Colloque IMT
« Entrons-nous dans une nouvelle ère de la cyber-Sécurité ? »

10 novembre 2017

Posters

Institut Mines-Télécom

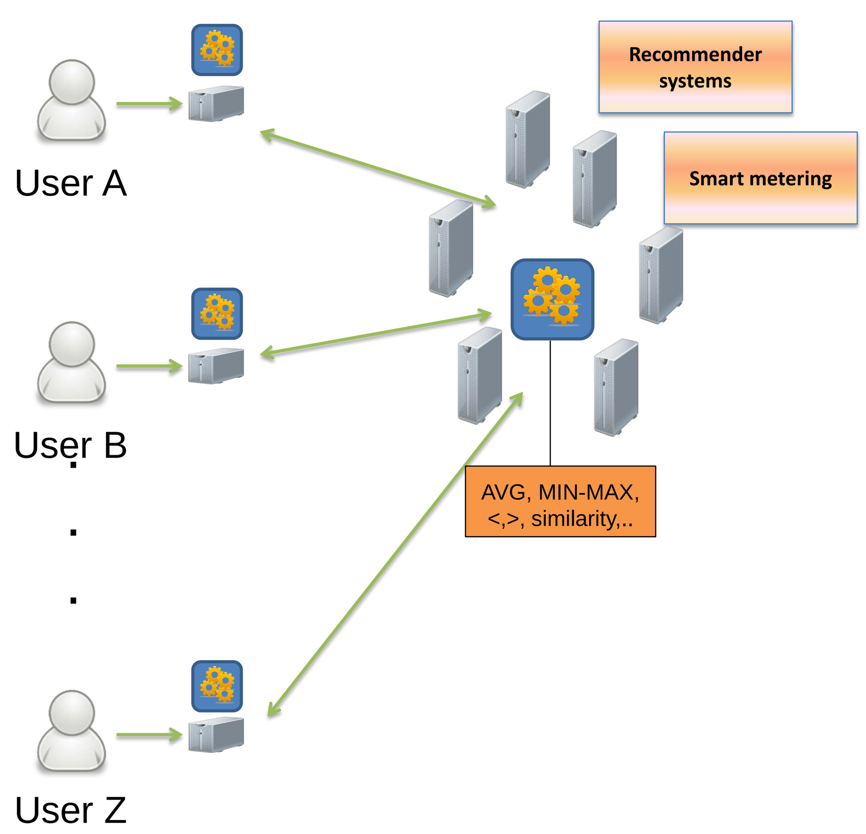
EURECOM

Privacy for User Centric Networking

Monir Azraoui, Refik Molva, Melek Önen and Cédric Van Rompay

User Centric Networking

Overview

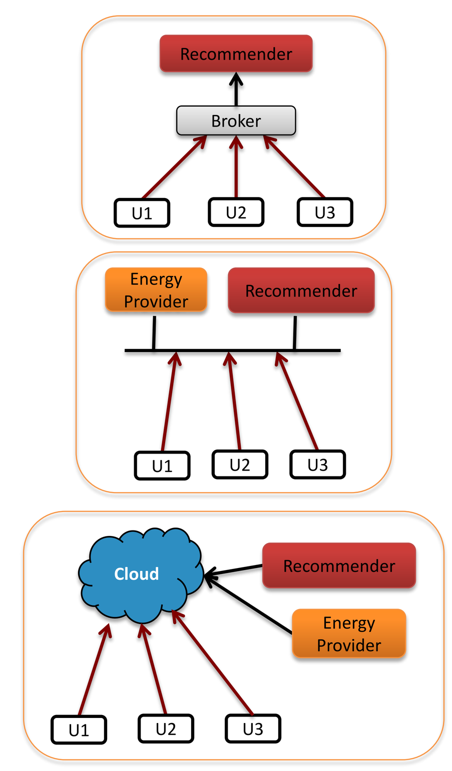


Privacy & Security Challenges

- Environment
  - Data about users collected individually
  - Limited storage ⇒data outsourcing
  - Access by third parties (honest but curious or totally malicious)
  - No coordination/trust among users
- Use cases
  - Smart home
  - Recommender systems

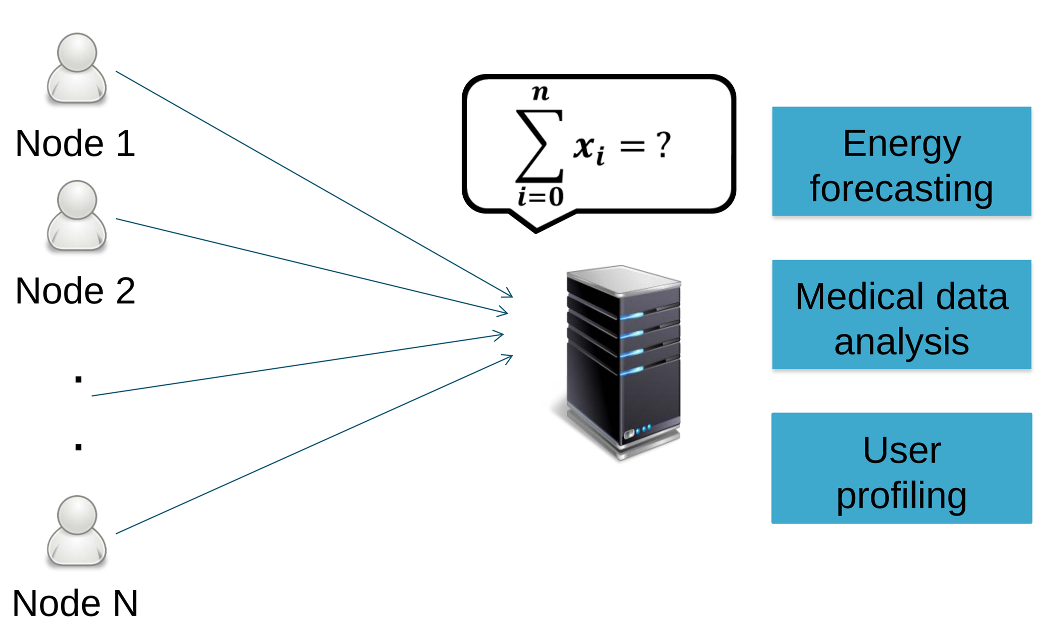
Security Models

- No access to data
  - Users' private information is not leaked to any third party
- Partial access to data
  - External parties are allowed to learn some information about users' data
- Full access to data
  - Access is controlled: third parties only learn the result of the search and nothing more



Privacy preserving and unforgeable data aggregation [CANS'14, CANS'15]

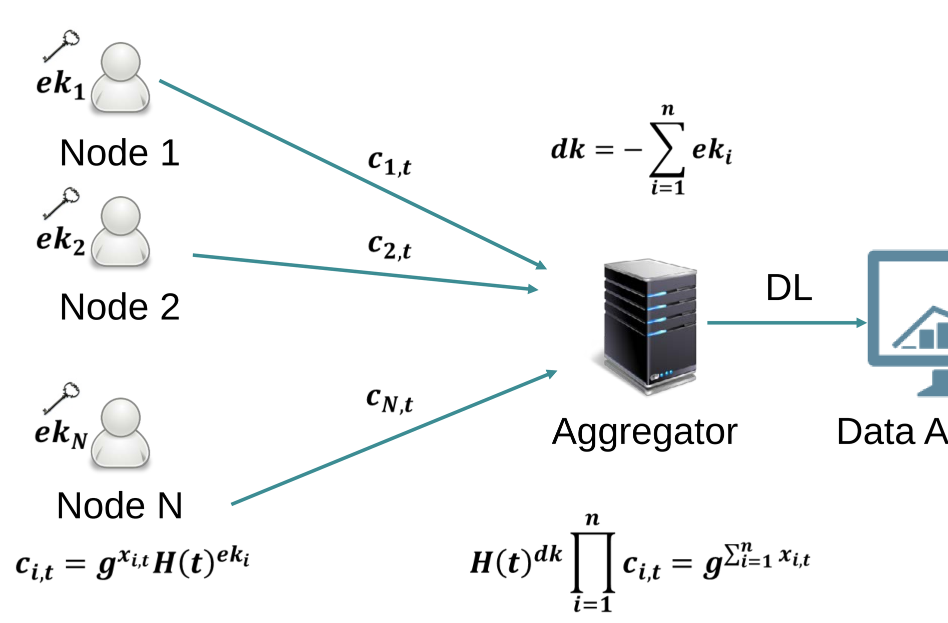
Privacy Preserving Data Aggregation



Aggregator of users' data is not trusted

➢**Compute sum of users' data without revealing individual values to aggregator**

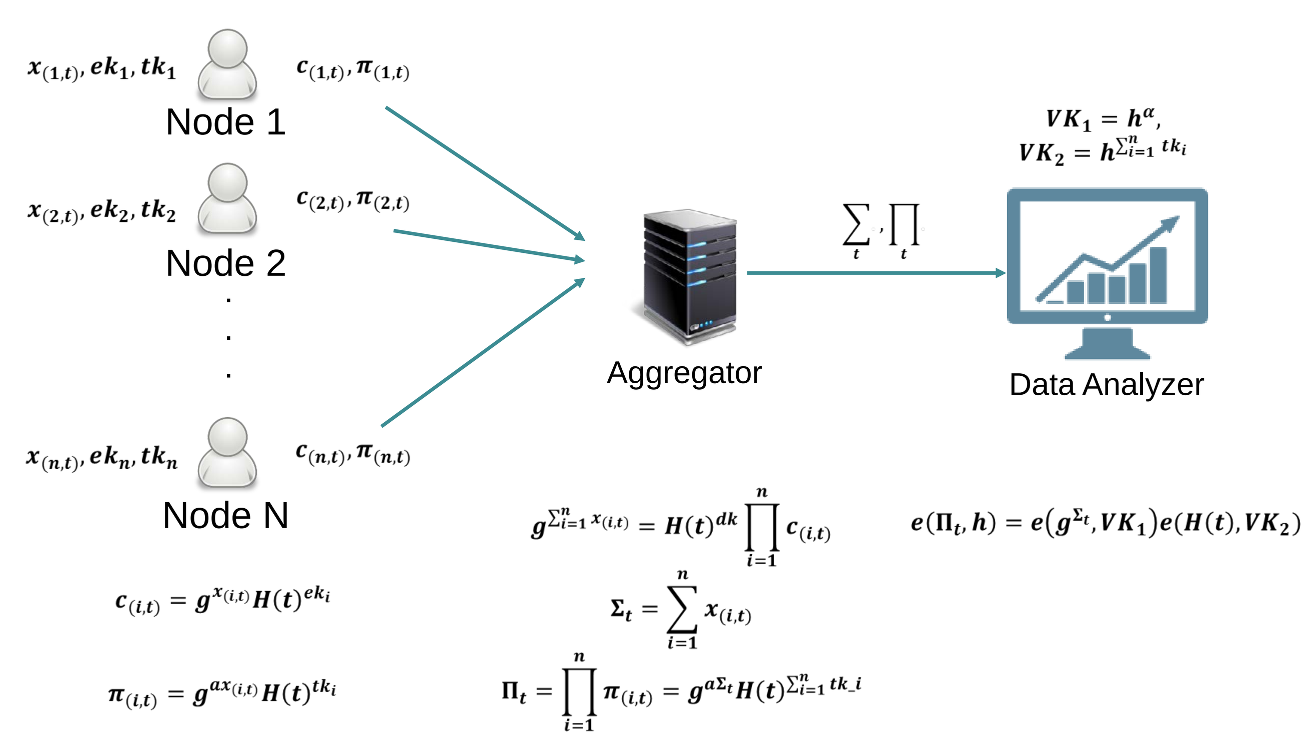
Private data aggregation [Shi et al.'11]



➢**Aggregator obliviousness**
No access to individual data

➢**New challenge: Result unforgeability**
Aggregation correctness
Efficient verification

Our solution PUDA

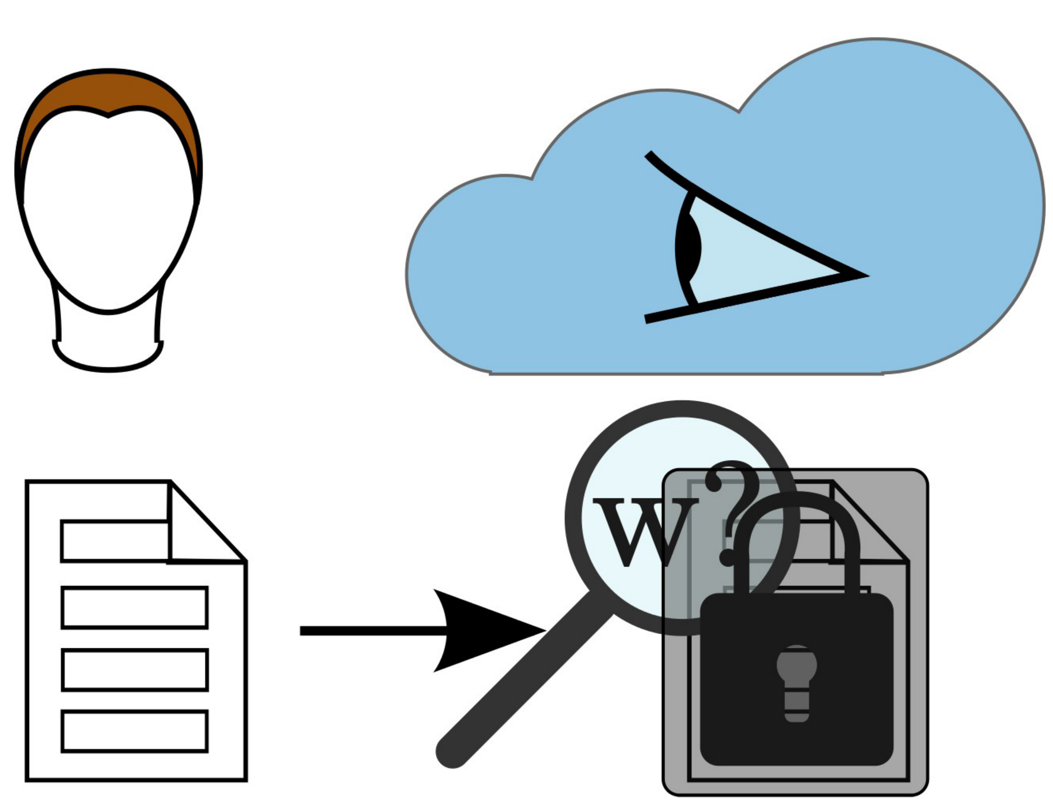


➢**Aggregator obliviousness**
Proof based on DDH and ROM

➢**Result unforgeability**
Proof based on new assumption LEOM

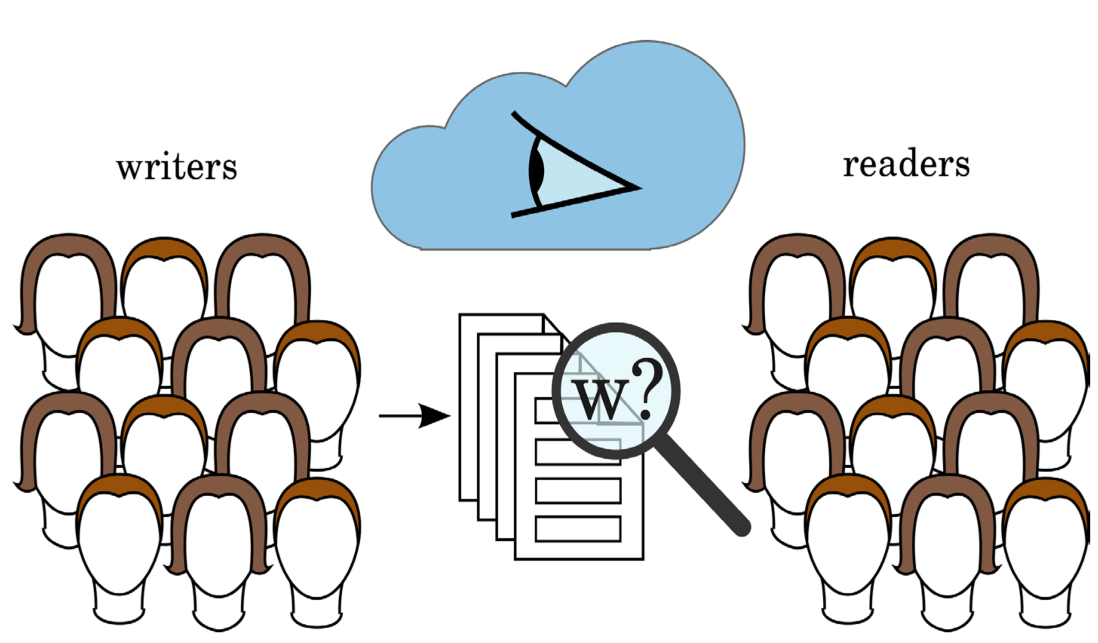
Multi-User searchable encryption [ISC'15, PETS'17]

