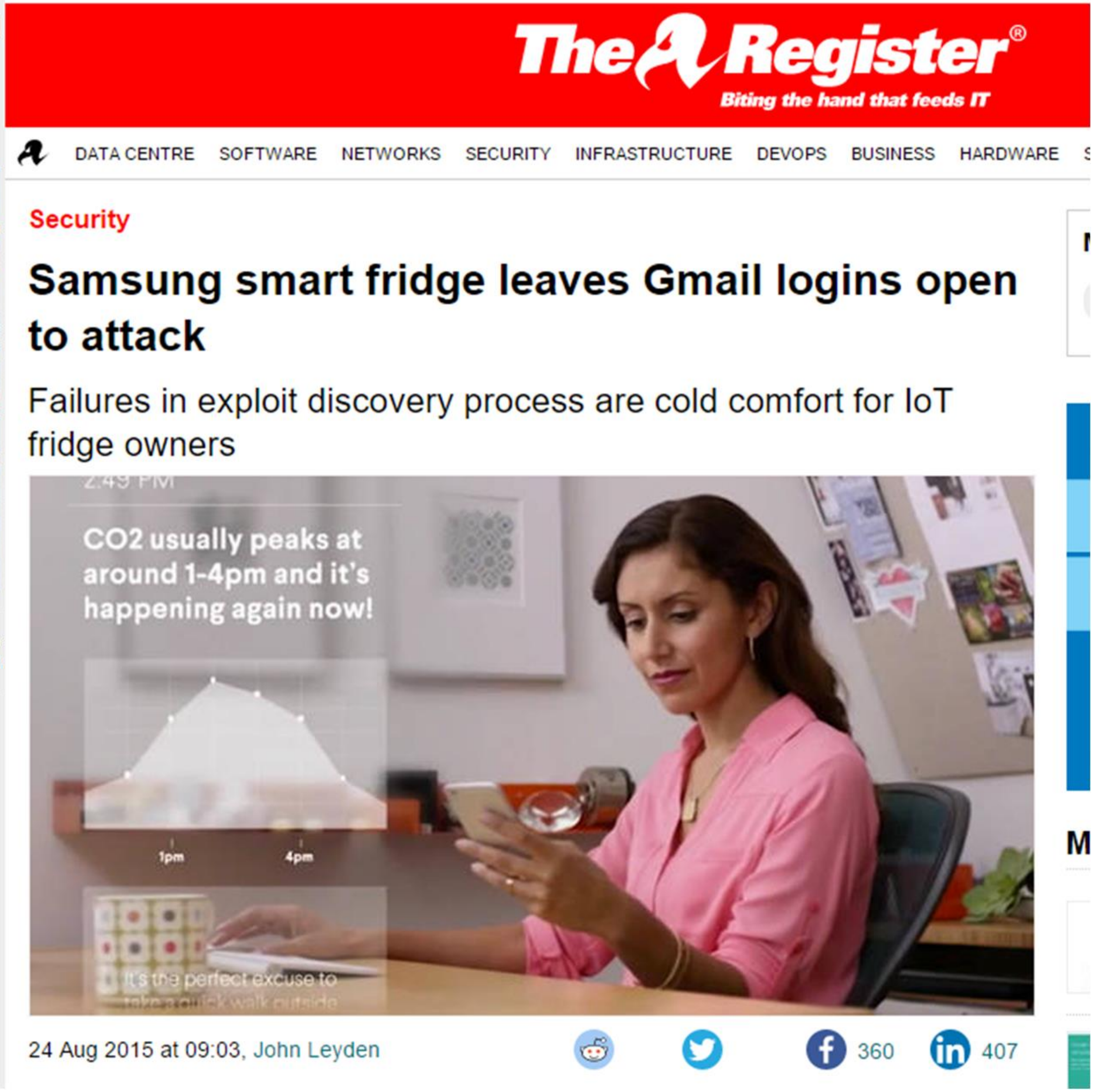
PRIVACY

Computing Internet IT Mobile Tech Reviews Security Technology Tech Blog

TechNewsWorld > Security > Privacy | Next Article in Privacy

Concerns Emerge About Samsu Smart TVs 'Bugging' Owners

By Richard Adhikari
Feb 9, 2015 2:55 PM PT



The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWARE

Security

Samsung smart fridge leaves Gmail logins open to attack

Failures in exploit discovery process are cold comfort for IoT fridge owners

2:49 PM
CO2 usually peaks at around 1-4pm and it's happening again now!
1pm
4pm
It's the perfect excuse to take a quick walk outside

24 Aug 2015 at 09:03, John Leyden

Five most infamous attacks

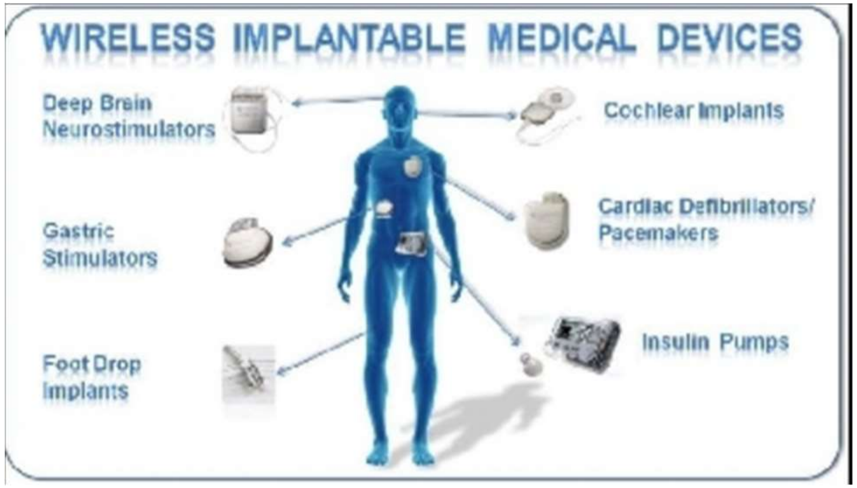
- The Mirai Botnet
- Hackable Cardiac Devices
- The Owlet Wi-Fi Baby Heart Monitor
- The TRENDnet Webcam Hack
- The Jeep Hack

The Mirai Botnet

- October of 2016
- DDOS attack
- Targeted a DNS service provider Dyn
- botnet of IoT devices

Hackable Cardiac Devices

- 2017: serious vulnerability in implantable pacemakers
- Vulnerability laid in the transmitter
- Once attackers were able:
  - to alter its functioning,
  - deplete the battery,
  - administer potentially fatal shocks.
  - monitoring


WIRELESS IMPLANTABLE MEDICAL DEVICES
Deep Brain Neurostimulators
Cochlear Implants
Gastric Stimulators
Cardiac Defibrillators/ Pacemakers
Insulin Pumps
Foot Drop Implants

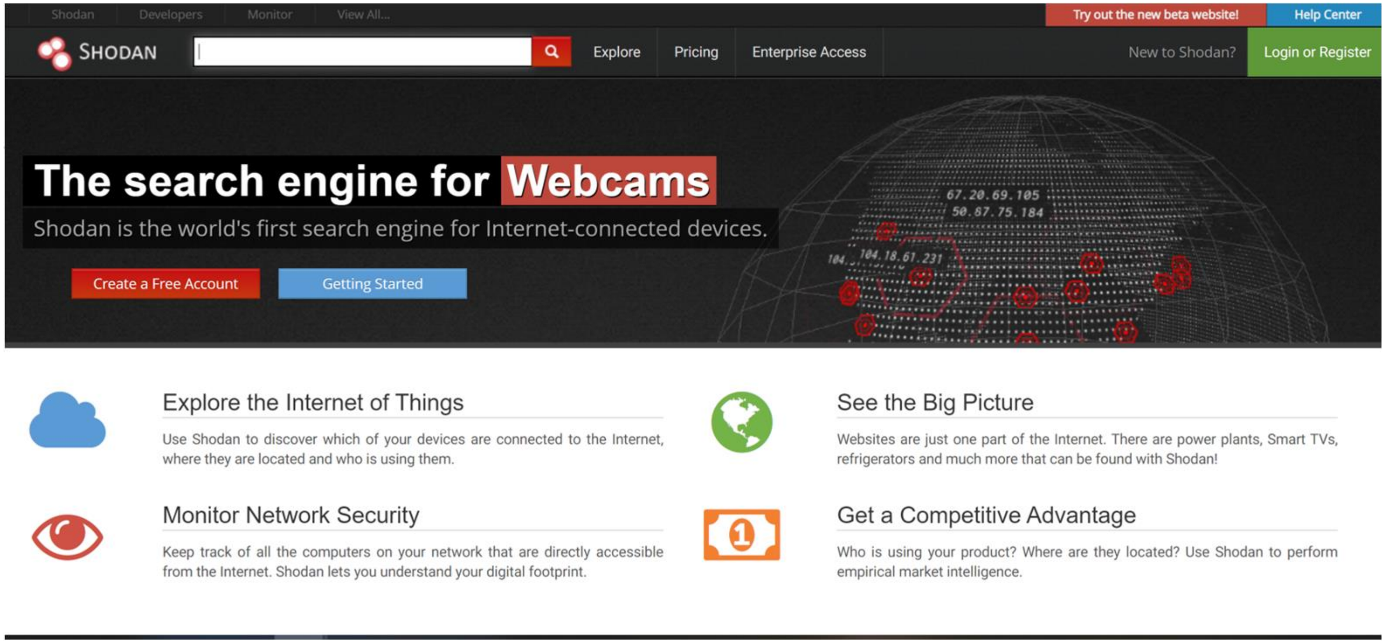
The Owlet Wi-Fi Baby Heart Monitor

- vulnerable to hacking
- target other smart devices on the same network

TRENDnet Webcam Hack

- security camera
- Supposed to be secure
- anyone who was able to find the IP address of any of these devices could easily look through it!
- snoopers were also able to capture audio
- TRENDnet was transmitting users' login information over the internet without any encryption as clear, readable text

Shodan



The search engine for Webcams

Shodan is the world's first search engine for Internet-connected devices.

Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

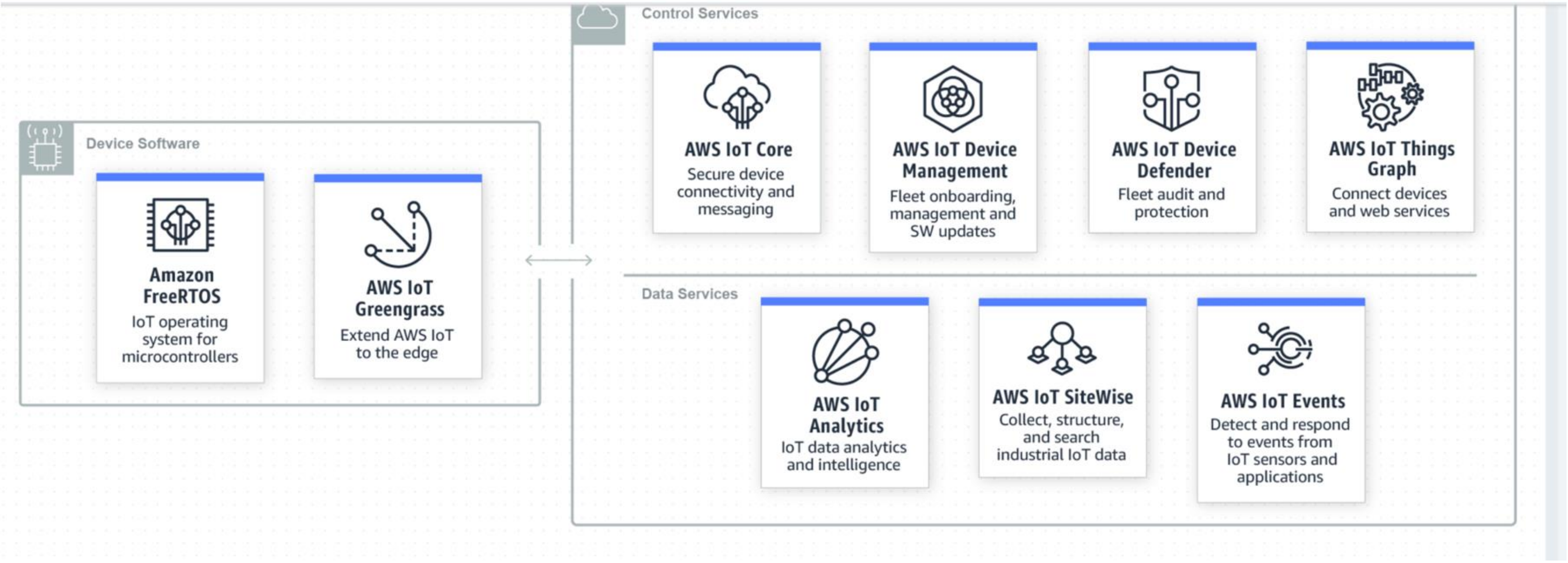
- Shodan is the world's first search engine for Internet-connected devices
- Finds systems including control systems for water plants, power grids and a cyclotron

The Jeep Hack

Steal cars with a laptop

- NEW YORK - Security technology created to protect luxury vehicles may now make it easier for tech-savy thieves to drive away with them.
- In April '07, high-tech criminals made international headlines when they used a laptop and transmitter to open the locks and start the ignition of an armor-plated BMW X5 belonging to soccer player David Beckham, the second X5 stolen from him using this technology within six months.
- … Beckham's BMW X5s were stolen by thieves who hacked into the codes for the vehicles' RFID chips …

