Blockchain : les cas d'usage à l'épreuve de la cybersécurité

Nabil Bouzerna – Architecte Plateforme IRT SystemX

Renaud Sirdey – Directeur de Recherche CEA LIST

Préparée pour France Stratégie « Enjeux et perspectives de la blockchain »

Audition du 9 mars 2017 à Paris

Nabil Bouzerna

Architecte Plateforme @ IRT SystemX (Paris-Saclay)

Biographie

Nabil Bouzerna est Architecte Plateforme à l'**IRT SystemX (Paris-Saclay)** qu'il a rejoint en 2014 après plusieurs années dans l'industrie de Défense/Renseignement puis de la Cybersécurité. Il assure le management technique du projet de cybersécurité EIC, regroupant des acteurs industriels et académiques désireux de proposer des solutions innovantes adaptées à l'Internet des Objets en général, à l'usine de futur, aux véhicules connectés et aux « Smart Grids » en particulier.

Nabil pilote notamment la conception et la réalisation de la plateforme d'expérimentation en cybersécurité CHESS, financée par l'ANSSI dans le cadre du plan NFI Confiance Numérique, afin de soutenir les efforts de R&D et de favoriser l'émergence de nouveaux acteurs nationaux répondant aux défis technologiques stratégiques actuels en cybersécurité. Nabil a notamment assuré le développement du prototype SODA-IIoT en s'appuyant sur la technologie « blockchain » pour la sécurisation des IoT/IIoT.

Renaud Sirdey

Directeur de Recherche @ CEA Tech LIST (Paris-Saclay)

Biographie

Renaud Sirdey (HDR) est directeur de recherche au **CEA (Paris-Saclay)** qu'il a rejoint en 2007 après plusieurs années au sein de l'industrie des télécoms. Ses thèmes de recherche privilégiés concernent la cryptographie, le parallélisme et la compilation. Ces dernières années, il travaille sur la cryptographie homomorphe sous l'angle de sa mise en œuvre dans des infrastructures pratiques de manipulation de données chiffrées ainsi que sur la cryptographie dite légère principalement sous l'angle de la résistance à certaines classes d'attaques physiques.

La chaîne de blocs restant pour lui une solution qui cherche un problème (au-delà de celui des cryptomonnaies), il ne s'intéresse à ce sujet (après avoir longtemps volontairement évité de le faire) que depuis qu'il s'est convaincu de l'apport potentiel de cette technologie sur au moins un cas d'utilisation concret. Sur un plan plus académique, Renaud est l'auteur ou le co-auteur de plus 60 articles scientifiques ainsi que de plus de 5 brevets et il a également contribué à et coordonné plusieurs projets de recherche collaboratifs nationaux et européens.

Plan

- Les IRT et SystemX en quelques mots
- L'expérimentation au cœur de la démarche d'innovation technologique sur la plateforme CHESS
- Problématique de la sécurité des objets connectés (ANSSI)
- Exposé « Can blockchain help increasing the security of IoT software upgrades? »
- Démonstration SODA-IIoT

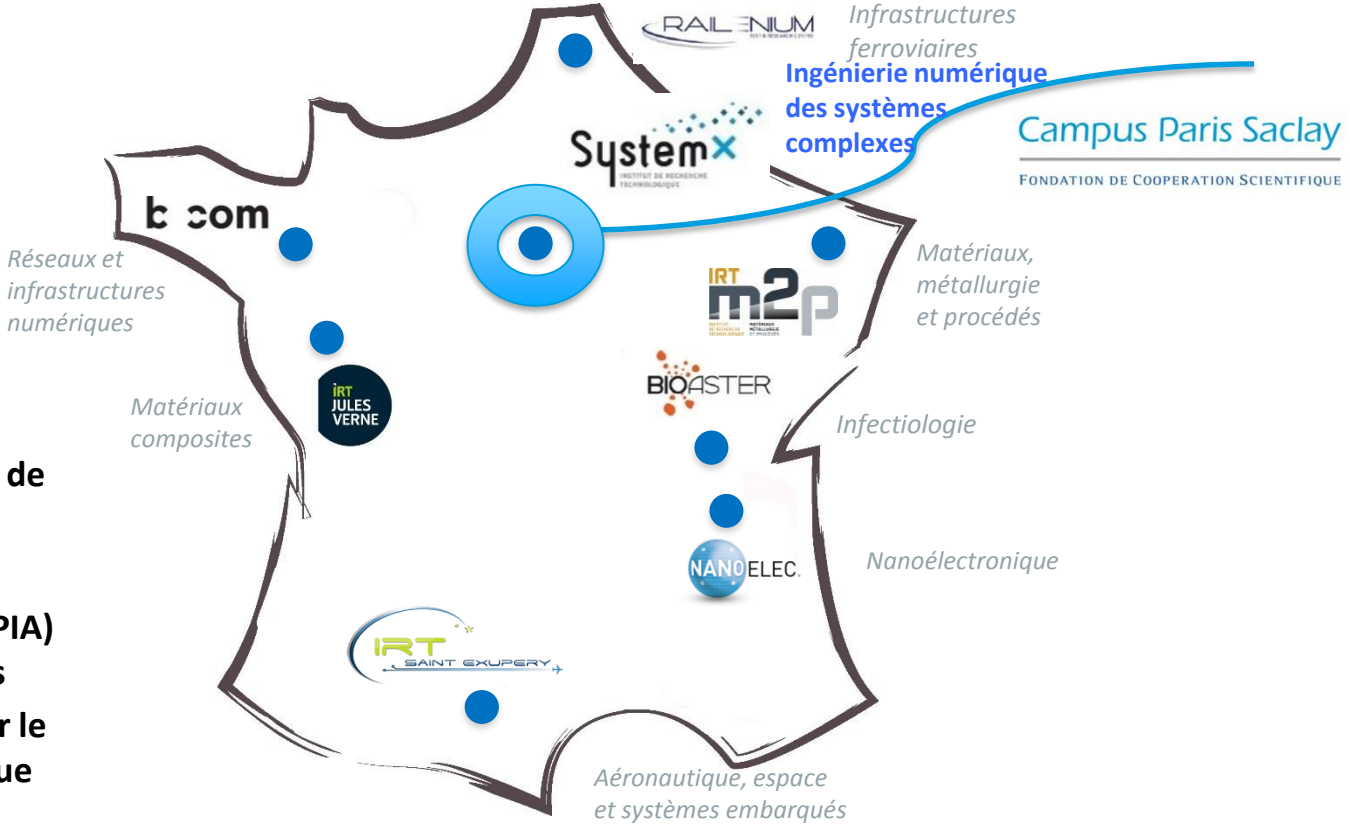
Les Instituts de Recherche Technologique