Searchable Encryption



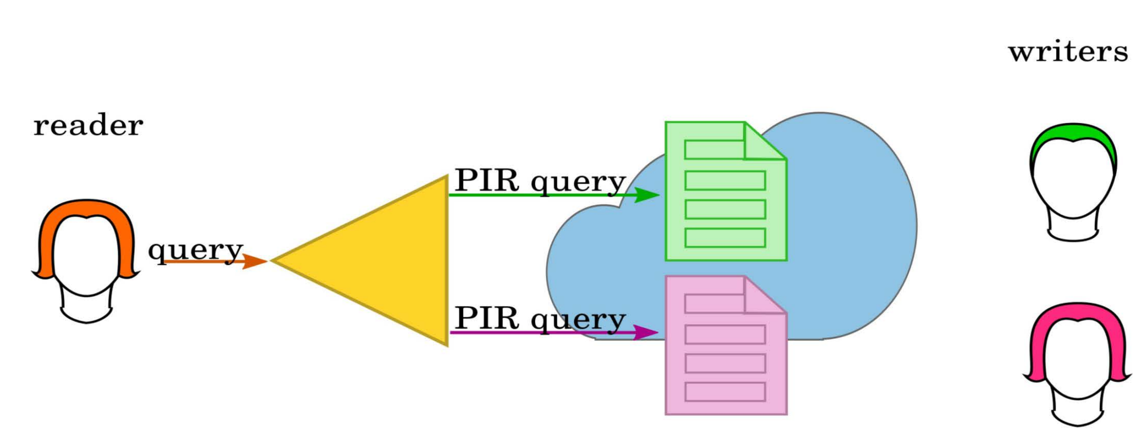
- Honest-but-curious cloud
- Privacy through encryption
- Remote search queries

Multi-User Architecture



- Privacy requirements
  - search pattern privacy
  - access pattern privacy
- New threat model
  - Collusion between users and cloud
- Performance requirements
  - scalable search

MUSE: Multi-User Searchable Encryption



- PIR based searchable encryption
- Scalability with Proxy based search
- Untrusted Cloud and untrusted Proxy

Avatar² - Enhancing Binary Firmware Security Analysis with Dynamic Multi-Target Orchestration

Marius Muench, Dario Nisi, Aurélien Francillon, Davide Balzarotti

EURECOM, Campus SophiaTech, 450 Route des Chappes, 06410 Biot France

Introduction

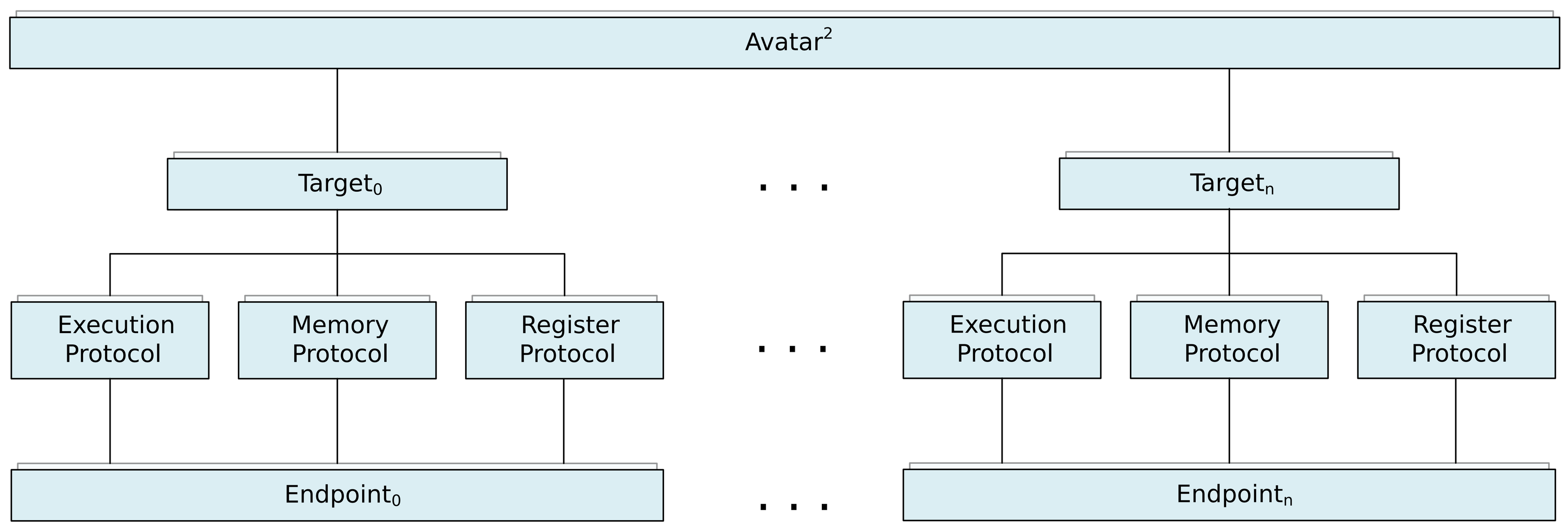
Avatar² is a python based target orchestration framework, which...

- **Is capable communicating and controlling different targets.**
- **Is designed to support a variety of targets**
- **Gives special emphasis on security analysis for *embedded systems***

It has been a long way

The foundation of avatar² dates back to the work of Zaddach et al. [1]. While core concepts have been inherited, avatar² has been re-designed and re-implemented from scratch to improve performance, usability, and flexibility.

Avatar²: Design & Core Concepts



The architectural design of avatar² consists of the following components:

- **The avatar² object** is the root of every avatar² setup and is responsible for orchestrating a non-empty set of targets.
- **Targets** are python abstractions of endpoints and are the basic block for every analysis task.*
- **Protocols** form the communication layer between the target and the actual endpoint and are separated by purpose.
- **Endpoints** can be anything worth orchestrating for an analysis, e.g. emulators, physical devices or binary analysis frameworks.

*Supported targets: QEMU, PANDA, OpenOCD, GDB & (soon) angr

Target Orchestration

Avatar² enables to **programmatically control the execution of different targets**, both in an sequential and event-based manner. This forms the basic block for any analysis involving more than one target.

Separation of Execution and Memory

While **execution and memory are tightly linked together** in traditional analysis approaches, **avatar² decouples them**. This, among others, allows the usage of *remote memory*, which is especially useful for analysing embedded devices.

State transfer and Synchronization

During an analysis, different targets are rarely orchestrated side by side. Instead, the **state needs quite often to be transferred** from one target to another at different points of the orchestration and avatar² provides easy methods for this.

Case Study: Enhancing Fuzz Testing of Embedded Devices (Joint work with Siemens AG, to be presented at NDSS 2018)

Challenges of Fuzzing Embedded Systems

- **Fault Detection.** Most fuzzing techniques are relying on *observable crashes*, and while desktop systems offer protection measurements which are triggering a crash upon a fault, embedded devices are often lacking according mechanisms.
- **Performance and Scalability.** Fuzzing greatly benefits from multiple instances of the software under test. While this is easy achievable for desktop systems, it would require the availability of multiple devices for embedded systems.
- **Instrumentation.** In recent years, a variety of instrumentation techniques for aiding fuzzing have been developed. Unfortunately, they often rely on primitives not available when fuzzing embedded systems, such as advanced operating system features or recompilation of source code.

To understand the impact of faults a variety of different devices devices have been selected.

	Platform	Manufacturer & Model	CPU Family	Operating System	LIBC	MMU
Desktop	Single Board Computer	Beaglebone Black	Cortex A-9	Debian GNU/Linux	glibc	✓
Type-I	Router	Linksys EA6300v1	Cortex A-9	Embedded Linux	uclibc	✓
Type-II	IP camera	Foscam FI8918W	ARM7TDMI-S	uCLinux	uclibc	✗
Type-III	Development Board	STM Nucleo-L152RE	Cortex M-3	None	libmbed	✗

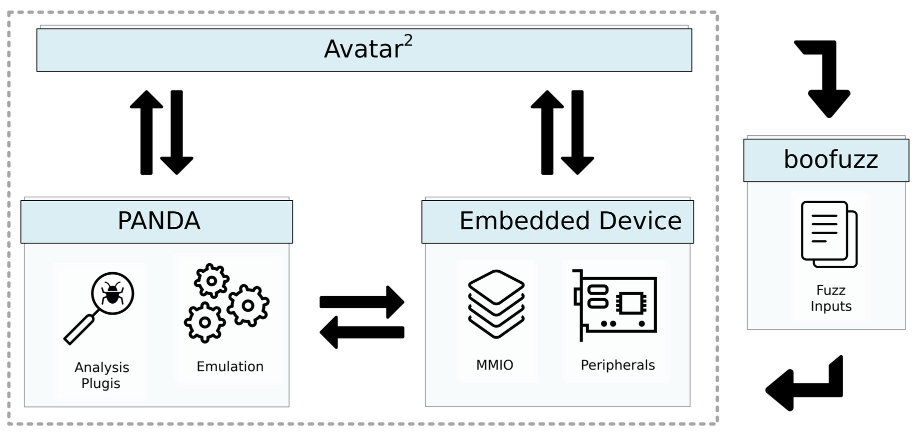
Artificial vulnerabilities have been inserted in two widely used software libraries and the behaviour of the devices when triggering those vulnerabilities has been studied.

	expat				mbed TLS			
Platform	**Desktop**	**Type-I**	**Type-II**	**Type-III**	**Desktop**	**Type-I**	**Type-II**	**Type-III**
Format String	✓	✓	✗	✗	✓	✓	✗	!
Stack-based buffer overflow	✓	✓	✓	!	✓	✓	✓	!
Heap-based buffer overflow	✓	!	✗	✗	✓	!	✗	✗
Double Free	✓	✓	✗	✗	✓	!	✗	✗
Null Pointer Dereference	✓	✓	✓	✗	✓	✓	✓	✗

✓: Observable Crash or Reboot - !: Hang or Late Crash ✗: Malfunctioning or No Effect

Orchestration Setup

- **Avatar²** orchestrates the two targets and drives *boofuzz*, an open source, python based fuzzing framework.
- **PANDA** The Platform for Architecture-Neutral Dynamic Analysis [3] emulates the core of the embedded device's firmware, while utilizing analysis plugins to detect eventually occurring faults.
- **The Embedded Device** serves memory request from PANDA, in case where hardware interactions can not be emulated.



Analysis Plugins

Several PANDA plugins for fault detection have been developed.

Analysis Plugin	Format String	Stack-based Bof	Heap-based Bof	Double Free	Null Pointer Deref.
a) Call Stack Tracking	✗	✓	✗	✗	✗
b) Call Frame Tracking	✗	✓	✗	✗	✗
c) Stack Object Tracking	✗	✓	✗	✗	✗
d) Segment Tracking	✓	✓	✗	✓	✓
e) Format Specifier Tracking	✓	✗	✗	✗	✗
f) Heap Object Tracking	✗	✗	✓	✓	✓
Combined	✓	✓	✓	✓	✓

Results

The above described setup was evaluated in different scenarios, ranging from full emulation of the device over partial emulation with peripheral forwarding to just fuzzing of the native device. From this evaluation, the following conclusions could be drawn:

- Liveness checks alone, as commonly deployed when fuzzing embedded devices, are prone to missing faults.
- Full emulation is the best strategy, but unfortunately emulators for embedded devices are rarely available.
- Partial emulation can lead to accurate vulnerability detection, with a significant performance impact.

References

[1] J. Zaddach, L. Bruno, A. Francillon, D. Balzarotti, *"AVATAR: A Framework to Support Dynamic Security Analysis of Embedded Systems' Firmwares"*, NDSS 2014.

[2] M. Muench, J. Stijohann, F. Kargl, A. Francillon, D. Balzarotti, *"What You Corrupt Is Not What You Crash: Challenges in Fuzzing Embedded Devices"*, to appear at NDSS 2018.

[3] B. Dolan-Gavitt, J. Hodosh, P. Hulin, T. Leek, R. Whelan, *"Repeatable Reverse Engineering with PANDA"*, PPREW 2015.

This work has been supported by SIEMENS

For more information, please visit: `http://github.com/avatartwo`

IMT ATLANTIQUE

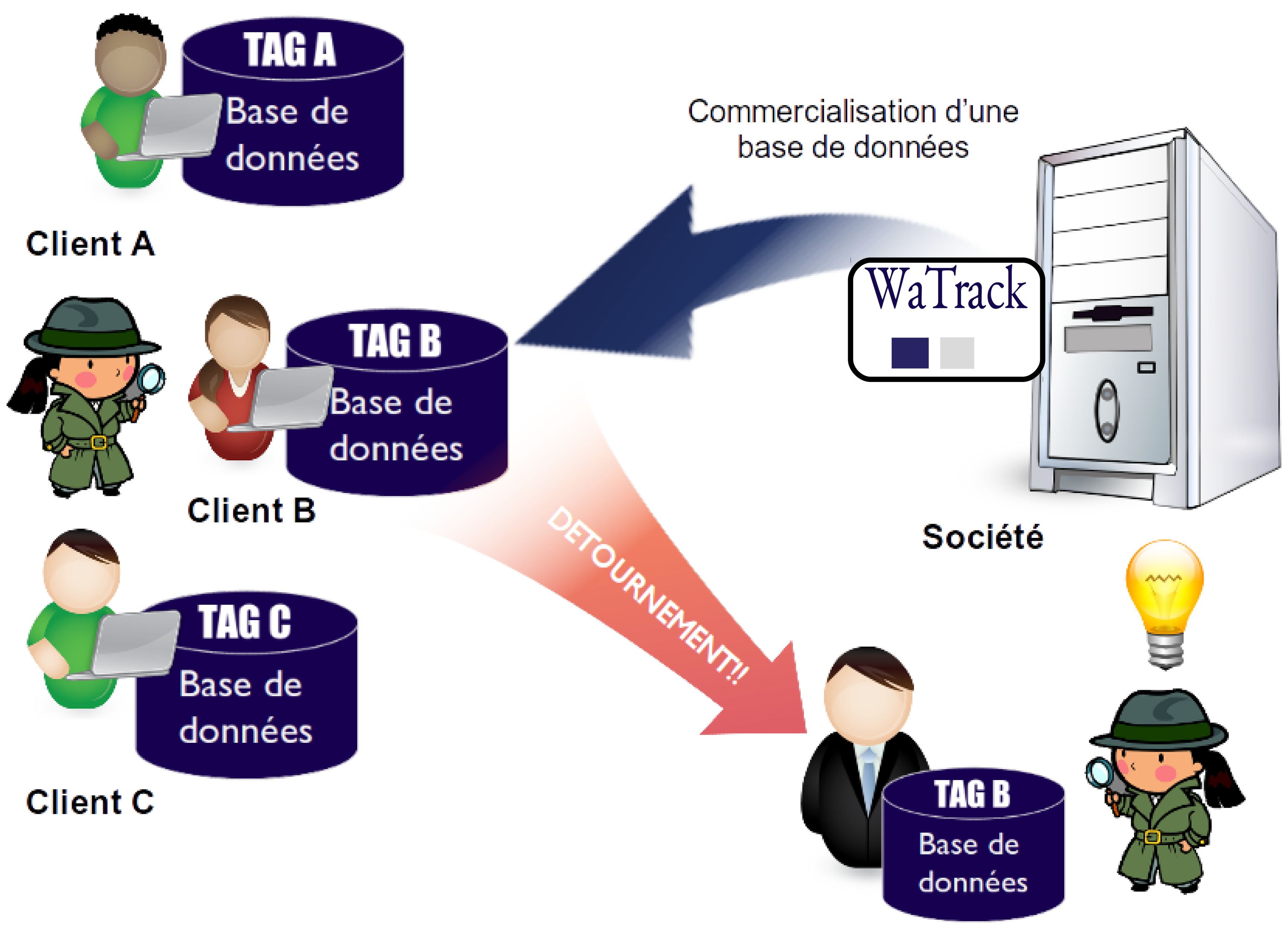
WaToo

« Comment m'assurer que les données que je commercialise ne sont pas redistribuées illégalement ? » *(Question d'un chef d'entreprise concerné)*

WaTrack protège vos données sensibles contre la redistribution non-autorisée. WaTrack identifiera de manière unique un acheteur peu scrupuleux.

