SECURE-IC
THE SECURITY SCIENCE COMPANY

5G Global event - security session

May 24, 2017 - Tokyo, Japan

Sylvain GUILLEY – Co-founder, director of the "Think Ahead" business line

Session Outline

Introduction about 5G and security

Presentation of panelists
- Koji Nakao
- Anand Prasad

Round table and discussion with the audience

Session Outline

Introduction about 5G and security

Presentation of panelists

- Koji Nakao
- Anand Prasad

Round table and discussion with the audience

5G security

Sylvain Guilley

- Standard editor at ISO SC27 and active in TC CYBER of ETSI
- Design and evaluation of smart objects

- Professor in cryptographic engineering
- Research interest in side-channel and fault injection attacks

- Director of the *Think Ahead* business line
- In charge of innovation

CORPORATE PRESENTATION

OUR ACTIVITY

WHAT DO WE DO?

SECURITY TECHNOLOGIES

FOR EMBEDDED SYSTEMS

FOR WHOM?

CHIPSET/DEVICE VENDORS

IC DESIGN HOUSES

CERTIFICATION LABS

GOVERNMENTAL AGENCIES

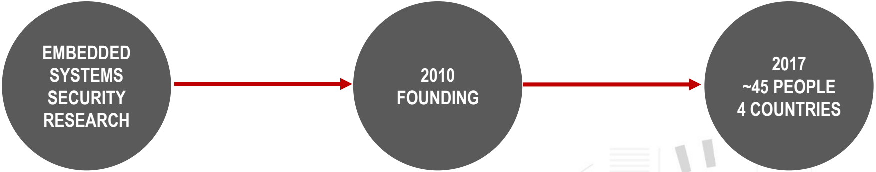
FOR WHICH MARKETS?

OUR VISION

Going forward, there will be more and more interconnected devices or objects in various market verticals, this is what we call Internet of Things or Internet of Everything. All those objects being interconnected to the cloud, each and every object could be a threat for the whole network. Therefore the security of the objects or the devices is key. Even more, security will become one of the most important asset of the digital world.

CORPORATE PRESENTATION

THE COMPANY


EMBEDDED SYSTEMS SECURITY RESEARCH
2010 FOUNDING
2017 ~45 PEOPLE 4 COUNTRIES

MORE THAN
15 YEARS OF RESEARCH

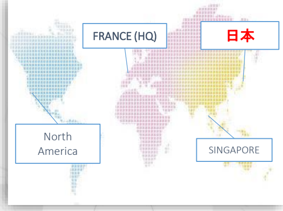
MORE THAN
200 PUBLICATIONS

SPIN-OFF FROM
INSTITUT MINES-TELECOM

Institut Mines-Télécom

SECURE-iC
THE SECURITY SCIENCE COMPANY

PÔLE D'EXCELLENCE CYBER



Technology Fast 50 2015 FRANCE

bpifrance EXCELLENCE

PASS FRENCH TECH IMAGES & RÉSEAUX 2015

CORPORATE PRESENTATION

BUSINESS LINES

PROTECT

SECURYZR

COMBINATION OF **SMART UNITS** AND **EXPERTISE RESULTS**

EVALUATE

LABORYZR

READY-TO-USE **PRE** AND **POST-SILICON ANALYSIS PLATFORMS**

SERVICE

EXPERTYZR

THE **NEXT STEPS** TOWARDS **SECURITY CHALLENGES**

Security?

Yesterday, what were the security issues?
Major security breaches identified in legacy networks

- 2G **cryptography** has been broken [BBK08]
- **Man-in-the-middle** attack successfully perpetrated between 3G-WLAN interworking [ZJWY10]
- **4G SIM cards** have been cloned thanks to power-line analysis [LYS^{+}15]

Applicable cyber attacks: *(a tsunami!)*

Hardware	Hardware trojans, counterfeited and/or repackaged devices, FIB, probing, DPA, EMA, etc.
Operating sys.	Buffer overrun, corrupted error management, insufficient verificiation of data authenticity, numeric errors, integer overflow/underflow, OS command injection, permissions, priviledges, access control, race conditions, resource management error, time and state abuse, etc.
Application	ROP, stack smashing, code injection, command injection, CSRF, XSS, format string vulnerability, information leak / disclosure, link errors, path equivalence, path traversal, SQL injection, etc.

