Design for Security:
a Déjà-vu story

Paolo PRINETTO
President of CINI
Paolo.Prinetto@polito.it
Mob. +39 335 227529

cini
Cybersecurity
National Lab

cini
consorzio
interuniversitario
nazionale
per l'informatica

www.consorzio-cini.it

consorzio interuniversitario nazionale per l'informatica

- Is a consortium of 44 Italian Universities that
  - do research in CS/CE
  - deliver MS/PhD degrees
  - are public funded

consorzio interuniversitario nazionale per l'informatica

Mission

Providing added value to:

- the member Universities
- the Italian production system
- the Italian Public Administration
- the overall country

being the representative of the almost whole Italian Academic Informatics Community

Acknowledgment

- CINI Cybersecurity National Lab within the Italian Project "*FilieraSicura: Securing the Supply Chain of Domestic Critical Infrastructures from Cyber Attacks*"

cini
Cybersecurity
National Lab

4 Objectives + 2 Real Testbeds

Obj. 2.1 – Trusted Components & Design-for-Trust

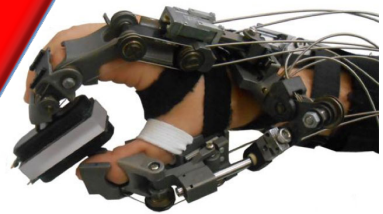
Obj. 2.2 – Secure Multi-Processor System Design Methodology

Obj. 2.3 – Open Security Platforms

Obj. 2.4 – Security in Emerging Technologies components

Water supply systems

Robots for healthcare



Internet of Things

- Everyone & Everything connected, always
- Enabling every object you can imagine with web capabilities

Internet of Things

- Everyone & Everything connected, always
- Enabling every object you can imagine with web capabilities
- 6 billion “things” estimated to be connected to the internet
- There will be an estimated 20.8 billion by 2020

Everything connected, always

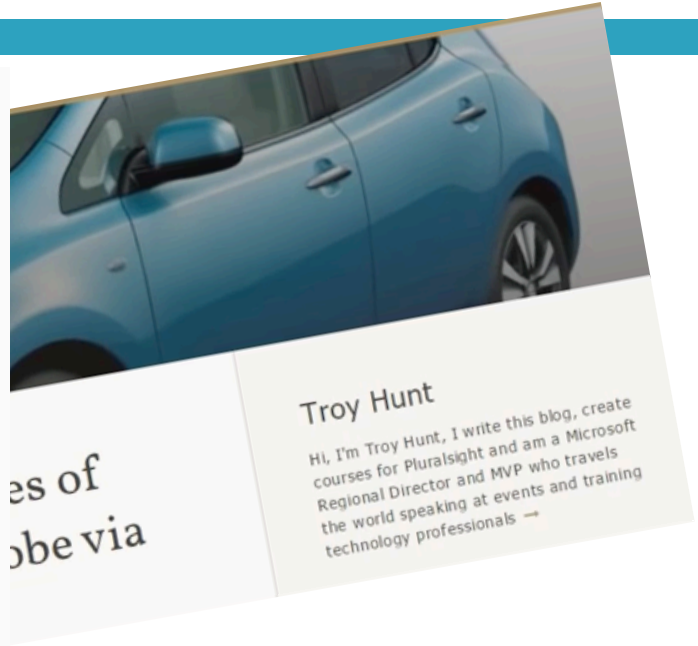
Effects

- The *surface of attack* for cybersecurity attackers is increasing exponentially

Surface of attack

Surface of attack

This was the vehicle's VIN which clearly, left us curious (obfuscation is mine, it's legible in its entirety on the web).



Surface of attack

PRIVACY AND SECURITY FANATIC

By Ms. Smith, Network World | FEB 12, 2017 8:15 AM PT

University attacked by its own vending machines, smart light bulbs & 5,000 IoT devices

A university, attacked by its own malware-laced soda machines and other botnet-controlled IoT devices, was locked out of 5,000 systems.