Amazon as an example



Device Software

Amazon FreeRTOS
IoT operating system for microcontrollers

AWS IoT Greengrass
Extend AWS IoT to the edge

Control Services

AWS IoT Core
Secure device connectivity and messaging

AWS IoT Device Management
Fleet onboarding, management and SW updates

AWS IoT Device Defender
Fleet audit and protection

AWS IoT Things Graph
Connect devices and web services

Data Services

AWS IoT Analytics
IoT data analytics and intelligence

AWS IoT SiteWise
Collect, structure, and search industrial IoT data

AWS IoT Events
Detect and respond to events from IoT sensors and applications

ENISA and IoT

Reading material

- Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures

https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

Elements of IoT

- Intelligent decision making
- Sensors and actuators
- Embedded systems

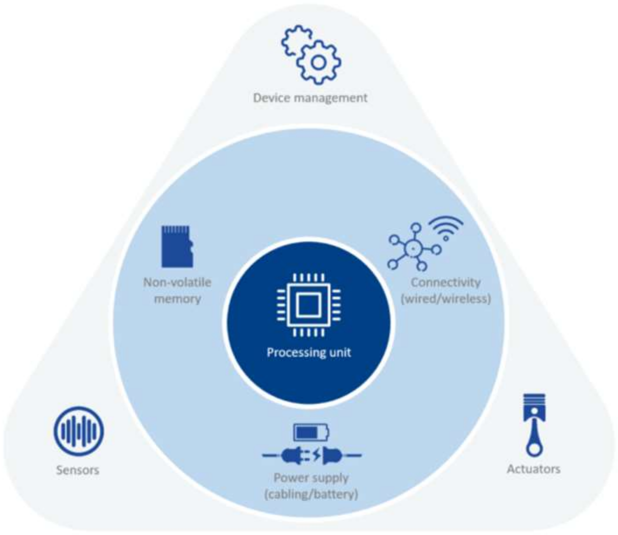
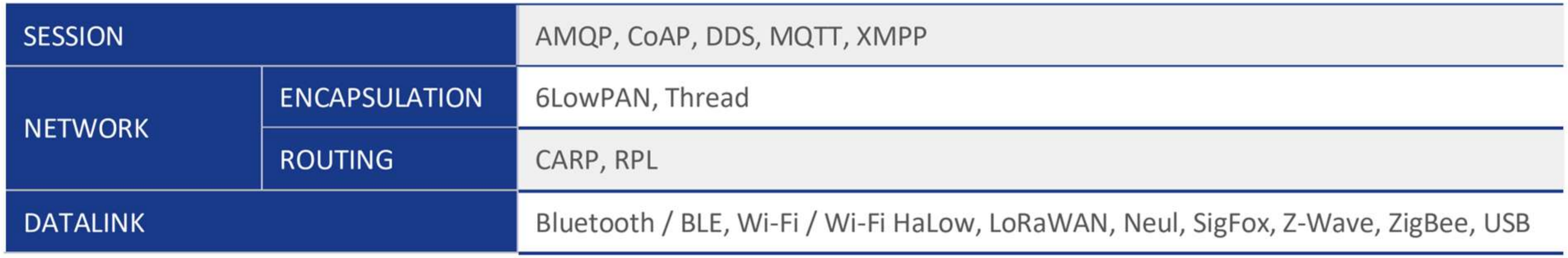


Figure 3: Structure of an IoT embedded system

Elements IoT

- Communications
  - depending on their purpose and resource constraints
  - short-range radio protocols
    - ZigBee, Bluetooth/Bluetooth Low Energy (BLE), Wi-Fi/Wi-Fi HaLow, Near Field Communication (NFC), Radio Frequency Identification (RFID)
  - mobile networks and longer-range radio protocols
    - LoRaWAN53, SigFox, NarrowBand-IoT (NB-IoT), or LTE-M

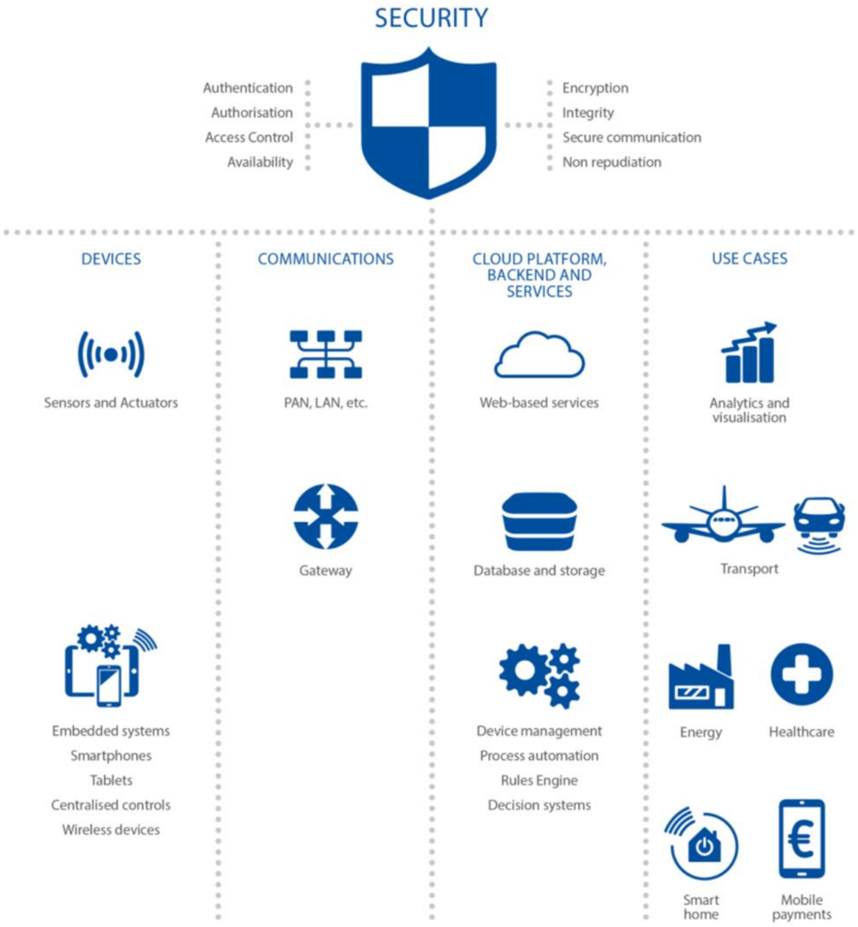


SESSION		AMQP, CoAP, DDS, MQTT, XMPP
NETWORK	ENCAPSULATION	6LowPAN, Thread
	ROUTING	CARP, RPL
DATALINK		Bluetooth / BLE, Wi-Fi / Wi-Fi HaLow, LoRaWAN, Neul, SigFox, Z-Wave, ZigBee, USB

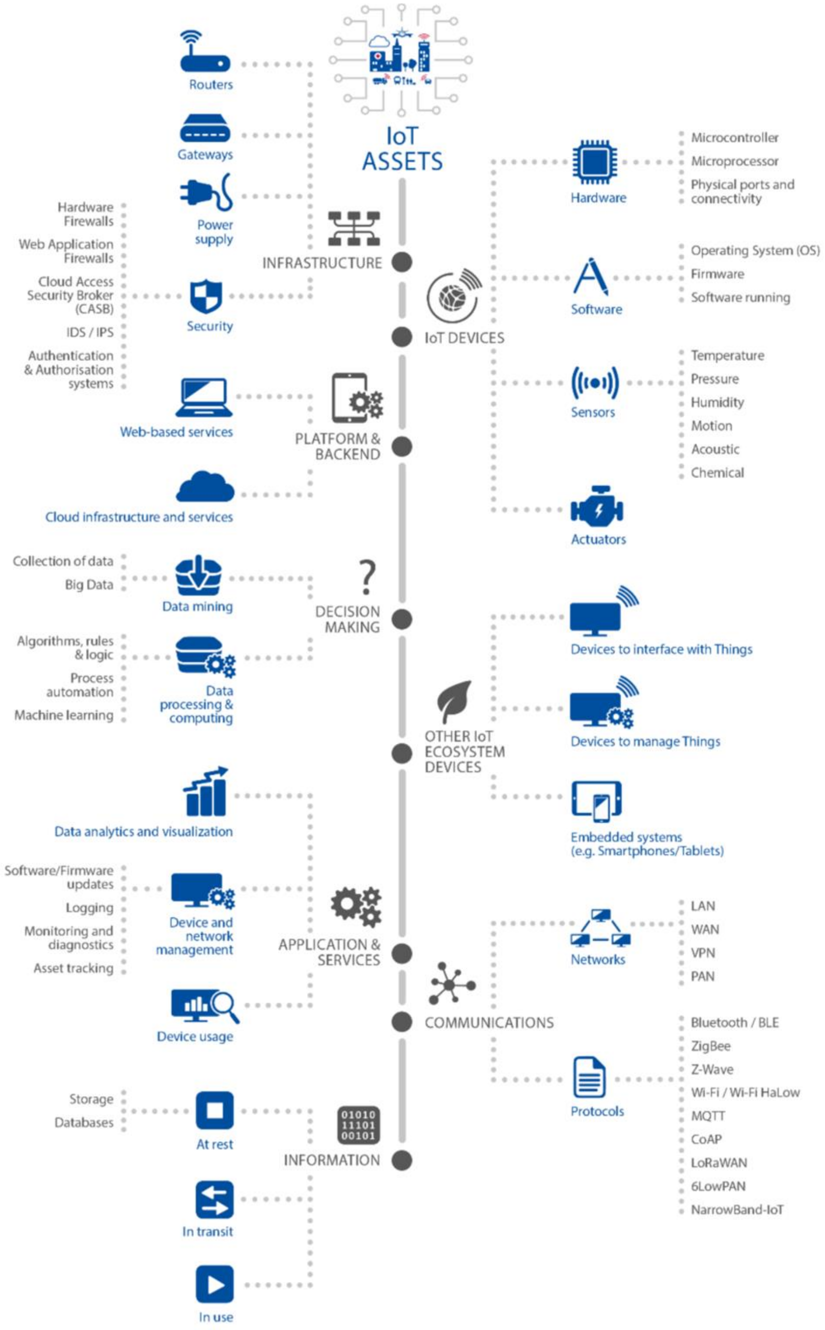
Elements IoT

- Security considerations
  - Very large attack surface
  - Limited device resources
  - Complex ecosystem
  - Fragmentation of standards and regulations
  - Widespread deployment
  - Security integration
  - Safety aspects
  - Low cost
  - Lack of expertise
  - Security updates
  - Insecure programming
  - Unclear liabilities