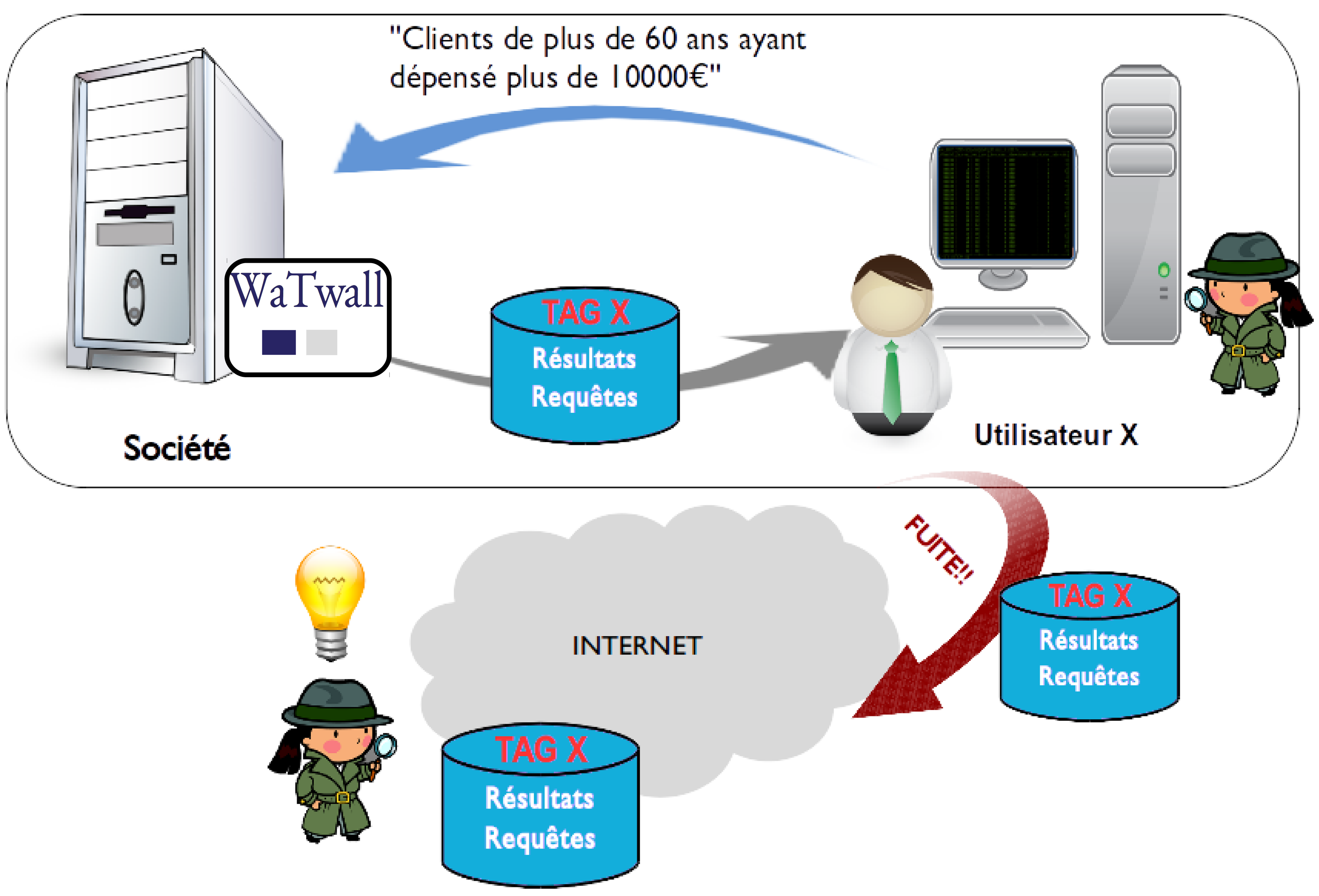
TAG : Information de traçabilité (ID du destinataire et ID d'origine, date d'envoi, …) dissimulée lors de l'export de données.

- Pas d'interférences dans les usages.
- Protection indépendante du format de stockage.
- Identification unique de l'utilisateur malhonnête même s'il modifie les données.



« Comment dissuader un utilisateur de « fuiter » les données de l'entreprise et l'identifier si besoin? » *(Question d'un responsable de sécurité inquiet)*

WaTwall, vous permet d'éviter les fuites et le détournement de données par des utilisateurs au sein de votre société.



Identification fine et unique de l'utilisateur responsable de la fuite de données.

Les utilisateurs sont informés de la protection : MESURE DE DISSUASION !

- Le TAG de l'utilisateur est dissimulé lors de l'accès aux données.
- Solution intégrée au système d'information.
- Pas d'interférences dans les usages.

www.watoo.tech

Accompagné par :

IMT Atlantique Bretagne-Pays de la Loire École Mines-Télécom

EMERGYS

LATIM

135 rue Claude Chappe, 29280 Plouzané
Tel. : 0686372875
javier.francocontreras@watoo.tech

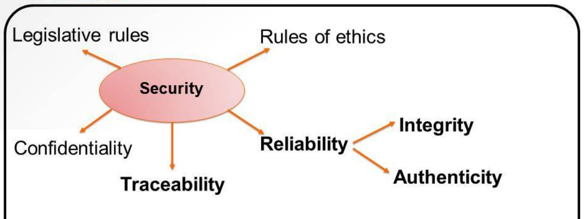
JOINT WATERMARKING AND LOSSLESS JPEG-LS COMPRESSION FOR MEDICAL IMAGE SECURITY

S. Haddad[1,2], D. Bouslimi[1,2], G. Coatrieux[1,2]

1. IMT Atlantique, Bretagne-Pays de la Loire 2. LATIM INSERM U1101, Brest 29238, France;

Objectives/Solution/Results: Trace medical images and verify their integrity or authenticity directly from the compressed bitstream.// The proposed scheme allows message insertion into the image, during the JPEG-LS encoding. // This scheme grants message extraction from the compressed bitstream.// Achieved capacities can provide different watermarking based security services.

1. Issues



Reliability: a degree of confidence to medical data

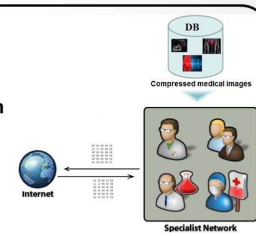
Constraints

- Protection of large volumes of medical data (transmission time and space storage)

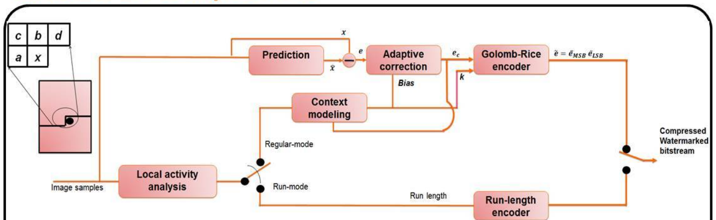
➡ **Interest for joint watermarking and compression**

- Needs to give access to security services in the compressed domain.

➡ **Watermark extraction directly from the compressed domain**



2. JPEG-LS Compression



-Lossless JPEG-LS procedure-

- x : current encoding pixel of an image
- $\{a, b, c, d\}$ the causal neighborhood of x
- Based on the values of the causal neighborhood of x, JPEG-LS works in 2 modes:

1) Run-mode, if $\boldsymbol{a = b = c = d}$ ➔ Encoding the number of repetition of pixel value

2) Regular-mode, **otherwise:**

i) Predict $\hat{x}$ of x based on the values of $\{a, b, c\}$

➔ Prediction error : $e = x - \hat{x}$

ii) Compute the context Q associated to x

iii) Correct e to e_c by eliminating the prediction bias depending on Q

iv) Golomb-Rice encoding of the mapped prediction-error $\tilde{e}$ of e_c using the context-dependent factor k :

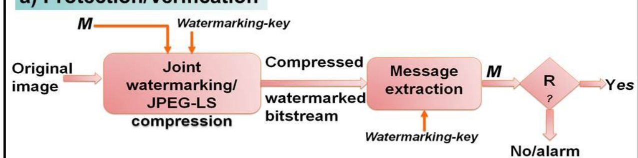
$$\tilde{\boldsymbol{e}} = '\tilde{\boldsymbol{e}}_{\boldsymbol{MSB}}\ \tilde{\boldsymbol{e}}_{\boldsymbol{LSB}}'$$

Unary code of $\lfloor \tilde{e}/2^k \rfloor$ $\tilde{\boldsymbol{e}}_{\boldsymbol{MSB}} = '0X1'$; X : sequence of '0's

Binary code of $(\tilde{e}/2^k)$ reminder represented on $\boldsymbol{k}$ bits

3. Joint Watermarking/JPEG-LS Compression

a) Protection/Verification



M: message

R: Reliability

b) Message embedding during the regular-mode of JPEG-LS encoding

- $\tilde{\boldsymbol{e}} = '\tilde{\boldsymbol{e}}_{\boldsymbol{MSB}}\ \tilde{\boldsymbol{e}}_{\boldsymbol{LSB}}'$: Golomb-Rice encoded mapped prediction-error
- $\widetilde{\boldsymbol{e_w}}$: watermarked mapped prediction-error
- $\boldsymbol{k}$: Golomb-Rice factor
- $m_i \in \{0,1\}$: the i^{th} bit of the message M to be embed

if $\tilde{\boldsymbol{e}}_{\boldsymbol{MSB}} = '\boldsymbol{0X1}'$ ➔ embed m_i in the higher order bit of $\tilde{\boldsymbol{e}}_{\boldsymbol{LSB}}$

e.g. $\tilde{\boldsymbol{e}} = '0011001'$; where $\tilde{\boldsymbol{e}}_{\boldsymbol{MSB}} = '001'$ and $\tilde{\boldsymbol{e}}_{\boldsymbol{LSB}} = '\boldsymbol{1}001'$

$\tilde{\boldsymbol{e}} \xrightarrow{\text{watermarking}} \widetilde{\boldsymbol{e_w}} = '001\boldsymbol{m_i}001$

c) Some constraints of implementation

To ensure an error-free extraction of a message:

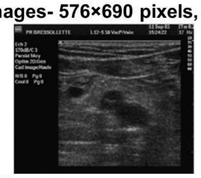
- **When** $\tilde{\boldsymbol{e}}_{\boldsymbol{MSB}} = '\boldsymbol{0X1}'$ & $\boldsymbol{k \neq 0}$ $(\boldsymbol{i.e.}\ \tilde{\boldsymbol{e}}_{\boldsymbol{LSB}}$ exist) ➔ message embedding

  Otherwise $(\boldsymbol{k = 0})$, $\tilde{\boldsymbol{e}}_{\boldsymbol{MSB}}$ is shifted to $'\boldsymbol{X1}'$
- Avoid $'0X1'$ sequences in $\tilde{\boldsymbol{e}}_{\boldsymbol{LSB}}$

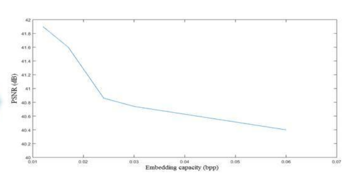
4. Experimental results

❖**Data set: Ultrasound images- 576×690 pixels, 8-bit depth.**

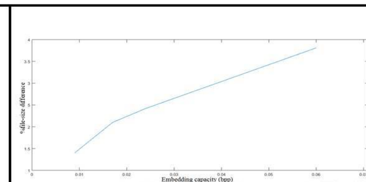
Original image



Decompressed watermarked image



PSNR (dB) vs. Capacity (bpp)



% Compressed file-size difference vs Capacity (bpp)

5. Conclusion and future works

❖ The proposed joint watermarking-JPEG-LS scheme allows the access to watermarking based security services directly from the image compressed bitstream.

❖ The embedding capacity is large enough so as to allow various security services

❖ The visual quality of the watermarked image is close to the original.

❖ **Future works** will focus on improving the robustness of the watermark to attacks (e.g. lossy image compression, additive noise,...) while preserving a better image quality.

[1] G. Coatrieux, H. Maitre, B. Sankur, Y. Rolland, R. Collorec, « Relevance of watermarking in medical imaging », in proc. Of Int. Conf. On IEEE EMBS ITAB, USA, 250-255, 2000

[2] I. FCD14495, Lossless and near-lossless coding of continuous-tone still image jpeg-ls.

Contact: {sahar.haddad, dalel.bouslimi, gouenou.coatrieux}@telecom-bretagne.eu - http://www.telecom-bretagne.eu

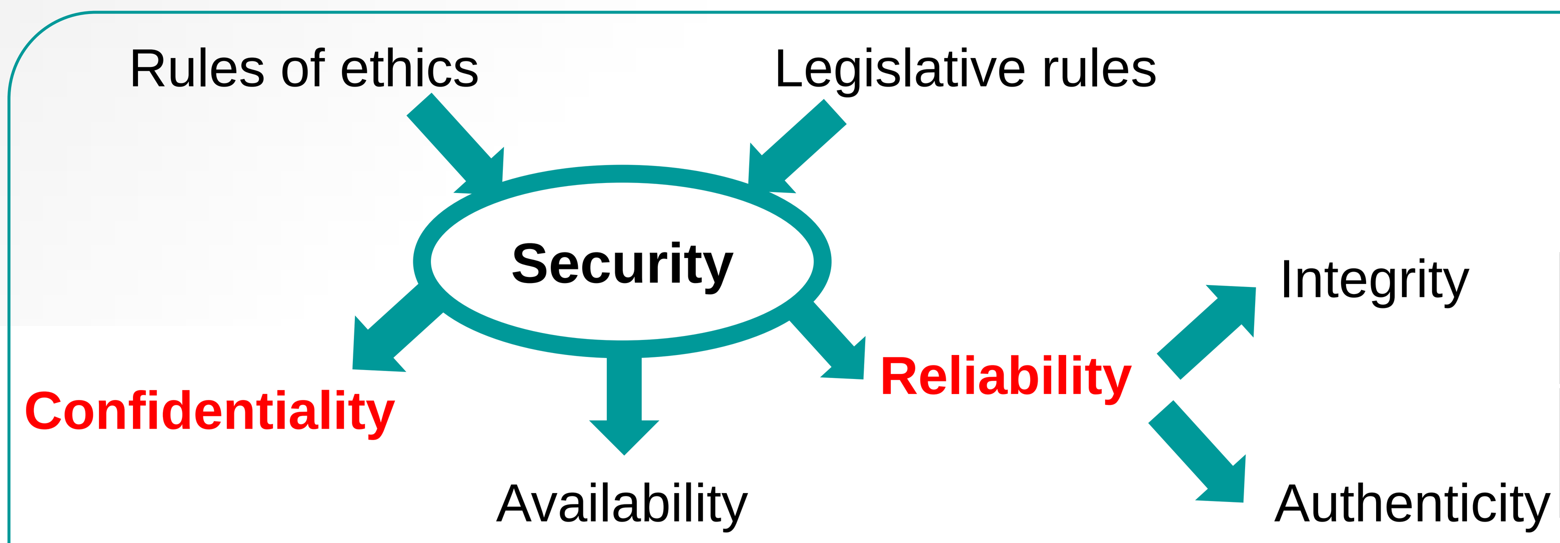
DATA HIDING IN HOMOMORPHICALLY ENCRYPTED MEDICAL IMAGES FOR VERIFYING THEIR RELIABILITY IN BOTH ENCRYPTED AND SPATIAL DOMAINS

D. Bouslimi[1,2], R. Bellafqira[1,2], G. Coatrieux[1,2]

1. Institut Mines- Telecom/Telecom Bretagne 2. LATIM INSERM U1101, Brest 29238, France;

Objectives/Solution/Results: Verify the reliability (i.e. authenticity and integrity) of medical images whether they are encrypted or not // A data hiding approach for encrypted images. It relies on the insertion into the image, before its encryption, of a predefined watermark, a "pre-watermark". It is the impact of the message insertion into the encrypted image onto the "pre-watermark" that gives access to the message into the spatial domain // Our approach allows the embedding of security attributes available in both spatial and encrypted domains while minimizing image distortion.

