Internet of Everything and Cultural Cyber Security Challenges

Dr. Dimitrios Patsos,

Chief Technology Officer,

ADACOM S.A.

A bit About Me

- RHUL M.Sc. In Information Security Graduate (Class of 2002),
- Ph.D. and Post-Doctoral Research in Incident Response at the University of Piraeus, GR (2004-2012),
- Literati Network's Award for Excellence (2011),
- Chief Technology Officer of ADACOM, Startup Advisor, Cyber Volunteer,
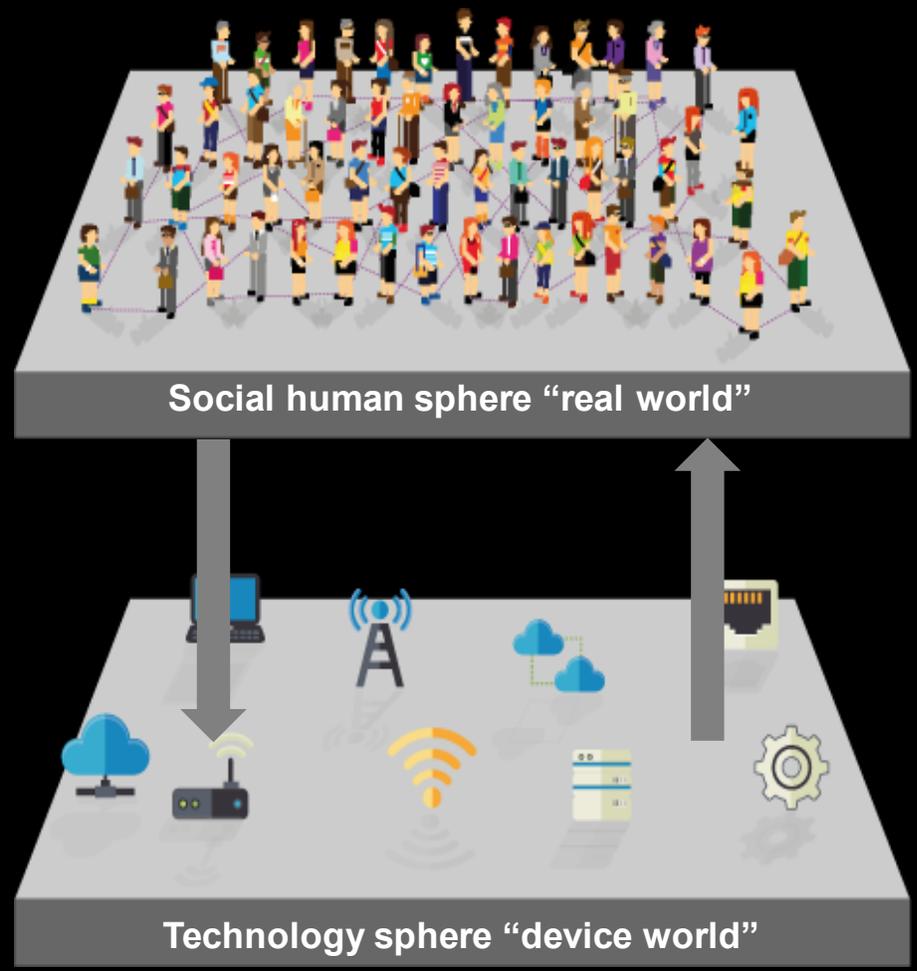- Managed and delivered projects in 28 countries.

Disclaimer:

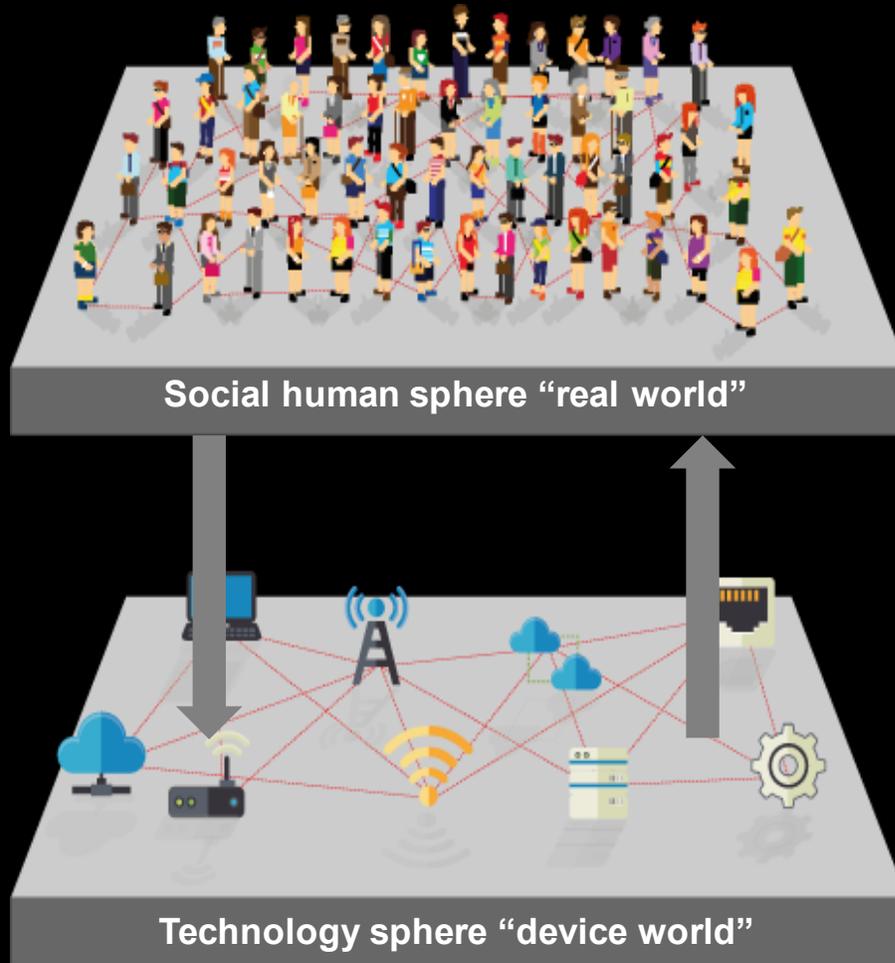**Opinions expressed herein are only of myself**