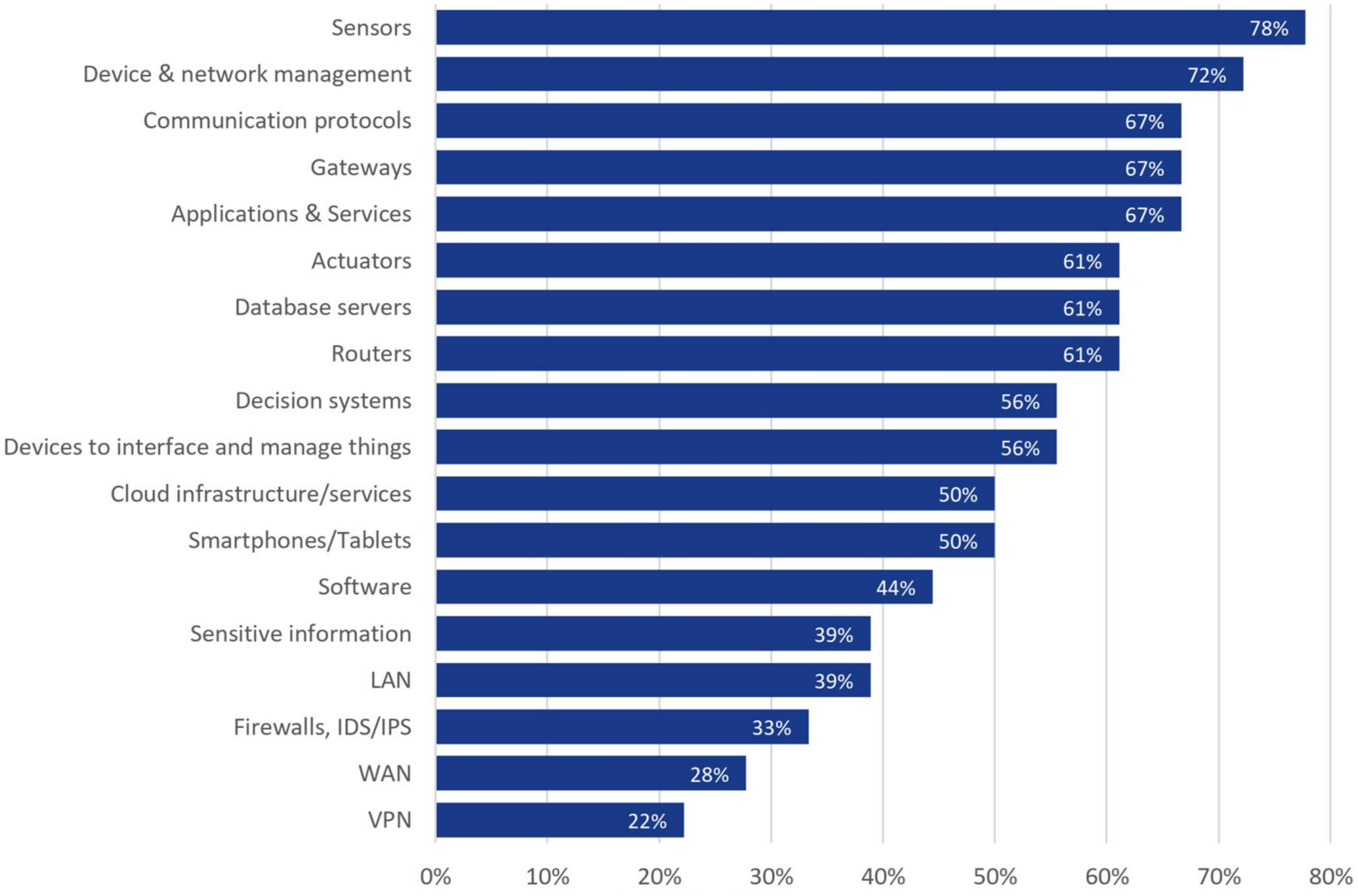
Architecture



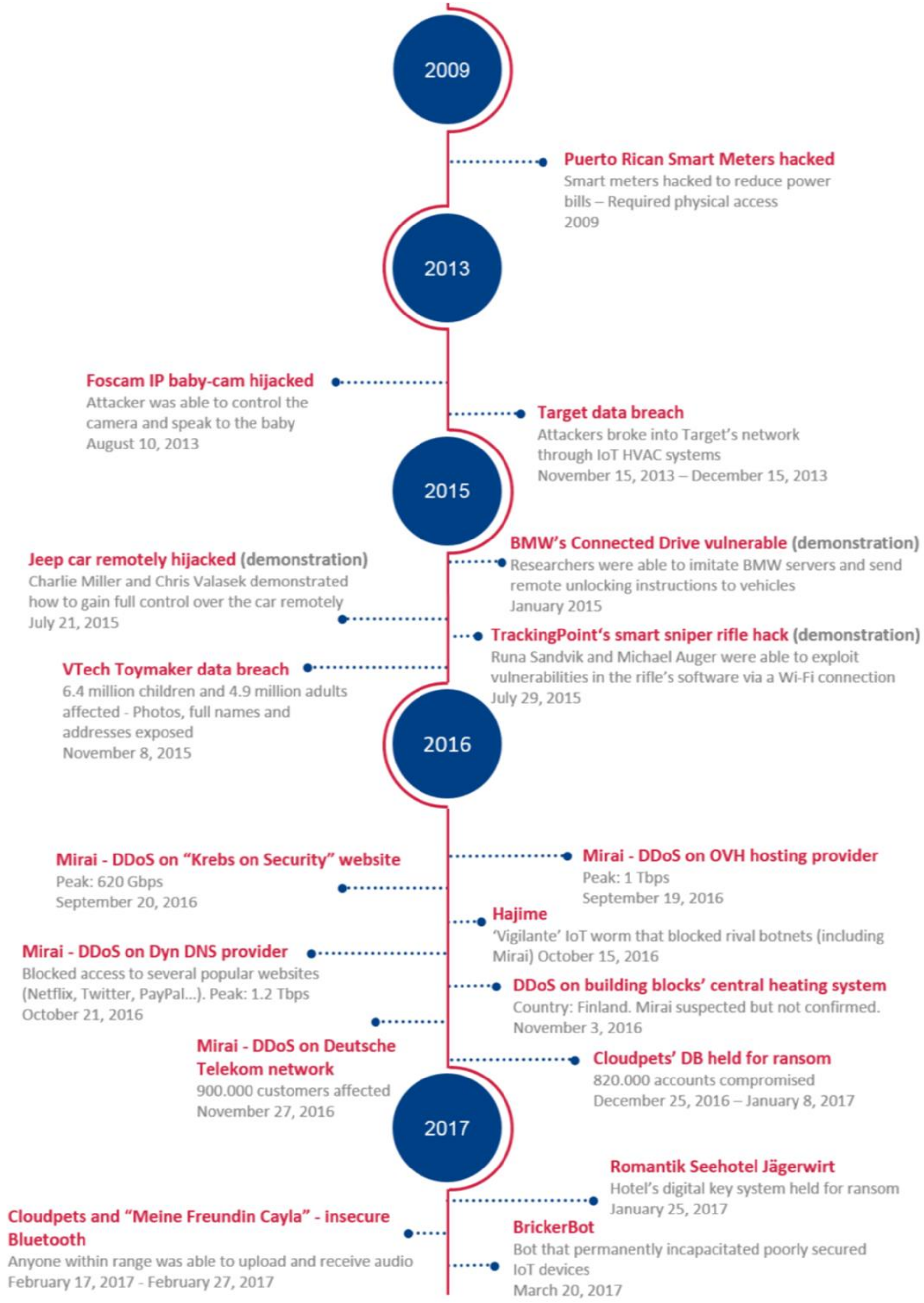
Asset taxonomy



Asset Criticality



Incidents



Puerto Rican Smart Meters hacked
Smart meters hacked to reduce power bills – Required physical access
2009

Foscam IP baby-cam hijacked
Attacker was able to control the camera and speak to the baby
August 10, 2013

Target data breach
Attackers broke into Target's network through IoT HVAC systems
November 15, 2013 – December 15, 2013

BMW's Connected Drive vulnerable (demonstration)
Researchers were able to imitate BMW servers and send remote unlocking instructions to vehicles
January 2015

Jeep car remotely hijacked (demonstration)
Charlie Miller and Chris Valasek demonstrated how to gain full control over the car remotely
July 21, 2015

TrackingPoint's smart sniper rifle hack (demonstration)
Runa Sandvik and Michael Auger were able to exploit vulnerabilities in the rifle's software via a Wi-Fi connection
July 29, 2015

VTech Toymaker data breach
6.4 million children and 4.9 million adults affected - Photos, full names and addresses exposed
November 8, 2015

Mirai - DDoS on OVH hosting provider
Peak: 1 Tbps
September 19, 2016

Mirai - DDoS on "Krebs on Security" website
Peak: 620 Gbps
September 20, 2016

Hajime
'Vigilante' IoT worm that blocked rival botnets (including Mirai) October 15, 2016

Mirai - DDoS on Dyn DNS provider
Blocked access to several popular websites (Netflix, Twitter, PayPal...). Peak: 1.2 Tbps
October 21, 2016

DDoS on building blocks' central heating system
Country: Finland. Mirai suspected but not confirmed.
November 3, 2016

Mirai - DDoS on Deutsche Telekom network
900.000 customers affected
November 27, 2016

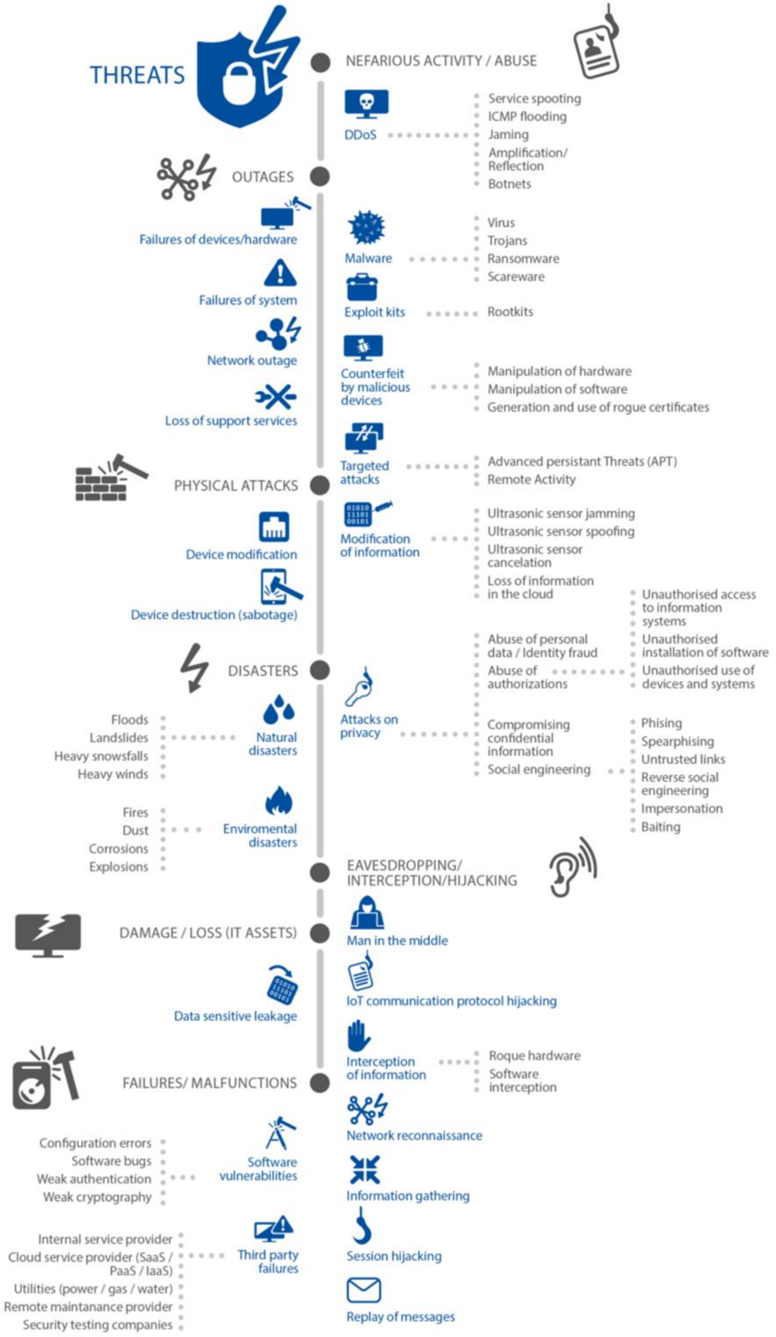
Cloudpets' DB held for ransom
820.000 accounts compromised
December 25, 2016 – January 8, 2017

Romantik Seehotel Jägerwirt
Hotel's digital key system held for ransom
January 25, 2017

Cloudpets and "Meine Freundin Cayla" - insecure Bluetooth
Anyone within range was able to upload and receive audio
February 17, 2017 - February 27, 2017

BrickerBot
Bot that permanently incapacitated poorly secured IoT devices
March 20, 2017

Threats Taxonomy



THREATS

OUTAGES
- Failures of devices/hardware
- Failures of system
- Network outage
- Loss of support services

PHYSICAL ATTACKS
- Device modification
- Device destruction (sabotage)

DISASTERS
- Natural disasters: Floods, Landslides, Heavy snowfalls, Heavy winds
- Enviromental disasters: Fires, Dust, Corrosions, Explosions

DAMAGE / LOSS (IT ASSETS)
- Data sensitive leakage

FAILURES/ MALFUNCTIONS
- Software vulnerabilities: Configuration errors, Software bugs, Weak authentication, Weak cryptography
- Third party failures: Internal service provider, Cloud service provider (SaaS / PaaS / IaaS), Utilities (power / gas / water), Remote maintanance provider, Security testing companies

NEFARIOUS ACTIVITY / ABUSE
- DDoS: Service spooting, ICMP flooding, Jaming, Amplification/ Reflection, Botnets
- Malware: Virus, Trojans, Ransomware, Scareware
- Exploit kits: Rootkits
- Counterfeit by malicious devices: Manipulation of hardware, Manipulation of software, Generation and use of rogue certificates
- Targeted attacks: Advanced persistant Threats (APT), Remote Activity
- Modification of information: Ultrasonic sensor jamming, Ultrasonic sensor spoofing, Ultrasonic sensor cancelation, Loss of information in the cloud
- Attacks on privacy: Abuse of personal data / Identity fraud; Abuse of authorizations (Unauthorised access to information systems, Unauthorised installation of software, Unauthorised use of devices and systems); Compromising confidential information; Social engineering (Phising, Spearphising, Untrusted links, Reverse social engineering, Impersonation, Baiting)

EAVESDROPPING/ INTERCEPTION/HIJACKING
- Man in the middle
- IoT communication protocol hijacking
- Interception of information: Roque hardware, Software interception
- Network reconnaissance
- Information gathering
- Session hijacking
- Replay of messages

