Security of the IoT

Christine HENNEBERT

Avril 2014

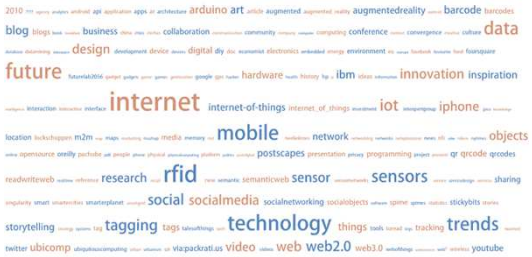
Laboratory Security of Connected Objects and Systems

CEA GRENOBLE LETI/DSIS/STCS/LSOC

Two modern definitions of the IoT

"L'**internet des objets** est **un réseau de réseaux** qui permet, via des systèmes d'identification électronique normalisés et unifiés, et des dispositifs fixes ou mobiles, d'**identifier directement et sans ambiguïté** des entités numériques et des objets physiques et ainsi de pouvoir récupérer, stocker, transférer, traiter et **interagir sans discontinuité entre mondes physiques et virtuels**, les données s'y rattachant à partir du **protocole de l'internet** (IP)."

FONCTIONNELLE



SOURCE MC2014 SYMPOSIUM

SOCIÉTALE

"L'**internet des objets** peut être compris comme **un espace "indéterminé et ouvert"** dans lequel évolueront des entités, **des objets réels et des objets virtuels autonomes**, dotés d'une **intelligence propre**, et capables de s'auto-organiser en fonction des **circonstances, contextes et environnements**".

Attack on/from IoT

LEMONDE INFORMATIQUE

Le 17 Octobre 2012

Pacemaker hacké : risque de décharge mortelle

Crédit Photo: D.R

Les stimulateurs cardiaques de plusieurs fabricants peuvent être piratés depuis un ordinateur portable et déclencher une décharge mortelle. Le chercheur à l'origine de cette découverte pointe du doigt la faiblesse des logiciels embarqués sur ces dispositifs médicaux.

Le 12 Avril 2013

Un chercheur pirate un avion avec une application Android

Crédit Photo: D.R

Lors de la conférence Hack in the Box à Amsterdam, des chercheurs ont démontré qu'il était possible d'exploiter les vulnérabilités des systèmes embarqués des avions et de les attaquer en vol à l'aide d'un smartphone Android.

Le 21 Septembre 2012

NFC : une app Android utilise une faille pour utiliser gratuitement les transports urbains américains

Un portique de contrôle utilisé avec la carte modifiée par l'app Android UltraReset

Selon les chercheurs qui ont développé l'application pour Android, les systèmes de validation par cartes sans contact des transports locaux de plusieurs villes américaines pourraient être piratés.

Le 26 Novembre 2013

Mail Online — Science & Tech

Is your TV spying on YOU? It sounds like science fiction but many new TVs can watch you - telling advertisers your favourite shows or even filming you on the sofa. And there's no off switch!

By GUY ADAMS

PUBLISHED: 01:37 GMT, 26 November 2013 | **UPDATED:** 09:37 GMT, 26 November 2013