Constant Change

Evolving Threat

Evolving Technology

Evolving Compliance

Cost Complexity Risk

Evolving Socio-Economics

Evolving Business

ADACOM CYBER SECURITY

Source: iamthecavalry.org

The traditional Internet

Social human sphere "real world"

Technology sphere "device world"

Level of intelligence	Decision capabilities
Vision & Innovation	Strategic decisions
Wisdom	Tactical decisions
Knowledge	Operational decisions
Intelligence	
Information	Zero Decision Making Capability
Data	

2016 EY Research: Digital - Changing frame of the World

The "Internet of Things" (IoT)/ Industry 4.0

ADACOM
CYBER SECURITY

Level of intelligence

Decision capabilities

Vision & Innovation

Wisdom

Knowledge

Strategic decisions

Tactical decisions

Social human sphere "real world"

Intelligence

Information

Data

Operational Decisions

Technology sphere "device world"

The "Internet of Everything" (IoE)

Social human sphere "real world"

Technology sphere "device world"

Level of intelligence	Decision capabilities
Vision & Innovation	Strategic decisions
Wisdom	
Knowledge	Tactical decisions
Intelligence	
Information	Operational Decisions
Data	

ADACOM
CYBER SECURITY

Threat Evolution

Performance

Digital Assets

IP and Trade Secrets

Human Rights

Safety and Human Life

s/Software/Vulnerability

s/Network/Exposed

The Intelligent Car
(Almost) as Smart as You

The Internet of Things (IoT) is spurring the development of innovative technologies that are delivering new ways for cars to inform, entertain and assist drivers in a safe and comfortable way. Here's a look at how technology is changing daily commutes, both now and in the future.

Smart Traffic Environments

Smarter traffic management could **reduce vehicle wait time by 40%, and travel time by 26%.** Think smart street lights and roads that better manage traffic flow efficiency, and street signs that display relevant location-based data.

TODAY
Car owners and buyers want the latest technologies in their vehicles, and safety is key.

60% of roadway collisions could be avoided with half a second's warning

90% of collisions could be avoided with a full second's warning

Intelligent Maintenance

Local analytics could be applied to thousands of on-board sensors to flag abnormal events and take corrective action. The data may then be sent to automakers for deeper insight into trends across entire vehicle fleets.

TOMORROW
Car buyers will have new demands too!