About

Ms. Smith (not her real name) is a freelance wr
programmer with a special and somewhat per
interest in IT privacy and security issues.

Surface of attack

PRIVACY AND SECURITY FANATIC

By Ms. Smith, Network World | FEB 12, 2017 8:15 AM PT

University attacked by its machines, smart light bul devices

A university, attacked by its own malware-laced controlled IoT devices, was locked out of 5,000

THE INTERNET OF HACKABLE THINGS

Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings

LORENZO FRANCESCHI-BICCHIERAI

Feb 27 2017, 10:00pm

A company that sells "smart" teddy bears leaked 800,000 user account credentials—and then hackers locked it and held it for ransom.

UPDATE, Feb. 28, 12:25 p.m. ET: After this story was published, a security researcher revealed that the stuffed animals themselves could easily be hacked

Consequences for companies

Consequences for companies

- Selling unsecure IoT means:
  - Low quality products
    ➔ Market loss

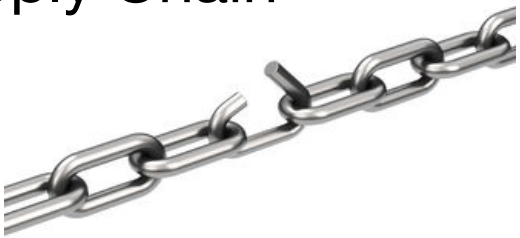
Consequences for companies

- Selling unsecure IoT means:
  - Low quality products
    ➔ Market loss
- Your IoT can be the gateway to attack something bigger
  ➔ Legal problems

Consequences for companies

- Selling unsecure IoT means:
  - Low quality products
    ➔ Market loss

- Your IoT can be the gateway to attack something bigger
  ➔ Legal problems
- Be sure not to be the weakest “link” in a Supply Chain