1. Medical data protection

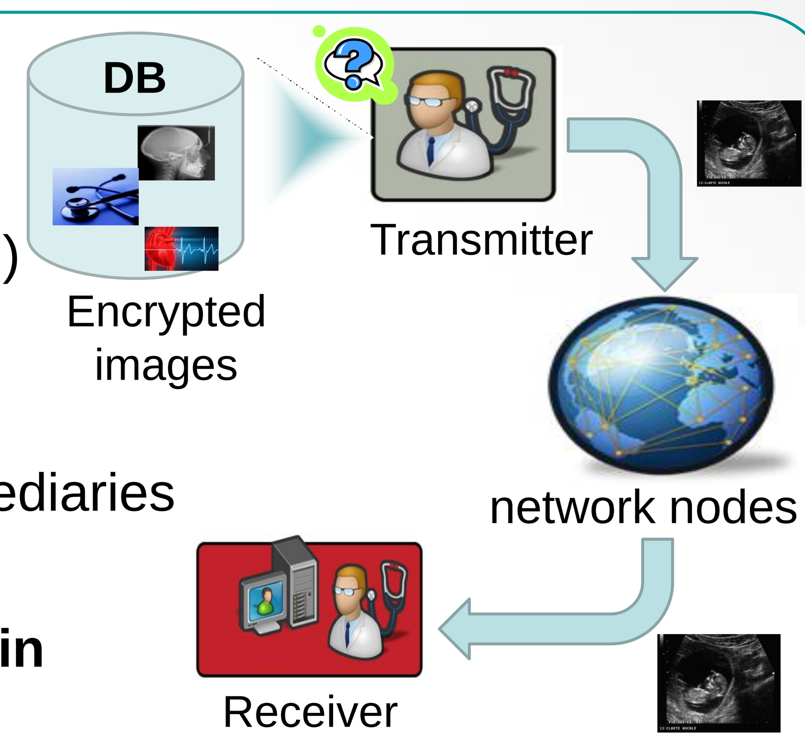


Reliability: *a degree of confidence/trust in medical data*

Merging encryption (*a priori* protection) and watermarking (*a posteriori* protection) *into a single security mechanism*

Constraints

- ❑ Maintain data confidentiality without discontinuity
- ❑ Protection of large volumes of data (time computing)
  - **Interest for Directly watermarking encrypted images**
- ❑ Allows verifying encrypted data reliability by intermediaries (e.g. network nodes)
  - **Needs to give access to security attributes in both encrypted and spatial domains**

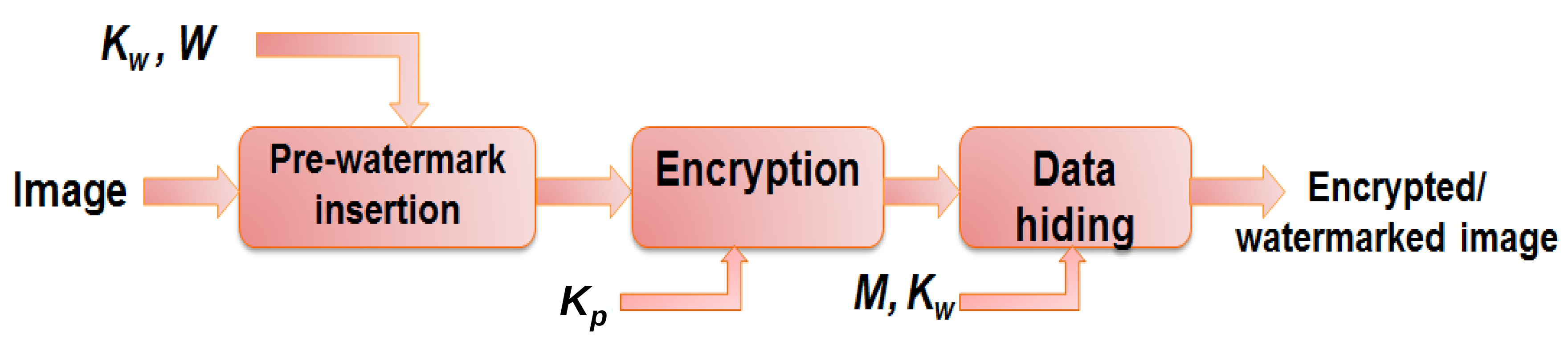


2. Data Hiding in Homomorphic Domain(DHHD)

Principle

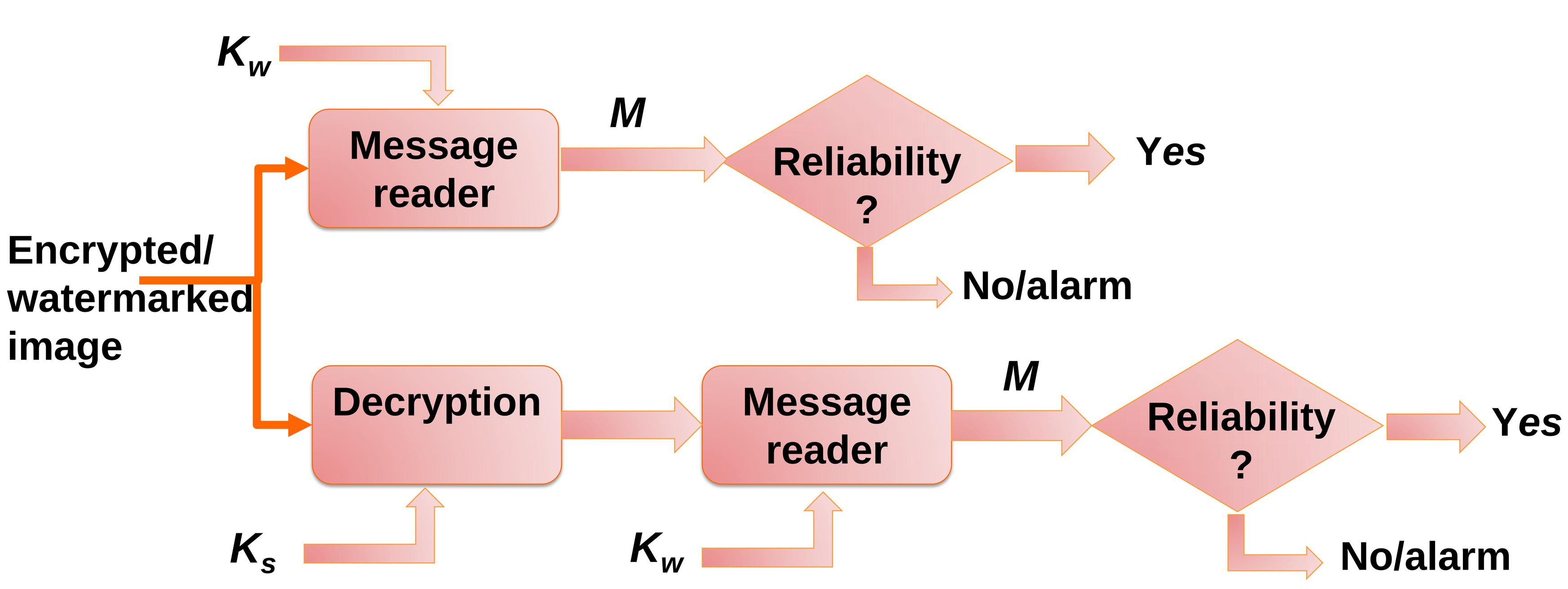
❖ Controlled distortion of a "pre-watermark" inserted before the encryption process to encode a message in both encrypted and spatial domains.

Protection



K_w, (K_p, K_s): watermarking and receiver public-private key pair, W: pre-watermark, M: message (some security attributes)

Verification



3. DHHD Implementation

Implementation with Paillier cryptosystem and Quantization Index Modulation (QIM)

- Based on the additive homomorphic property of Paillier cryptosystem (E):

$$E[m_1, r_1] \times E[m_2, r_2] = E[m_1+m_2, r_1+r_2]$$

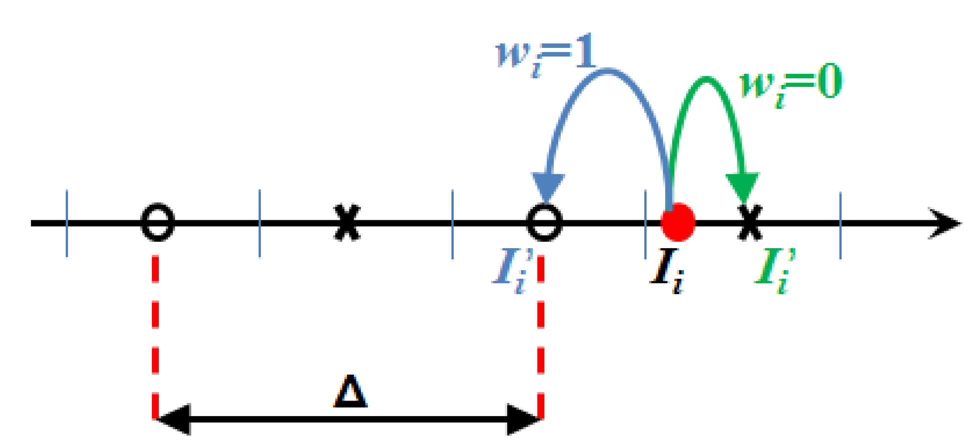
m_1, m_2: two cleartexts, r_1, r_2 : random integers associated to m_1 and m_2.

- I : a subset of p pixels, $I=\{I_1, I_2, \ldots, I_p\}$, $W=\{w_1, w_2, \ldots, w_p\}$: a pre-watermark, m_i: one bit of the message M to be inserted into I.

❑ **Pre-watermark embedding**

- Insertion of W into I using QIM:

$$I_i' = QIM(I_i, w_i)$$



❑ **Insertion of m_i into I_e, the encrypted version of I':** $I_{ie} = E[I_i', r_i]$

$$I_{iew} = I_{ie} \times E[d_w, r_k] = E[I_i', r_i] \times E[d_w, r_k] = E[I_i' + d_w, r_i + r_k]$$

- r_k: a random integer that verifies $QIM_{ext}(I_{ie} \times E[d_w, r_k]) = m_i$
- QIM_{ext}: QIM extraction function
- d_w verifies:

$$\begin{cases} \frac{\Delta}{4} < |d_w| < \frac{3\Delta}{4} & if\ \ m_i = 1 \\ |d_w| < \frac{\Delta}{4} & if\ \ m_i = 0 \end{cases}$$

4. Experimental results

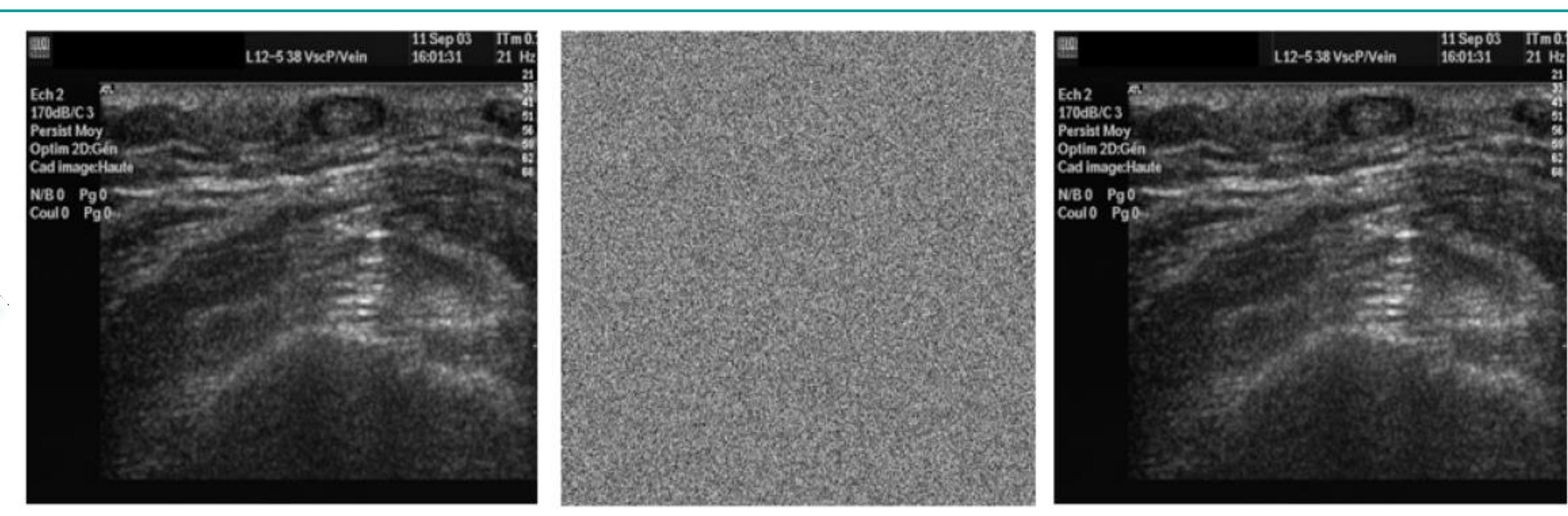
❖**Performance Indicators**

- Image distortion measure: Peak Signal to Noise Ratio (dB).
- Capacity rate (bpp: Bit Per Pixel).

❖**100 ultrasound images- 576×688 pixels, 8-bit depth.**

- Capacity rate: $1/p$ bpp (e.g. 396 Kbits per image for p=1).
- Lower theoretical PSNR bound ($PSNR_{th}$): 20 $Log_{10}(408/\Delta)$.

Δ	2	4	8
$PSNR_{th}$	46.19 dB	40.17 dB	34.15 dB
Experimental PSNR	51.15 dB	44.2 dB	37.8 dB



Original image **Watermarked encrypted image** **Deciphered watermarked image**

5. Conclusion and future works

❖ The proposed data hiding approach of encrypted images guarantees an *a priori* as well as an *a posteriori* image protection.

❖ The use of a pre-watermark makes the insertion /extraction processes independent of the encryption/decryption processes, and vice versa.

❖ Message insertion introduces very low image distortion.

❖ **Future works** will focus on making our approach more robust to attacks (e.g. lossy image compression) so as to satisfy traceability objectives, for example.

[1] D. Bouslimi, *et al.*, "A joint encryption/watermarking system for verifying the reliability of medical images", *IEEE TITB* 16 (2012) 891–899.
[2] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity classes", *Proc Eurocrypt*, 1592 (1999) 223-238.
[3] B. Chen et *al.*, "Quantization Index Modulation: A Class of Provably Good Methods for Digital watermarking and information embedding," *IEEE Trans. on Inform. Theory*, 47(4) (2001), 1423- 1443.