69% said they would like to use a semi-autonomous lane-keeping system

63% would like to use car-to-car communications

63% would welcome a fatigue warning device in their vehicles

Data, Data Everywhere

152 million connected cars will be on the road by 2020, generating 11 petabytes of data annually. Intelligent cars could collect and analyze data from each other, the cloud and the transportation infrastructure to provide the right information, at the right time, and in the right way to keep drivers safe.
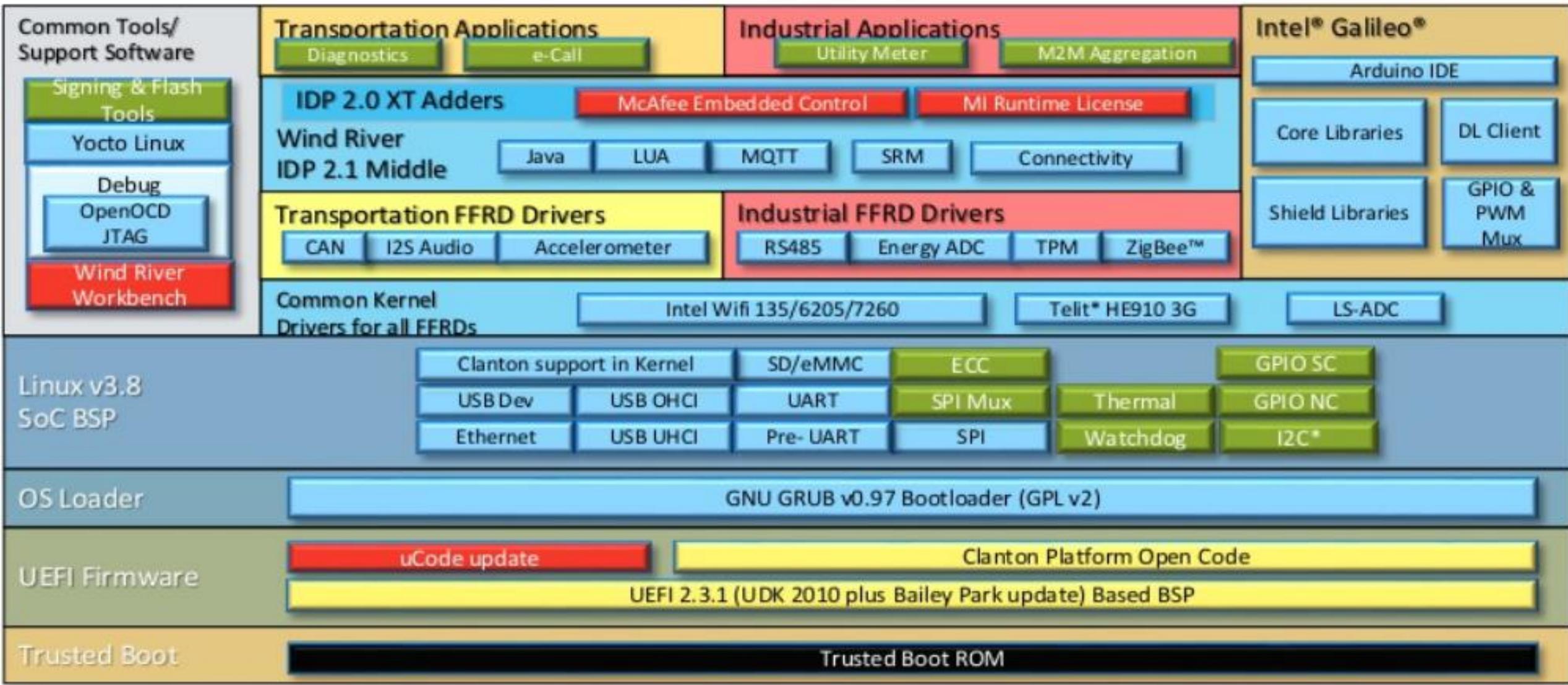
Vehicle-to-Vehicle Communication

Intelligent cars have the potential to **reduce 79% of crashes** by exchanging information about location, speed and direction. As a result, cars could then take proactive measures to keep traffic moving efficiently and safely.

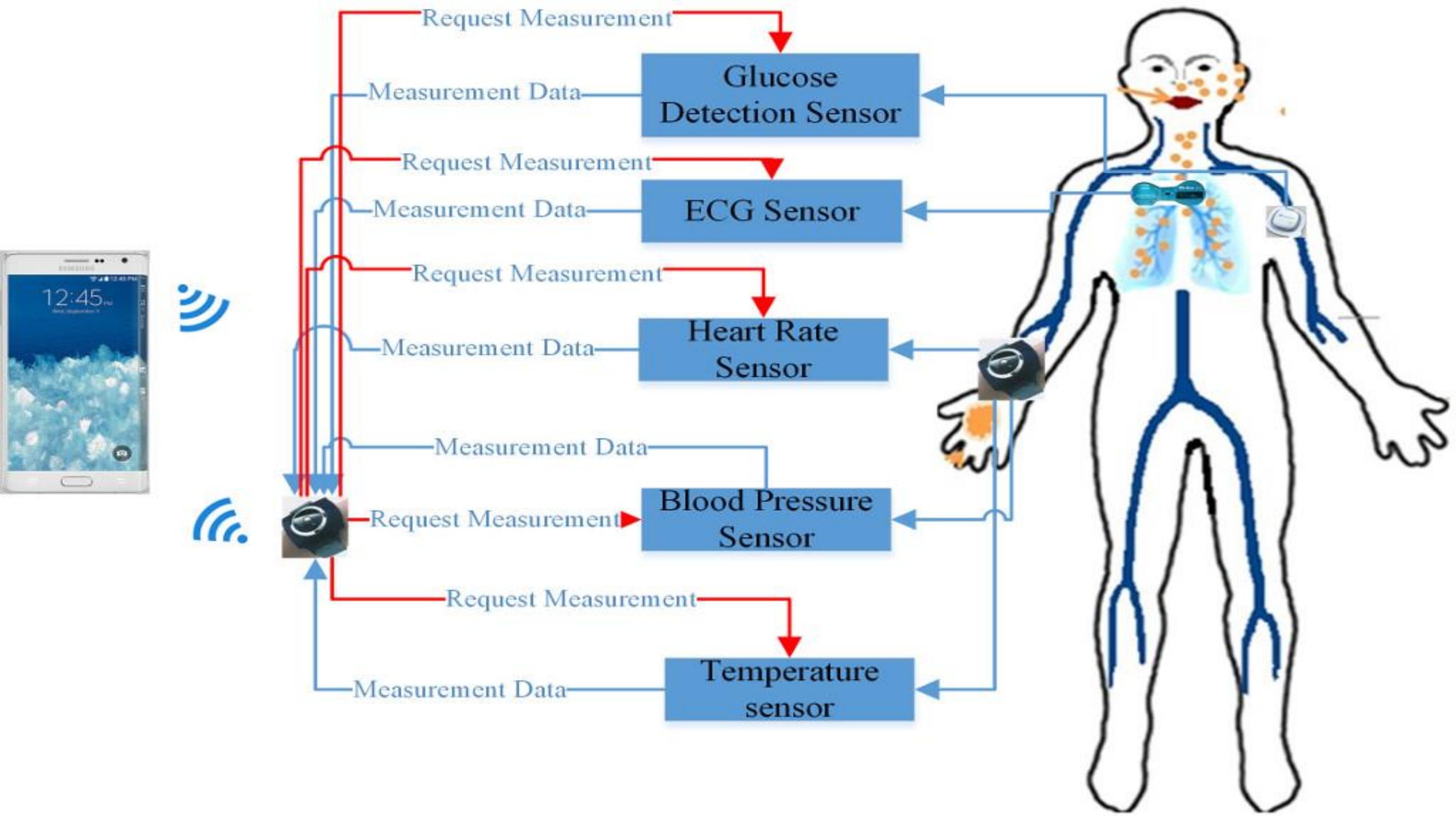(intel)