Action Items

For all

- Rise the level of awareness everywhere

Rise the level of awareness

@companies

- CEO
- Technical
- Risk assessment & management
- …

Rise the level of awa

@companies

- CEO
- Technical
- Risk assessment & management
- …

Rise the level of awareness

@companies

- CEO
- Technical
- Risk assessment & management
- …

@ society

- @ home
- @ work

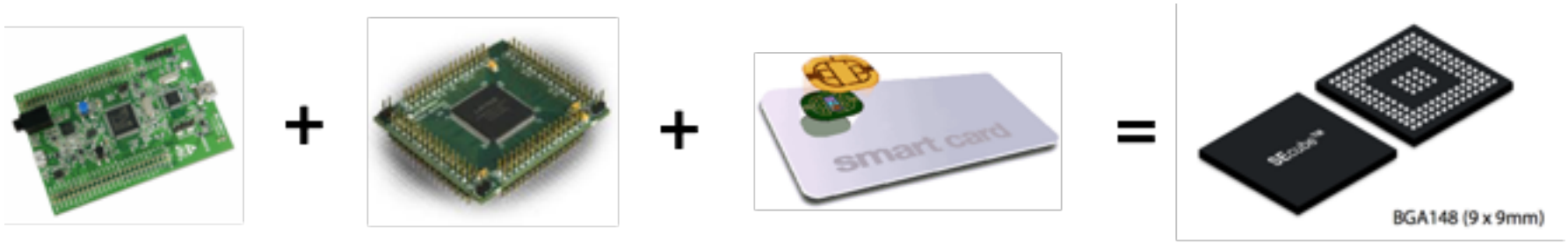
Action Items

For R&D

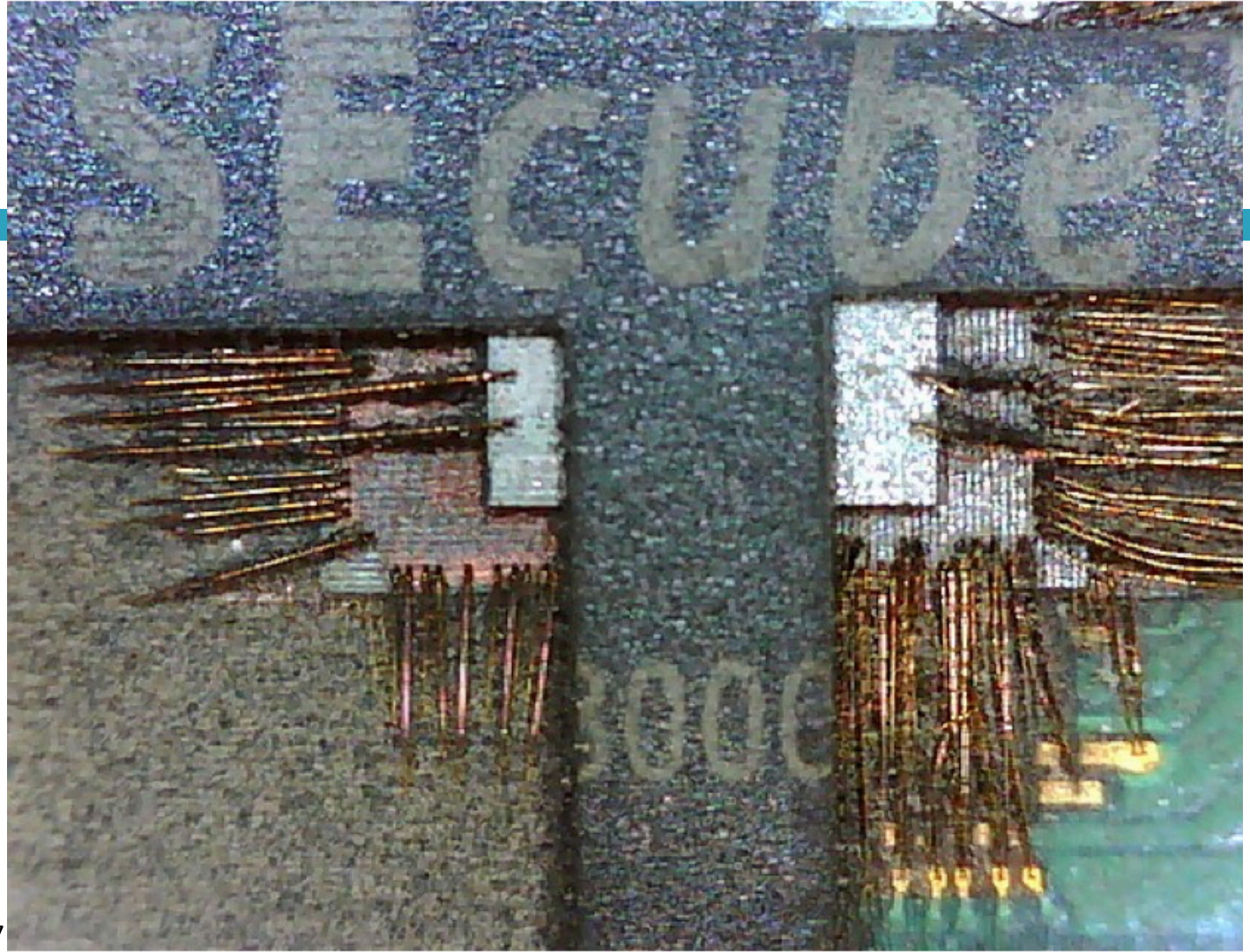
- Holistic cost-effective solutions

SEcube™
Open Source Security Platform

The First Open Security Platform in a 3-D SiP:



CPU + FPGA + Smart Card = SEcube™



Sharing a déjà-vu experience

Design for Testability

- R.G. “Ben” Bennetts fights against “overheads”

Design for Testability

- R.G. “Ben” Bennetts fights against “overheads”

- “*If you consider testability as part of the specifications, its costs cannot be considered an overhead*”

Design for Security

- “We cannot implement *Design for Security* because it’s too expensive and, at the end of the story, there is no law in Italy that enforces us to do it …”

[Power grid component providers]

