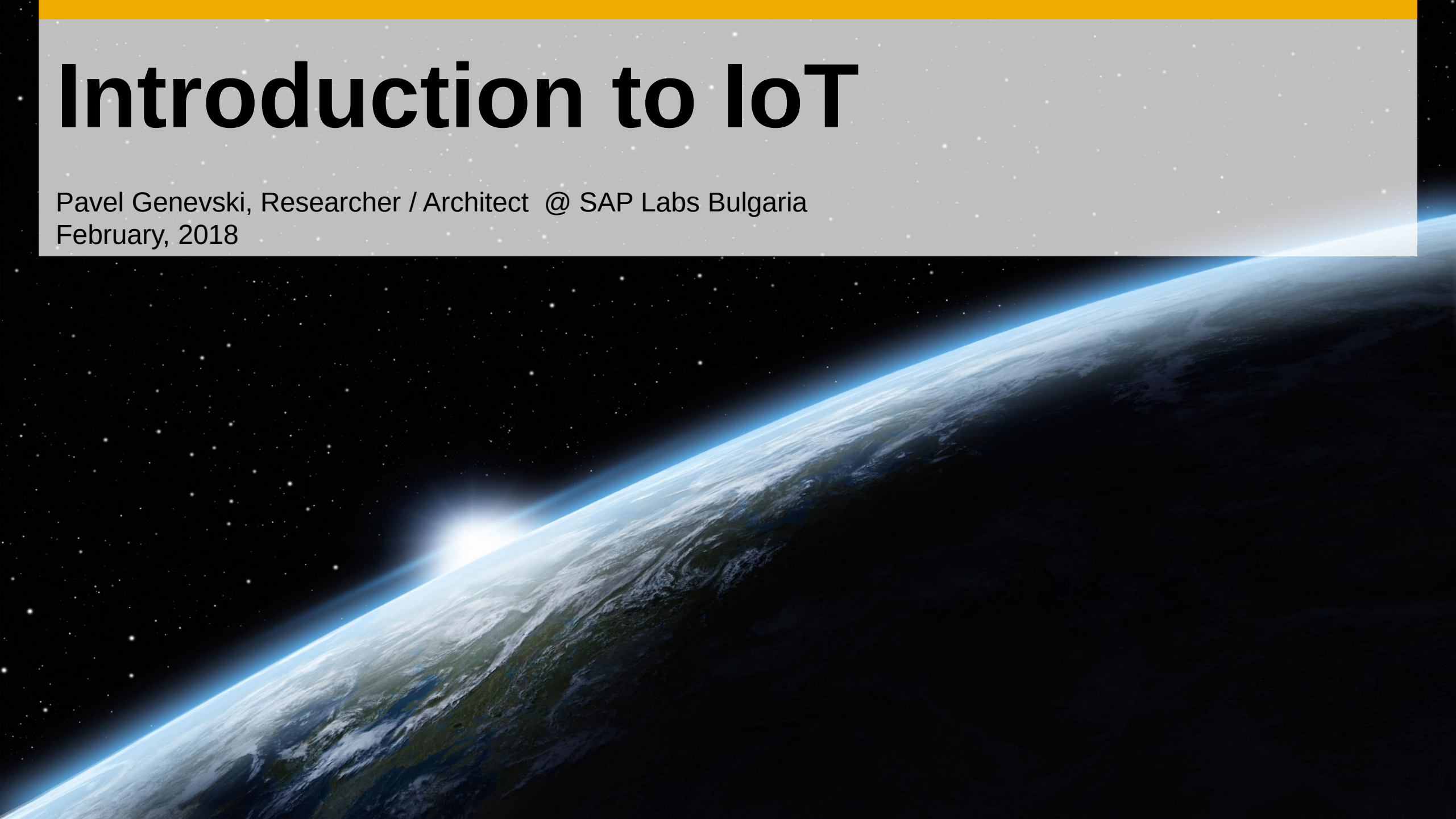
Introduction to IoT

Pavel Genevski, Researcher / Architect @ SAP Labs Bulgaria
February, 2018



Teachers

SAP Labs

Pavel Genevski

Vladimir Savchenko

Hristo Kirilov

Vladimir Nachev

FMI

Trayan Iliev

Administrative Q&A

Кога?