Indu/Transport Software Stack

Software License Types
- Dual BSD/GPL License
- GPL License
- BSD License
- Branded or Licensed Binary
- On Die Silicon based ROM

Common Tools/ Support Software
- Signing & Flash Tools
- Yocto Linux
- Debug
  - OpenOCD JTAG
- Wind River Workbench

Transportation Applications
- Diagnostics
- e-Call

Industrial Applications
- Utility Meter
- M2M Aggregation

Intel® Galileo®
- Arduino IDE
- Core Libraries
- DL Client
- Shield Libraries
- GPIO & PWM Mux

IDP 2.0 XT Adders
- McAfee Embedded Control
- MI Runtime License

Wind River IDP 2.1 Middle
- Java
- LUA
- MQTT
- SRM
- Connectivity

Transportation FFRD Drivers
- CAN
- I2S Audio
- Accelerometer

Industrial FFRD Drivers
- RS485
- Energy ADC
- TPM
- ZigBee™

Common Kernel Drivers for all FFRDs
- Intel Wifi 135/6205/7260
- Telit® HE910 3G
- LS-ADC

Linux v3.8 SoC BSP
- Clanton support in Kernel
- SD/eMMC
- ECC
- GPIO SC
- USB Dev
- USB OHCI
- UART
- SPI Mux
- Thermal
- GPIO NC
- Ethernet
- USB UHCI
- Pre- UART
- SPI
- Watchdog
- I2C*

OS Loader
- GNU GRUB v0.97 Bootloader (GPL v2)

UEFI Firmware
- uCode update
- Clanton Platform Open Code
- UEFI 2.3.1 (UDK 2010 plus Bailey Park update) Based BSP

Trusted Boot
- Trusted Boot ROM

May not include all software required to enable 3rd party devices or OS for FFRD support (e.g. WR, McAfee, IMC components).
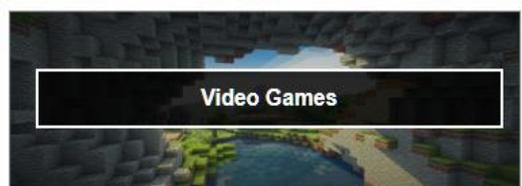
Request Measurement

Measurement Data

Glucose Detection Sensor

Request Measurement

Measurement Data

ECG Sensor

Request Measurement

Measurement Data

Heart Rate Sensor

Measurement Data

Blood Pressure Sensor

Request Measurement

Request Measurement

Measurement Data

Temperature sensor

12:45

Next-generation vehicle center(operation center)

Battery storage systems

Wind farm

Environment-friendly design buildings

Regional EMS (Control center)

Smart Buildings linked through Regional EMS

MegaSolar

Intelligent Transportation System (ITS)