Contact: {dalel.bouslimi, reda.bellafqira, gouenou.coatrieux @imt-atlantique.fr - http://www.imt-atlantique.fr

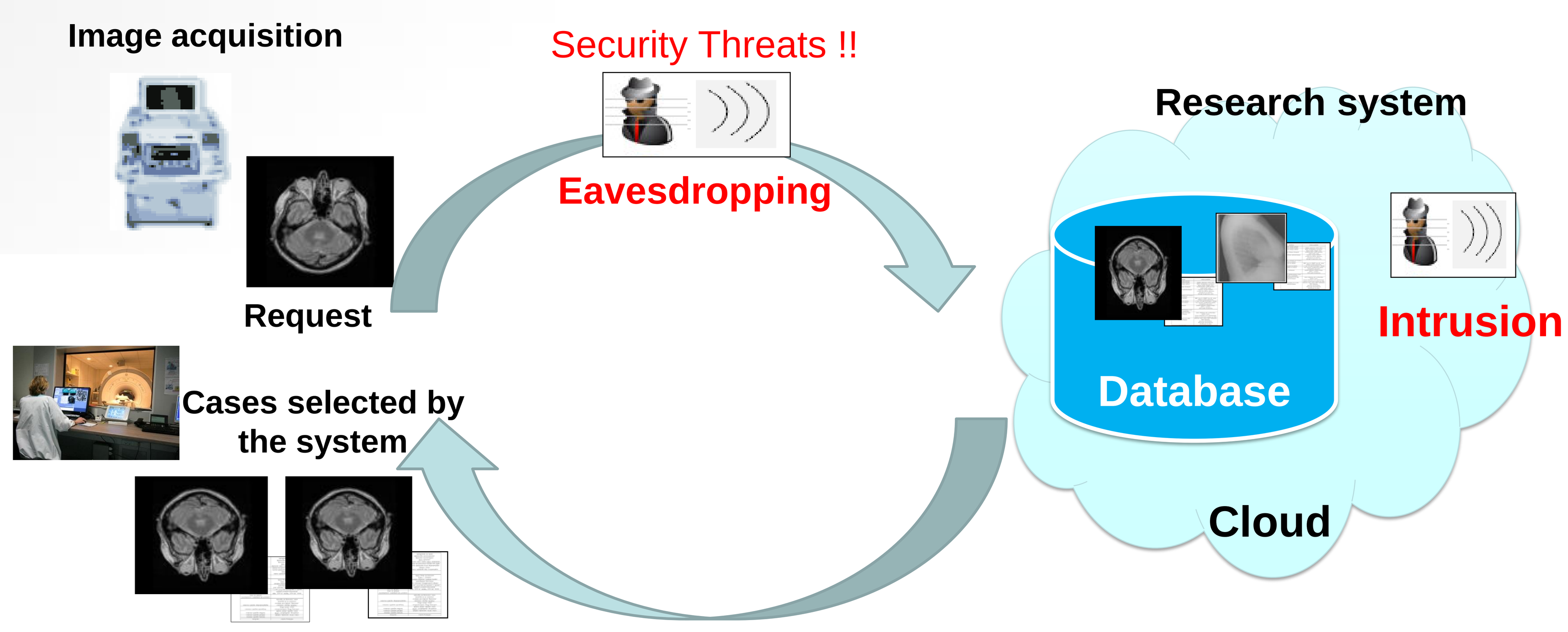
AN END TO END SECURE CBIR OVER ENCRYPTED MEDICAL DATABASE

R. Bellafqira[1,2], G. Coatrieux[1,2], D. Bouslimi[1,2], G. Quellec[2]

1. IMT Atlantique, Dpt ITI, Brest 29238, France; 2. INSERM U1011, LaTIM, Brest 29238, France

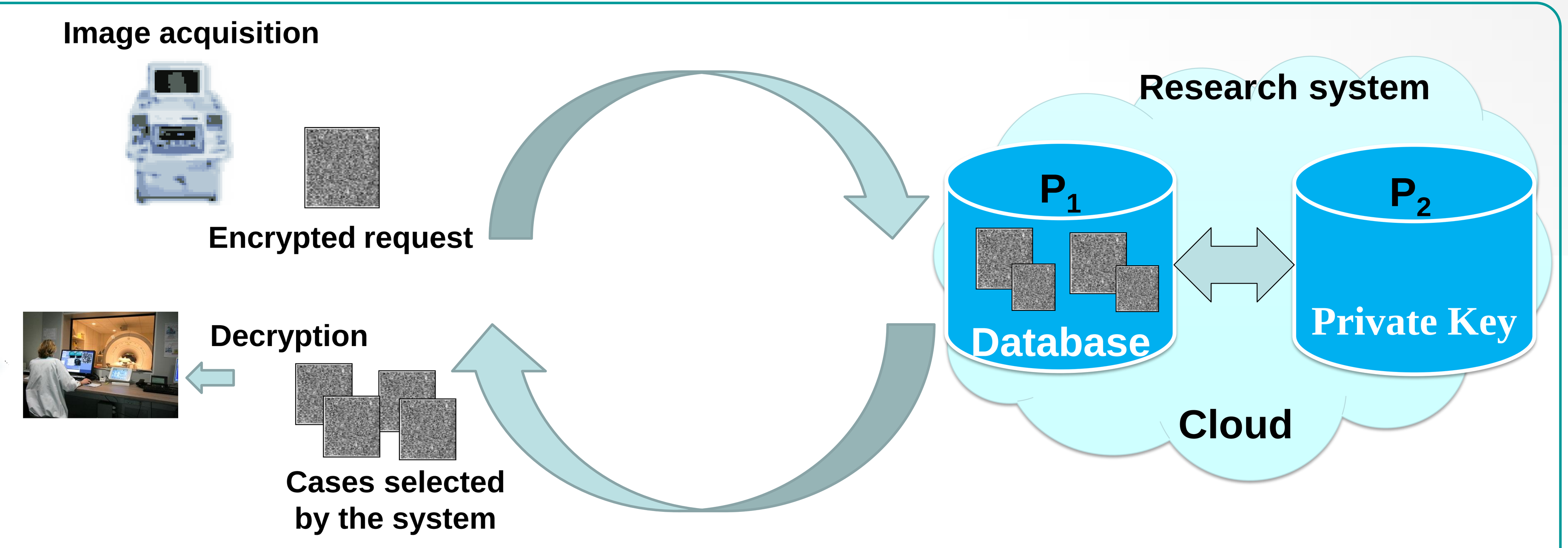
Objectives/Solution/Results: Secure implementation of a Content-Based Image Retrieval (SCBIR) that makes possible diagnosis aid systems to work in outsourced environment (e.g. Cloud) / Using homomorphic encryption and two non-colluding servers to compute the Discrete Wavelet Transform (DWT) in the Paillier domain and build the encrypted histograms of an image from its encrypted form/ Our SCBIR achieves retrieval performance as good as if images were processed in their non-encrypted form.

1. Outsourced content based image retrieval



❖ **Main security concern**: **confidentiality** and **privacy** of medical data

2. Secure outsourced content based image retrieval

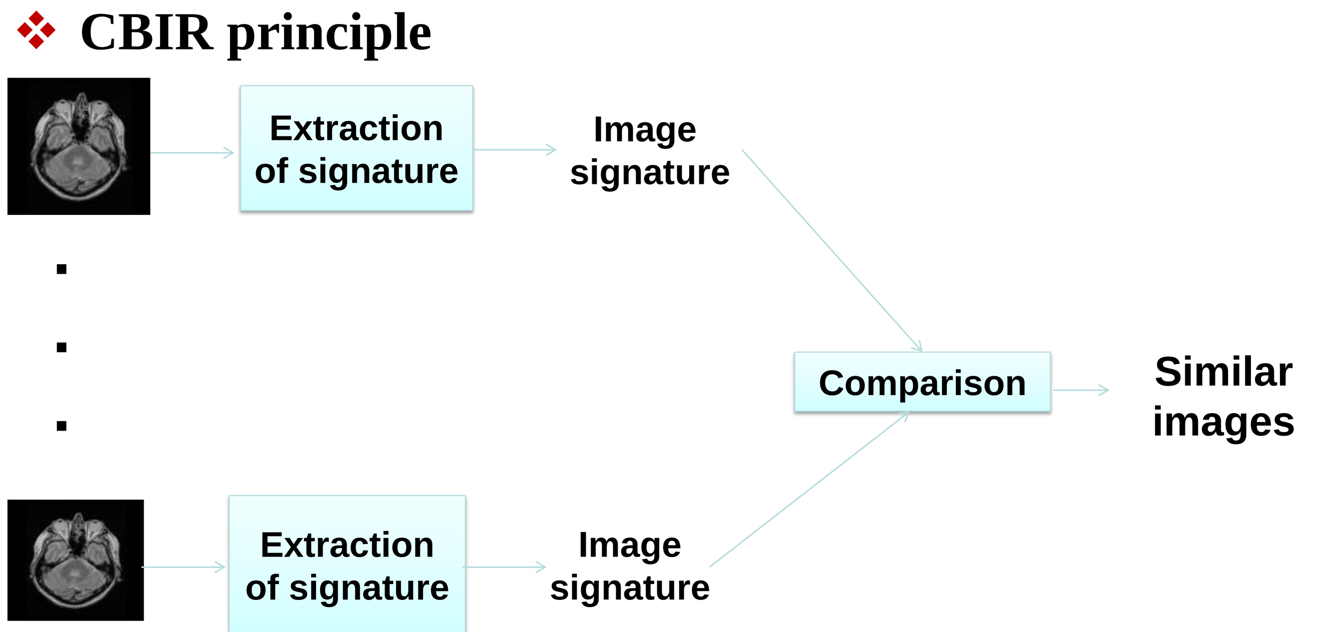


❖ **Solution:**

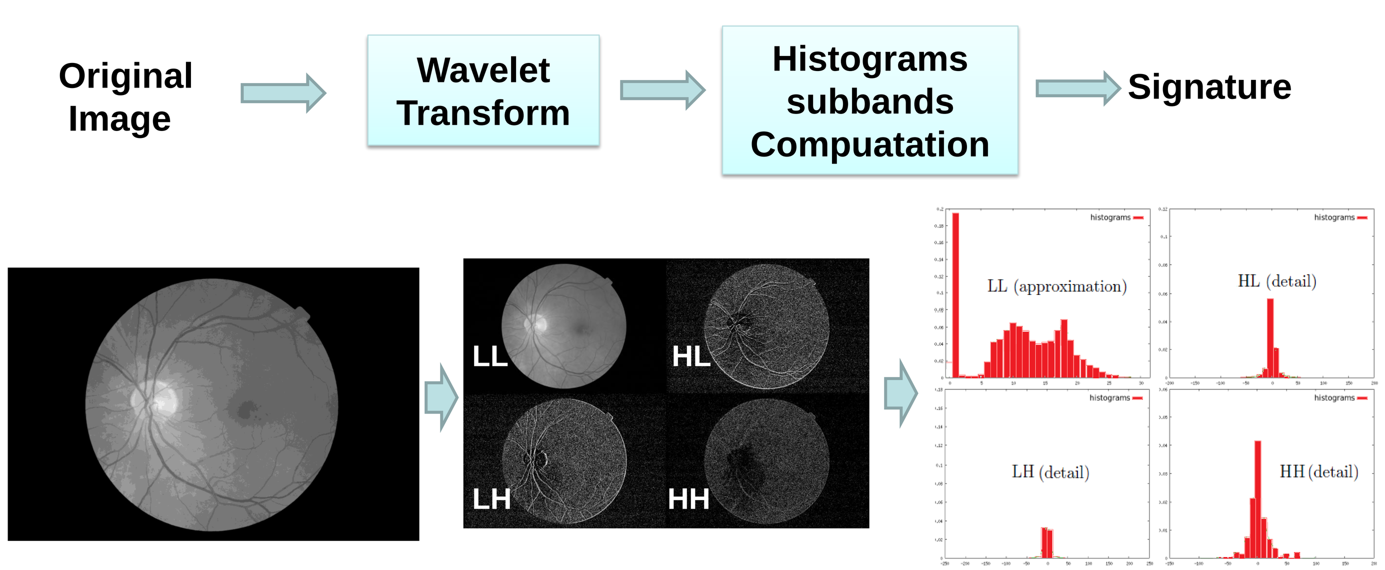
➢ Encrypting request image and images stored in the database

3. Content based image retrieval (CBIR)

❖ **CBIR principle**



❖ **Signature extraction principle**



Signature: concatenation of the different wavelet coefficient sub-band histograms.

4. Secured Content based image retrieval (SCBIR)

❖ **Secure Image Discrete Wavelet Transform**

➢ Use of homomorphic Paillier Cryptosystem E [.]:

$$E[m_1]E[m_2]=E[m_1+m_2]\ ;\ E[m_1]^{m_2}=E[m_1 m_2]$$

m_1,m_2: two cleartexts

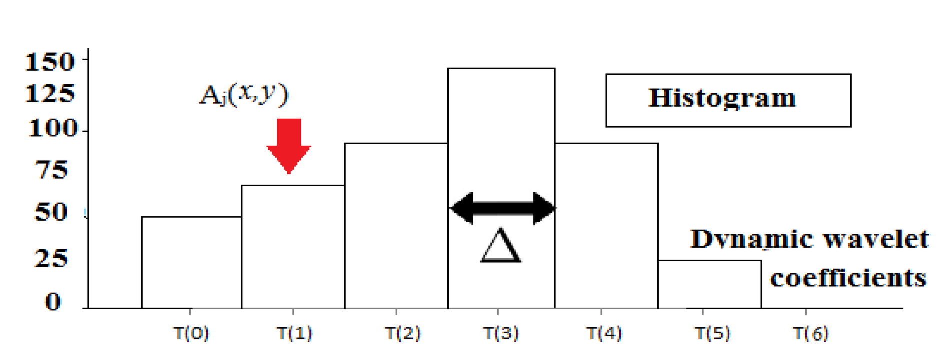
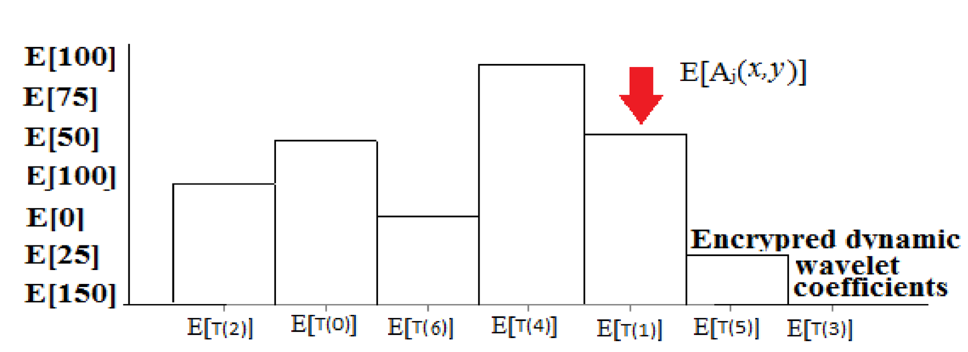
➢ Discrete Wavelet Transform in Paillier Domain

2D Wavelet Transform	Using Homomorphic properties
$A_j(x,y)=\sum_{l,l'} H(2x-l)H(2y-l')A_{j-1}(x,y)$	$E[A_j(x,y)]=\prod_{l,l'} E[A_{j-1}(x,y)]^{H(2x-l)H(2y-l')}$

$A_j(x,y)$: Approximation coefficient at the j^{th} decomposition level at the position (x,y)

$H(.)$: Low-pass decomposition filter coefficient

❖ **Encrypted histogram computation in the encrypted domain**

Clear domain	Encrypted domain
 The nearest centroid $T(p)$ of $A_j(x,y)$ is: $p=\arg\min_i \lvert A_j(x,y)-T(i)\rvert$	 The nearest centroid $E[T(p)]$ of $E[A_j(x,y)]$ is computed by interaction between P_1 and P_2

5. Experimental results

❖ **Performance Indicators**

➢ Mean precision: rate of returned images with the same pathology as the query image

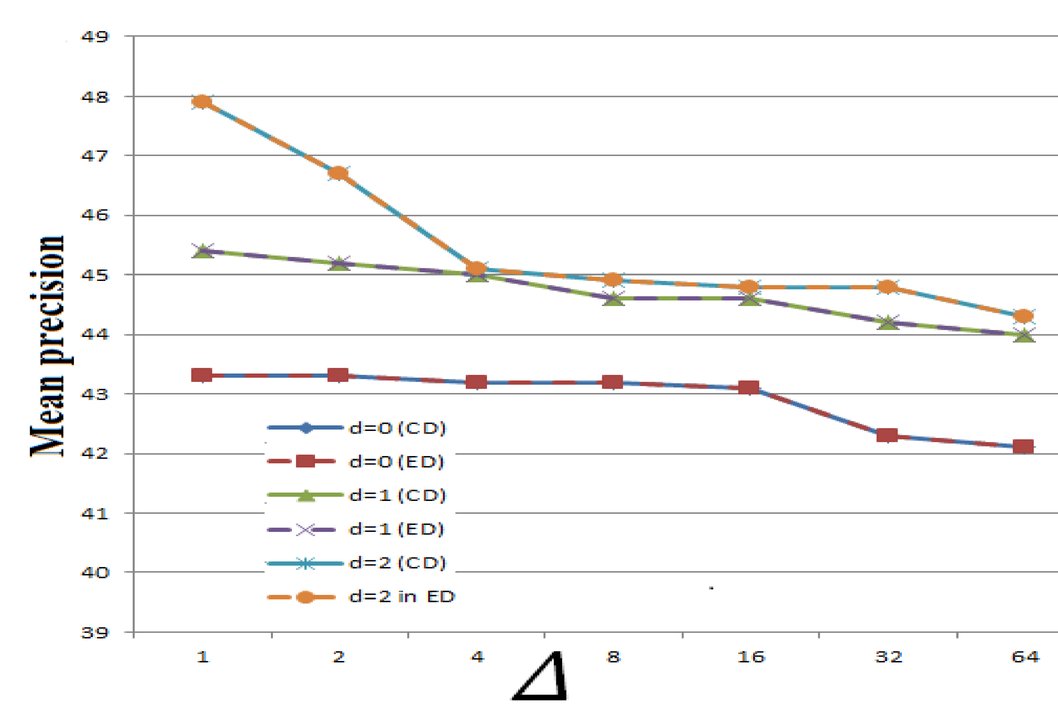
❖ **1200 retinopathy images-2240*1488 pixels, 8-bit depth**

➢ Five images returned by the system

➢ The Paillier cryptosystem encrypts an input of 8 bits into 2048 bits

➢ Working on encrypted data does not impact the image retrieval performance

➢ Decreasing **Δ** increases the number of histogram intervals, and consequently the computing complexity of our scheme



5. Conclusion and future works

❖ The proposed secure outsourced content-based image retrieval allows outsourcing and carrying out a search in an encrypted image database without extra communication with the user.