Четвъртък от 17:00 до 21:00

Къде?

Зала 320

Как да минем?

Защита на групов проект + quizzes / индивидуални впечатления

Let’s get started!

Over 20 billion connected devices

Consumer market: ~$546B

1.4B smartphones (flat*)

157M tablets (7% decline)

21M smartwatches (flat*)

Industrial market: ~$868B

Factories (Industry 4.0)

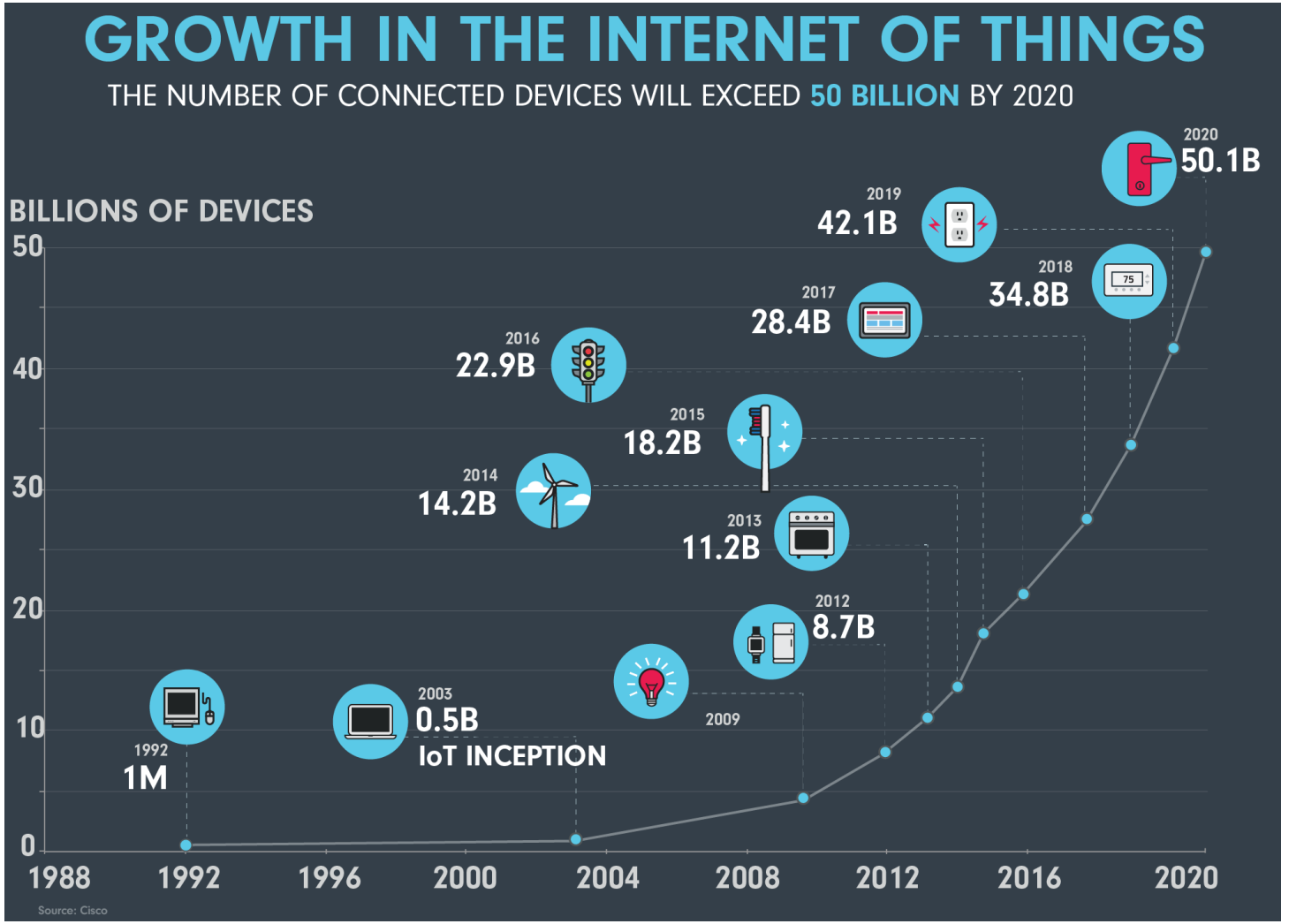
Logistics

Meters

Trains

Cities

….