Smart House

Biomass fuels

Multi-energy station

EV car sharing

EV car sharing

Smart House

Smart House

Electric bus

Solar panel

Offshore wind farm

Multi-energy station

Small / Medium-scale Smart Buildings

What We Can Do

A TALE OF TWO QUAKES

MODIFIED MERCALI INTENSITY SCALE

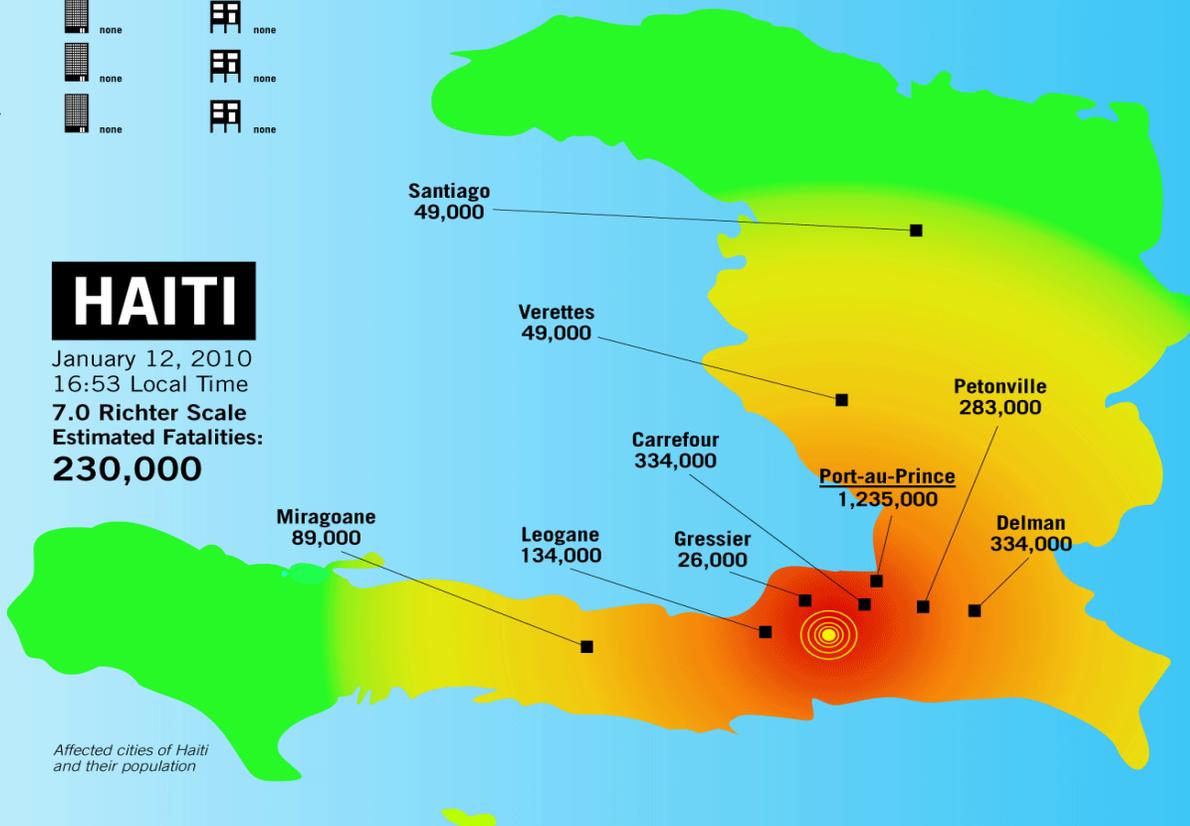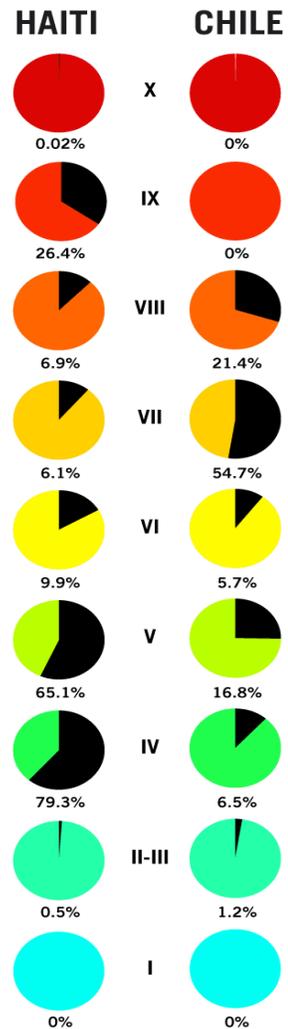| Shaking		Structural Damage to Resistant Buildings	Structural Damage to Vulnerable Buildings
X	EXTREME	very heavy	very heavy
IX	VIOLENT	heavy	heavy
VIII	SEVERE	moderate/heavy	heavy
VII	VERY STRONG	moderate	moderate/heavy
VI	STRONG	light	moderate
V	MODERATE	very light	light
IV	LIGHT	none	none
II-III	WEAK	none	none
I	NOT FELT	none	none

In the span of two months, two massive earthquakes struck in Haiti and Chile. But while the temblor in Chile registered much higher on the Richter scale, the loss of life and damage in Haiti was far more severe. Why is that? Chile—which has experienced serious earthquakes in recent decades—has a robust building code to make sure buildings are earthquake resistant; Haiti has no code to speak of. And a look at both quake's scores on the Modified Mercali Intensity Scale—which is used to measure how earthquakes affect those experiencing them—shows that while Chile's quake may have been stronger overall, Haiti had a larger population and more urban areas hit by more intense and damaging shaking.