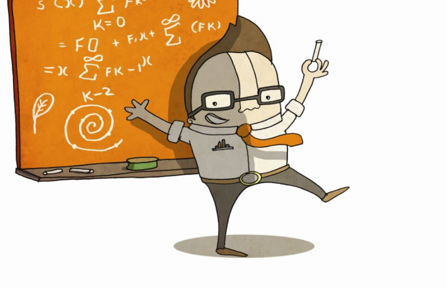
❖ Our solution is based on homomorphic cryptosystem and two cloud service providers so as to share encrypted histogram computation and comparison

❖ **Future works** will focus on reducing computational and storage complexity

[1] R. Bellafqira et al., Content-based image retrieval in homomorphic encryption domain. *37th Annual International Conference of the IEEE, EMBC*, 2015.

[2] G. Quellec et al., Wavelet optimization for content-based imageretrieval in medical databases. Med Image Anal, no 2, vol. 14, pp.227–241, 2010.

Contact: {reda.bellafqira, gouenou.coatrieux, dalel.bouslimi}@imt-atlantique.fr - https://www.imt-atlantique.fr



Identité pour l'IoT: Reprenons le contrôle de nos objets connectés

IRIS – Lab-STICC

Marco LOBE KOME
Frédéric & Nora CUPPENS

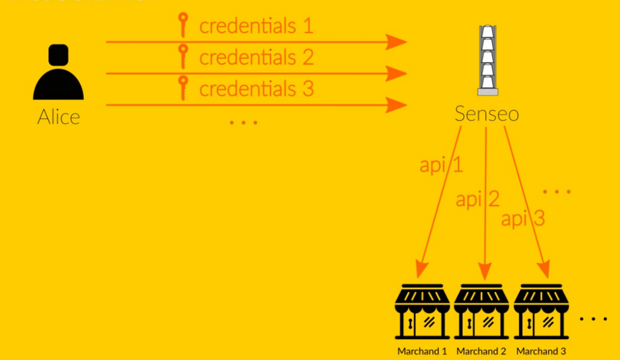
USAGE

PROTOCOLE

CONTEXTE

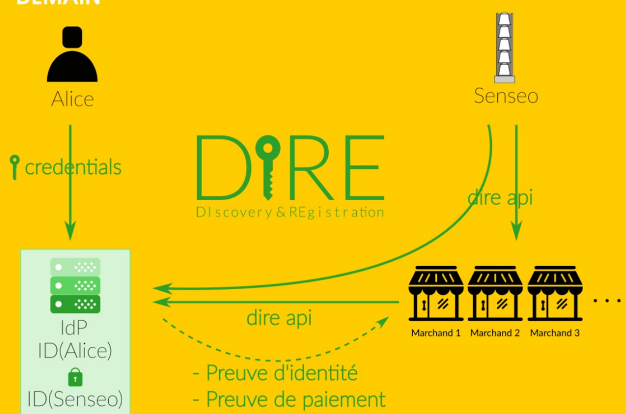
Les humains délèguent des tâches répétitives aux objets connectés en leur confiant leur identité numérique. Or étant donné leur faible niveau de sécurité, est-il judicieux de leur accorder notre confiance quant à la gestion de nos données secrètes ?

AUJOURD'HUI



- Identités de l'utilisateur et celle de l'objet confondues
- Autant d'interface que de fournisseur de service
- Le contrôle d'accès est statique

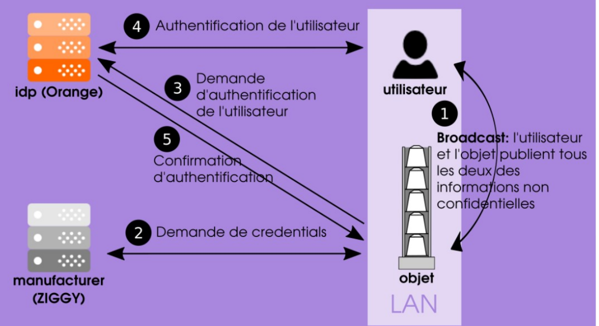
DEMAIN



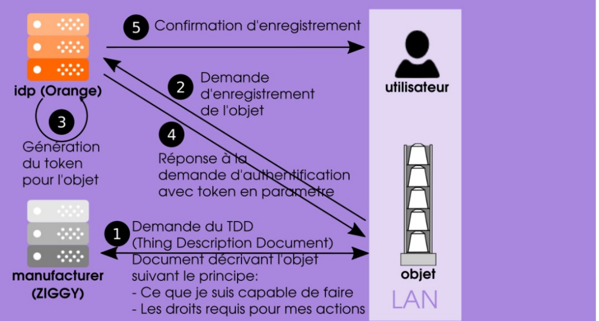
- Identité de l'objet clairement identifiée
- Une interface simplifiée pour s'adresser aux marchands
- Le contrôle d'accès est dynamique

Nous proposons un protocole permettant de lier l'identité d'une personne à celle d'un objet, facilitant ainsi le contrôle d'accès aux ressources de l'utilisateur. Il est composé de 2 phases : le **DIscovery** et le **REgistration**.

DISCOVERY: Phase de découverte de l'objet et d'authentification mutuelle



REGISTRATION: Phase de liaison de l'objet à son utilisateur



- Propriétés de sécurité formellement prouvées : **Intégrité, Anonymat, Confidentialité**
- **Prochaines contribution** : Moteur de contrôle d'accès dynamique

OPPORTUNITES

En devenant fournisseur d'identité pour les objets connectés, Orange deviendrait précurseur comme autorité de certification de l'identité des objets et normaliserait les échanges entres objets connectés et les plateformes de e-commerce. Nos clients s'appuieraient sur cette solution pour s'assurer de la loyauté du comportement de leurs objets.

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

orange™

Large Scale Anomaly Detection for Critical Infrastructures

Institut Mines-Télécom

Parties prenantes

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Lab-STICC cnrs

Auteurs

- **Reda Yaich** (Lab-STICC, IMT Atlantique)
- **Nora Cuppens-Boulahia** (Lab-STICC, IMT Atlantique)
- **Frédéric Cuppens** (Lab-STICC, IMT Atlantique)

Partenaires

ANSSI
AIRBUS DEFENCE & SPACE
Atos
QOSMOS The Network is Information
STORMSHIELD
OPPIDA

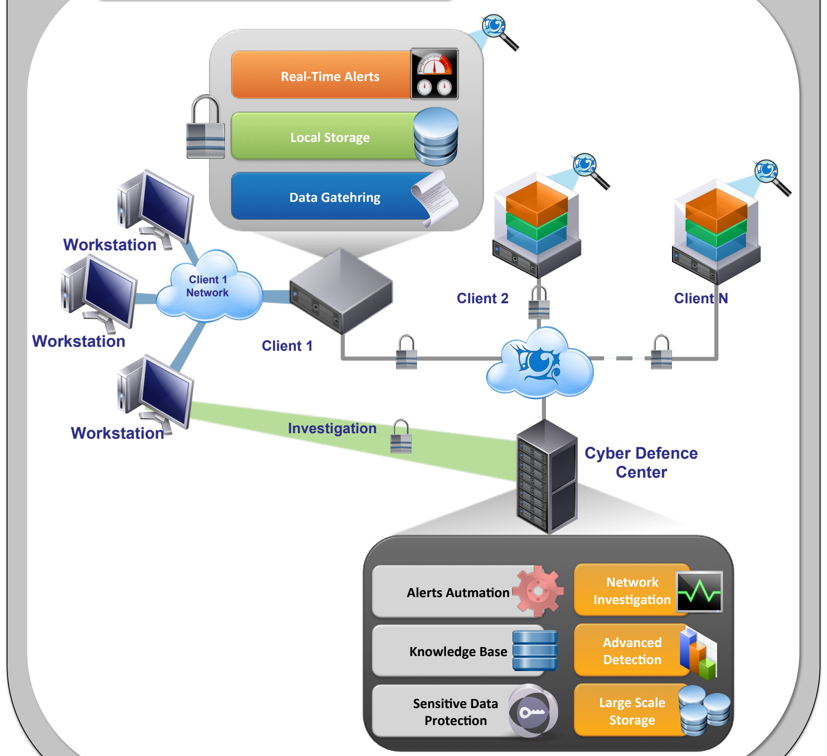
Context

Motivations

- Build a "Trusted" Intrusion Detection System for Critical Infrastructures.
- Classical Intrusion Detection Systems rely on "known" attacks patterns (signatures).
- Signatures creations is a time-consuming and error-prone task.
- Critical infrastructures require faster and more efficient intrusion detection mechanisms.

Rethink Intrusion detection using BigData and Machine Learning Technologies

IDOLE Project



Classification based IDS

Problematic

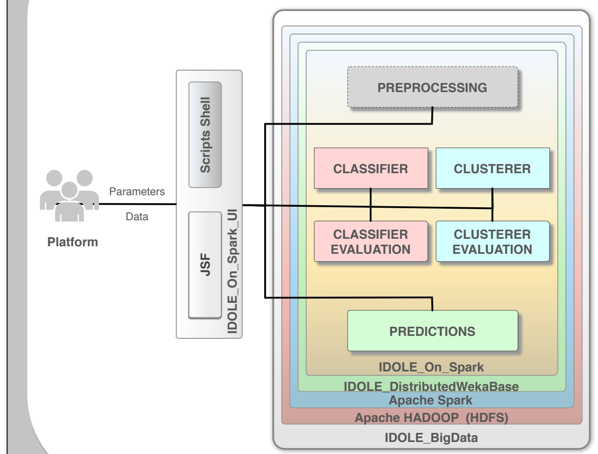
- New attacks are often variations of old and well known attacks
- Supervised Machine Learning Algorithms can be trained to learn and detect variations
- Learned Models depend on the quantity of training datasets (Learning Curve).
- Unfortunately, existing frameworks do not scale

Clustering based IDS

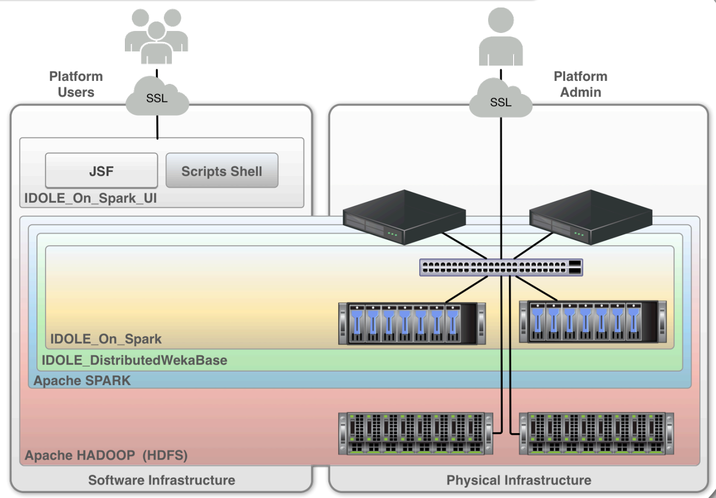
Problematic

- Supervised Machine Learning provide very good results.
- These results depend on the availability and the quality of training datasets.
- Datasets are hard to obtain.
- What about non-supervised machine learning?

BigData Machine Learning Platform for Intrusion Detection

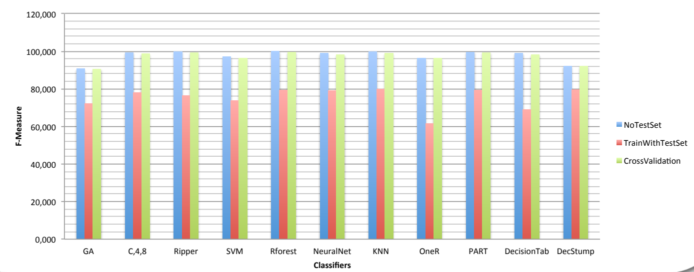


- Fully distributed and Large Scale Machine Learning Platform.
- Deployment on a physical BigData infrastructure:
  - 10 nodes
    - 32 vcores
    - 2,6 GHZ
    - 64 Go RAM
    - 1 To HDD



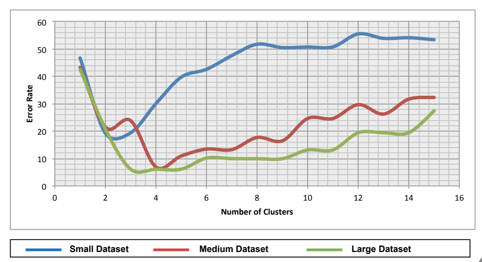
Results

- Very good accuracy with cross-validation



Results

- Preliminary evaluations on **Scalable K-Means++** [1].
- With larger datasets we build better models.



[1] Bahman Bahmani, Benjamin Moseley, Andrea Vattani, Ravi Kumar, and Sergei Vassilvitskii. 2012. Scalable k-means++. *Proc. VLDB Endow.* 5, 7 (March 2012), 622-633.

Contact **reda.yaich@imt-atlantique.fr**

Site web **http://projet-idole.fr**

USER-CENTRIC MANAGEMENT OF SECURITY AND DEPENDABILITY IN CLOUDS OF CLOUDS

MISSION

SUPERCLOUD aims to **support user-centric deployments** across multi-clouds, enabling the composition of innovative trustworthy services, to uplift Europe's innovation capacity and thus improve its competitiveness. SUPERCLOUD will thus build a **security management architecture** and infrastructure to fulfil the vision of user-centric secure and dependable cloud of clouds.

OBJECTIVES

Self-Service Security: Implementation of a cloud architecture that gives users the flexibility to define their own protection requirements and instantiate policies accordingly.

Self-Managed Security: Development of an autonomic security management framework that operates seamlessly over compute, storage and network layers, and across provider domains to ensure compliance with security policies.

End-to-End Security: Proposition of trust models and security mechanisms that enable composition of services and trust statements across different administrative provider domains.

Resilience: Implementation of a resource management framework that composes provider-agnostic resources in a robust manner using primitives from diverse cloud providers.

MOTIVATION

Despite many benefits in terms of business, distributed cloud computing raises many security and dependability concerns. At stake are an increase in complexity and a lack of interoperability between heterogeneous, often proprietary infrastructure technologies. The SUPERCLOUD project proposes new security and dependability infrastructure management paradigms that are:

- **user-centric**, for self-service clouds of clouds where customers define their own protection requirements and avoid lock-ins
- **self-managed**, for self-protecting clouds-of-clouds that reduce administration complexity through security automation

TECHNICAL APPROACH

The SUPERCLOUD project is planned to run for 36 months. It is organized into seven work packages with significant dependencies and expected synergies between them.