Rapport d'activité 2016 du CGI (Commissariat Général à l'Investissement)

- Les IRT sont :
  - des instituts de recherche technologique thématiques et interdisciplinaires ;
  - dont la mission est de faire émerger des innovations dans des filières économiques d'avenir au travers de partenariats stratégiques public-privé équilibrés ;
  - et qui opèrent des programmes de recherche en s'appuyant sur la co-localisation de chercheurs et sur des plateformes technologiques à la pointe de l'état de l'art ;

« En quatre ans, les IRT se sont imposés dans le paysage hexagonal. Ils sont aujourd'hui reconnus comme des **outils d'excellence** pleinement opérationnels mais aussi comme des acteurs agiles du renouveau industriel, économique et sociétal français. »

Les IRT: Une nouvelle dynamique de l'innovation



- **Lien fort avec un Pôle de compétitivité**
- **Effectifs co-localisés**
- **Financement public (PIA) sur 50% des dépenses**
- **Création de valeur par le transfert technologique**

Un écosystème dynamique au croisement des STIC

SYSTEMATIC
PARIS REGION SYSTEMS & ICT CLUSTER

700 partenaires (dont 450 PME & 125 grands groupes)

université PARIS-SACLAY

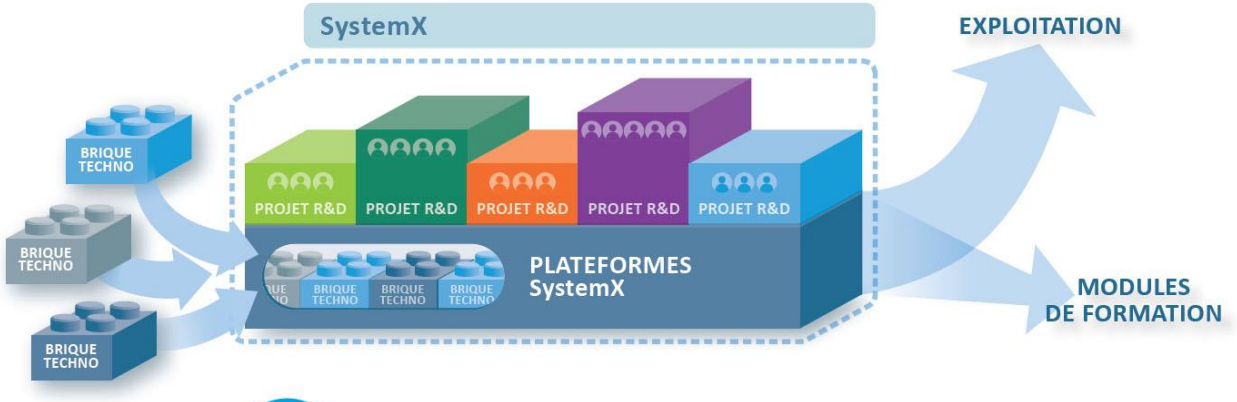
SystemX partenaire associé de l'Ecole Doctorale STIC

5 000 Chercheurs en Ingénierie et STIC

Missions

1 Création de valeur par le transfert technologique

2 Décloisonnement des mondes publics et privés



3 L'Excellence au service de l'Ingénierie Numérique des Systèmes

Ils nous ont déjà rejoints

Projet EIC et la plateforme CHESS @ IRT SystemX (2015)

- Inscrit dans l'action « plateformes » du plan Nouvelle France Industrielle (NFI) « Cybersécurité » piloté par l'ANSSI
- Labellisé par le Comité de la Filière Industrielle de Sécurité (CoFIS)

ANSSI Agence nationale de la sécurité des systèmes d'information

LA NOUVELLE FRANCE INDUSTRIELLE

Cofis Comité de la filière industrielle de sécurité

NOUVELLE FRANCE INDUSTRIELLE : FEUILLE DE ROUTE DU PLAN CYBERSÉCURITÉ

ACTION 8 : METTRE EN PLACE UN RÉSEAU DE PLATES-FORMES DE CYBERSÉCURITÉ DE TESTS ET DE DÉMONSTRATIONS

◆ Les participants ont constaté l'absence, au niveau national, de plates-formes de tests et de démonstration en matière de cybersécurité. Le développement d'une telle plate-forme (dans la pratique, il s'agirait d'un réseau de plates-formes) — dont la finalité serait de recréer un environnement aussi proche que possible d'environnements réels — aurait plusieurs intérêts :

> offrir un environnement de tests (passage à l'échelle, tests de performances, interopérabili-

ACTION 8

Mettre en place un réseau de plates-formes de cybersécurité.

PILOTE

Thales pour l'ACN.

ACTEURS PRIVÉS CONCERNÉS

Fournisseurs de cybersécurité : ACN, tous fournisseurs volontaires.
Utilisateurs de cybersécurité : CESIN, GITSIS, CLUSIF, SYNTEC, etc.
Pôles : IRT SystemX, pôle d'excellence cyber, IRT Bcom.