POPULATION AFFECTED (percentage)

HAITI		CHILE
0.02%	X	0%
26.4%	IX	0%
6.9%	VIII	21.4%
6.1%	VII	54.7%
9.9%	VI	5.7%
65.1%	V	16.8%
79.3%	IV	6.5%
0.5%	II-III	1.2%
0%	I	0%

SOURCE U.S. Geological Survey
A collaboration between GOOD and karlssonwilker

HAITI

January 12, 2010
16:53 Local Time
7.0 Richter Scale
Estimated Fatalities:
230,000

Santiago 49,000
Verettes 49,000
Petonville 283,000
Carrefour 334,000
Port-au-Prince 1,235,000
Delman 334,000
Miragoane 89,000
Leogane 134,000
Gressier 26,000

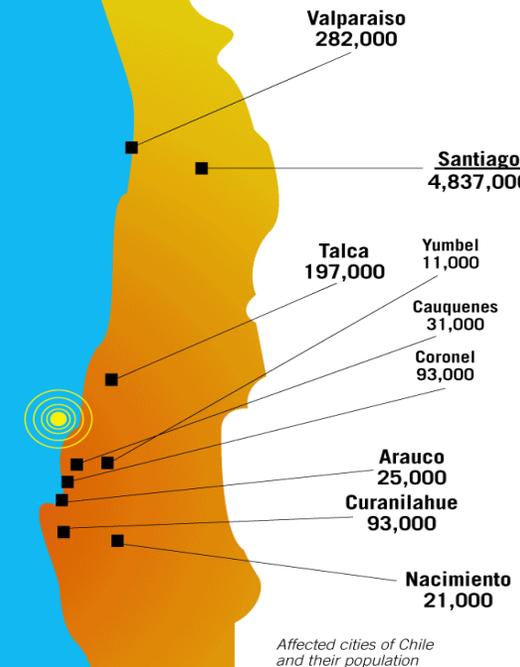*Affected cities of Haiti and their population*

CHILE

February 27, 2010
03:34 Local Time
8.8 Richter Scale
Estimated Fatalities:
279

Valparaiso 282,000
Santiago 4,837,000
Talca 197,000
Yumbel 11,000
Cauquenes 31,000
Coronel 93,000
Arauco 25,000
Curanilahue 93,000
Nacimiento 21,000

Affected cities of Chile and their population

IoT Security happens on four different levels
Device, Communications, Cloud, and Lifecycle Management

IoT Solution elements

User | Device(s) | Gateway | Connection | Cloud | Applications

Cloud: Analytics, Platform

Applications: CRM, ERP, SCM, PLM

Security components

2.1 Secure Device (Hardware)

- 2.1.1 Physical security
- 2.1.2 Data at rest
- 2.1.3 Chip security
- 2.1.4 Secure booting
- 2.1.5 Device authentication
- 2.1.6 Device identity

2.2 Secure Communications

- 2.2.1 Access control
- 2.2.2 Firewall / IPS / IDS
- 2.2.3 End-2-End encryption

2.3 Secure Cloud

- 2.3.1 Data at rest
- 2.3.2 Platform & application integrity verification
- 2.3.3 Unified threat management

2.4 Secure Lifecycle Management

- 2.4.1 Risk assessment
- 2.4.2 Policies & auditing
- 2.4.3 Activity monitoring
- 2.4.4 Updates & patches
- 2.4.5 Vendor control
- 2.4.6 User awareness assessment
- 2.4.7 Secure decommissioning

