Cybersecurity in industry and industrial products
(“The need for disruptive ideas”)

Michele Colajanni
Interdepartment Research Center on Security (CRIS)
Università di Modena e Reggio Emilia
michele.colajanni@unimore.it
The exponential progress or the dawn of 4th Industrial Revolution

- Novel materials and drugs
- Mobile growing
- 3D-4D printing
- Smart sensors rising
- Future health
- E-health
- Planetary IoT
- Big Data ecosystem: Real-time analytics, deep learning, predictive intelligence, problem solving
- Human Machine Interfaces
- Advanced robotics
- Autonomous agents
- Cloudification
- Augmented reality
- Virtual reality
- Processing and storage costs falling

Michele Colajanni - "Cyber Security in Industry" - CyberROAD - Cagliari, 25 May 2016
Cyber world

• Unlimited computational and storage resources
• Everything can be recorded, nothing will be forgotten
• All-to-all connections
• Pervasive computational thinking

“Whatever the future, it will depend on computing” (Grady Booch) …

… and computing depends on DATA
Today: Anything in common in smart objects?
“Smart” Things

They gather customer’s data. They learn to correlate different data:

– to better satisfy the needs of the customer

– to increase the efficiency of product advertisements

The informed consent about smart objects and services is formally perfect and actually a fraud. Yes, we know: it’s a customer error not to read and understand ToS, but …
“Data war”: C vs C
(C = Countries, Companies, Citizens, Customers, Criminals)

“Privatization of privacy”
Novel business models are appearing

Customer’s data have a value. Privacy is a value.

AT&T offers different prices based on how jealously users guard their privacy: $70 per-month for gigabit service and additional $29 a month to customers who opt out of AT&T's "Internet Preferences" program.

“Ethics by design”

Social network

“Online ads generate revenues for the TSU platforms. Our community gets up to 90% of all revenues to you. It’s your content, own it.”
We have other problems

HP 2014 study reveals: **70% of Internet of Things Devices are Vulnerable to Attacks**

On average, 25 vulnerabilities per device. Highlights include:

- Privacy concerns
- Insufficient authorization
- Lack of transport encryption
- Insecure Web interface
- Inadequate software protection
From personal to professional healthcare → IoT is becoming a serious scenario

WIRELESS IMPLANTABLE MEDICAL DEVICES

- Deep Brain Neurostimulators
- Cochlear Implants
- Gastric Stimulators
- Cardiac Defibrillators/Pacemakers
- Foot Drop Implants
- Insulin Pumps

Michele Colajanni - "Cyber Security in Industry" - CyberROAD - Cagliari, 25 May 2016
The scenario is becoming even more serious in *Industrial IoT* and *Industrial products*.
Consumer IoT

• Mandatory
  – Low prices
  – Eager Time to Market ("get ahead of the competitors")

• Acceptable
  – The customer pays for the object
  – The customer doesn’t pay for the service → Actually he/she pays through a (conscious) privacy violation
  – Minimum level of security and then patches
  – Standards are not so important
  – Rapid obsolescence of the object

→ More time for a more expensive, standardized and secure object does not really pay back the Producer
Industrial IoT

• Electric power transmission and distribution
• Industrial control systems
• Oil and natural gas systems
• Water and waste-water treatment plants
• Healthcare devices
• Transportation system
• …

• **Security-critical**: Industrial IoT systems collect data and are exposed to attacks
• **Safety-critical**: their failure can cause irreparable harm to the physical system under control and to the people
Security MUST be integrated with Safety

Confidentiality

Integrity

Availability

Safety

“Freedom from unacceptable risk of physical injury or of damage to the health of people, either directly, or indirectly as a result of damage to property or to the environment”
Crossroads of the digital revolution

Industrial IoT → Some hope: Security and privacy by design, compliance and incentives can win

Consumer IoT → No hope: The model based on Time-to-Market, privacy violation and products based on limited security is winning
Industrial IoT: An optimistic vision

1. Time-to-Market is less aggressive because quality is more important

2. Awareness of the (consumer) companies
   - IoT costs have a minor impact on the plant investment
   - Medium-long term technology is required
   - Security and safety have a value
   - Standards are important

3. Political and social awareness about security and safety of IoT is increasing

*Most IoT products in critical systems will be enriched by Security and Safety by design*
The day after tomorrow

PC

Internet

World Wide Web

Mobile Web + App

Cloud and social systems

Smart objects

Autonomous objects

INDUSTRIAL INTERNET OF THINGS
Your empathy?

OR

OR
Conclusions

• Pessimistic about *data privacy*
• Partially optimistic about *security in Industrial IoT*
• We are living in *exponential* times: data, attacks, information, traffic, technology, sensors, …
• Human are characterized by *linear* or *sublinear* growth capacity

→ It’s better to switch some investments from *linear improvements* to *disruptive ideas* if we want to avoid that the *dawn* of 4th industrial revolution coincides with *human sunset* → *It’s your time young researchers!*
email: michele.colajanni@unimore.it

home page: Google(Michele Colajanni)