Impact

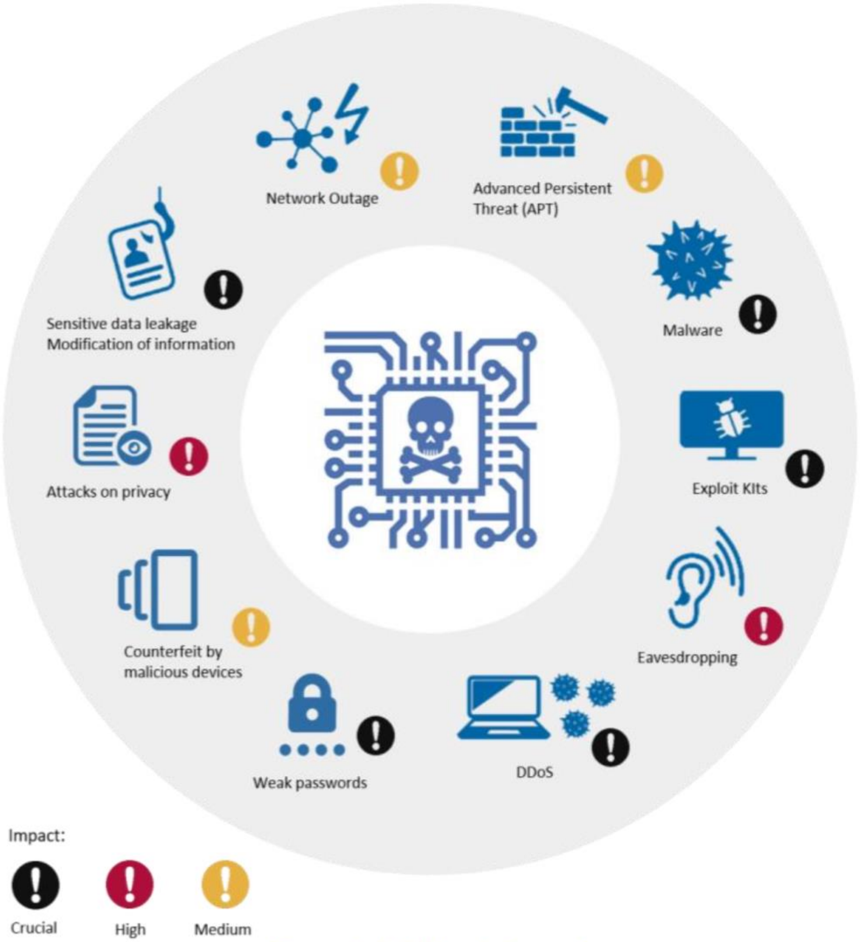
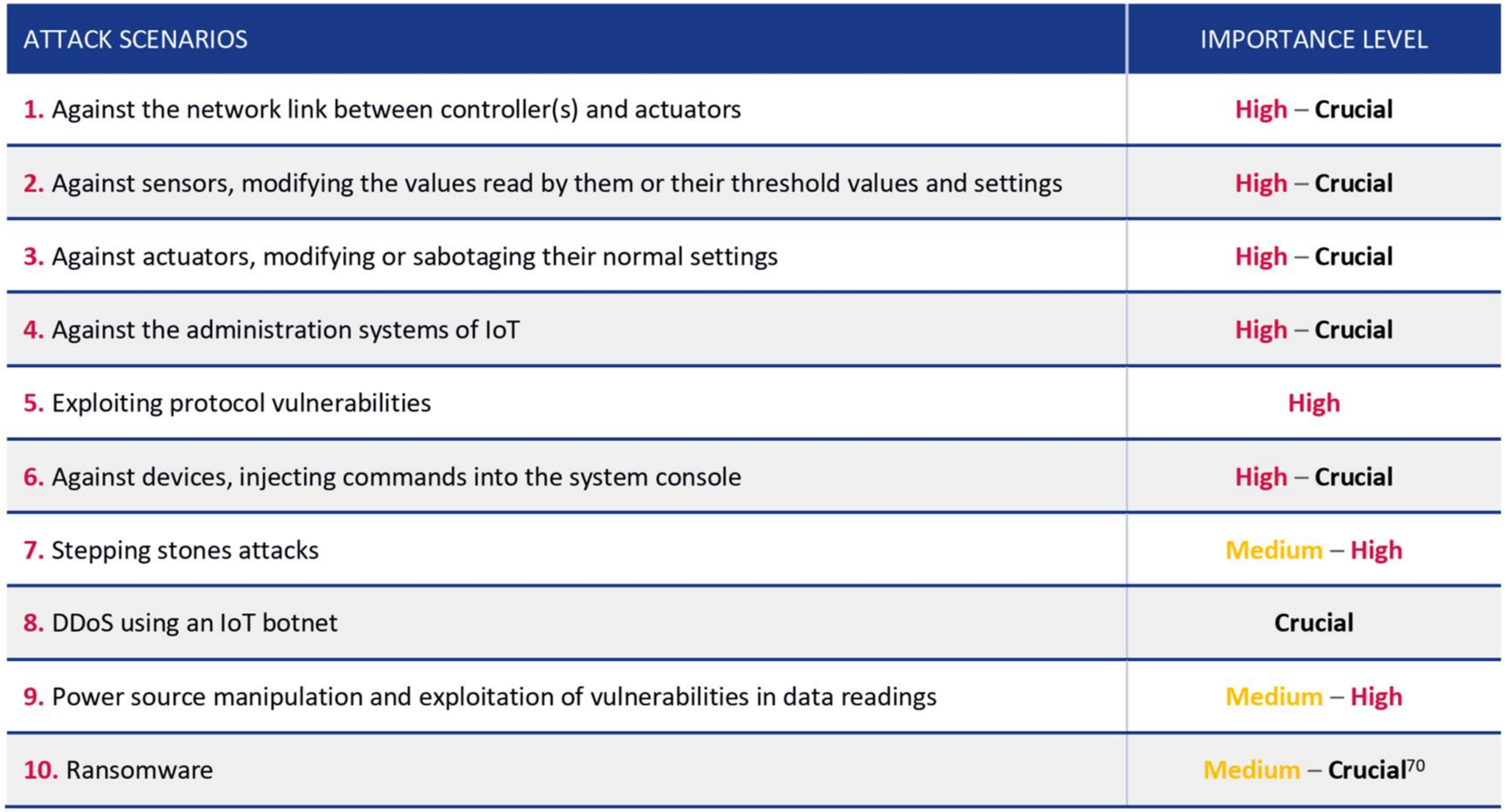

Network Outage
Advanced Persistent Threat (APT)
Sensitive data leakage Modification of information
Malware
Attacks on privacy
Exploit KIts
Counterfeit by malicious devices
Eavesdropping
Weak passwords
DDoS
Impact:
Crucial
High
Medium

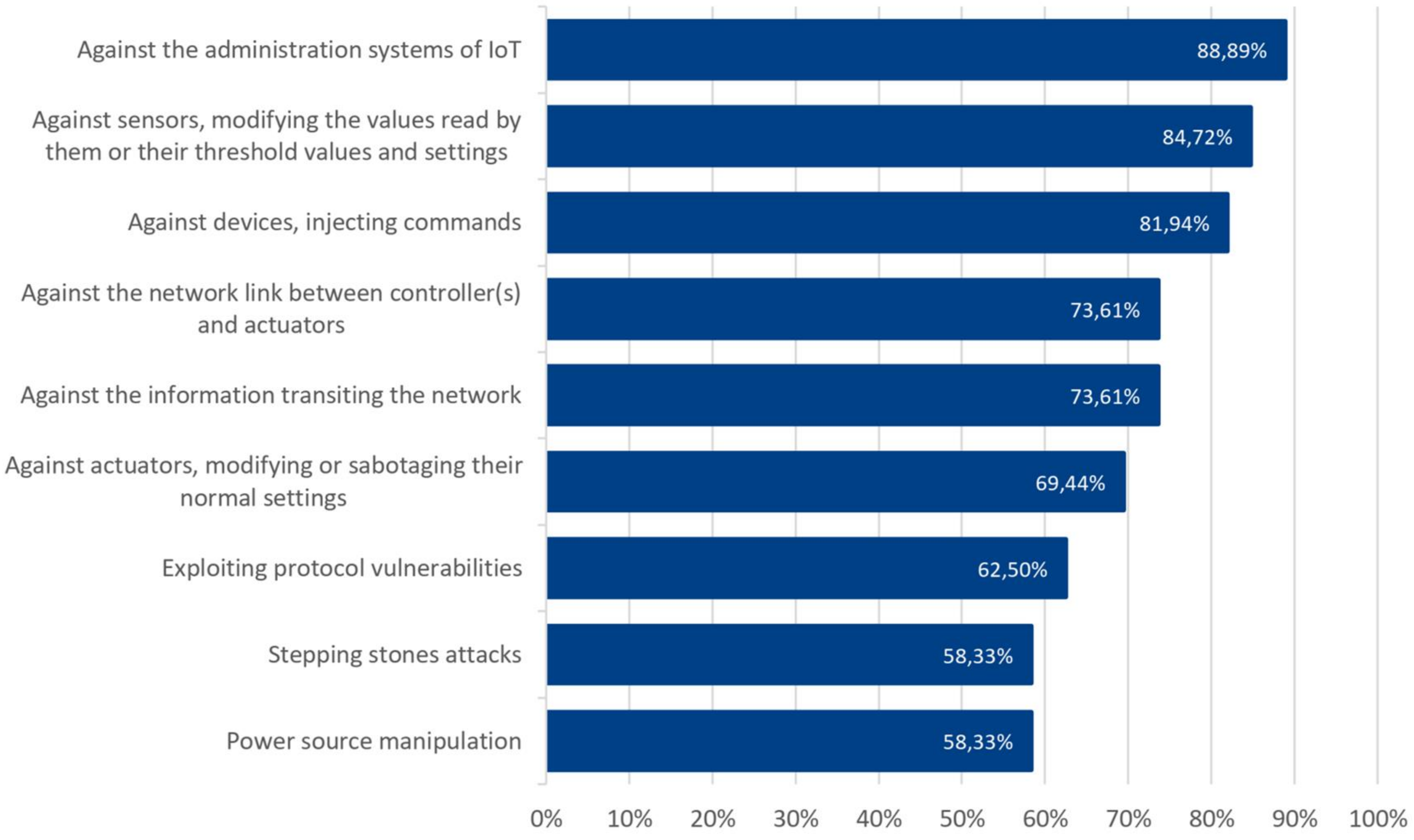
Figure 9: IoT threats impact

Attack scenarios



ATTACK SCENARIOS	IMPORTANCE LEVEL
1. Against the network link between controller(s) and actuators	High – Crucial
2. Against sensors, modifying the values read by them or their threshold values and settings	High – Crucial
3. Against actuators, modifying or sabotaging their normal settings	High – Crucial
4. Against the administration systems of IoT	High – Crucial
5. Exploiting protocol vulnerabilities	High
6. Against devices, injecting commands into the system console	High – Crucial
7. Stepping stones attacks	Medium – High
8. DDoS using an IoT botnet	Crucial
9. Power source manipulation and exploitation of vulnerabilities in data readings	Medium – High
10. Ransomware	Medium – Crucial[70]

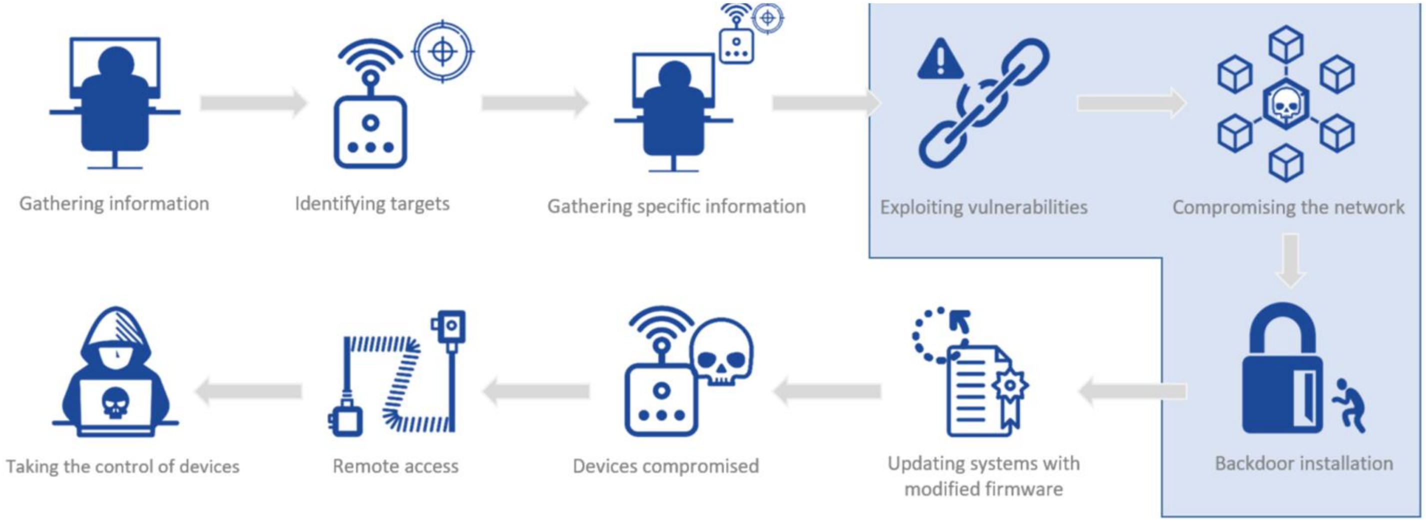
Criticality



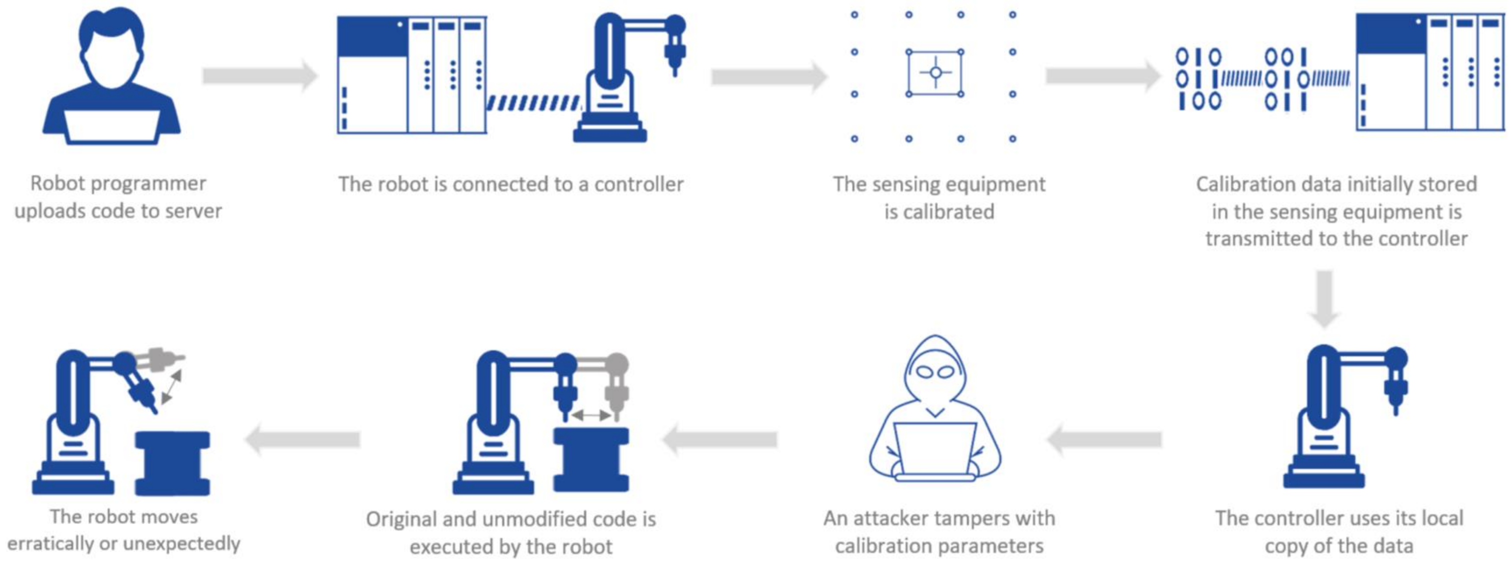
Critical Attack scenarios

- Attack Scenario 1: IoT administration system compromise
- Attack Scenario 2: Value manipulation in IoT devices
- Attack Scenario 3: Botnet / Commands Injection