Source: https://www.ncta.com/sites/prod/files/GROWTH_IOT-091516-IF-2000w.png

How did we get here?

Hardware is now …

Cheaper

Smaller

More connected

Less power hungry

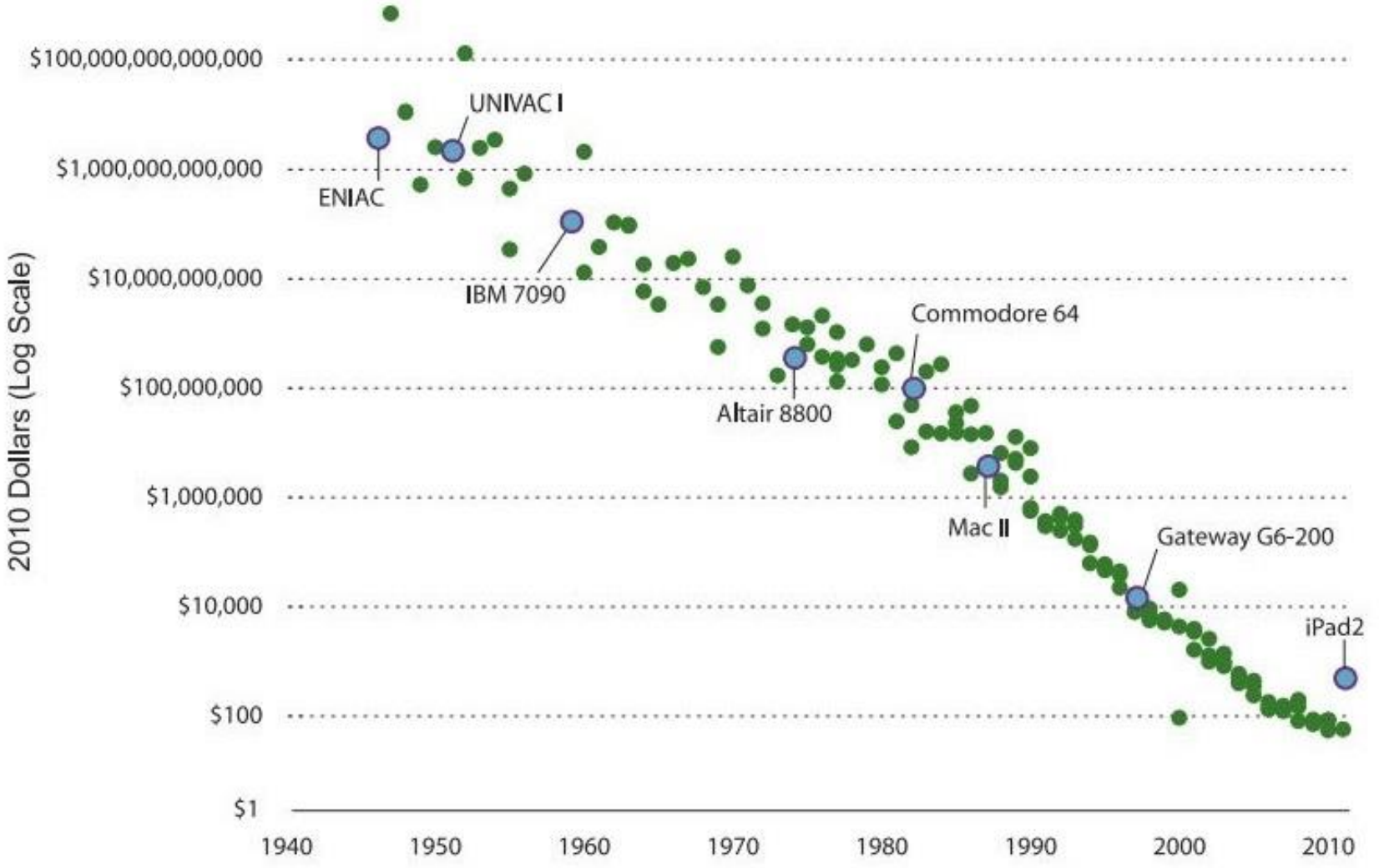
Easier to develop

Ecosystem

More knowledge

More opportunities

More investment



Source: http://www.hamiltonproject.org/ee-ce-image/made/assets/img/uploads/charts/cost_of_computing_power_equal_to_an_ipad2_1017_685_80.jpg

What is IoT?