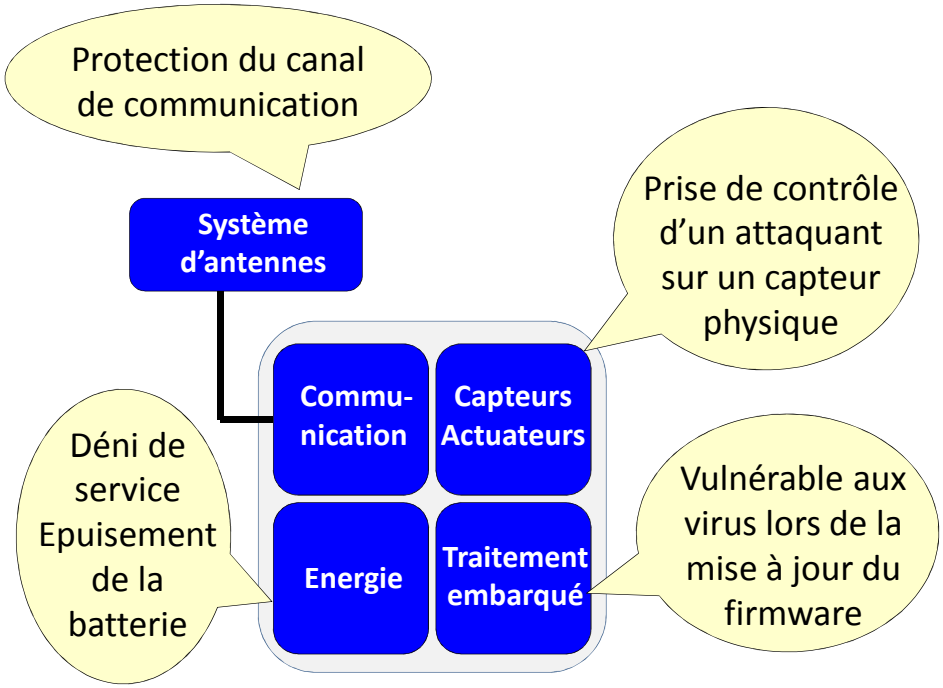
Fields of expertise

- **System** level security
- Applied **lightweight cryptography** : Symmetric, ECC, NTRU
- Embedded « **true** » Random Number Generator
- **Secure Protocols** on wireless low-power channel
- Authentication, **Bootstrapping**
- **6LoWPAN** compliance
- **Wireless** & **Contactless**
- Security at **physical** layer
- **RFID**
  - Noisy Reader
  - Delay-based as Relay Attack Counter-measure

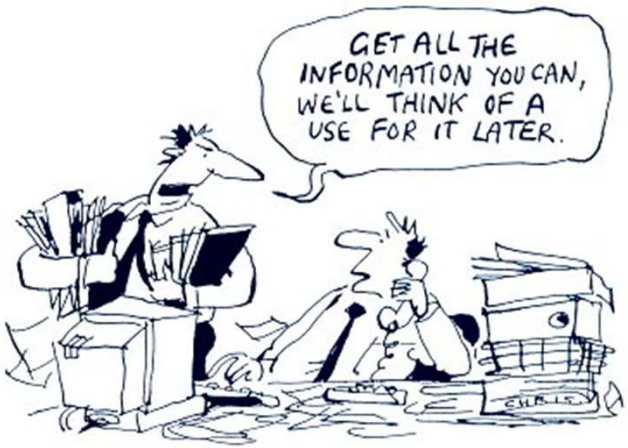
Services

Security

Confidentialité
Intégrité
Fraicheur
Authentification
Non Répudiation
Disponibilité