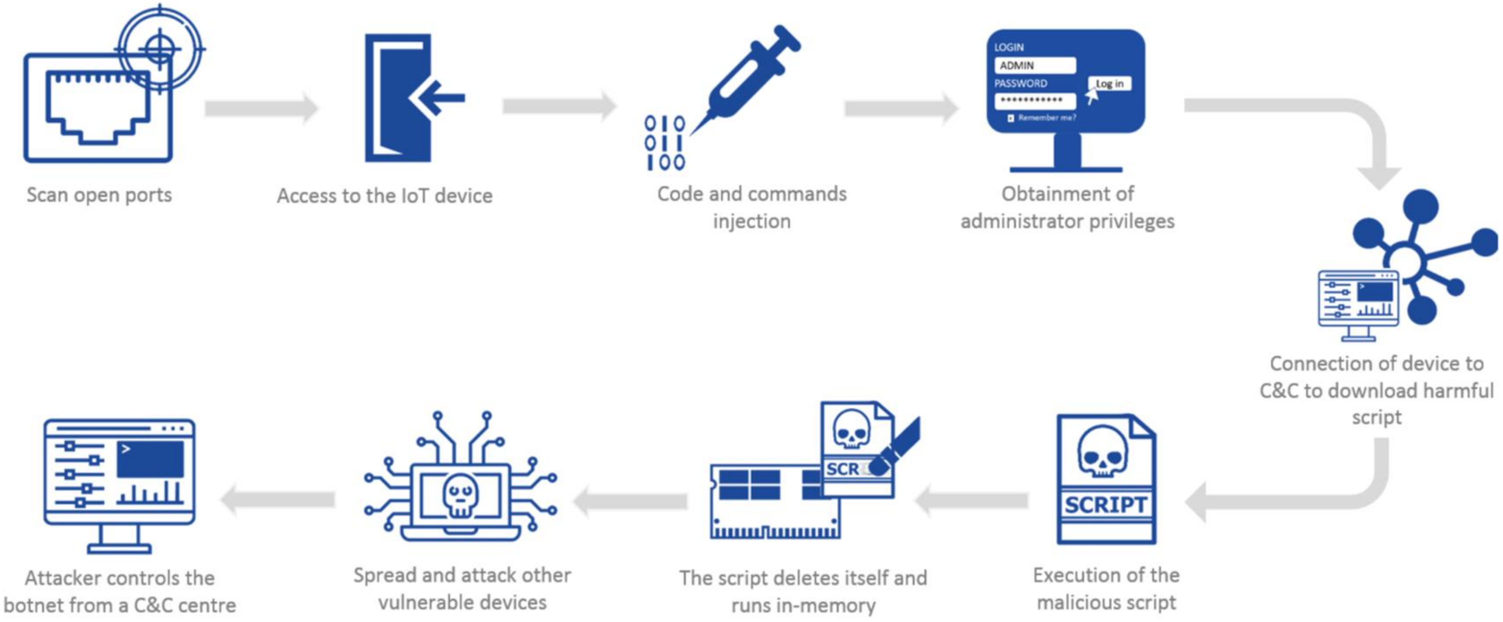
Attack Scenario 1: IoT administration system compromise


Gathering information
Identifying targets
Gathering specific information
Exploiting vulnerabilities
Compromising the network
Backdoor installation
Updating systems with modified firmware
Devices compromised
Remote access
Taking the control of devices

Attack Scenario 2: Value manipulation in IoT devices


Robot programmer uploads code to server
The robot is connected to a controller
The sensing equipment is calibrated
Calibration data initially stored in the sensing equipment is transmitted to the controller
010 001
01 010
100 011
The controller uses its local copy of the data
An attacker tampers with calibration parameters
Original and unmodified code is executed by the robot
The robot moves erratically or unexpectedly

Attack Scenario 3: Botnet / Commands Injection


Scan open ports
Access to the IoT device
010
011
100
Code and commands injection
LOGIN
ADMIN
PASSWORD
Log in
Remember me?
Obtainment of administrator privileges
Connection of device to C&C to download harmful script
SCRIPT
Execution of the malicious script
SCR
The script deletes itself and runs in-memory
Spread and attack other vulnerable devices
Attacker controls the botnet from a C&C centre

Security measures and good practices

- Policies
  - Security by design
  - Privacy by design
  - Asset Management
- Organisational, People and Process measures
  - End-of-life support
  - Proven solutions
  - Management of security vulnerabilities and/or incidents
  - Human Resources Security Training and Awareness
  - Third-Party relationships

Security measures and good practices

- Technical Measures
  - Hardware security
  - Trust and Integrity Management
  - Strong default security and privacy
  - Data protection and compliance
  - System safety and reliability
  - Secure Software / Firmware updates
  - Authentication
  - Authorisation
  - Access Control - Physical and Environmental security

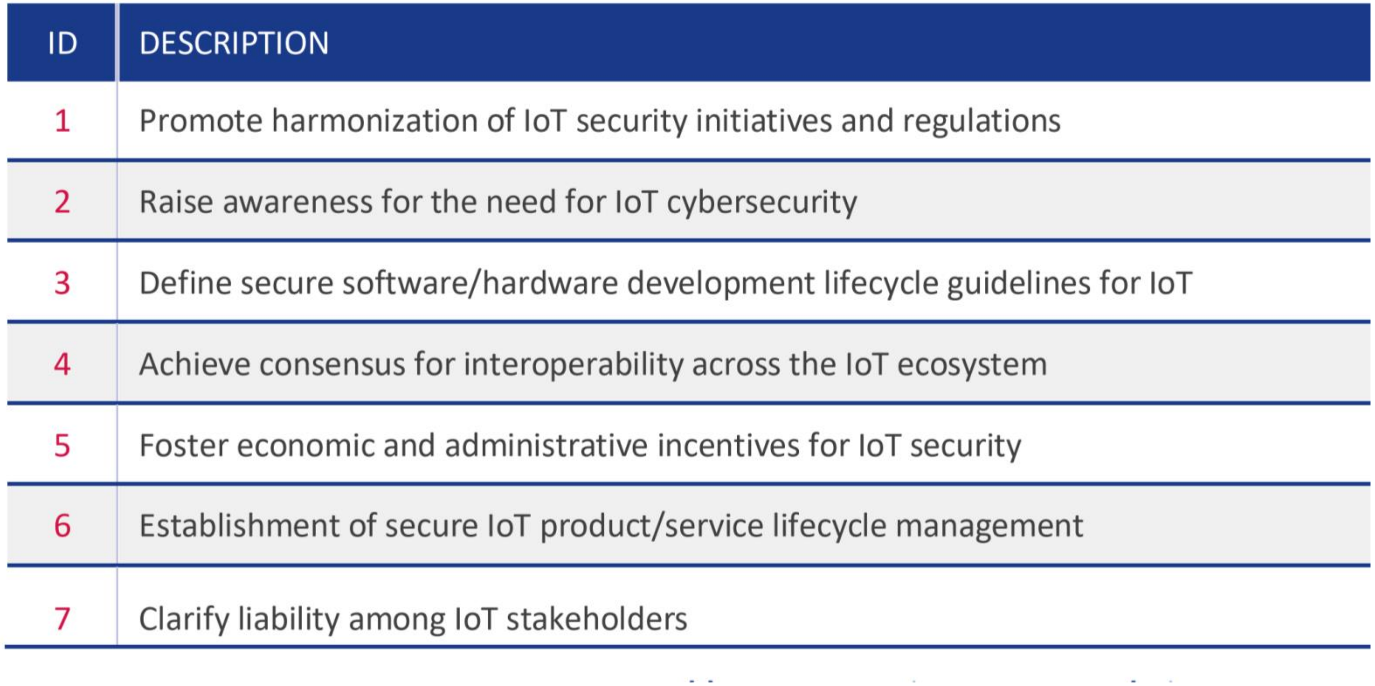
Security measures and good practices

- Technical Measures
  - Cryptography
  - Secure and trusted communications
  - secure Interfaces and network services
  - Secure input and output handling
  - Logging
  - Monitoring and Auditing

Gaps

- Gap 1: Fragmentation in existing security approaches and regulations
- Gap 2: Lack of awareness and knowledge
- Gap 3: Insecure design and/or development
- Gap 4: Lack of interoperability across different IoT devices, platforms and frameworks
- Gap 5: Lack of economic incentives
- Gap 6: Lack of proper product lifecycle management

Recommendations



ID	DESCRIPTION
1	Promote harmonization of IoT security initiatives and regulations
2	Raise awareness for the need for IoT cybersecurity
3	Define secure software/hardware development lifecycle guidelines for IoT
4	Achieve consensus for interoperability across the IoT ecosystem
5	Foster economic and administrative incentives for IoT security
6	Establishment of secure IoT product/service lifecycle management
7	Clarify liability among IoT stakeholders

Cybersecurity Standardization for the IoT

NIST – 2/2018

- https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8200.pdf

Core Areas of Cybersecurity Standardization	Examples of Relevant SDOs	Connected Vehicles	Consumer IoT	Health IoT & Medical Devices	Smart Buildings	Smart Manufacturing
Cryptographic Techniques	ETSI; IEEE; ISO/IEC JTC 1; ISO TC 68; ISO TC 307; W3C	Standards Available May Need Revisions Slow Uptake May Need Updates	Standards Available May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates	Standards Available May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates
Cyber Incident Management	ETSI ; ISO/IEC JTC 1; ITU-T; PCI	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates
Hardware Assurance	ISO/IEC JTC 1; SAE International	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Not Implemented	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Not Implemented	Some Standards May Need Revisions Not Implemented
Identity and Access Management	ETSI; FIDO Alliance; IETF; OASIS; OIDF; ISO/IEC JTC 1; ITU-T; W3C	Standards Available May Need Revisions Slow Uptake May Need Updates	Standards Available May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates	Standards Available May Need Revisions Slow Uptake May Need Updates	Standards Available May Need Revisions Slow Uptake May Need Updates
Information Security Management Systems	ATIS; IEC; ISA; ISO/IEC JTC 1; ISO TC 223; OASIS; The Open Group	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates
IT System Security Evaluation	ISO/IEC JTC 1; The Open Group; UL	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates

Core Areas of Cybersecurity Standardization	Examples of Relevant SDOs	Connected Vehicles	Consumer IoT	Health IoT & Medical Devices	Smart Buildings	Smart Manufacturing
Network Security	3GPP; 3GPP2; IEC; IETF; IEEE; ISO/IEC JTC 1; ITU-T; The Open Group; WiMAX Forum	Standards Available May Need Revisions Implemented May Need Updates	Standards Available May Need Revisions Implemented May Need Updates	Standards Available May Need Revisions Implemented May Need Updates	Standards Available May Need Revisions Implemented May Need Updates	Standards Available May Need Revisions Implemented May Need Updates
Physical Security	ASIS International; IEC; IEEE; ISO/IEC JTC 1; NEMA; SIA	Standards Available May Need Revisions Implemented May Need Updates	Standards Available May Need Revisions Implemented May Need Updates	Standards Available May Need Revisions Implemented May Need Updates	Standards Available May Need Revisions Implemented May Need Updates	Standards Available May Need Revisions Implemented May Need Updates
Security Automation and Continuous Monitoring	IEEE; IETF; ISO/IEC JTC 1; TCG; The Open Group	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates
Software Assurance	IEEE; ISO/IEC JTC 1; OMG; TCG; The Open Group; UL	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates
Supply Chain Risk Management	IEEE; ISO/IEC JTC 1; IEC TC 65; The Open Group; UL	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates	Some Standards May Need Revisions Slow Uptake May Need Updates
System Security Engineering	IEC; IEEE; ISA; ISO/IEC JTC 1; SAE International; The Open Group	Some Standards May Need Revisions Slow Uptake May Need Updates	Standards Needed	Some Standards May Need Revisions Slow Uptake May Need Updates	Standards Needed	Standards Needed