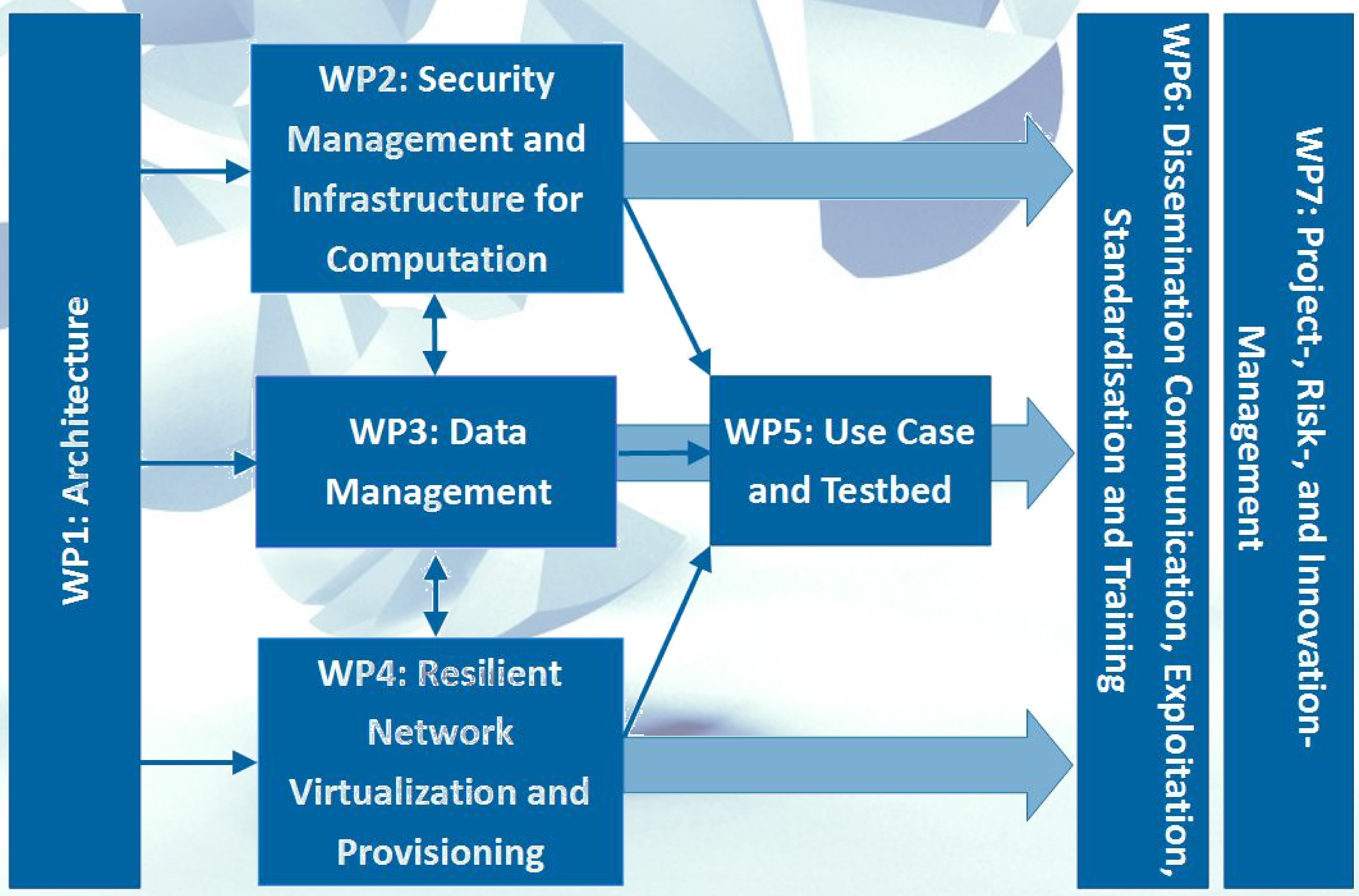
WP1 Architecture is the technical backbone of the SUPERCLOUD project as it defines the architecture and framework for the remaining work packages.

WP2 Security Management and Infrastructure for Computation specifies and implements the main components and protocols of the federated cloud infrastructure for computing and the design of the corresponding security self-management framework.

WP3 Data Management designs and implements SUPERCLOUD protection of user assets in the distributed cloud, focusing on autonomic security provisioning and end-to-end security.

WP4 Resilient Network Virtualization and Provisioning enables to create virtual networks for multi-clouds with resilience and security guarantees.

WP5 Use-case and testbed enables to demonstrate and validate SUPERCLOUD core technology. A testbed that will enable the reproduction in realistic settings of the two use cases will be set up.



WP6 Dissemination, Communication, Exploitation, Standardization and Training focuses on communication and dissemination of scientific research results to outside parties as well as to participating entities.

WP7 Project-, Risk-, and Innovation-Management ensures a successful project lifetime with respect to risk and innovation management. WP7 coordinates the tasks so that they are in line with the project work plan in order to reach the objectives of SUPERCLOUD.

Project Coordinator:
Dr. Klaus-Michael Koch
Technikon Forschungs- und Planungsgesellschaft mbH
Burgplatz 3a
A-9500 Villach
Austria
Tel.: +43 4242 233 55 - 71
Fax: +43 4242 233 55 - 77
Email: coordination@supercloud-project.eu
Web: www.supercloud-project.eu

Technical Lead:
Dr. Marc Lacoste
Orange Labs, Department of Security
38-40 rue du Général Leclerc
92794 Issy-Les-Moulineaux
France
Tel.: +33 1 45 29 67 24
Email: marc.lacoste@orange.com

Project start: 1st February, 2015
Project duration: 3 years

Project Partners:
TECHNIKON, Ciências ULisboa, Technische Universität Darmstadt, orange, Institut Mines-Télécom, Philips, IBM, maxdata

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 643964.

This work was supported (in part) by the Swiss State Secretariat for Education, Research and Innovation (SERI) under contract number 15.0091.

CyberCOP3D
Visualisation Collaborative et Immersive pour la cybersécurité

Contexte

Auteur

Alexandre KABIL

Directeurs de thèse

Thierry DUVAL
Nora CUPPENS

Partenaires

Constats

Visualisation pour la cyber sécurité

- Traitement de gros volumes de données hétérogènes (paquets et trames réseau, historiques de connexions, alertes d'intrusions ou virales) [Shiravi2012]
  - La *Visual Analytics* facilite la coopération humain-IA pour le traitement et la corrélation des données [Sun2013]
  - Acquisition d'une *Cyber Situation Awareness* [Franke2014] via le biais d'une *Common Operational Picture (Figure 1)*

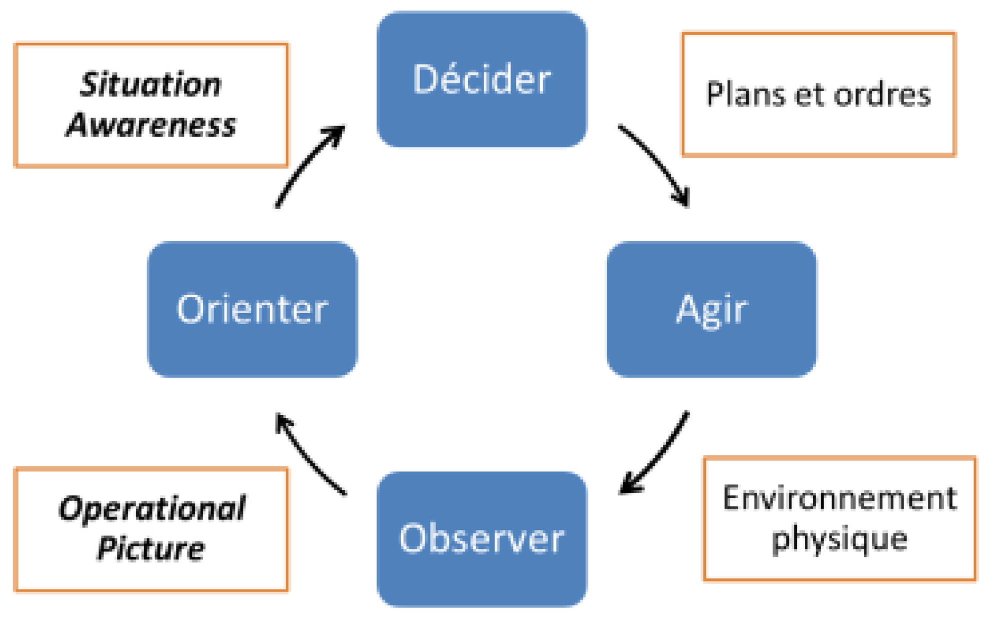


Figure 1 : Cycle de prise de décision « Observ, Orient, Decide, Act »

- Peu de visualisations collaboratives et immersives ou 3D pour la cybersécurité:
  - Complexité plus importante du développement 3D (risques d'occultation et de pertes de repères, manque de librairies adaptées…)
  - Non prise en compte du point de vue de l'utilisateur (non-détection des mouvements de tête)
  - Émergence de nouveaux moyens immersifs encourageant l'*Immersive Analytics* [Hackathorn2016]

- Les Security Operations Center (SOCs), centres névralgiques de la sécurité des systèmes (Figure 2)
  - Environnements collaboratifs
  - Gestion des incidents de sécurité et monitoring continu de l'état des réseaux
  - Différents rôles et outils d'analyses
  - Peu d'interactions naturelles ou immersives (grands écrans non tactiles et interfaces individuelles de type GUI)

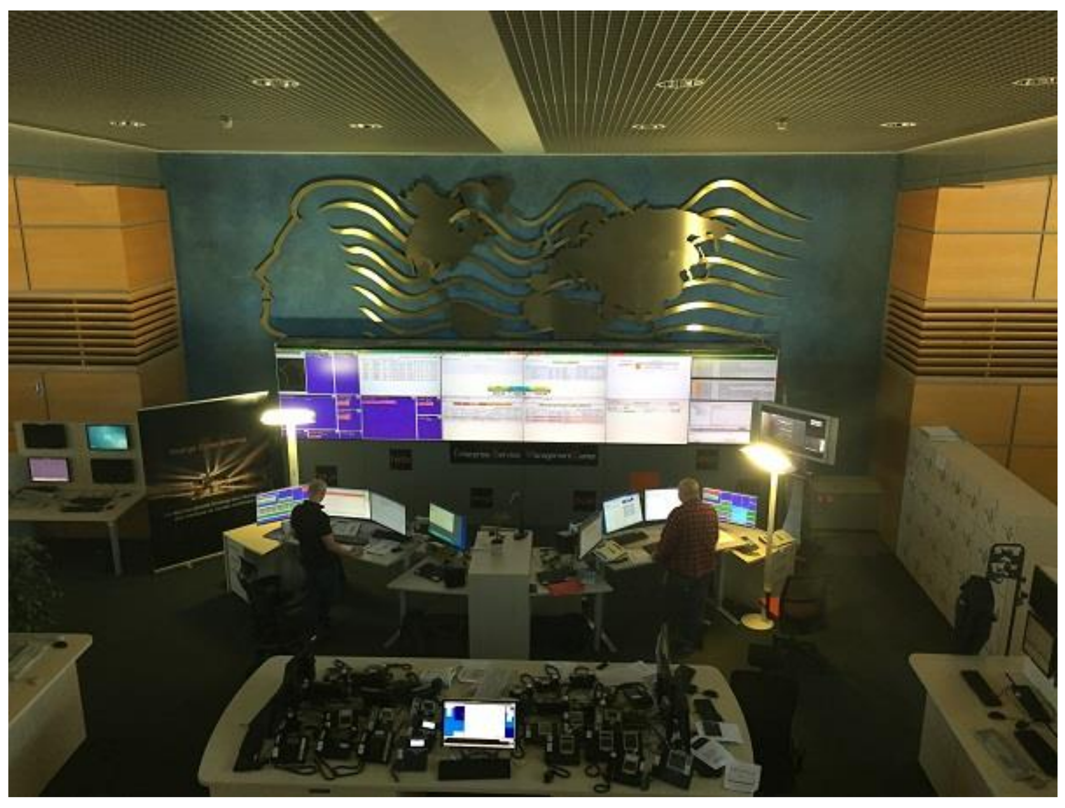
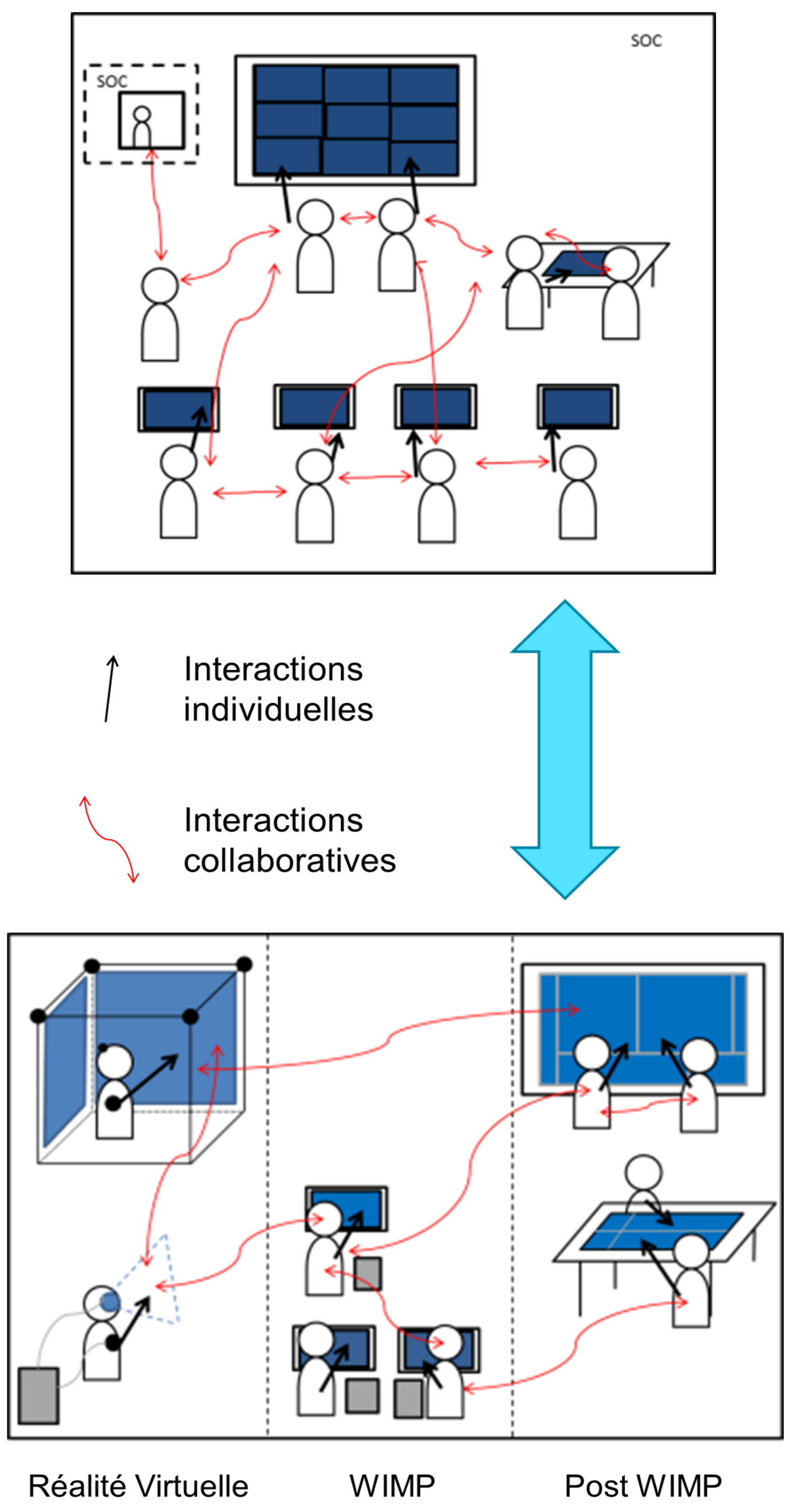


Figure 2 : Vue d'une partie du CyberSOC d'Orange (Crédit photo : Orange)



Proposition

CyberCOP 3D

- Application immersive collaborative pour la visualisation de données
  - Hybridation 2D/3D afin de proposer des vues asymétriques
  - Collaboration horizontale (complémentarité des vues) et verticale (visualisation du système à différentes échelles)

- Cadres d'études : les SOCs et les Malwares
  - Analyse de l'activité collaborative au sein des SOCS
  - Modélisation fine de l'interaction d'un Ransomware [Popoola2017] avec un système

- Scénario collaboratif envisagé
  - Simulation d'un scénario d'expansion virale d'un Ransomware
  - Interaction naturelle et contextualisée sur les données
  - Collaboration asymétrique

- **Shiravi, H., Shiravi, A., & Ghorbani, A. A.** (2012). A survey of visualization systems for network security. *IEEE Transactions on visualization and computer graphics*, *18*(8), 1313-1329.
- **Franke, U., & Brynielsson, J.** (2014). Cyber situational awareness–a systematic review of the literature. *Computers & Security*, *46*, 18-31.
- **Sun, G. D., Wu, Y. C., Liang, R. H., & Liu, S. X.** (2013). A survey of visual analytics techniques and applications: State-of-the-art research and future challenges. *Journal of Computer Science and Technology*, *28*(5), 852-867.
- **Hackathorn, R., & Margolis, T.** (2016, March). Immersive analytics: Building virtual data worlds for collaborative decision support. In *Immersive Analytics (IA), 2016 Workshop on* (pp. 44-47). IEEE.
- **Popoola, S. I., Iyekekpolo, U. B., Ojewande, S. O., Sweetwilliams, F. O., John, S. N., & Atayero, A. A.** (2017). Ransomware: Current Trend, Challenges, and Research Directions. In *Proceedings of the World Congress on Engineering and Computer Science* (Vol. 1, pp. 169-174).