Source: IoT Analytics
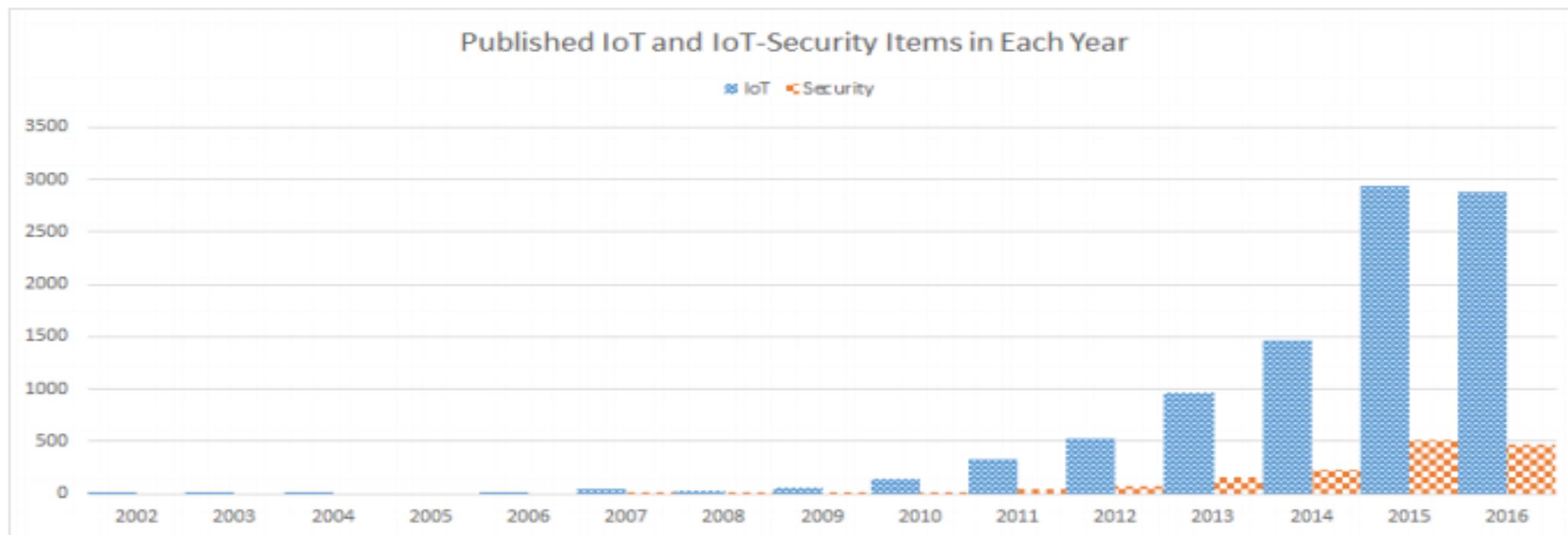
Research World

Fig. 3. Number of publications for Internet-of-Things and Internet-of-Things Security related articles. As of December 2016 [14].

Available Research Data

Table 2
A brief summary of the characteristics of IoT frameworks.

IoT Framework Company	SmartThings Samsung	AWS IoT Amazon	Calvin Ericsson	Brillo/Weave Google	Kura Eclipse	ARM Mbed ARM	HomeKit Apple	Azure IoT Microsoft
Architecture Components	+ Cloud Backend + Smart Devices + SmartThings Hub + SmartThings Home App.	+ Cloud services + Smart devices + Device Gateway + Rules Engine + Registry Unit + Device Shadow	+ Actors: smart embedded devices, smart phones, cloud, servers. + Flow based computing	+ physical devices with Brillo/Android as OS + OTA servers + Cloud Services	Java/OSGi based.	+ Mbed OS + Mbed device Connector + mbed Cloud + mbed Client + ARM Cortex-M MCU	+ Home Conf. D.B. + HAP + HomeKit API + HomeKit-enabled devices	+ Cloud backend + Cloud Services + Cloud Gateway + Smart Devices
Programming Language	Groovy	Any language can use Restful API	+ CalvinScript + Python + others	Any programming language can talk through Weave SDK	Java	+ C++ for device side + multiple for user side	+ Swift + Objective-C	+ C + Node.js + Java + Python + .Net
Hardware Dependencies	+ SmartThings Hub	+ (optionally) AWS hub	NONE	NONE	NONE	+ ARM MCU	+ (optionally) Apple TV + (optionally) HomeKit bridge	+ Azure IoT Hub
Software Dependencies	The Home app.	NONE	NONE	+ Brillo OS + Weave SDK	+ JVM 7.0 or later	+ mbed OS + mbed Client	+ iOS + watchOS + tvOS + HomeKit app.	NONE
Compatible Hardware	All MCUs that support compatible communication protocols.	Any MCU can be configured using C, arduino platforms, or Node.js	Any MCU with communication capabilities	Any MCU with memory = 35 MB	Linux based devices that support JVM 7.0+	+ 32 bits ARM Cortex-M MCUs	+ All devices that support Apple's MFi licensed technology + All devices can connect to HomeKit bridge	All devices that have 64KB RAM and RTC and support SHA-256
Supported Application Protocols	+ HTTP	+ HTTP + WebSockets + MQTT	+ HTTP	+ HTTP + XMPP	+ MQTT + CoAP	+ CoAP + HTTP + MQTT + others	+ HTTP	+ HTTP + MQTT + AMQP
Supported Communication Protocols	+ ZigBee + Z-wave + WiFi + BLE	All	+ WiFi + i2c + BT + others	+ WiFi + BLE + Ethernet	+ WiFi + BLE	All	+ WiFi + BLE + ZigBee + Z-wave	+ WiFi + ZigBee + Z-wave + others
Security								
Authentication	+ OAuth/ OAuth2 protocol.	+ X.509 Certificates + AWS IAM + AWS Cognito	+ X.509 Certificates + Sim-based Identity	+ OAuth 2.0 + TEE	+ secure sockets	+ X.509 Certificates + other standards (mbed TLS)	+ Ed25519 public/private key signature + Curve25519 keys	+ X.509 certificates + HMAC-SHA256 signature
Access Control	+ Capability mode/ Rules for granting permissions + Sandboxing Technique	+ IAM Roles + Rules Engine + Sandboxing	+ Configuration files	+ SELinux + ACL + Sandboxing: UID&GID	+ Security Manager + Runtime Policies	+ uVisor + MPU	+ Sandboxing + iOS security architecture + ASLR Technique	+ Azure Active Directory Policies + Access control rules of Azure IoT hub
Communication	+ SSL/TLS	+ SSL/ TLS	+ SSL/ TLS	+ SSL/TLS	+ SSL/TLS	+mbed TLS	+ TLS/DTLS + Perfect Forward Secrecy	+ TLS/DTLS
Cryptography	+ 128-bits AES protocol.	+ 128-bits AES + other primitives	+ ECC protocol	Full disk encryption supported by Linux kernel	Multiple cryptography primitives	+ mbed TLS + Hardware Crypto.	+ 256-bits AES + many others	Multiple cryptography primitives