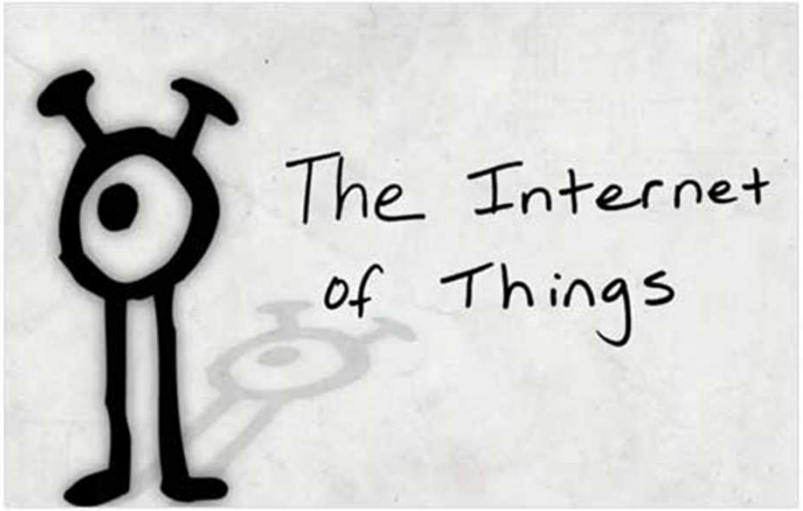


Privacy



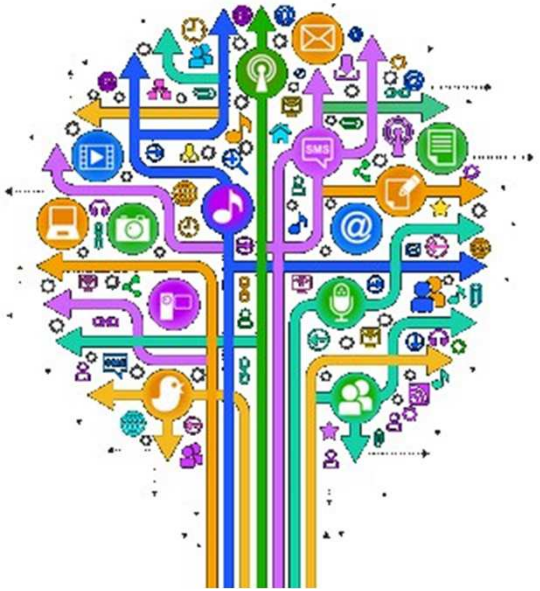
Constraints

- Constrained devices
- Energy Sufficient
- Wireless
- Plug & Play
- Large Scale Deployment
- Public environment



Technical Issues

- Secure deployment at **large scale**
- Heterogeneity, Interoperability
- Secure **protocols** for IoT
- **End-to-end** security
- Security by **design**
- Key management
- Privacy



- Untraceability
- Unlinkability
- Pseudonymization
- Anonymity

Realization

Santander Smart City

Vulnerability analysis of the IEEE 802.15.4

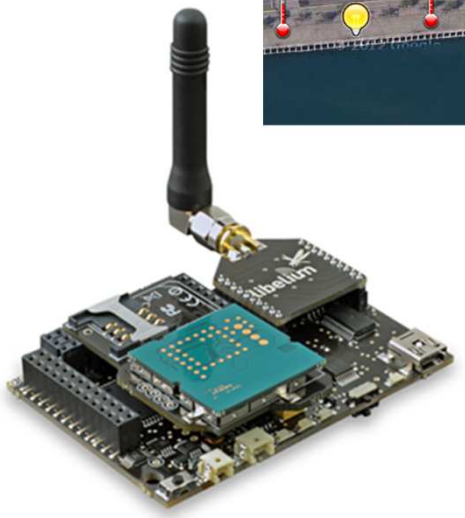
Key management framework

Security at link & application level

Deployment at large scale in a real environment

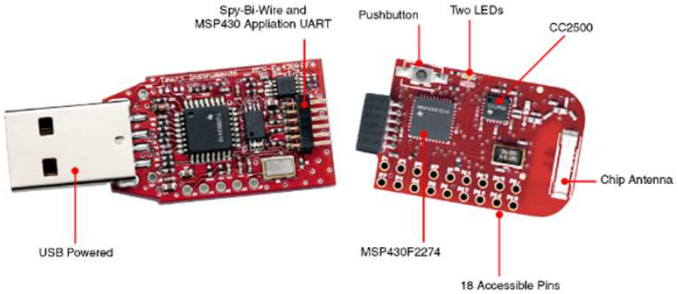
Secure protocols – Packet lost

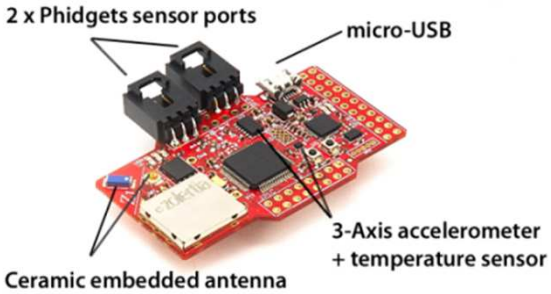
Energy monitoring – Node in sleeping mode