Activités de Recherche & Développement de SystemX

En ligne avec le plan « Cybersécurité » de la Nouvelle France Industrielle (NFI)

- **Cybersécurité & Confiance Numérique à l'IRT SystemX**
  - Environnement d'Intégration & Interopérabilité Cybersecurité (**EIC**) 2015
  - Cyber Sécurité du Transport Intelligent (**CTI**) 2016
  - Blockchain for Smart Transaction (**BST**) 2016
  - SOC Next Generation & Cyber Threats Intelligence (**SNG** en cours de montage) 2017
  - Usine du Futur & IIoT / Industrie 4.0 (**Io4** en cours de montage) 2017

Nouvelle France Industrielle (2017)

Les outils spécifiques à l'Économie des données

Label France Cybersecurity

Faire référencer et connaitre à l'export son offre en matière de cybersécurité, avec le label France Cybersecurity.

Plateforme CHESS portée par l'IRT System'X

Répondre aux défis que rencontrent les industriels dans les phases de conception, de modélisation, de simulation et d'expérimentation des innovations futures pour la sécurité du numérique avec la plateforme CHESS.

Appel à projets PIAVE 2 (clôture le 17 février 2017)

Axe 5 – Démonstrateur Cybersécurité des systèmes industriels

Les Systèmes Industriels présents dans les infrastructures critiques et les usines de fabrication, ont

- la capacité à détecter les signaux faibles précurseurs d'attaques ;
- la standardisation et la certification des solutions proposées ;
- la prise en compte des aspects humains et opérateurs dans les solutions développées ;
- la capacité à intégrer la dimension cyber aux outils de supervision de production ;
- la formation des personnels impliqués ;
- la cohérence avec les travaux déjà engagés, notamment autour de la plate-forme Chess de l'IRT SystemX.

« Sécurité des personnes et des biens, des infrastructures et des réseaux»

EIC : La Cybersécurité appliquée à 4 cas d'usage innovants

- **L'Usine du Futur**
  - Des SCADA à l'Usine 4.0 reposant sur l'Internet des Objets Industriels (IIoT)
- **Les Smart Grids**
  - Les futurs Réseaux d'énergie numérisés et intelligents (IIoT)
- **Le Véhicule Connecté & son Environnement**
  - Le transport connecté et autonome (IIoT)
- **Les Systèmes d'Information d'Entreprise, la gestion de la mobilité et les nouveaux services associés**
  - L'Internet des Objets (IoT/M2M) et les menaces émergentes

Une plateforme c’est bien, mais pour faire quoi concrètement ?

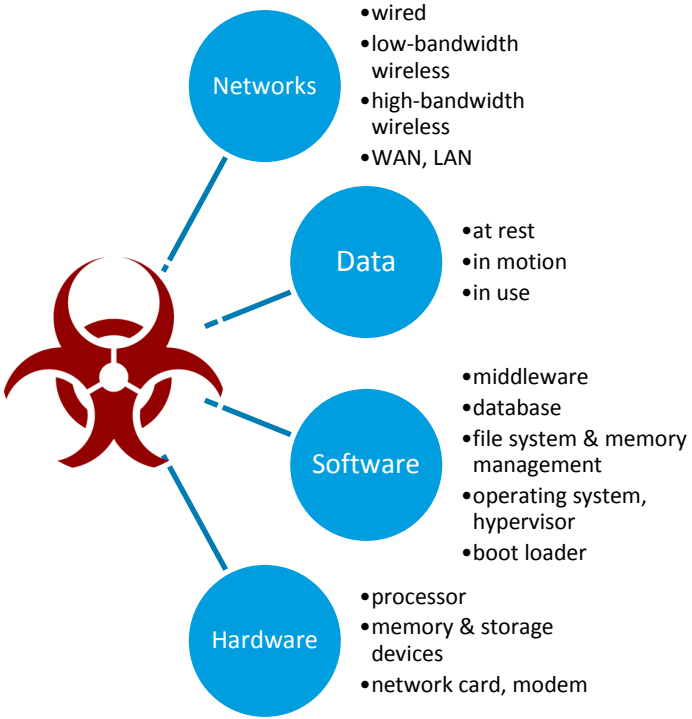
Feuille de route suivie à partir des cas d'usage

Architectures sécurisées et/ou durcissement

Recherche de vulnérabilité/faille

Reproduction de l'architecture cible

Expérimenter : variabilité offerte par la plateforme CHESS



Moyen d'expérimentation et/ou de simulation

Des capacités significatives « Hardware » et « Software » pour l'expérimentation et le prototypage rapide

Capacités matérielles

- Equipements de terrain
- Boards de développement (>30 types)
- Démonstrateurs pour les 4 cas d'usage
- 25 serveurs @ISX dont un HPC Bullx
  - 848 cœurs physiques
  - 1696 cœurs logiques
  - 5 Téraoctets RAM
  - Up to 6,72 Pétaoctets de stockage

Capacités logicielles

- Virtualisation & Simulation
- Ateliers à base de COTS et/ou OSS
- Couche d'intégration/d'interopérabilité
- Déploiement semi-automatique
- Preuves de Concepts pour valider expérimentalement nos travaux théoriques

Moyen d'expérimentation et/ou de simulation

Des capacités significatives « Hardware » et « Software » pour l'expérimentation et le prototypage rapide

- **Capacités m**
  - Equipeme
  - Boards de
  - Démonstr
  - 25 serveu
    - 848 c
    - 1696
    - 5 Téra
    - Up to

OSS

pérabilité

ue

ider

ux

Capacité d'expérimentation et de simulation

Passage à l'échelle IT/IoT/IIoT avec la Blockchain (ou pas)