Physical

Sensors, Actuators

Connected

WiFi, Bluetooth, Cellular, LPWAN …

Programmable

Arduino, C/C++, Python, Java, Assembly ..

(Atmel, **Espressif**, TI, Microchip, MIPS, ARM …)

```
/**
 * Test led: Arduino uno
 */

#include "Arduino.h"

int redPin = 9;
int greenPin = 10;
int bluePin = 11;

void setColor(int red, int green, int blue)
{
    red = 255 - red;
    green = 255 - green;
    blue = 255 - blue;
}

void setup() {
  Serial.begin(9600);
  Serial.println("Setup");
  pinMode(redPin, OUTPUT);
  pinMode(greenPin, OUTPUT);
  pinMode(bluePin, OUTPUT);
}
```

Industrial vs Consumer IoT

Industrial IoT

***Drivers**:* cost and risk reduction, business agility, informed decision making

***Challenges**:* security, compliance, compatibility, reliability, connectivity, support …

Consumer IoT

Drivers: coolness, convenience, health, some cost reduction

Challenges: UX, hype vs value, time to market, some privacy and security

Source:http://www.clipartpanda.com/clipart_images/stacks-of-money-clipart-1-57831954

Industrial IoT examples

Predictive maintenance & Remote management

Solar & wind power, pipelines, bridges, facilities, vehicles, crops …

Smart utilities (meters)

Remote and continuous metering of water, electricity, gas …

Source: http://www.metering.com/wp-content/uploads/2016/05/smart-meters-768x510.jpg

Industrial IoT examples contd.

Smart buildings

HVAC, lighting, security & access control, safety monitoring, indoor positioning …

Source:http://blueapp.io/wp-content/uploads/2016/08/How-IoT-optimize-building-performance-with-in-minimal-operational-cost.jpg

Smart City

Pollution, traffic, controlling, services …

Source: http://www.libelium.com/libelium-images/generico2/sensor_polvo-490.png

Consumer IoT examples

Personal productivity & fashion

Smartphones, smartwatches …

Home Automation

Smart locks, Bulbs, Smart TVs, Baby monitors*…*

Source: https://42xaiz2iny9m45jqzf36ofk2-wpengine.netdna-ssl.com/wp-content/uploads/2014/08/Front.jpg
https://c.slashgear.com/wp-content/uploads/2011/12/NO-4.jpg

Consumer IoT examples contd.

Sports & Health

Fitness & health trackers

Professional sport gadgets

Connected cars …

Predictive maintenance, accident reaction, theft protection …

Source: https://tctechcrunch2011.files.wordpress.com/2014/11/victoria-secret-heart-rate-bra.jpg?w=738 https://cochlearimplanthelp.files.wordpress.com/2015/04/mi-band.jpg, http://d3dc23s9xy125m.cloudfront.net/images/baseball/baseball_setup_connect@2x.pngTesla

What?

Course assignment

Objectives

Challenge yourself. No idea is too brave!

Try to make something useful

Learn new things

Examples

Smart beehive, A/C monitoring

Smart home / company / city

You name it …☺

?

Source: https://www.smartbin.com/markets/level-sensor-general-waste-recyclables/, LG air conditioners

How?

IoT development platforms

Android & iOS

Phones, wearables, TVs …

Linux

Raspberry PI, Beaglebone …

RTOS

FreeRTOS, Nucleus …

Bare metal

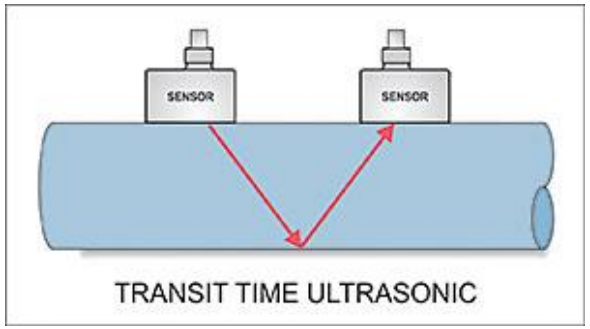
Vendor SDKs: Espressif, NXP, TI, Atmel, Microchip …

