

A decorative background consisting of a field of small, scattered dots in various shades of grey, green, and red, creating a digital or network-like pattern.

HARDWARE SECURITY CHALLENGES FACING THE IOT NODES

LA CYBER SECURITE AU SEIN DE L'IRT NANOEELEC | FOURNIER Jacques | November 24, 2016

Recent events that have been rocking the field of IoT security

- **DDoS attack on Dyn's DNS nameservers**
 - 100s of websites (GitHub, Twitter, Netflix, AirBnb...) unaccessible for several hours.
 - Knocking off entire countries (Liberia)
 - Estimated over a million of Mirai infected devices involved!
 - > 1TBps attack!
- **Chain-reaction of worm spread on Philips' Hue connected bulbs**
 - <http://iotworm.eyalro.net/iotworm.pdf>

**IoT Goes Nuclear:
Creating a ZigBee Chain Reaction**

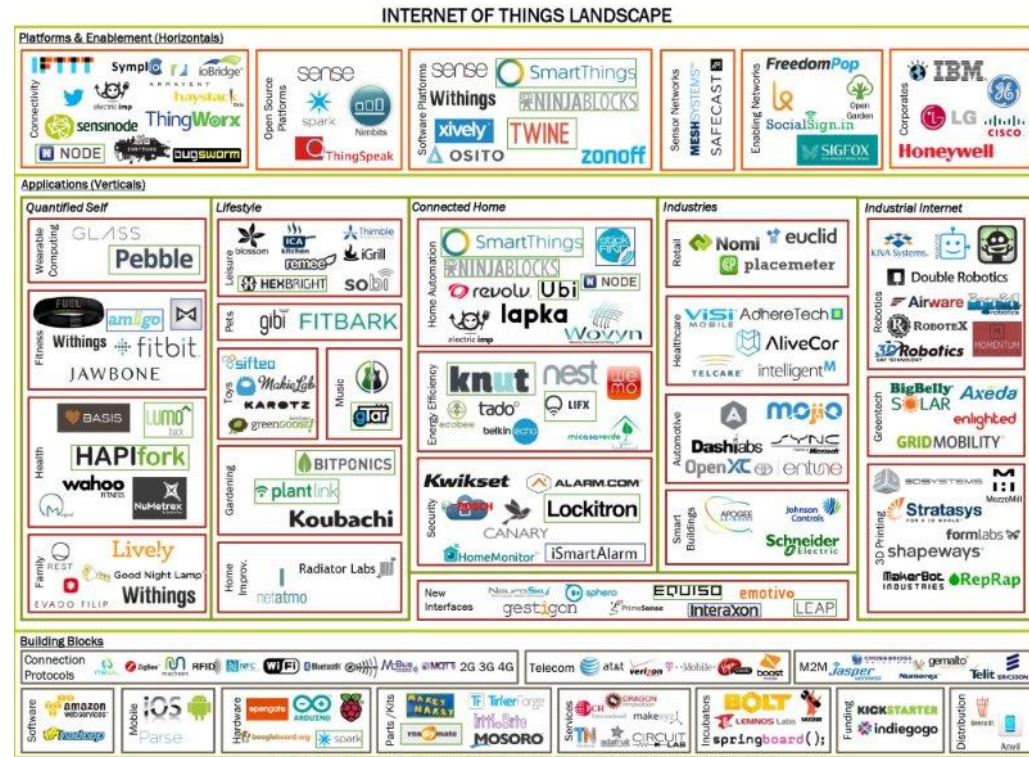
Eyal Ronen(✉)*, Colin O'Flynn†, Adi Shamir* and Achi-Or Weingarten*

PARTICULARITIES OF THE IOT

- 50 billions of connected devices estimated [1] by 2020...
 - ... but not so big finally... More towards 10s of billions by 2027 according to a latest IDTechEx report [2]

- **Limiting factors**

- Lack of clear standards
- Heterogeneity
- Scale of deployment
- Increasing bargaining value of manipulated data
- Legacy management