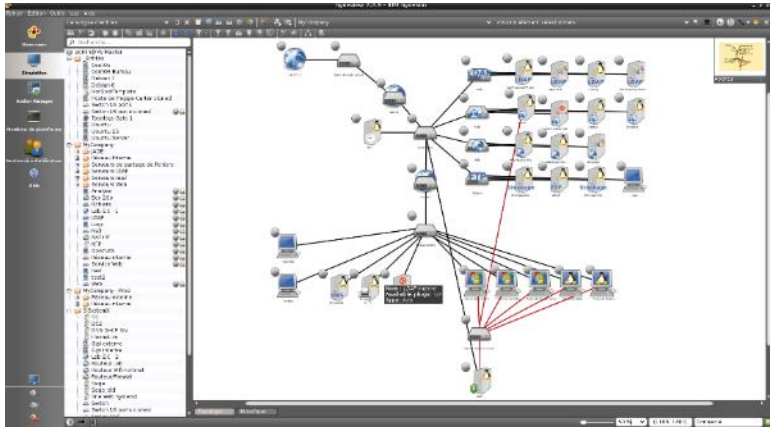
- **vIT (virtual IT) & vIoT (virtual IoT)**
  - Capacité à provisionner rapidement un grand nombre de VMs IT (x86) et IoT (ARM)
  - Jusqu'à 800 VMs ARM par serveur en 20 minutes
    - Ex : **SODA-IIoT/Blockchain soit 12 000 nœuds**

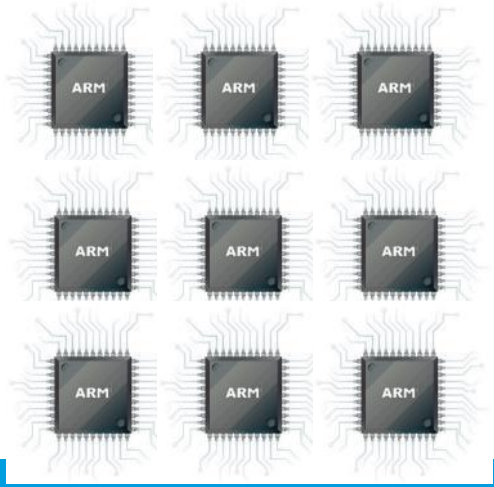
- **BMPC: Bare Metal Provisioning and Configuration**
  - Capacité de « provisioning » et de configuration « bare-metal »

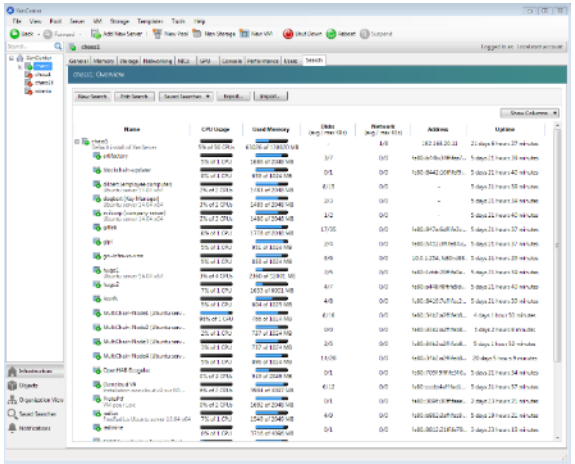
Capacités d'expérimentation et de simulation

Socle de la plateforme CHESS

- **Capacités de virtualisation : vIT, vIoT et BMPC**
  - OSS : KVM, QEMU, Proxmox, Apache MESOS, OpenStack, …
  - OSS/COTS : XenServer, Hynesim (Diateam), VMware, VirtualBox, Hyper-V…
- **Capacités de « conteneurisation » :**
  - OSS : Kubernetes, Docker Swarm, LXC, …



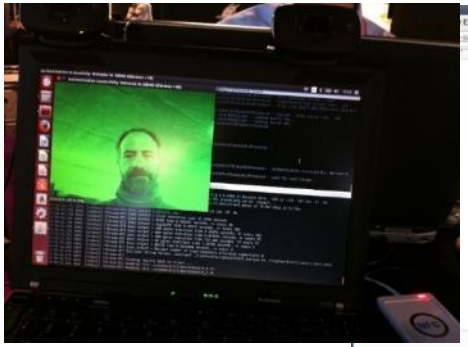


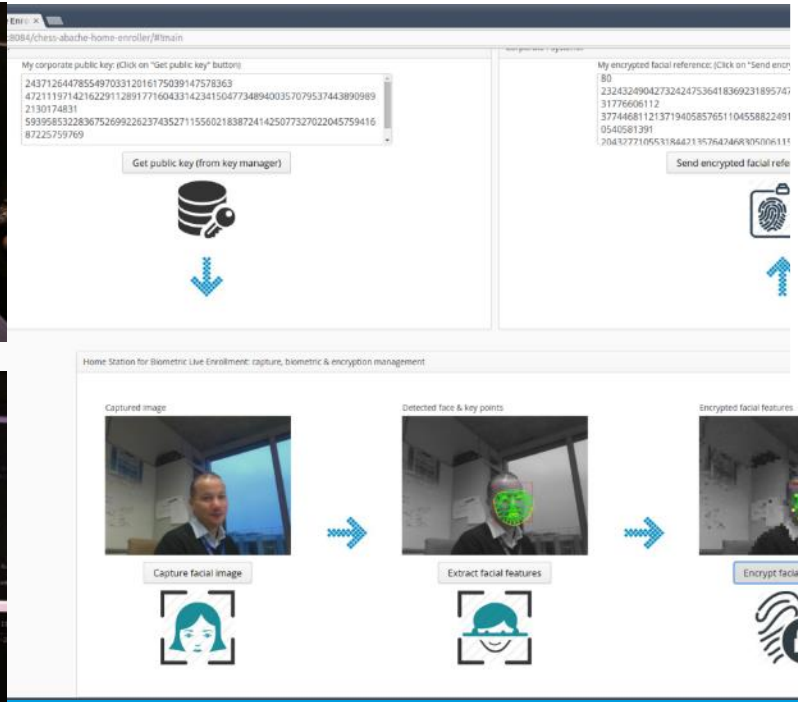


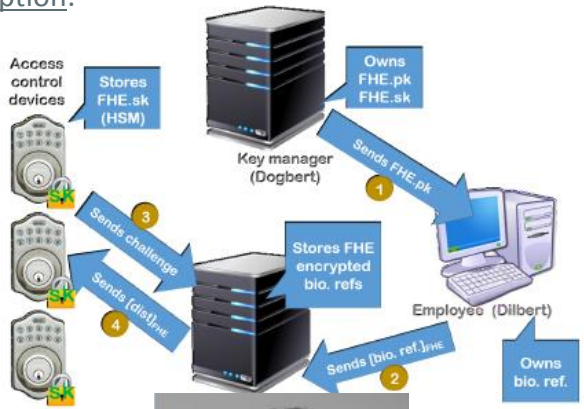
ABACHE (Data Privacy)