Arduino: Atmel, **ESP8266 (we will use this one)**

Sensors

So many sensors …

- Touch, movement, compass, acceleration, video, sound
- Temperature, humidity/moisture, light / infrared
- Pressure, gas detection,
- Force (tenso), proximity, motion
- Liquid level, flow, magnetic field (hall), radiation
- Fingerpring, heart rate …



Source: http://www.imagesco.com/geiger/buying-a-geiger-counter-pg3.html, http://www.greyline.com/twotechnologies.htm, http://www.noshok.com/force_2351_series.shtml

Sensors characteristics

Functional

Range

Accuracy

Precision (repeatability, noise)

Resolution & Sensitivity

Speed

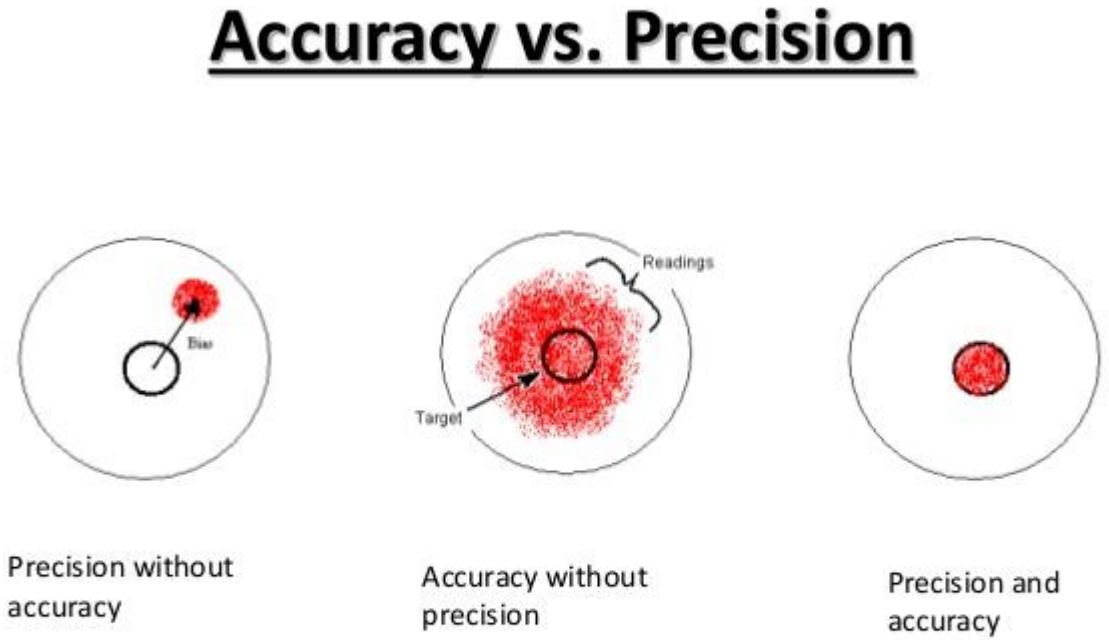
Non-functional

Longevity & Reliability (MTBF, triplication)

Power consumption

Price

Op. environment: combustive, corrosive, military



Source: https://www.slideshare.net/akashmaurya24/shashank-soni-sensors-presentation

Connectivity (media access)