Fire Safety

1. MINIMISE THE POTENTIAL FOR FIRES

2. MINIMISE THE DANGERS TO STAFF

3. MAINTENANCE OF FIRE PRECAUTIONS

4. FIRE ACTIONS

5. FIRE EXTINGUISHERS

6. CONTACTING THE EMERGENCY SERVICES

FIRE BREAK GLASS PRESS HERE

Fire extinguisher

Powder

Water

Foam

CO_2

Foam

FIRE EXTINGUISHER

Fire precaution keep clear

In case of FIRE

FIRE

1. SOUND THE ALARM
2. CALL 911
3. USE EXTINGUISHER
4. EXIT BUILDING USING STAIRS
5. CLOSE DOORS BEHIND YOU
6. ... add what fits best your situation

ADACOM
CYBER SECURITY

ATTACK ORIGINS

#	COUNTRY
347	United States
272	China
30	Ukraine
17	Czech Republic
14	Netherlands
13	South Korea
13	Germany
11	Spain
8	Romania
7	Moldova

ATTACK TYPES

#	PORT	SERVICE TYPE
277	25	○ smtp
147	23	○ telnet
145	8080	○ http-alt
55	5900	○ rfb
42	3389	○ ms-wbt-server
19	50864	○ xsan-filesystem
17	445	○ microsoft-ds
15	3306	○ mysql
11	138	○ netbios-dgm
10	1433	○ ms-sql-s

ATTACK TARGETS

#	COUNTRY
497	United States
207	United Arab Emirates
42	Spain
22	Italy
15	Singapore
11	Norway
7	Saudi Arabia
5	Thailand
5	United Kingdom
5	France

LIVE ATTACKS

TIMESTAMP	ATTACKER	ATTACKER IP	ATTACKER GEO	TARGET GEO	ATTACK TYPE	PORT
16:28:48.575	Telenet Operaties N.V.	84.193.112.92	Hasselt, BE	De Kalb Junction..	telnet	23
16:28:48.342	Chinanet Hubei Province Network	116.211.0.90	Wuhan, CN	Ubon Ratchatha...	ndl-aas	3128
16:28:48.163	Vodafone Turkey	188.38.108.69	Istanbul, TR	Lynnwood, US	telnet	23
16:28:47.956	Sprint S.A.	188.68.224.62	Olsztyn, PL	Dubai, AE	http-alt	8080
16:28:47.755	Gestín De Direccionamiento Uninet	201.122.217.24	Tlaquiltenango, ...	Dubai, AE	microsoft-ds	445
16:28:47.570	Microsoft Corporation	157.56.110.245	Redmond, US	De Kalb Junction..	smtp	25
16:28:47.226	Microsoft Corporation	207.46.100.254	Redmond, US	De Kalb Junction..	smtp	25
16:28:46.974	Microsoft Corporation	157.56.110.249	Redmond, US	De Kalb Junction..	smtp	25
16:28:46.607	Microsoft Corporation	207.46.100.254	Redmond, US	De Kalb Junction..	smtp	25
16:28:46.421	Chinanet Yunnan Province Network	182.243.33.3	Kunming, CN	Lynnwood, US	xsan-filesystem	50864

SECURING
SMART
CITIES

OTA
Online Trust Alliance

I Am The Cavalry

OWASP

BuildItSecure.ly

Thanks for Watching !
dpatsos@adacom.com

United Kingdom

London

16 Great Queen St.,

WC2B5AH Covent Garden

+44 203 126 4590

Greece

Athens

25 Kreontos St.,

104 42 Athens

+30 210 5193740

Israel

Tel Aviv

16th Ha' Melecha St.

48091 Rosh Ha'Ayin

+972 74 7019424