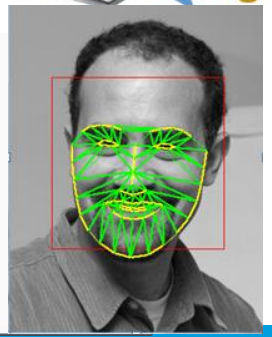
Démarche scientifique (évaluation par ses pairs) et industrielle (prototypage rapide)

- **Démonstrateur ABACHE intégré à la plateforme CHESS**
  - An access control system with mullti-factor authentication (Biometric and NFC/RFID card and/or secure token) which strengthens confidentiality of biometric data thanks to homomorphic encryption.





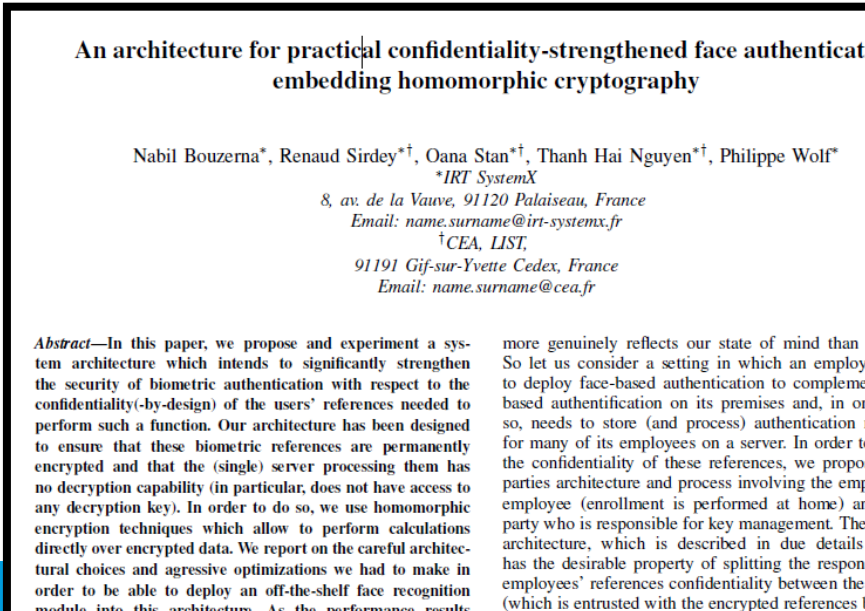




ABACHE (Data Privacy)

Démarche scientifique (évaluation par ses pairs) et industrielle (prototypage rapide)

- **ABACHE : Anonymous Biometric Access Control based on Homomorphic Encryption**
  - An access control system with multi-factor authentication (Biometric and NFC/RFID card and/or secure token) which strengthens confidentiality of biometric data thanks to homomorphic encryption
  - Démonstrateurs
    - ABACHE Cryptosystème de Paillier (Java)
    - N-ABACHE Cryptosystème de Paillier (C++)
    - H-ABACHE Cryptosystème « Fully Homomorphic » (C++)
    - T-ABACHE Cryptosystème embarqué sur tablette Android
  - Publication à la conférence IEEE CloudCom 2016 le 15/12/2016 dans le track 6 « Security and Privacy »



An architecture for practical confidentiality-strengthened face authenticat
embedding homomorphic cryptography

Nabil Bouzerna*, Renaud Sirdey*†, Oana Stan*†, Thanh Hai Nguyen*†, Philippe Wolf*
*IRT SystemX
8, av. de la Vauve, 91120 Palaiseau, France
Email: name.surname@irt-systemx.fr
†CEA, LIST,
91191 Gif-sur-Yvette Cedex, France
Email: name.surname@cea.fr

Abstract—In this paper, we propose and experiment a system architecture which intends to significantly strengthen the security of biometric authentication with respect to the confidentiality(-by-design) of the users' references needed to perform such a function. Our architecture has been designed to ensure that these biometric references are permanently encrypted and that the (single) server processing them has no decryption capability (in particular, does not have access to any decryption key). In order to do so, we use homomorphic encryption techniques which allow to perform calculations directly over encrypted data. We report on the careful architectural choices and agressive optimizations we had to make in order to be able to deploy an off-the-shelf face recognition

more genuinely reflects our state of mind than
So let us consider a setting in which an employ
to deploy face-based authentication to compleme
based authentification on its premises and, in or
so, needs to store (and process) authentication
for many of its employees on a server. In order t
the confidentiality of these references, we propo
parties architecture and process involving the emp
employee (enrollment is performed at home) ar
party who is responsible for key management. The
architecture, which is described in due details
has the desirable property of splitting the respon
employees' references confidentiality between the
(which is entrusted with the encrypted references

Sécurisation des protocoles « Smart Grids » : MQTT + Blockchain

- **Sécurité des « smart meters » avec la « blockchain » (Oct. 2016)**
  - Intégration au sein de la plateforme CHESS du prototype « Secure MQTT » de Gemalto pour la gestion du contrôle d'accès dans la « Smart Grids » et l'IoT

Design & développement d'une version **décentralisée** par IRT SystemX
Décentralisation en exploitant la technologie « **Blockchain** »

  - Gestion centralisée des ACL (Single Point of Failure / **Single Point of Attack**)
  - Demande d'étude @SystemX pour remédier au SPoF / **SPoA**

BLOCKCHAIN

FIC 2017 : Pour Guillaume Poupard, de l'Anssi, «les objets connectés industriels sont la priorité»