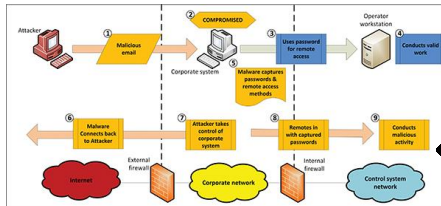
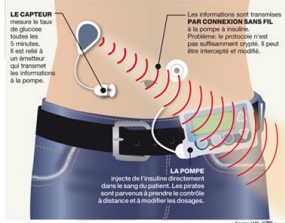


[1] « Ceo to shareholders: 50 billion connections 2020”, Ericsson Press Release, April 13, 2010. <http://hugin.info/1061/R/1403231/357583.pdf>
 [2] “Internet of Things (IoT) 2017-2027 Things that think: IP addressed sensor node systems” by Dr Jon Harrop, Dr Peter Harrop and Dr David Pugh, Nov 2016. <http://www.idtechex.com/research/reports/internet-of-things-iot-2017-2027-000499.asp>

SECURITY PRIORITIES OF THE IOT

- Defined today by the 'vertical' applications with their specificities:
 - Not an exhaustive list...

UNE CONNEXION SANS FIL VULNERABLE



IoT Goes Nowhere:
Creating a ZigBee Chain Reaction

Paul Rowberry, Colin O'Hanlon, Ash Sanger, and Ash O'Neill

Wireless Car Sensors Vulnerable to Hackers
 Researchers figure out how to hijack sensor communications.
 By Robert Lewis
 THURSDAY, AUGUST 13, 2010

'Carjacking' for the twenty-first century.
 Posted by Del in Articles, Cars - 12th August 2010

So the time has finally come when we are no longer in total control of our vehicles. The trend to rely more and more on electronic devices to control every aspect of our cars is steadily increasing. From the more mundane tasks of maintaining climate control to sending service reports to the dealer, our cars are no longer the mechanical beasts of yesteryear.

Invented in the 20's but made viable in the 80's, the ECU (Electronic Control Unit) sits quietly monitoring sensors around your engine. This ECU controls everything from the air/fuel mixture to the ignition timing, providing a more dynamic method of controlling the performance and efficiency of the engine. As technology has advanced, ECUs have become more complex and software driven, providing additional control of functions such as cruise control, transmission control, anti-lock brake, and anti-theft control.

sure sensors built into many cars these researchers a vehicle or force its electronic control system to crash and Rutgers University researchers say.

in team, which successfully hijacked two regular fire-escape-monitoring systems (TMS), will describe the job at the [LCCNIX Carjacking](#) conference in Arlington, DC, this week.

in the near-term attacks pose little immediate risk to users. However, in recent months, research groups have been fielding other security weaknesses in vehicle software systems. As automakers add more powerful modules to cars, and connect these computers to their components, in-car systems will need to be guarded against hackers, experts warn.