Security?

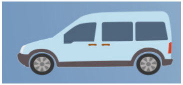
Today, yearly loss due to cyber attacks: **$400 Billion**
(Intel Security)

Today and tomorrow, we want E2E security for 5G:

- What does security means? . . it is vertical industry-dependent
- Where to secure? . . . . .each node + its links
- How to secure? . . . . first need: to identify the threats

Security: what for?

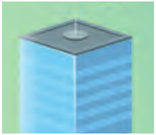
Automotive
→ **safety**



Industry 4.0
→ **availability**

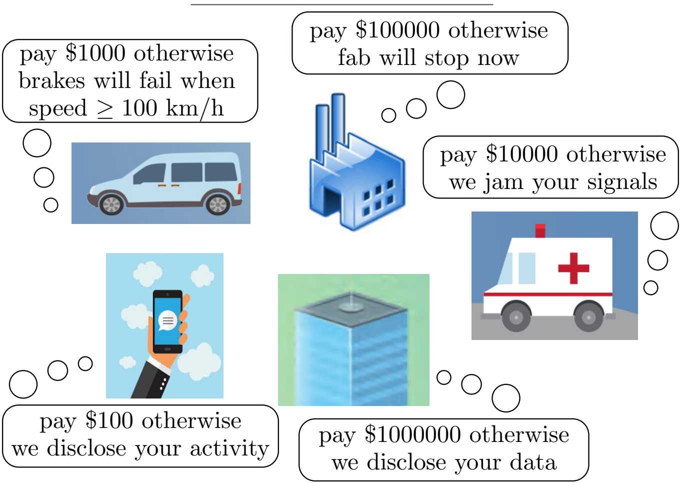
Emergency
→ **genuine info**

End user
→ **privacy**



Business
→ **confidentiality**

Security: exemple of ransomware



pay $1000 otherwise brakes will fail when speed $\geq$ 100 km/h

pay $100000 otherwise fab will stop now

pay $10000 otherwise we jam your signals

pay $100 otherwise we disclose your activity

pay $1000000 otherwise we disclose your data

Predicting security in 3 years with 5G ?

Context: 5G communicates with the IoT

Today, facts

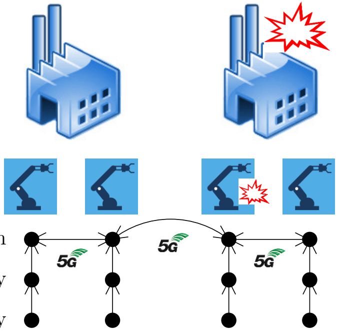
- **botnets** (including IoT devices) are growing: Mirai, Hajime, etc.
- current attacks are seen by many as **warning shots**
- vulnerabilities are **everywhere**: hardware, OS, apps, etc.

Future

- **More value** in 5G means **more attacks**!
- Get prepared today!

Solution ❶: Security by design

5G + IoT (M2M) = CPS (Cyber Physical Systems)



Solutions:

Mutual authentication

Firmware integrity

Hardware integrity

Threats:

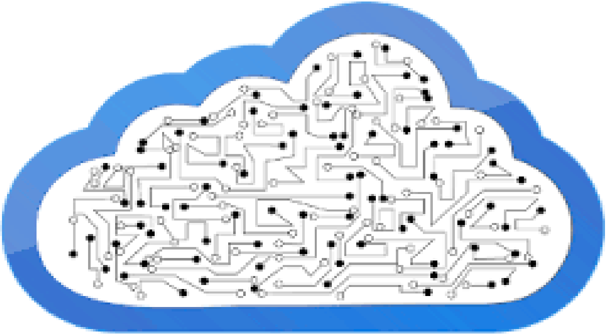
Rogue equipment

Malware
Downgrade

Hardware trojan
Tampering
Probing, FIB, etc.