INTERVIEW | NUMÉRIQUE & INFORMATIQUE | CYBERSÉCURITÉ | INTERNET DES OBJETS | OBJETS CONNECTÉS

PAR JULIETTE RAYNAL PUBLIÉ LE 23/01/2017 À 09H00

Guillaume Poupard, responsable de l'Anssi
© Guittet Pascal Guittet Pascal

La 9ème édition du Forum international pour la cybersécurité (FIC), qui doit ouvrir ses portes demain, accordera une place prépondérante à la sécurité des objets connectés, dont les attaques ont largement occupé la scène médiatique au cours des derniers mois (Tesla, serveur DNS de Dyn, ampoules Philips). Sommes-nous bien préparés pour faire face à cette déferlante ? Quels scénarios sont à craindre ? Comment répondre à ces enjeux ? Existe-t-il des verrous technologiques particuliers ? Guillaume Poupard, le chef de l'agence nationale de la sécurité des systèmes d'information (Anssi), a répondu aux questions *d'Industrie & Technologies* dans une interview exclusive.

Industrie & Technologies : Outre le marché grand public, les objets connectés envahissent également le monde industriel...

Guillaume Poupard : C'est ça, notre priorité. On se rend compte que le numérique envahit le monde industriel. Que ce qui était encore

SUR LE MÊME SUJET

Cybersécurité : des chercheurs américains craignent des morts à cause des objets connectés
06/12/2016

Sécurité des objets connectés

Attaques qui ont largement occupé la scène médiatique au cours des derniers mois

[Vidéo] Le freinage brutal d'une Tesla piratée

[Vidéo] Des chercheurs piratent les lampes connectées de Philips

CYBERSÉCURITÉ | PHILIPS | NUMÉRIQUE & INFORMATIQUE | INTERNET | INTERNET DES OBJETS | VIDÉO
PAR JULIETTE RAYNAL PUBLIÉ LE 04/11/2016 À 15H53

Attaque contre Dyn : Comment les objets connectés ont servi à paralyser le web

AVIS D'EXPERT | CYBERSÉCURITÉ | NUMÉRIQUE & INFORMATIQUE | OBJETS CONNECTÉS | INTERNET DES OBJETS
PUBLIÉ LE 24/10/2016 À 16H02

Vendredi 21 octobre, une cyberattaque majeure a perturbé les internautes du monde entier. En effet, une attaque par déni de service (DDoS) a paralysé le service DNS Dyn, utilisé notamment par Netflix, Twitter, Spotify ou encore le Playstation Network, bloquant l'accès à ces services. David Emm, chercheur en sécurité chez l'expert Kaspersky Lab, explique comment les attaquants ont exploité les failles de sécurité des objets connectés pour faire trembler une partie de la toile.

- **Problématique adressée sur la plateforme CHESS :**
  - **le maintien en condition de sécurité** des millions (**milliards ?**) d'objets connectés i.e. mise à jour corrective et/ou évolutive software ou firmware
  - Typologie d'attaque contre le service « DNS » (résolution des nom serveur vers adresse IP, colonne vertébrale de l'Internet)
    - Point d'accès wifi malicieux
    - DNS local compromis au niveau d'une « box Internet »
    - Vulnérabilité d'un équipement réseau de routage (Cisco) ou de sécurité (Fortinet) :
      - Documents « Shadow Brokers » NSA
      - Documents « Snowden » concernant l'équipe TAO NSA