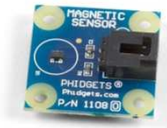


Realization

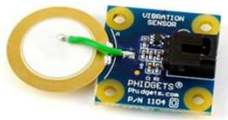
Zolertia z1







TI ez430 RF2500



Entropy source	$\mathbf{Est}(Y)$	sample size	acqui. mode	consumption
LQI	0.47	8 bits	passive	14.1 mA to 17.0 mA
Packet payload	2.8	320 bits	passive	14.1 mA to 17.0 mA
Accelerometer.X	0.22	9 bits	active	1.9 mA
Accelerometer.Y	0.42	9 bits	active	1.9 mA
Accelerometer.Z	0.36	9 bits	active	1.9 mA
Vibration sensor	0.17	16 bits	active	4.9 mA
Magnetic sensor	0.62	16 bits	active	4.9 mA

Butler Smart Life

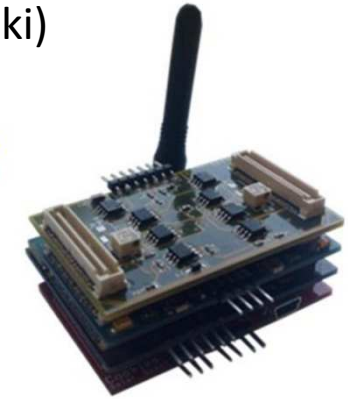
Entropy harvesting on headless devices

Zero-Knowledge secure ECC-based bootstrapping

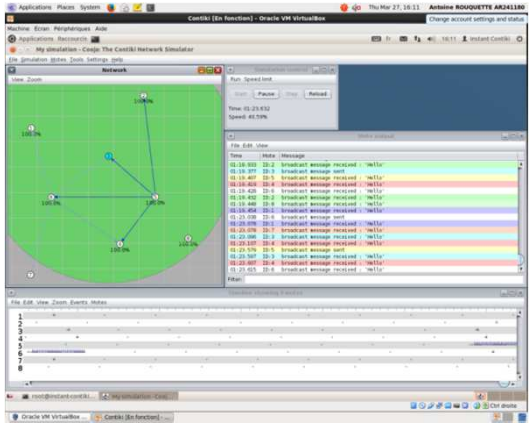
Contiki OS

Realization

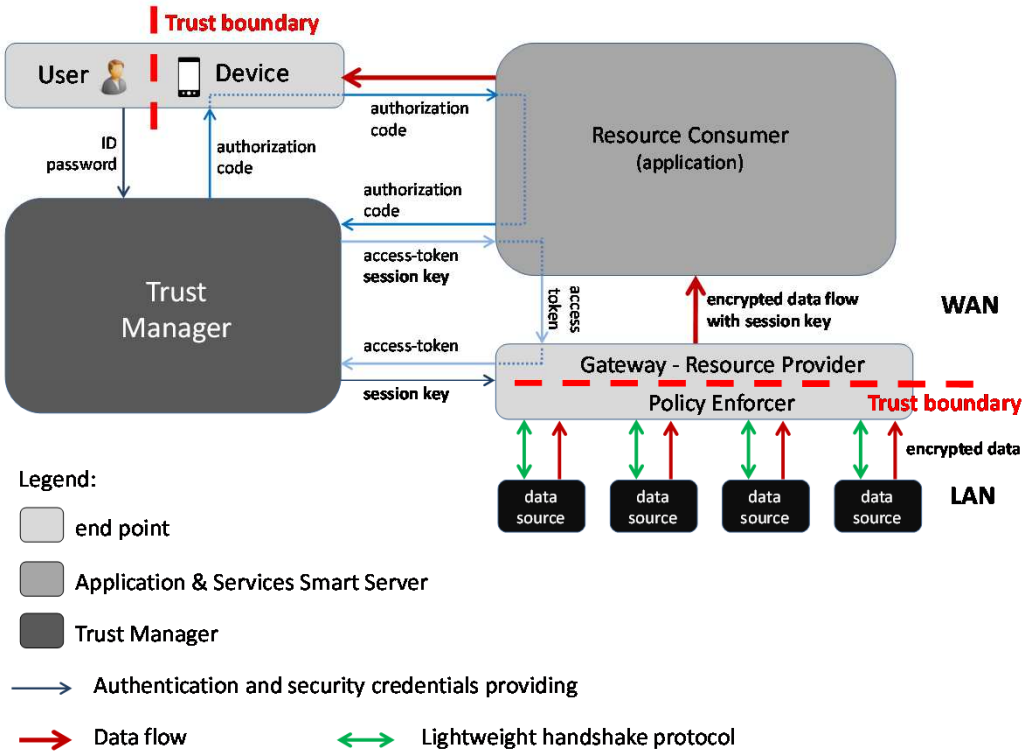
Wismote (Contiki)