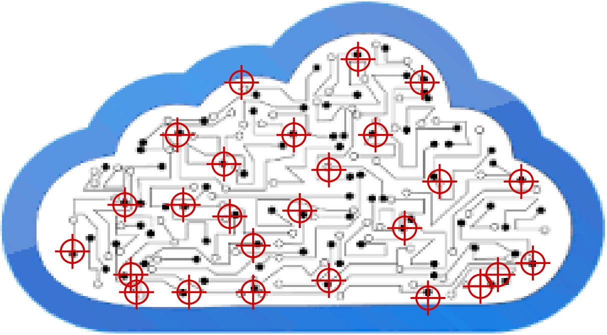
Solution ❶: Security by design

The strength of a chain is the strength of its weakest element and/or link



■ Solution ❶: Security by design

The strength of a chain is the strength of its weakest element and/or link



Solution ❷: Standardization effort

- International efforts:
  - ITU-T: ITU SG-17: Security
  - 3GPP A GLOBAL INITIATIVE: SA WG3: Security
- Regional efforts:
  - ETSI World Class Standards → www.etsi.org/SECURITYWEEK and TC Cyber
  - 5G-Ensure under 5G PPP PUBLIC-PRIVATE PARTNERSHIP
  - European H2020 projects.
  - etc.

Coordination is needed!

Session Outline

Introduction about 5G and security

Presentation of panelists

- Koji Nakao
- Anand Prasad

Round table and discussion with the audience

Panelists

Koji Nakao

- Involved in ITU-T SG17 and ISO/IEC JTC1/SC27/WG4
- KDDI: "Information Security Fellow" to manage all the security issues
- NICT: "Group Leader" to manage research activities for network security technologies
- Steering committee member of Japan-France cybersecurity research group

Panelists

Anand Prasad

- Chairman of 3GPP SA3
- Member of the governing body of Global ICT Standardisation Forum for India (GISFI)
- Chief Advanced Technologist, Executive Specialist, at NEC Corporation, Japan

Session Outline

Introduction about 5G and security

Presentation of panelists
- Koji Nakao
- Anand Prasad

Round table and discussion with the audience

Round table: next steps?

- How to coordinate cyber and telecom worlds?
- How to interoperate with legacy networks?
- How about creating security subgroups in 5G associations? How to coordinate the worldwide standardization?

Exemple of cautionary note:

conflicting requirements

Objectives of 5G

- high speed (10 Gbps),
- high capacity ($10,000$ simultaneous connections),
- low latency (< 1 ms),

Objectives of security

- AES encryption at 10 Gbps needs hardware acceleration
- Authentication of $10,000$ devices also requires hardware acceleration
- RSA/ECC/post-quantum crypto $\lll 1$ ms requires hardware acceleration

Evaluation	*and*	Test
Common Criteria		CMVP Conformance through Testing FIPS VALIDATED 140-2
ISO/IEC 15408:2009		ISO/IEC 19790:2012

Bibliographical references

[BBK08] Elad Barkan, Eli Biham, and Nathan Keller.
Instant ciphertext-only cryptanalysis of GSM encrypted communication.
J. Cryptology, 21(3):392–429, 2008.

[LYS+15] Junrong Liu, Yu Yu, François-Xavier Standaert, Zheng Guo, Dawu Gu, Wei Sun, Yijie Ge, and Xinjun Xie.
Small tweaks do not help: Differential power analysis of MILENAGE implementations in 3g/4g USIM cards.
In Günther Pernul, Peter Y. A. Ryan, and Edgar R. Weippl, editors, *Computer Security - ESORICS 2015 - 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015, Proceedings, Part I*, volume 9326 of *Lecture Notes in Computer Science*, pages 468–480. Springer, 2015.

[ZJWY10] Lizhuo Zhang, Weijia Jia, Sheng Wen, and Di Yao.
A Man-in-the-Middle Attack on 3G-WLAN Interworking.
In *2010 International Conference on Communications and Mobile Computing*, volume 1, pages 121–125, April 2010.
IEEE. Shenzhen, China.

SECURE-IC

THE SECURITY SCIENCE COMPANY

5G
THE 3rd
GLOBAL 5G EVENT
"Creating the Crossover Collaboration for 5G Eco-Society"
Workshop: 24-25 MAY, Exhibition: 24-26 MAY
2017, TOKYO, JAPAN

THANKS FOR YOUR ATTENTION

CONTACT

EUROPE	sales-EU@secure-IC.com
APAC	sales-APAC@secure-IC.com
JAPAN	sales-JAPAN@secure-IC.com
AMERICAS	sales-US@secure-IC.com