Cisco, Fortinet issue fixes against Equation Group exploits

August 18, 2016 By Pierluigi Paganini

My Page

G+1 8

Customers of Cisco and Fortinet security firms need to patch

Forbes LOG IN

YOUR READING LIST

Cisco And Fortinet Confirm Flaws Exposed By Self-Proclaimed NSA Hackers

The Limit Does Not Exist: Explore, Experiment And

Security / #CyberSecurity

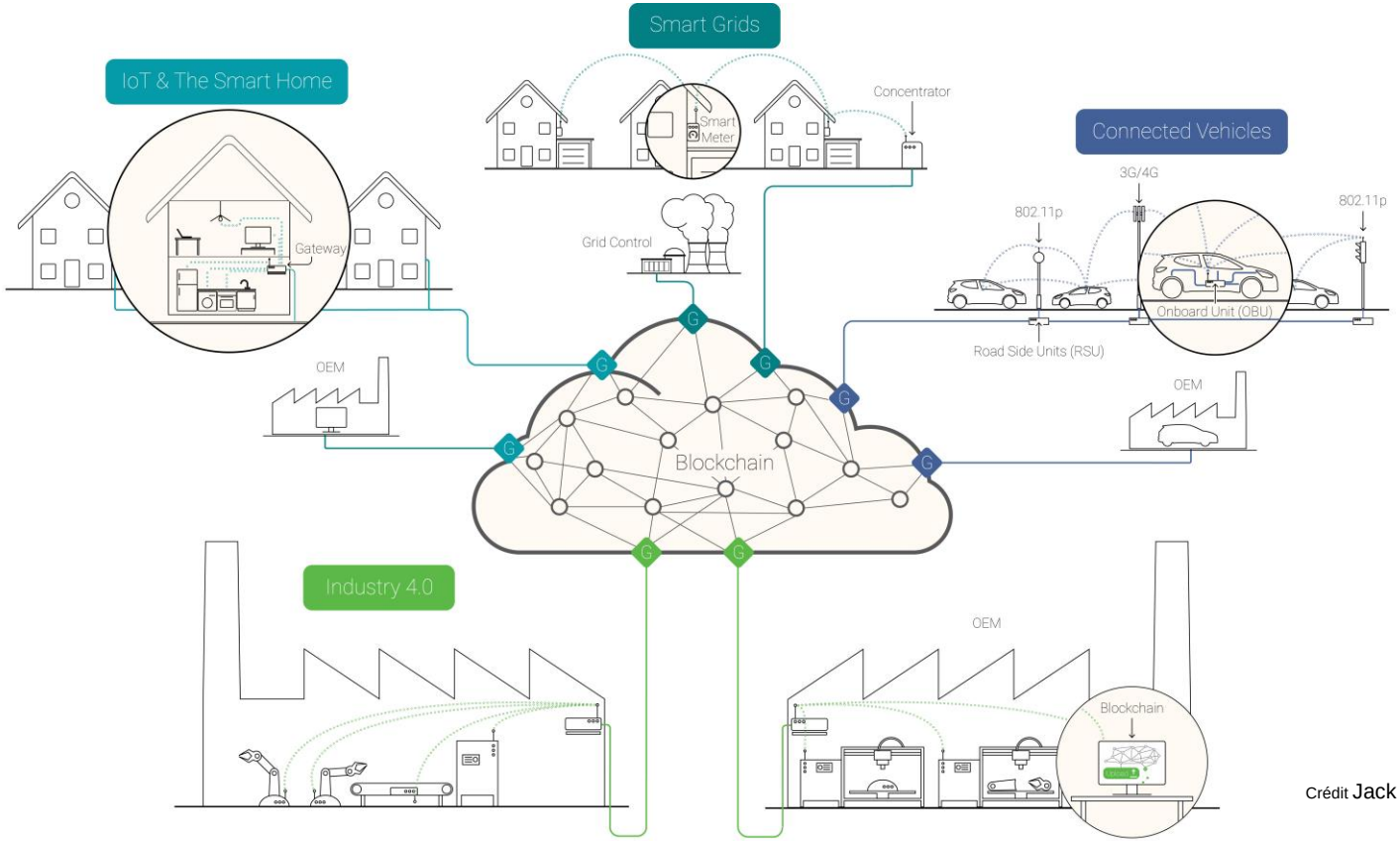
AUG 17, 2016 @ 04:19 PM 15,997 VIEWS

The Little Black Book of Billionaire Secrets

Cisco And Fortinet Confirm Flaws Exposed By Self-Proclaimed NSA Hackers

SODA-IIoT : une option pour la MaJ sécurisée des « IIoT »

Architecture décentralisée pour la MaJ « Firmware/Software » des « IIoT » via une « blockchain »



Crédit Jack FAZAKERLEY

Publication scientifique IEEE S&B 2017

Démarche scientifique (évaluation par ses pairs) et industrielle (prototypage rapide)

IEEE SECURITY & PRIVACY ON THE BLOCKCHAIN (IEEE S&B)

AN IEEE EURO SECURITY & PRIVACY AND EUROCRYPT AFFILIATED WORKSHOP

29 April 2017

H

Security ar

Today, the se
of further rese
a practical me
decentralized
properties ass
transactions c
privacy. Gene
Ethereum are
contracts in E
need to be de

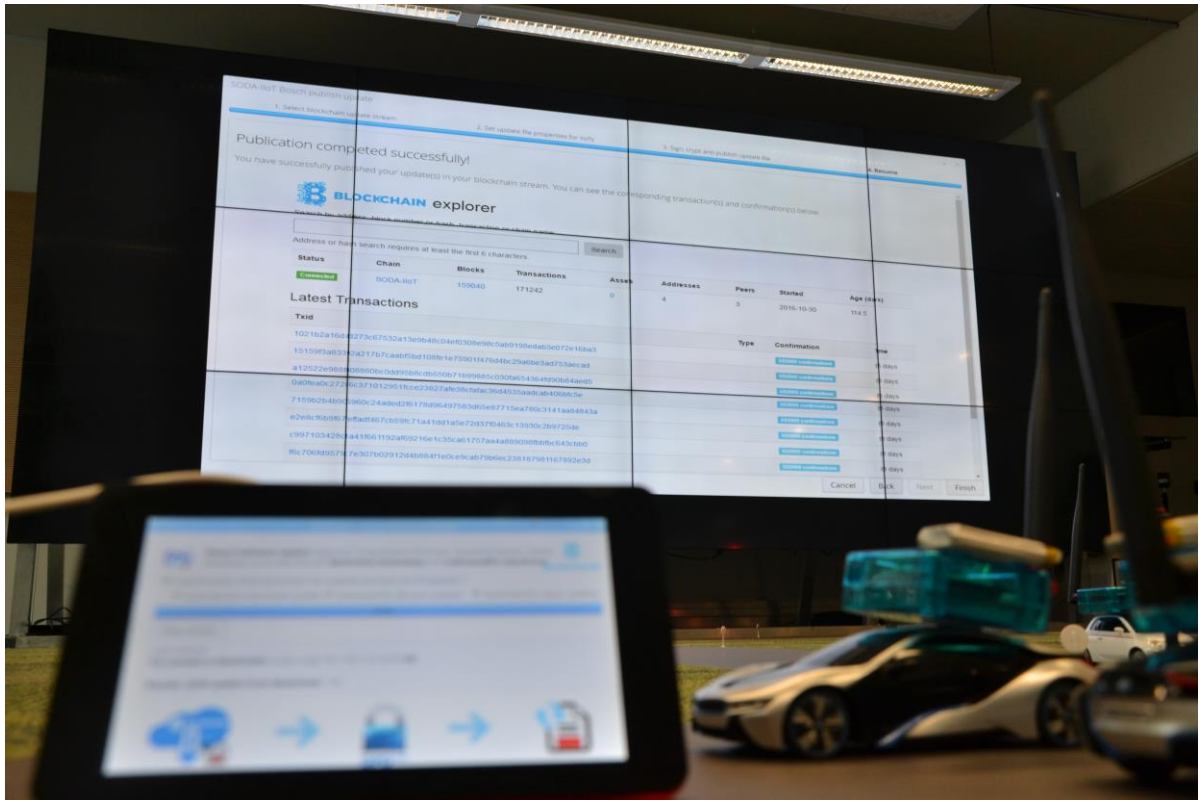
Call for P

Towards Better Availability and Accountability for IoT Updates by means of a Blockchain