- Smart Health
- Smart Grids
- Smart Cities
- Smart Vehicles
- Smart Industries

Public safety

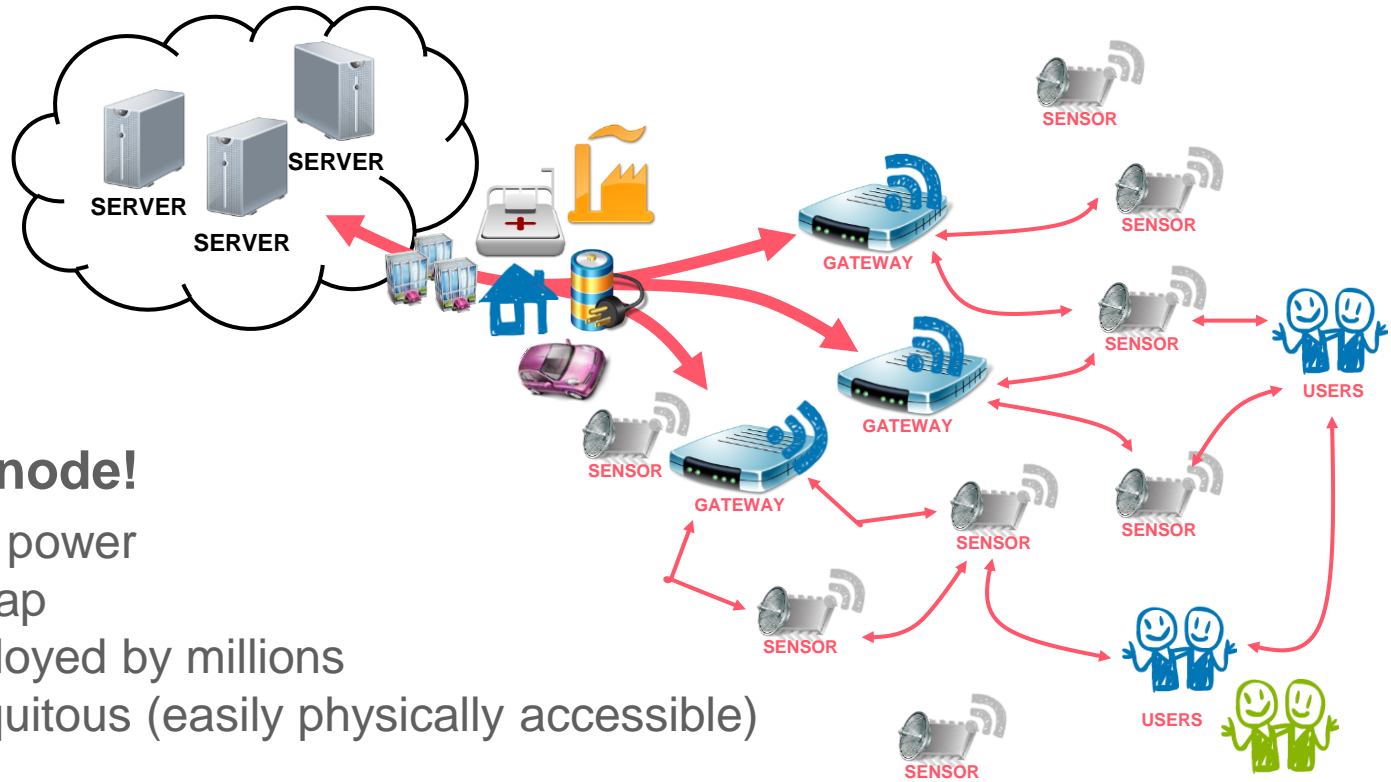
System Resilience

Cost Impact

User privacy

AAA : Accountability, Auditability & Assurance

(ONE OF) THE MOST VULNERABLE PART OF THE IOT



It's the node!

- Low power
- Cheap
- Deployed by millions
- Ubiquitous (easily physically accessible)

CORE CHALLENGES

- Trusted hardware / counterfeiting
- Low power, fast cryptographic primitives for confidentiality, integrity, authenticity & privacy
- Massive deployment & on-the-field management
- Long lived security
- Protocols for end-to-end security

HOW TO TACKLE THE HARDWARE SECURITY CHALLENGES?

- Consider short-term and long-term challenges
- **Short term : Securing the Internet of *existing* Things (IO_ET)**
 - Enhancing the security of existing systems and devices
 - Using existing and proven security technologies
 - Integrating them « at-design-time »
 - So that in 5-10 years' time things are more or less done securely.
- **Long term : Securing the Internet of *future* Things (IO_FT)**
 - Researching fundamentally new paradigms and architectures suited to the IoT constraints.
 - Thinking « out the box ».
 - **Being disruptive innovationwise while not disrupting existing infrastructures!**
 - Beyond the 10-year perspective.

SHORT TERM SECURITY CHALLENGES

- **Trusted hardware & designs**
 - Solutions to verify the integrity and genuineness of ICs
 - Compatible with industrial constraints of IC manufacturing [1].
 - Eventually more invasive low cost approaches [2].
- **Lightweight cryptography resistant to physical attacks**
 - Classical cryptography does not satisfy the performance and power requirements of IOT devices & are vulnerable to physical attacks.
 - A new breed of crypto algorithms, Light Weight Crypto (LWC), has to be designed to be intrinsically resistant to physical attacks [3].
- **Efficient on-chip key generation and storage**
 - Physically Unclonable Functions (PUFs) [4] have been extremely complex to design [5] so far.
 - A new breed of PUFs needs to be researched, most probably on the technological level.
- **Power efficient & secure low-level protocols**
 - Many IoT devices will be in-the-field for decades, so they need to be updated and secure firmware and data update mechanisms have to be defined and standardised [6].
 - Low level secure wireless communications have to be researched and deployed (6LoWPAN) for privacy-by-design architectures [7].