Long range

LoRaWAN, Sigfox, 6LoWPAN (868MHz), 3G/GPRS

Medium range

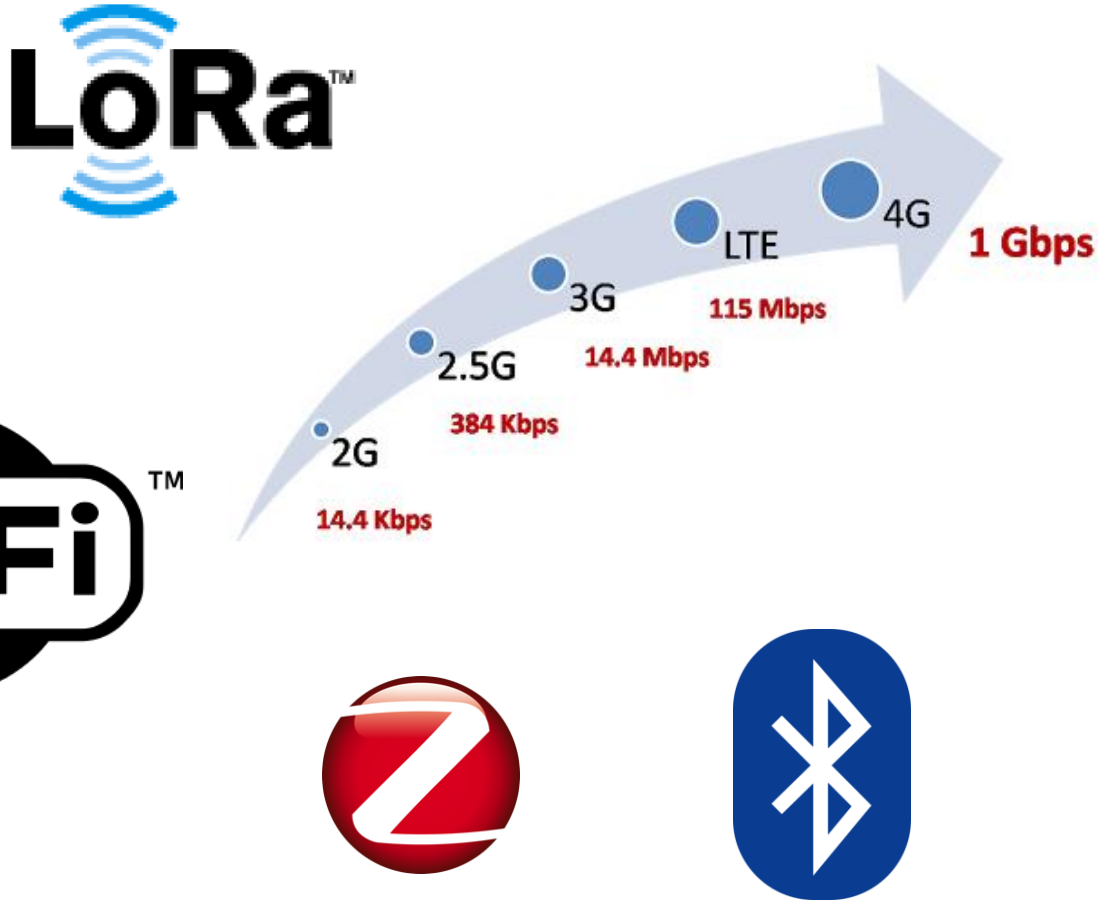
ZigBee, WiFi

Short range

Bluetooth 4.0/BLE, NFC/RFiD

Wired

Ethernet, RS-485, 4-20 mA …



Source: http://hitlistsofts.blogspot.bg/2015/05/difference-between-gsm-gprs-edge-3g.html

Connectivity (application)

HTTP (REST)