Aymen Boudguiga*, Nabil Bouzerna*, Louis Granboulan†, Alexis Olivereau‡,
Flavien Quesnel*, Anthony Roger* and Renaud Sirdey‡*
*IRT SystemX, 8 avenue de la Vauve 91120–Palaiseau, *firstName.lastName@irt-systemx.fr*
†Airbus Group Innovations, *louis.granboulan@airbus.com*
‡CEA–LIST, 91191 Gif-sur-Yvette, *firstName.lastName@cea.fr*

***Abstract*—Building the Internet of Things requires deploying a huge number of objects with full or limited connectivity to the Internet. Given that these objects are exposed to attackers and generally not secured-by-design, it is essential to be able to update them, to patch their vulnerabilities and to prevent hackers from enrolling them into botnets. Ideally, the update infrastructure should implement the CIA triad properties,** and *innocuousness* for IoT objects. Availability and also integrity result from the persistence property of the blockchain. That is, once an update is added to the blockchain as part of a valid block, it becomes impossible to erase it. As such, we defeat malicious entities that prevent software updates from being distributed, in order to benefit from current

L'espace d'expérimentation pour la cybersécurité@SystemX



Crédit Flavien Quesnel

Can blockchains help increasing the security of IoT software upgrades?

(in terms of availability)

Renaud Sirdey
Research Director @ CEA LIST
(based on work with other people)

March 2017

- **Assets.**
  - Stuff that we care about.
    - E.g. personnal data, passwords, cryptographic key, bitcoins, etc.
- **Threats.**
  - Bad things we think may happen to the stuff we care about.
    - E.g. divulgation of personnal data, etc.
- **Countermeasures.**
  - Things we can do that prevents those bad things to happen to the stuff we care about.

The CIA triad

- **Confidentiality.**
  - The property of an asset to remain secret for as long as it is supposed to.
- **Integrity.**
  - The property of an asset to remain unaltered for as long as it is supposed to.
- **Availability.**
  - The property of (probability of) an asset to be accessible when it is supposed to.

A solution in search of a problem…

- **Do we need a blockchain in a given application setting?**
- **Well, only if it provides an effective countermeasure to a well identified threat.**
  - Think of bitcoin and the double-spending threat.
- **Otherwise there's no point! So let's see.**

- **Context:**
  - A bunch of connected object manufacturers deploying…
  - … (hopefully) many connected objects…
  - … Hacked around subject to TTM-constraints.

- **Constraints:**
  - So the objects' software must be upgradable.
  - Asset: the software of a connected object.
  - W. r. t. threats coming from the diffusion network infrastructure.

- **Integrity (mandatory):**
  - Only unaltered genuine software may be deployed on an object.
    - Though it might contains unintentional bugs.
- **Confidentiality (optional):**
  - The object software might not just be an aggregate of off-the-shelf open source libs.
    - So there might be Intellectual Property to protect (PS: reverse-engineering of binaries is NOT that hard).

Crypto (as often) to the rescue

- **Integrity (mandatory):**
  - The manufacturer has a public/private key pair it uses for signing stuff.
    - That public key is somehow « burnt » into the objects.
  - (An hash of) every software update must be signed.

- **Confidentiality (optional):**
  - Each object has its own public/private key pair.
  - Every software uprade is encrypted under the object's public key.
    - The object secret key is somehow « burnt » into the object before commisioning.
    - The manufacturer owns all the keys so there's no PKI.

Sweeping availability back from under the rug…

- **Scary movie: an entity wishes to prevent a software upgrade to reach a pool of connected object so as to maintain an actionable vulnerability.**

- **Think how easy it is to DoS or impersonate a small startup infrastructure.**
  - But can someone do that on the bitcoin p2p support network?

- **So there might be something to do with (a massive enough) blockchain to solve availability issues.**

What exactly is (a massive enough) blockchain?

- **Functionaly, it is a public, causal, highly-available, immutable (more or less general-purpose) register*.**
- **And that's all.**
- **Then there's the « how » (more on that later):**
  - Causality: through hash chaining.
  - Unalterability: by ensuring that register updates have a real-world cost.
    - And such that it becomes prohibitively costly to rewrite the past.

* Even smart contract-enabled blockchain are registers storing programs and successive program states (just like if the programs were executed by hands on a workbook).

Back to our IoT setup

- **Let's use a blockchain as a high-availability communication channel.**
- **A given manufacturer puts signed, encrypted updates into the chain in question.**
  - And can check it is effective.
- **A given object can periodically poll random support nodes to check whether an update is available.**
  - Objects apply only genuine updates.
  - And acknowledge successfull updating in the blockchain as well.

On mining (sweeping the « massive enough » back from under the rug)

- **Mining is functionaly equivalent to organizing a lotery amongst the nodes of the supporting p2p network.**
  - Finding a partial hash-collision commits the player to spend energy=CPU=money.
  - When the collision eventually happens (for a miner) is by construction random.
  - « Richer folks » win more often than « poorer ones » (but the latter can sometimes be lucky).

- **Finding partial hash collisions is the fundamental mecanism allowing to assign a real-world cost to registry updates.**
  - If you’re a bunch of mutually trusting friends: please don’t mine!

- **My theory: bitcoin will be the only genuine (public) blockchain ever in human history.**
  - Consider it's now pacing at ~ 2^{60+} hashes/secs vs ~2^{40} for the (hence vulnerable) « fastest looser ».
- **But the difference between the pre- and post-bitcoin era, is that we now have one massive enough blockchain!**
- **Corollary: any new « blockchain » should be built upon the bitcoin blockchain.**
  - So we need to find generic ways of doing this (and we are pursuing serious options to do that).

De l’idée au concret → Démonstration SODA-IIoT

Merci de votre attention
Des questions? (ou pas ☺)

nabil.bouzerna@irt-systemx.fr (Architecte Plateforme)

www.irt-systemx.fr

Renaud.sirdey@cea.fr (Directeur de Recherche CEA)

http://www-list.cea.fr