RFID: Threats against privacy and countermeasures

(in Greek)

Ενδεικτική βιβλιογραφία

- Προστασία της Ιδιωτικότητας και Τεχνολογίες Πληροφορικής και Επικοινωνιών, **Τεχνικά και Νομικά Θέματα.**

Κ. Λαμπρινουδάκης, Λ. Μήτρου, Στ. Γκρίτζαλης, Σ. Κάτσικας

Εκδόσεις Παπασωτηρίου

Outline

- Τεχνολογία RFID
- Απειλές και Επιθέσεις κατά της Ιδιωτικότητας
- Μέτρα Προστασίας
- Κρυπτανάλυση πρωτοκόλλων αυθεντικοποίησης

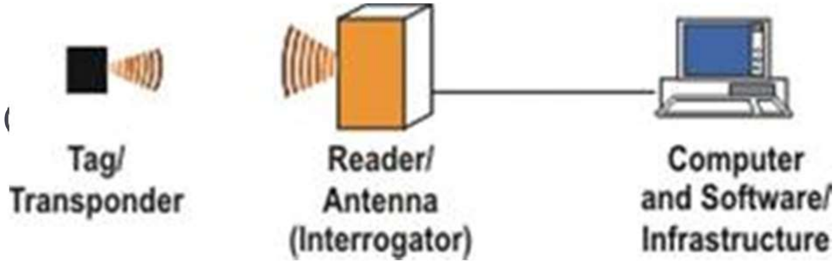
Τεχνολογία RFID (1/9)

- RFID = Radio Frequency IDentification
- Πρωτοεμφανίστηκε 1940
- Πρώτη εμπορική χρήση 1960
- Με την ανάπτυξη της τεχνολογίας των ημιαγωγών αναμένεται να αποτελέσει την πιο ευρέως διαδεδομένη τεχνολογία

Τεχνολογία RFID (2/9)

Ένα σύστημα RFID αποτελείται από 3 τμήματα

1. Ετικέτα (tag)
2. Κεραία
3. Back-end υπολογιστικό σύ



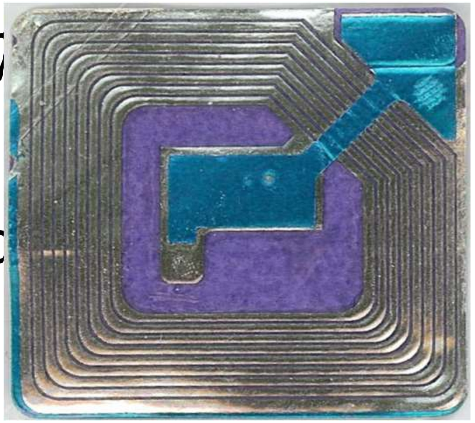
Τεχνολογία RFID (3/9)

- Ενεργές
  - τροφοδοτούνται από μπαταρία ή άλλη αυτόνομη πηγή ενέργειας
  - λειτουργούν στις συχνότητες UHF και μικροκυμάτων
- Παθητικές
  - δεν περιέχουν κάποια πηγή ενέργειας, αλλά μπορούν να αξιοποιούν τα ραδιοκύματα που εκπέμπει ο αναγνώστης
  - UHF και μικροκυματικών συχνοτήτων και στις LF και HF συχνότητες
  - περιορισμούς στην απόσταση εκπομπής(~3 μέτρα)

Τεχνολογία RFID (4/9)

Πλεονεκτήματα ενεργών ετικετών:

- ✓ Επικοινωνούν με τον αναγνώστη από μεγαλ αποστάσεις
- ✓ Αναγνώστης μπορεί να χρησιμοποιήσει ένα μικρότερης ισχύος
- ✓ Εκκινούν μία επικοινωνία
- ✓ Υλοποιούν πιο σύνθετα κυκλώματα
- ✓ Αποθηκεύουν πληροφορίες για το αντικείμενο



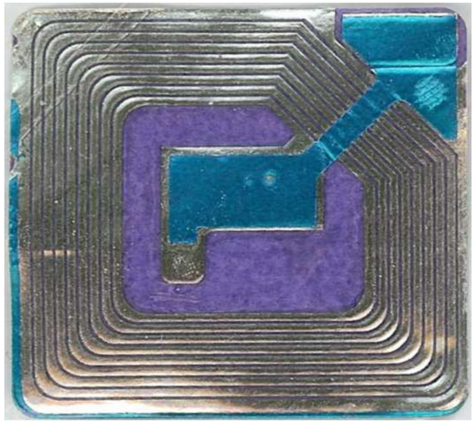
ΑΛΛΑ!!! Είναι πιο ακριβές

Τεχνολογία RFID (5/9)

Μέγεθος μιας ετικέτας?

✓ 0,05x0,05 χιλιοστά

- Hitachi
- 0,4x0,4 χιλιοστά



Εμβέλεια ανάγνωσης

✓ 180 μέτρα

Mojix

Ανθεκτικότητα

✓ Πλένεται και σιδερώνεται

Fujitsu

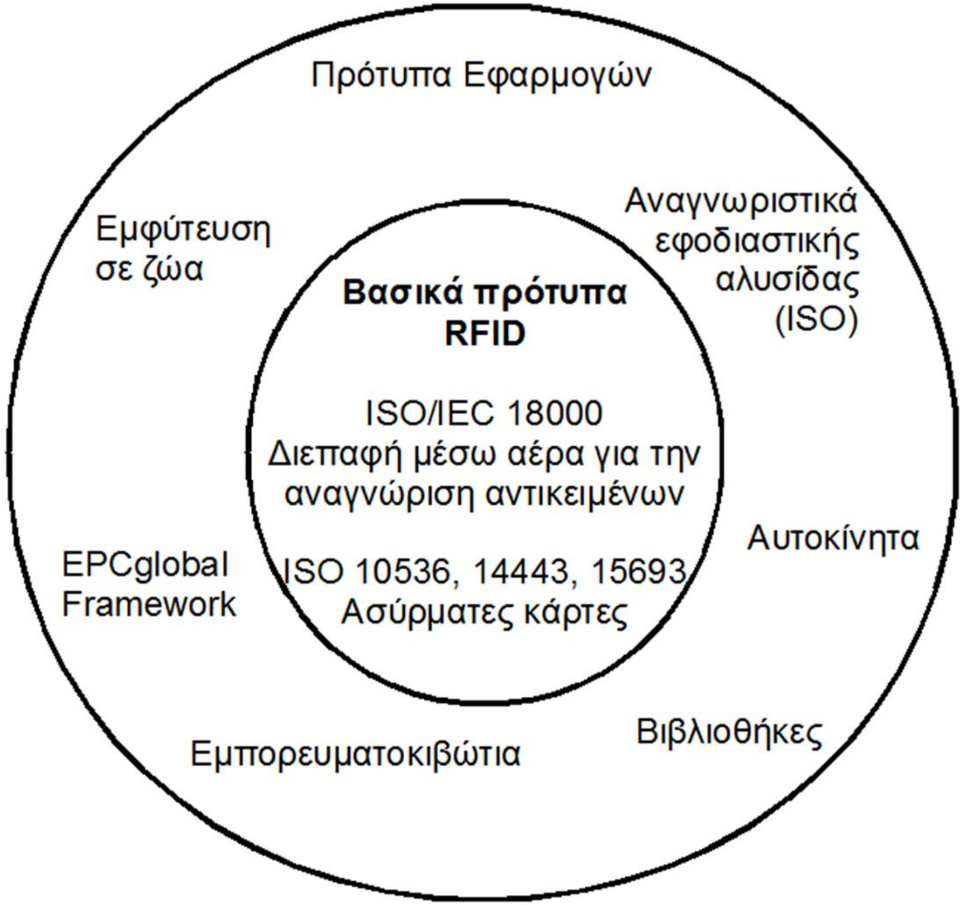
Τεχνολογία RFID (6/9)

Ποια είναι τα πρότυπα που αφορούν τα RFIDs??

- Ασύρματη επικοινωνία
- Ασφάλεια
- Κωδικοποίηση πληροφορίας

Τεχνολογία RFID (7/9)

Προτυποποίηση



Τεχνολογία RFID (8/9)

Προτυποποίηση

✓ ETSI =European Telecommunications Standards Institute

✓ ISO = International Organization for Standarization

✓ EPCGlobal

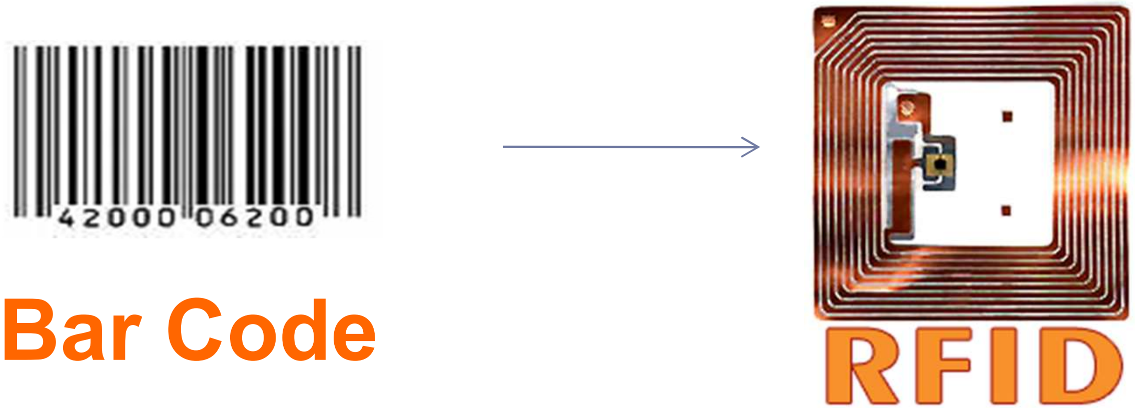
Τεχνολογία RFID (9/9)

Προτυποποίηση

- ✓ ISO 15962 Radio Frequency IDentification for item management –Data protocol: data encoding rules and logical memory functions (η κωδικοποίηση των δεδομένων)
- ✓ ISO 15961 Radio frequency identification (RFID) for item management – Data protocol: application interface (τα πρωτόκολλα επικοινωνίας)
- ✓ EPC = Electronic Product Code
  - ➢ αντικατάσταση του bar code
  - ➢ Τρίτη έκδοση
  - ➢ IPv6
- ✓ ISO 18000-6C = EPCGen 2 Class 1 UHF, της EPCGlobal (τροπολογία στο πρότυπο 18000-6)

Εφαρμογές (1/8)

- Αντικατάσταση του bar code



- Αναρίθμητες!! Πρακτικά παντού…

Εφαρμογές (2/8)

- Logistics (Gas bottles, Beer barrels, Garbage cans, …)
- Industry (Tool identification,…)
- Entertainment (Casino Roulette Chips,…)
- Access systems (Door locks, Working time recording, clubs, Stadium, Theme parks, cars …)
- Payment systems (Cafeteria, restaurants,…)
- Public transportation (Bus, underground, ferries,…)
- National Identity and passport

- **Ό,τι μπορείτε να φανταστείτε!**

Εφαρμογές (3/8)

Auto Immobilizers

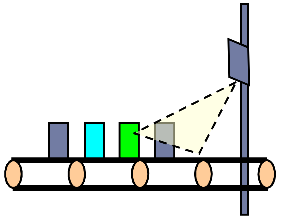
NEDAP true hands-free AVI

Automated Vehicle Id

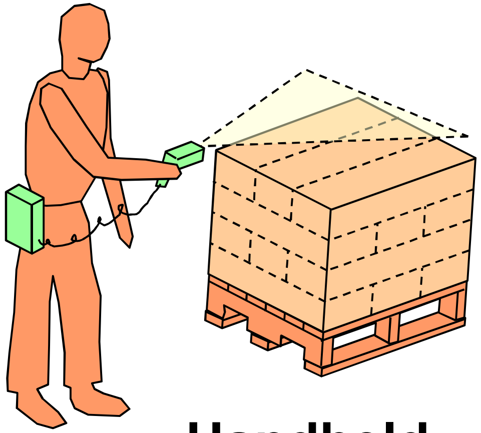
Access Control

Εφαρμογές (5/8)