CoAP

Stripped down, datagram based HTTP over UDP/SMS …

Goal: Interop with the web

MQTT

Open standard, Client/server (broker), pub/sub

SSL/TLS, user/pass auth

Many others: IRC, XMPP, AMQP …

CoAP

Data management and analytics

Data ingestion

Edge processing, batching & compression

Data ingestion: Kafka, HDFS, Cassandra …

Analytics

Spark/Hadoop, Python

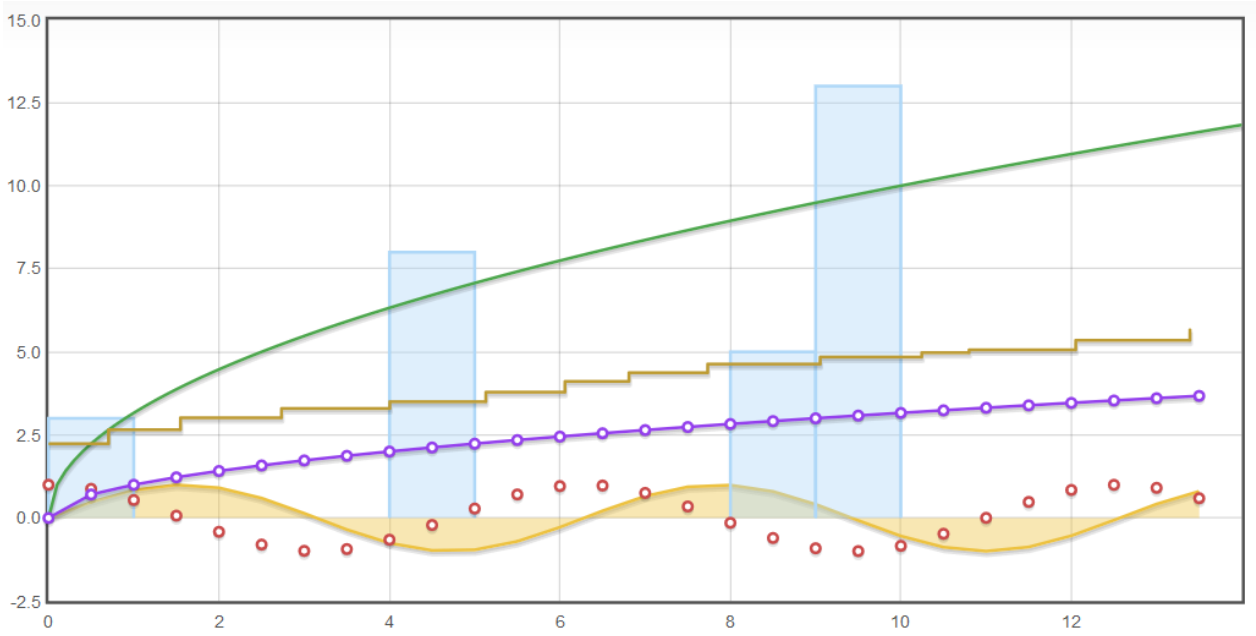
Keras, Theano, TensorFlow …

Visualization

Matplotlib

D3 + plugins (e.g. c3js)

Dygraphs, Flot



Security

http://1.bp.blogspot.com/-1EN9zxdS6PQ/UKJSChMxu9I/AAAAAAAABEk/wheTrU34TBU/s640/I+am+Hacker.jpg

Who’s the hacker?