Simulation with Cooja

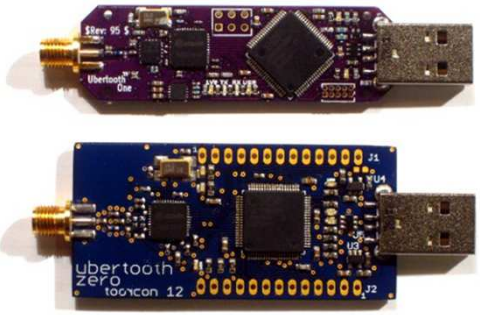


Embedded 6LoWPAN stack
End-to-end communication
End-to-end security
Security by design
Lightweight authentication
Easy bootstrapping



Realization

Ubertooth one



WiFi

AIRCRACK-NG

RFID

SocIoTal

Eavesdropping demonstrator

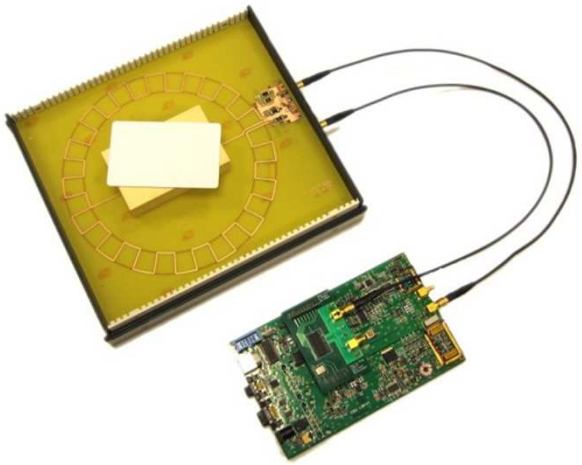
Privacy

Plan to experiment

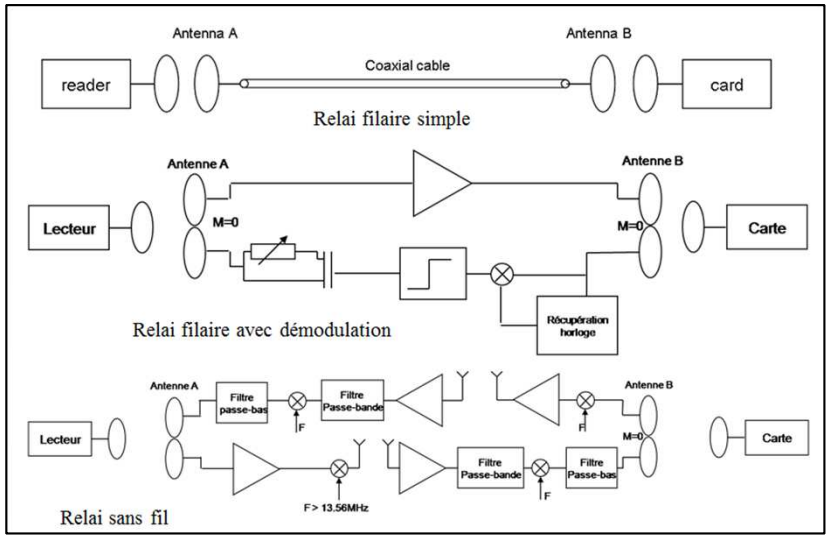
USRP

Realization

Lecteur bruité



Attaques relais



RFID

Noisy reader

Delay-based as Replay attack countermeasure

Leti

LABORATOIRE D'ÉLECTRONIQUE
ET DE TECHNOLOGIES
DE L'INFORMATION

CEA-Leti
MINATEC Campus, 17 rue des Martyrs
38054 GRENOBLE Cedex 9
Tel. +33 4 38 78 36 25

www.leti.fr

Thank you!