DfT vs. DfS

DfT

- We had to convince:
  - Designers
  - Management

DfT vs. DfS

DfT

- We had to convince:
  - Designers
  - Management

DfS

- We have to convince:
  - Designers
  - Companies
  - Policy makers

History Lessons

Internet

The Internet was not built with security in mind

History Lessons

Internet

The Internet was not built with security in mind

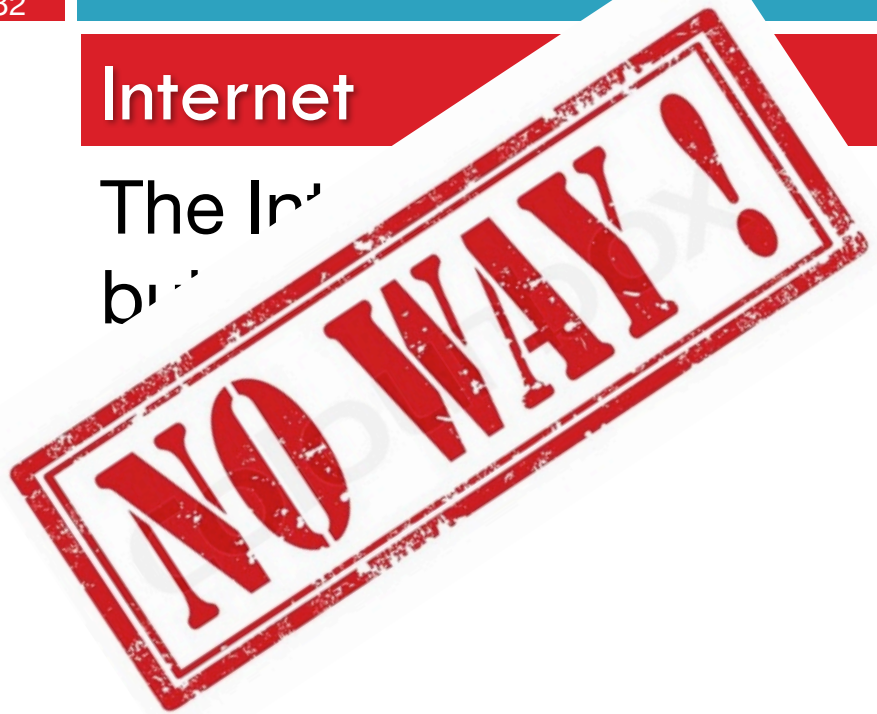
IoT

Can we afford to think the same way while building the IoT ?

History Lessons

Internet

The In
bu



IoT

Can we afford to think the same way while building the IoT ?

Малые Автюхи, Калинковичский район
Республики Беларусь

Paolo PRINETTO

President of CINI

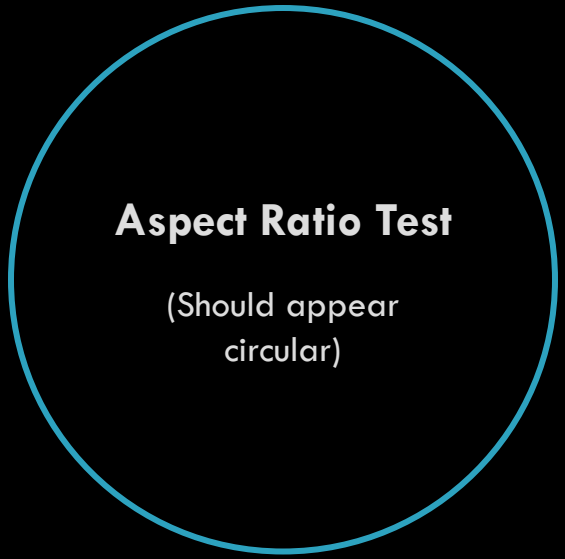
Paolo.Prinetto@polito.it

Mob. +39 335 227529

cini consorzio interuniversitario nazionale per l'informatica

www.consorzio-cini.it

Widescreen Test Pattern (16:9)



4x3

16x9