Dock Door



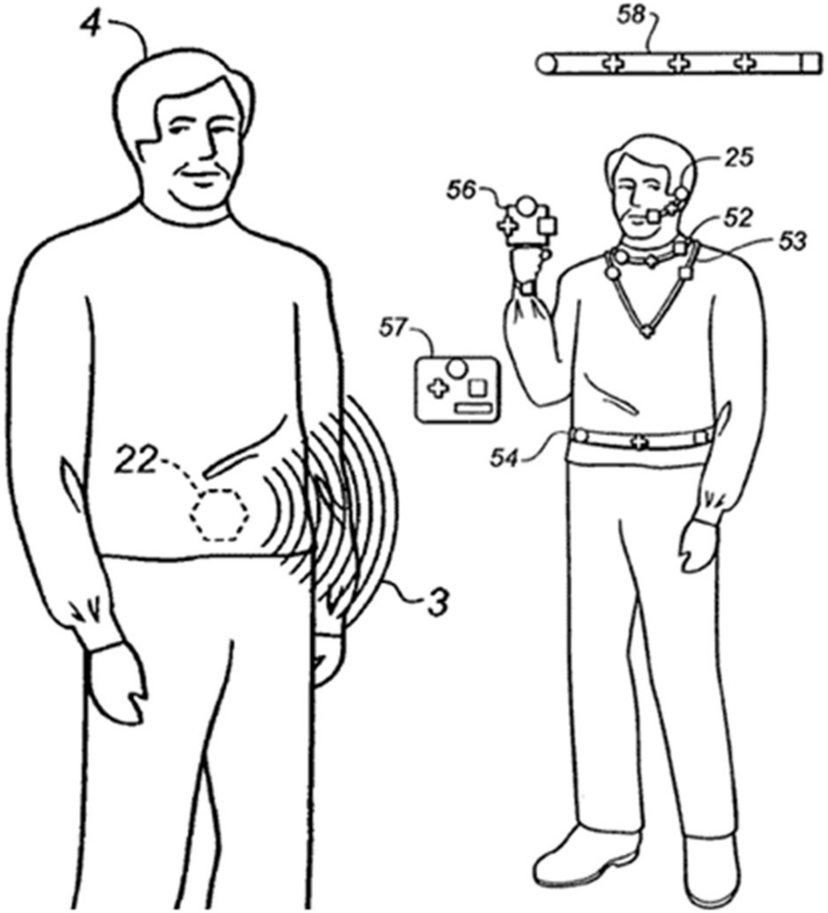
Conveyor Belt



Handheld

Smart Shelves

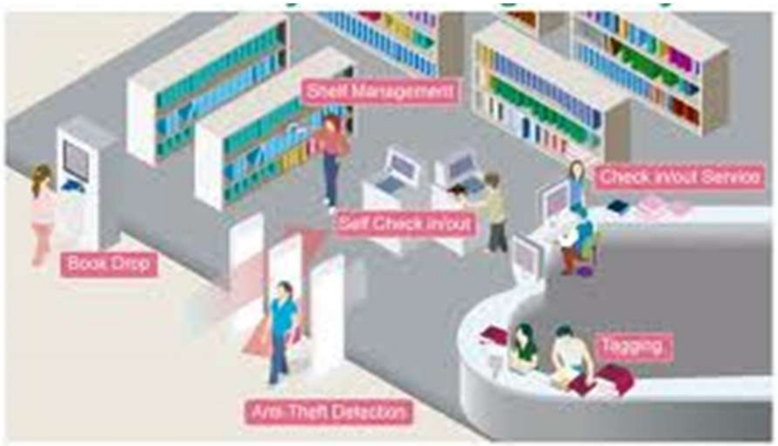
Εφαρμογές (6/8)

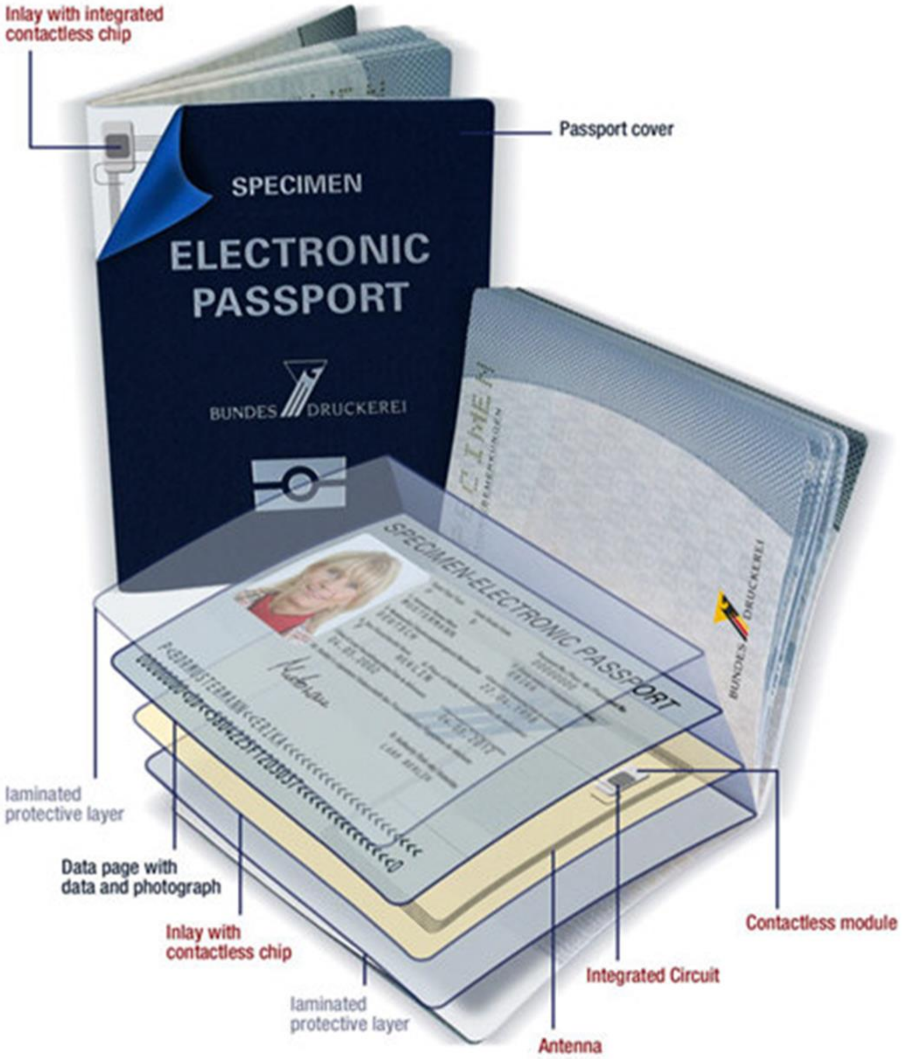


Forklift

Point of Sale

Εφαρμογές (7/8)





Inlay with integrated contactless chip
Passport cover
SPECIMEN
ELECTRONIC PASSPORT
BUNDES DRUCKEREI
SPECIMEN-ELECTRONIC PASSPORT
laminated protective layer
Data page with data and photograph
Inlay with contactless chip
laminated protective layer
Antenna
Integrated Circuit
Contactless module

Εφαρμογές (8/8)

Animal Tracking

Απειλές (1/4)

- Osaka της Ιαπωνίας και Doncaster του Ηνωμένου Βασιλείου
  - έχουν ραφτεί στις σχολικές στολές ετικέτες RFID που χρησιμοποιούνται για τον έλεγχο της θέσης των μαθητών
  - Στο άμεσο μέλλον, και πληροφορίες που αφορούν το μαθητή..

Απειλές (2/4)

"τον Ιανουάριο του 1999 το γραφείο του Πρωθυπουργού ανακοινώνει ότι τα μουσουλμανικά ζευγάρια θα εφοδιάζονται στο εξής με μικροτσίπ για να αποδεικνύουν το καθεστώς του γάμου τους, ώστε η ισλαμική αστυνομία, έχοντας στη διάθεσή της ηλεκτρονικά όργανα, να επαληθεύει αν δύο άτομα αντίθετου φύλλου που εντοπίζονται μαζί είναι παντρεμένα ή πρέπει να συλληφθούν για έγκλημα 'κάλους' ή αλλιώς για παράνομη 'κοντινή γειτνίαση'...

Απειλές (3/4)

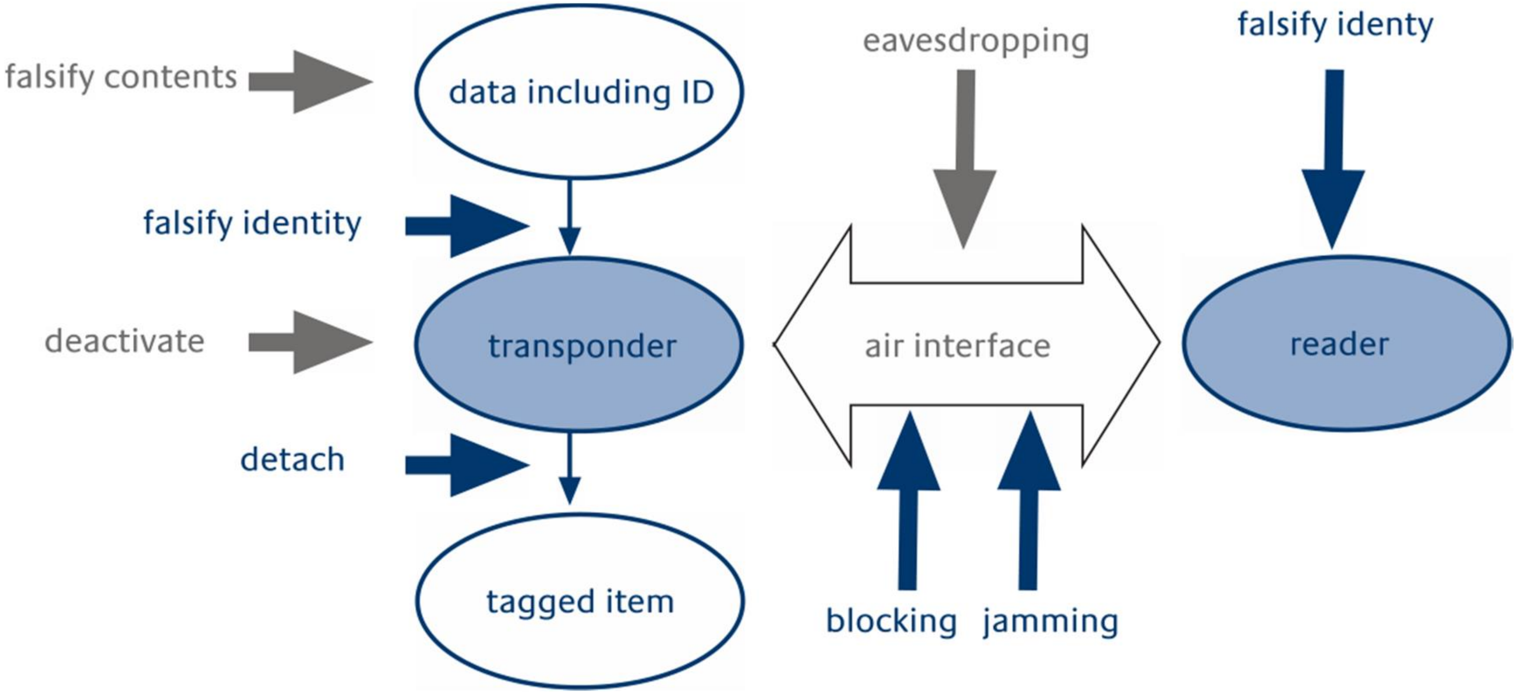
- Διαφάνεια Επικοινωνίας
  - Συνάθροιση ελεύθερης πληροφορίας
- Αποκάλυψη Δράσης
  - Έξυπνα ράφια
- Συσχέτιση
  - Συσχέτιση ατόμου με προϊόντα
- Ιχνηλάτηση
  - Ηλεκτρονικό ψίχουλο..

Απειλές (4/4)

- Αποκάλυψη Τοποθεσίας
- Αποκάλυψη Προτιμήσεων
  - ληστεία
- Αστερισμοί Ετικετών
  - Σύνολο αντικειμένων
- Αποκάλυψη Συναλλαγών

Επιθέσεις

BSI, 2005



Αντίμετρα

- Φυσικά Αντίμετρα
- Μη-κρυπτογραφικά Αντίμετρα
- Κρυπτογραφικά Αντίμετρα

Αντίμετρα

Φυσικά Αντίμετρα

- Κλωβός Faraday (Faraday Cage)
  - τοποθέτηση της ετικέτας σε μία θήκη κατασκευασμένη από μεταλλικές ίνες
- Μέθοδος των Ενεργών Παρεμβολών (Active Jamming)
  - χρήση συσκευής εκπομπής ραδιοσημάτων θορύβου
  - Παράνομο
  - Πρόβλημα για την ιδιωτικότητα….