Motivation

Emotion

Profit

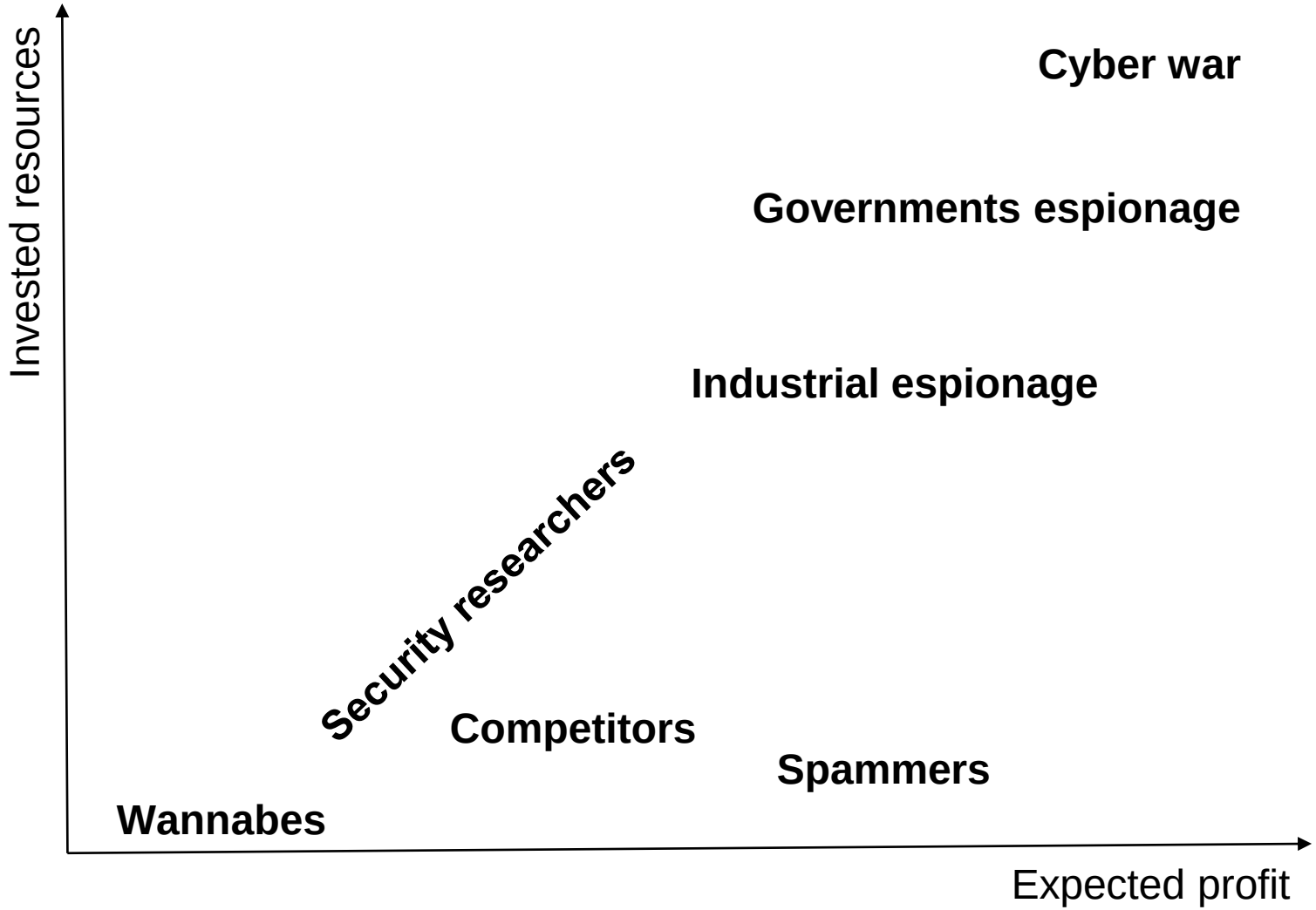
Scientific interest

Black hats vs White hats

Damage

Money flow

Breaking the law?



Solution?

No silver bullet

Balance between risks and profits

Learn from the others' mistakes

Plan countermeasures

Source: https://www.youtube.com/watch?v=WyM2r-ixDvg

Showcase: Self aiming, social rifle …

Hackers: Runa Sandvik & Michael Auger

Target: 2013 TrackingPoint TP750 WiFi rifle

Payload:

Detune scope (e.g shoot wrong target)

DoS the entire scope

Source: http://adrenaline.uol.com.br/files/upload/noticias/2015/07/mateus/sniper-pc_2.jpg

Hacks

WiFi hotspot

WPA2 key is guessable and can’t be changed

Mobile API (tune ammo weight etc.)

“Secret” admin commands, one of which opens the SSH port

Raw backend access

Tune ammo weight without validation (persistently and without validation)

Firmware updates

GPG signed, but private key is on the device

Vendor’s official response

You can continue to use WiFi if you are confident no hackers are within 100 feet.

Stuxnet … an APT

Hackers: No Such Agency

Target: Iran's Natanz uranium enrichment centrifuges

Attack: Spin rate could be controlled. Monitoring data tampered.

IoT specific security concerns

Doom's day scenarios

e.g. Natanz

Privacy attacks

Samsung TV, Amazon Echo

IoT botnets

Devices turn to DDoS zombies (Mirai botnet -> 100K nodes)

Business risk & disruption

Bricked devices

Limited ability to update crypto (due to e.g. vendor, power, computing)

Wider the security perimeter

Possible security counter measures

Before the fact: Make attacker's life harder

Strong crypto, SSO, 2FA

OWASP Internet of Things

Pentest hardware too (Logic analyzers, SDR …)

After the fact: Plan for mitigation

Technical (DDoS protection, device blacklisting, recall and factory reset)

PR & Legal (Ready made responses, limitation of liability)

Financial (Insurance, indemnification from partners)

Device management

Problems being solved

Secure device onboarding & off-boarding / blacklisting

Maintenance:

- OTA updates, restarts
- Diagnostics: uptime/heartbeat, network quality (latency, error rate)
- Locating a device
- Bulk operations scheduling & maintenance plans …

Solutions

OpenHAB, Kura

Blynk, Thingspeak, Beebotte, SAP, IBM …

And probably lots of home grown stuff due to specifics of business

Thank you

Contact information:

Pavel Genevski
Researcher / Architect
SAP Labs Bulgaria