LONG TERM SECURITY CHALLENGES

- **Disruptive processor architectures**
 - One fundamental problem with current IOT nodes is that the underlying processor cores are vulnerable to a series of physical & logical attacks.
 - **The concept of CIA (Confidentiality-Integrity-Authenticity) must be integrated with the processor core itself in an energy and cost-efficient way for off-the-shelf devices!**

- **Rethinking the key management and distribution problem**
 - Current traditional PKIs,
 - an exponential $O(n^2)$ number of transactions are necessary to share keys among n parties
 - Complex management of certificates and revocation lists, which might be a problem when dealing with billions of objects
 - **Alternative solutions like Identity Based schemes based on Pairings should be investigated ! The number of necessary transactions for sharing the keys is linear with the number of parties involved.**

- **Computing power of the IOT node for end-2-end security**
 - Homomorphic cryptography is being touted as the « ultimate » way of securely handling and working on data on the server side
 - No decryption of the data is required.
 - Cross-encryption schemes can be implemented
 - **IOT infrastructures must be rethought in integrate those homomorphic concepts from one 'node' end to another 'server' end (and from there probably to other 'node' ends)!**

FINAL WORD... WHY NOT THE « INTERNET OF NOTHING »?

- **Finally, if we want to have some disruptive thinking, we might ask ourselves:**
 - Why the INTERNET of Things?
 - Do we want to connect « everything » to the « internet »?
- **Why not some other form of « connection » that would be intrinsically secure against the plethora of attacks that poison our day-to-day life?**

- [1] “On-Chip HT and counterfeits detection” by M. Lecomte, J.J.A. Fournier & P. Maurine, to appear in the IEEE Transactions on Very Large Scale Integration Systems, 2016.
- [2] “SEMBA: A SEM Based Acquisition technique for fast invasive Hardware Trojan detection” by F. Courbon, P. Loubet-Moundi, J.J.A. Fournier & A. Tria, in proceedings of ECCTD’15, Trondheim, Norway, August 2015
- [3] “On the importance of considering physical attacks when implementing lightweight cryptography” by Alexandre Adomnicai, Benjamin Lac, Anne Canteaut, Laurent Masson, Renaud Sirdey, Assia Tria and Jacques J.A. Fournier, NIST Workshop on Light Weight Cryptography, October 2016.
- [4] “A practical framework for assuring authenticity and integrity of hardware components” by C. Rust, H. Bock, V. Brunner, M. Deutschmann, J.J.A. Fournier, J. Hermans & D. Singelee, in the proceedings of Smart Systems Integration international conference & exhibition (SSI 2014), Vienna, March 2014.
- [5] "Physically Unclonable Function: Design of a Silicon Arbiter-PUF on CMOS 65nm", by Jacques J.A. Fournier & Guillaume Reymond, in "Trusted Computing for Embedded Systems", Candaele Bernard, Soudris Dimitrios, Anagnostopoulos Iraklis (Eds.), pp 135-142, Springer, ISBN 978-3-319-09419-9, November 2014.
- [6] « Report from the Internet of Things (IoT) Software Update (IoTSU) Workshop 2016” by H. Tschofenig & S. Farrell. <https://tools.ietf.org/html/draft-iab-iotsu-workshop-00>
- [7] C. Hennebert and J. Dos Santos, “Security protocols and privacy issues into 6lowpan stack: A synthesis”, Internet of Things Journal, IEEE, vol. 1, no. 5, pp. 384-398, Oct 2014.



SAVE THE DATE

LETI DAY AT GRENOBLE
JUNE 28-29, 2017

Leti, **50** years of pioneered innovations

Leti Day, **2** days of discovery, innovation & networking

Leti Gala Evening, **1** VIP Event for our partners & prospects