Αντίμετρα

Μη-κρυπτογραφικά Αντίμετρα

- Απενεργοποίηση ετικέτας (Tag Deactivation): οι εντολές ’τερματισμός’ και ‘ύπνωση’
  - EPC Class I Gen 1: συνθηματικό των 8-bits
  - EPC Class I Gen 2: συνθηματικό των 32-bits
  - Sleep/wake command
  - Πρόβλημα γραμμή παραγωγής
  - Ελαχιστοποιεί τις εφαρμογές

Αντίμετρα

Μη-κρυπτογραφικά Αντίμετρα

- Η μέθοδος 'Blocker tag'
  - Χρήση ετικέτας για να δυσχεράνει τα πρωτόκολλα επίλυσης συγκρούσεων (αλγορίθμου Διάσχισης Δυαδικού Δένδρου ή Aloha)
  - Denial of Service
  - η σωστή λειτουργία της επαφίεται στο χρήστη
  - η πιθανότητα παρεμβολής στην επικοινωνία ετικετών οι οποίες ανήκουν σε άλλους χρήστες

Αντίμετρα

Μη-κρυπτογραφικά Αντίμετρα

- Ετικέτες με δυνατότητα ανάλυσης της ενέργειας της κεραίας
  - Ο επιτιθέμενος χρησιμοποιεί συνήθως αναγνώστη ο οποίος βρίσκεται σε αρκετή απόσταση από την ετικέτα RFID
  - από μόνη της δεν προσφέρει ασφάλεια

Αντίμετρα

Κρυπτογραφικά Αντίμετρα

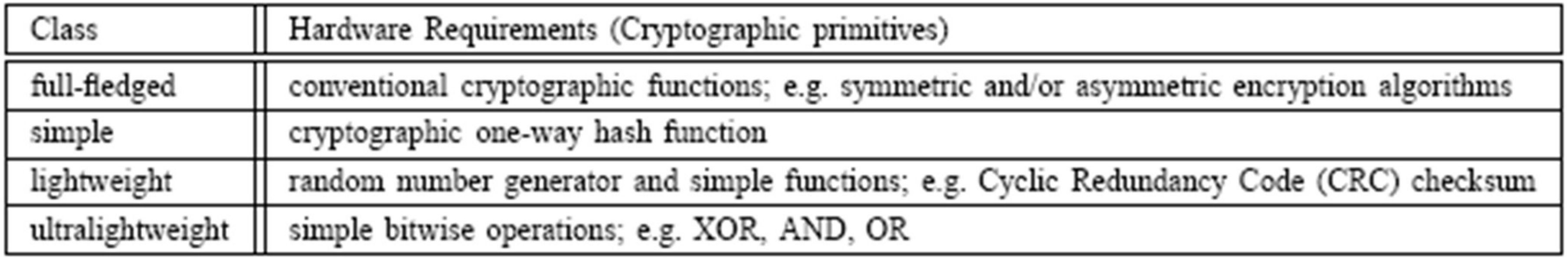
- Ιδανικά: υλοποίηση οποιοδήποτε «ασφαλούς» κρυπτογραφικού πρωτοκόλλου»
- Θέλω φτηνές ετικέτες…
- Περιορισμοί στην ενέργεια, στη μνήμη, στην υπολογιστική ισχύ, στο χώρο των κυκλωμάτων…

Αντίμετρα

Κρυπτογραφικά Αντίμετρα

- Πρακτικά: μόνο συμμετρική κρυπτογραφία (όχι πιστοποιητικά, δημόσια κλειδιά, zero-knowledge proofs…κλπ)
- Τι διαθέτουμε:
  - Πηγές τυχαιότητας
  - Βασικές πράξεις με bit
  - Hash functions (οριακά…)

Αντίμετρα



Class	Hardware Requirements (Cryptographic primitives)
full-fledged	conventional cryptographic functions; e.g. symmetric and/or asymmetric encryption algorithms
simple	cryptographic one-way hash function
lightweight	random number generator and simple functions; e.g. Cyclic Redundancy Code (CRC) checksum
ultralightweight	simple bitwise operations; e.g. XOR, AND, OR

Αντίμετρα

Απαιτήσεις Ασφάλειας

- Resistance to Tag impersonation
- Resistance to Reader impersonation
- Resistance to Denial of Service (DoS) attacks
- Indistinguishability
  - Forward security
  - Backward security

Αντίμετρα

Βασικές Λειτουργίες

1. Authentication
   - Tag
   - Reader
   - Mutual

2. Owner transfer

Αντίμετρα

Βασικές Λειτουργίες

3. Temporary Tag delegation
   - For practical reasons
   - Example airport

4. Secret update

5. Publicly known information update

(Too) Many papers

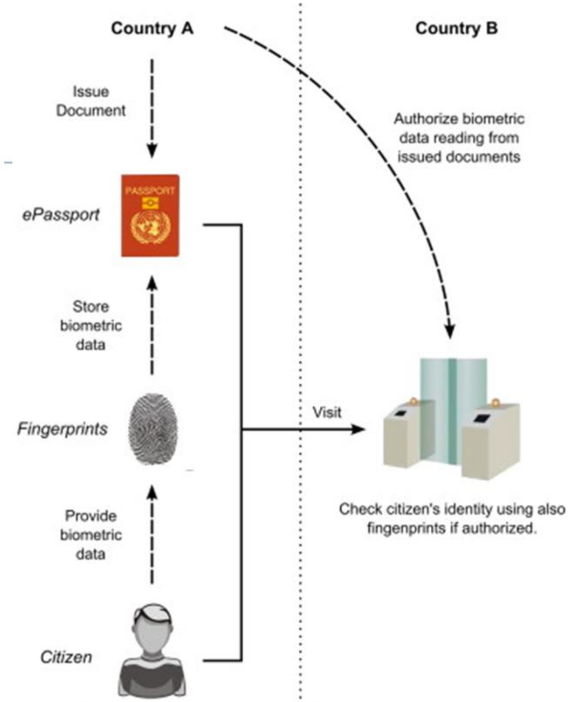
- Practically we cover everything (more than once)

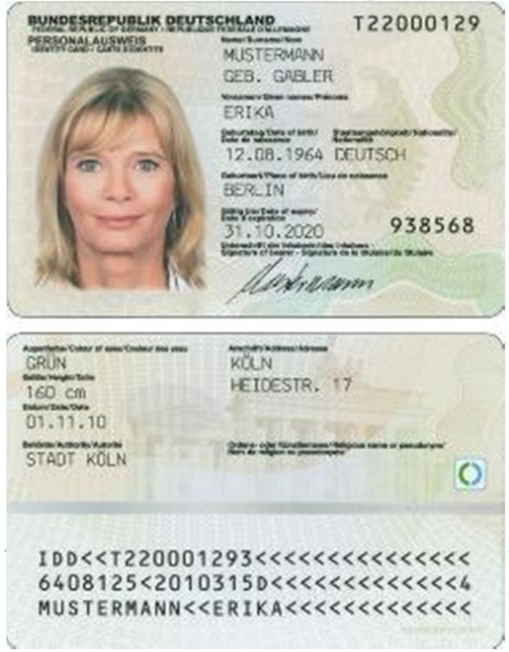
- Check the following

http://www.avoine.net/rfid/

Passports

- They use RFIDs
- Password Authenticated Connection Establishment (PACE)
- Ensures that the contactless RF chip in the electronic ID card cannot be read without direct access and the data exchanged with the reading device is transmitted encrypted.
- For reading devices with digital certificates for official use, such as boarder control, either the machine readable zone (MRZ) printed on the back of the electronic ID card or the six digits "Card Access Number" (CAN) printed on the front side is sufficient.


Country A
Country B
Issue Document
Authorize biometric data reading from issued documents
ePassport
PASSPORT
Store biometric data
Fingerprints
Visit
Provide biometric data
Check citizen's identity using also fingerprints if authorized.
Citizen


BUNDESREPUBLIK DEUTSCHLAND
PERSONALAUSWEIS
T22000129
MUSTERMANN
GEB. GABLER
ERIKA
12.08.1964 DEUTSCH
BERLIN
31.10.2020 938568

GRÜN
160 cm
01.11.10
STADT KÖLN
KÖLN
HEIDESTR. 17

```
IDD<<T220001293<<<<<<<<<<<<<<<
6408125<2010315D<<<<<<<<<<<<<4
MUSTERMANN<<ERIKA<<<<<<<<<<<<<
```

Lightweight Cryptography

LIGHTWEIGHT CRYPTOGRAPHY

- Cryptographic algorithms for constrained devices
  - Limited resources for cryptography
  - Internet of things

- Standardization efforts
  - ISO
  - NIST

ISO

- **Block ciphers**
- ISO/IEC 29192-2:2012 specifies two block ciphers suitable for lightweight cryptography:
- PRESENT: a lightweight block cipher with a block size of 64 bits and a key size of 80 or 128 bits;
- CLEFIA: a lightweight block cipher with a block size of 128 bits and a key size of 128, 192 or 256 bits.

- **Stream Ciphers**
- Enocoro: key size of 80 or 128 bits, based on a finite state machine and uses operations defined over the finite field GF(24) and GF(28).
- Trivium: key size of 80 bits, three nonlinear feedback registers, 288 bits of internal size.

ISO – HASH FUNCTIONS

- **ISO/IEC 29192-5:2016 specifies three hash-functions suitable for applications requiring lightweight cryptographic implementations.**

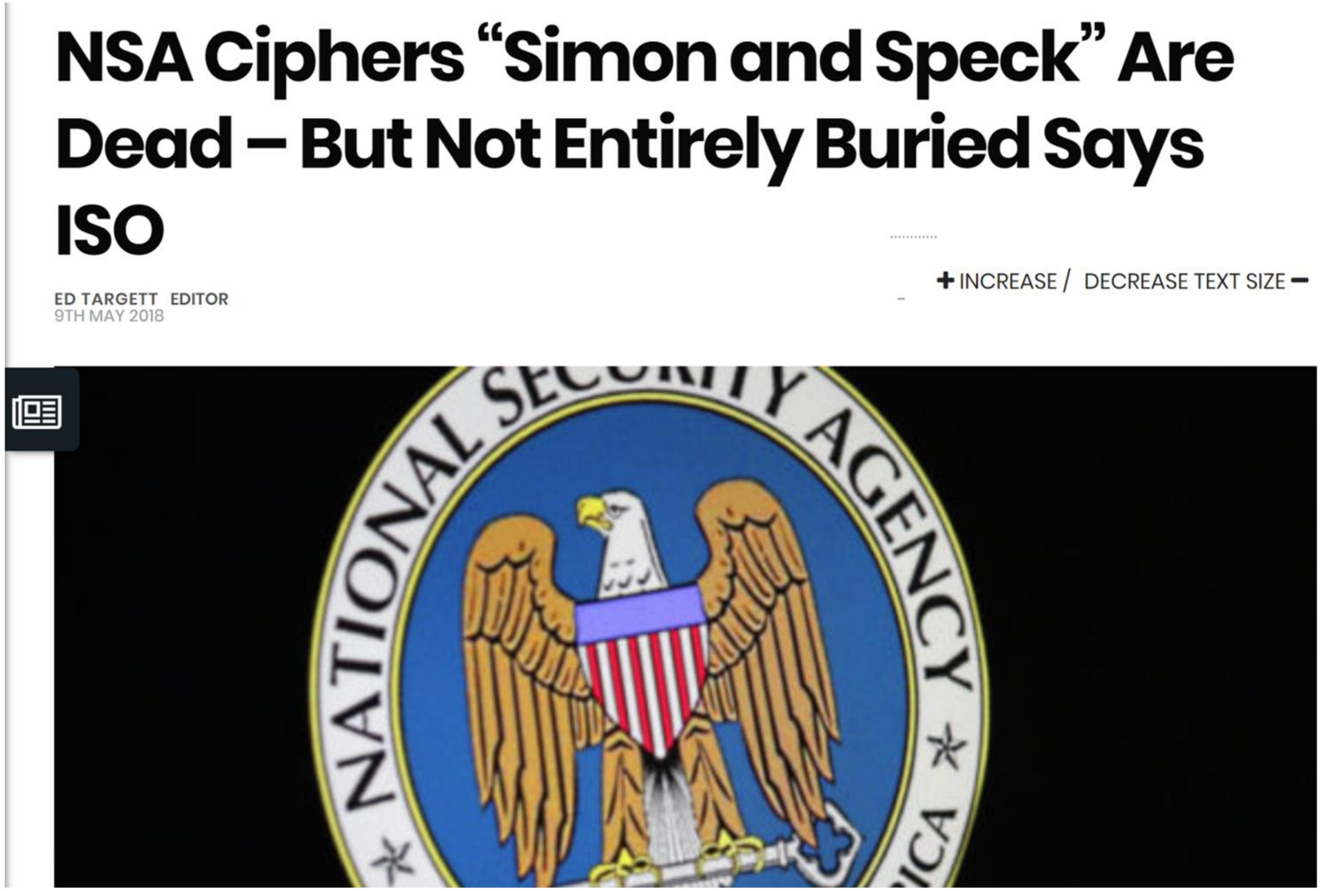
PHOTON: a lightweight hash-function with permutation sizes of 100, 144, 196, 256 and 288 bits computing hash-codes of length 80, 128, 160, 224, and 256 bits, respectively.

SPONGENT: a lightweight hash-function with permutation sizes of 88, 136, 176, 240 and 272 bits computing hash-codes of length 88, 128, 160, 224, and 256 bits, respectively.

Lesamnta-LW: a lightweight hash-function with permutation size 384 bits computing a hash-code of length 256 bits.

- **The requirements for lightweight cryptography are given in ISO/IEC 29192-1.**

NSA – SIMON AND SPECK



NSA Ciphers "Simon and Speck" Are Dead – But Not Entirely Buried Says ISO

ED TARGETT EDITOR
9TH MAY 2018

NIST LIGHTWEIGHT PROJECT

- https://csrc.nist.gov/Projects/Lightweight-Cryptography

- Scope:

- All cryptographic primitives and modes that are needed in constrained environments.
- Initial Focus: Symmetric Cryptography.

- Target functionality: Encryption, AE, hashing, key agreement, sensor/tag authentication.

- Target devices: ARM Cortex-M0 processors, Intel Quark SoC X1021, Atom E3826.

- Side channel resistance: In general, good to have.

NIST

- Target applications: Hardware encrypted data storage device, low-cost and low-consumption sensor data transmission, RAIN RFID tags for anti-counterfeiting solutions, IoTs, wearables, low power wireless sensor networks.

Modifications of well-analyzed designs: e.g., DESL, DESXL.

Old interesting algorithms: e.g., RC5, TEA, XTEA.

New dedicated algorithms: e.g., Skinny, Pride, Gimli, Simon, Speck, Simeck, Present, etc.

NIST PROJECT

- ✓ Early September 2018, NIST will publish FRN (Federal Register Notice) and the final Call for Submissions.
- ✓ December 2018, option for early submission for initial review.
- ✓ February 2019, deadline for submissions.

- ✓ NIST will publish the complete and proper submissions.
- ✓ Initial evaluation will be for approximately 12 months.

- ✓ Workshop will be held ten to twelve months after the submission deadline.
- ✓ Standardization within two to four years, after the public analysis starts

Questions?