Contact : alexandre.kabil@imt-atlantique.fr

A software-based approach to identify heavy-hitters in high-speed network traffic

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Partners

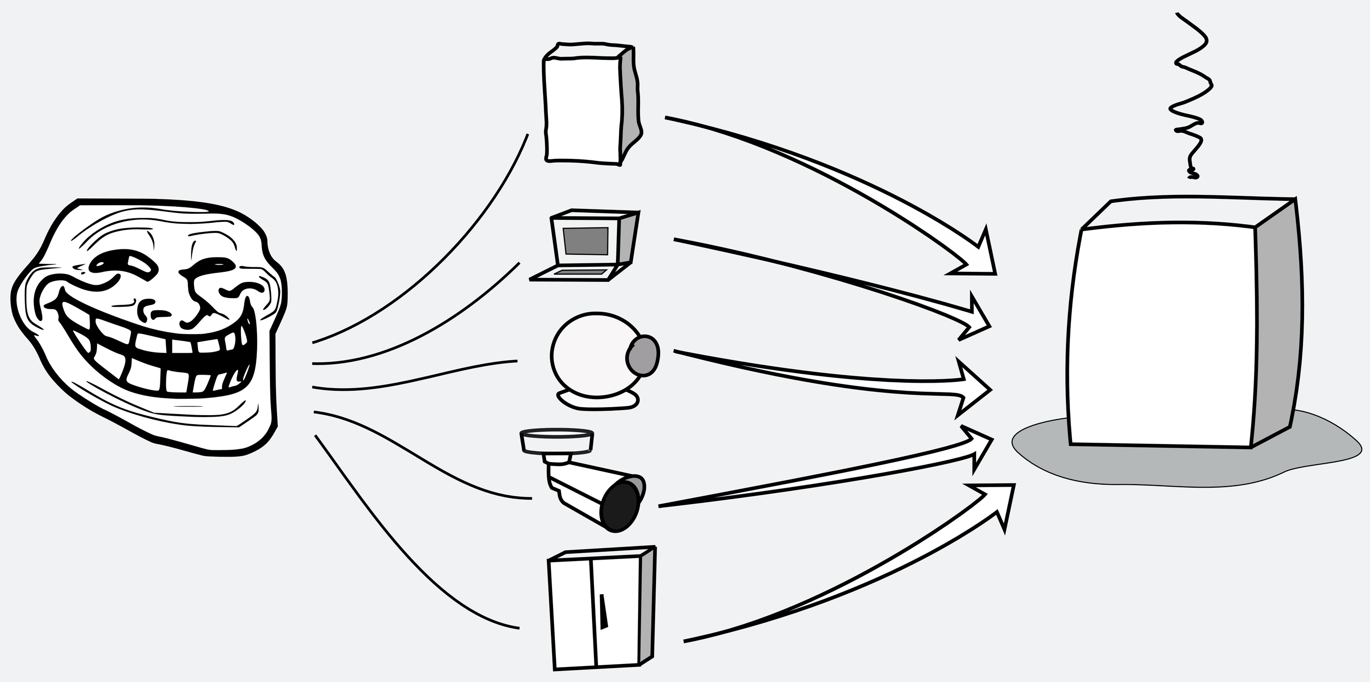
IRISA

CNRS

Authors

Santiago Ruano Rincón
Sandrine Vaton

1. The problem: Distributed Denial-of-Service



Case study: DNS

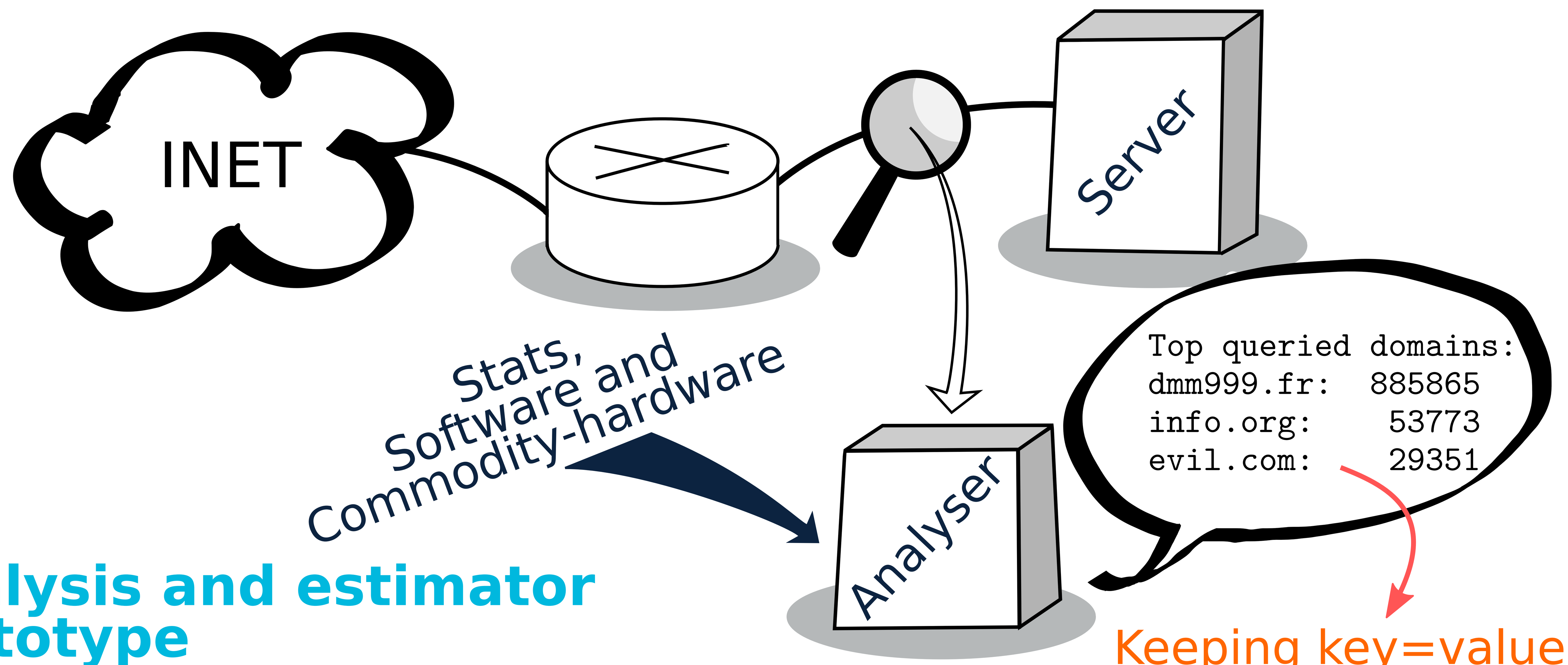
- Domain Name System (DNS)
- Essential Internet service

`wikipedia.org` ⟷ `2620:0:862:ed1a::1`

- AFNIC and dafa888.wf: 1 Mpps
- Cloudflare: 300 Mpps?
- Dyn, 21 Oct 2016: 1.4 Gpps?

What are the most frequent queried domains?

2. Approach to identify the source of problems



Keeping key=value tables is unfeasible

We use then CM Sketches to estimate the actual counts:

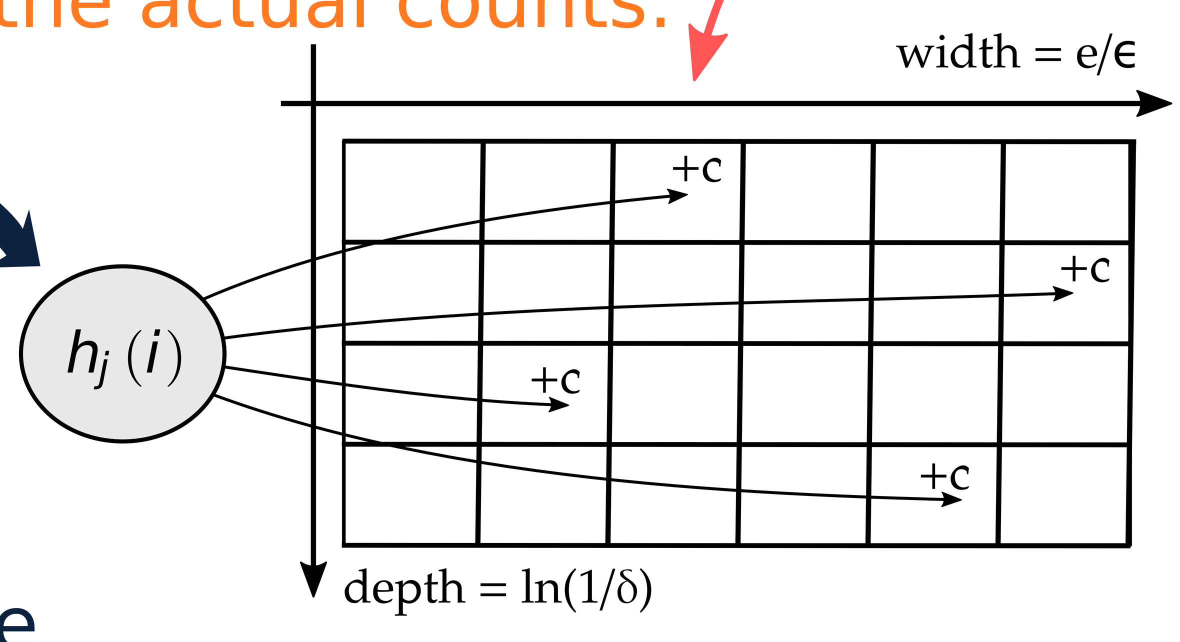
3. Analysis and estimator prototype

- DPDK http://dpdk.org/
- High-level scripting
- 10Gbps (12Mpps)
- Relaying on Count-Min Sketch

  Controlled error probability:

$$P||(\hat{a}_i - a_i) < (\epsilon * |s|_1)|| > (1-\delta)$$

s = traffic stream
ϵ,δ = sketch parameters (0...1)
$\hat{a}_i$ = estimated occurrences of item i
a_i = actual occurrences



To know more:

Prototype: https://frama.link/dns10gbe
Article: https://frama.link/RIPELabsHeavyHittersDNS

4. Conclusion

- Processes 99.99% of DNS traffic at 10GbE wire-rate
- Requires several CPU cores (8)
- Low estimation error
- Highly flexible and modifiable

5. References

- G. Cormode and S Muthukrishnan. An improved data stream summary: the count-min sketch and its applications. Journal of Algorithms, 55(1):58–75, 2005.
- S. Ruano Rincón, S. Vaton, and S. Bortzmeyer. Reproducing DNS 10Gbps flooding attacks with commodity-hardware. In IWCMC 2016.

Contacts : santiago.ruano-rincon@irisa.fr, sandrine.vaton@imt-atlantique.fr

What users need

Adapting qualitative research methods to security policy elicitation

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Authors

Vivien Rooney
Simon Foley

Partners

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

CHAIR OF CYBERCNI
Critical National Infrastructures

UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

Insight

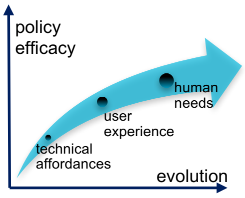
Funding

CHAIR OF CYBERCNI
Critical National Infrastructures

UNION EUROPÉENNE
UNANIEZH EUROPA
L'Europe s'engage en Bretagne
Région BRETAGNE

Fondúireacht Eolaíochta Éireann
sfi
Dá bhfuil romhainn

Security policy elicitation challenges

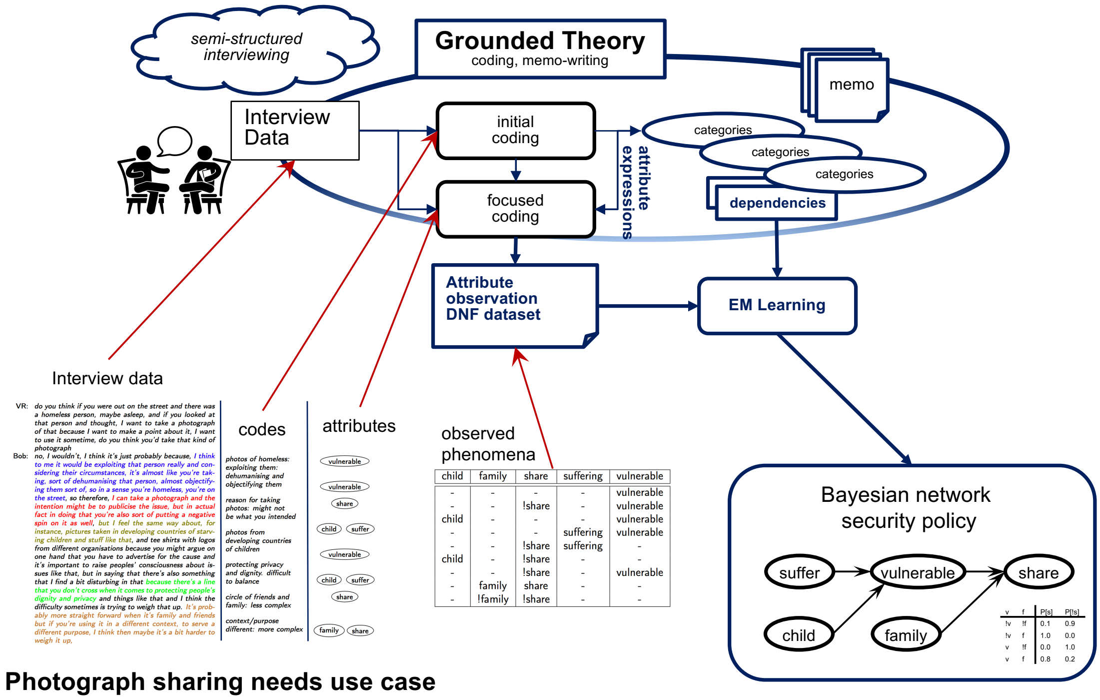


- Elicitation tends to focus on technical affordances at the expense of human needs.
- How can we consider human needs in elicitation?

Elicitation using Qualitative Research

- Qualitative research methods used in Psychology to find out how people make sense of their world.
- Use Grounded Theory research methods to discover user security policy needs. This provides:
  - Systematic, transparant techniques
  - Iterative data collection and analysis
- Proposed method incorporates:
  - Interviewing, data analysis
  - Generation of Bayesian network policy

A Grounded Theory method for attribute based policy elicitation



child	family	share	suffering	vulnerable
-	-	-	-	vulnerable
-	-	!share	-	vulnerable
child	-	-	-	vulnerable
-	-	-	suffering	vulnerable
-	-	!share	suffering	-
child	-	!share	-	-
-	-	!share	-	vulnerable
-	family	share	-	-
-	!family	!share	-	-

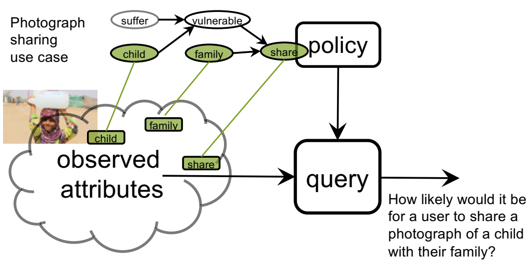
Photograph sharing needs use case

LaTeX markup of Grounded Theory analysis

- Markup of phenomena in interview text
  - phenomena occurs (`code`), not occurs (`!code`)
  - simultaneous occurrence (`<codeXpr>+<codeXpr>`)
  - independent occurrence (`<codeXpr>,<codeXpr>`)
- Markup dependencies between phenomena
  - `vulnerable -> share`

```
\qaCode{vulnerable}{I think to me it would be exploiting that person …},
so therefore, \qaCode{vulnerable+!share}{I can take a photograph and the
intention might be to publicise the issue, …}, \qaDep{vulnerable}{share}
\qaCode{((child,suffering)+vulnerable)}{but I feel the same way about,
for instance, pictures taken in developing countries of starving children
```

Approximating Attribute Based Policy Model



[vivien.rooney|simon.foley]@imt-atlantique.fr

Novembre 2017 Colloque de l'Institut Mines Télécom Paris

IMT LILLE DOUAI

A First Step Towards Security Extension for NFV Orchestrator

Partners

IMT Lille Douai
École Mines-Télécom
IMT-Université de Lille

SAMOVAR UMR 5157

orange™

Authors

Montida Pattaranantakul[1,2],
Yuchia Tseng[3],
Ruan He[4],
Zonghua Zhang[1,2],
Ahmed Meddahi[1]

Affiliations

[1] IMT Lille Douai, Institut Mine-Télécom, Univ. Lille

[2] CNRS UMR 5157 SAMOVAR Lab, TELECOM SudParis

[3] Paris Descartes University, Paris

[4] Orange Labs, Châtillon

References

[1] TOSCA Simple Profile for Network Functions Virtualization (NFV version 1.0), Mar 2016. http://docs.oasis-open.org/tosca/tosca-nfv/v1.0/csd03/tosca-nfv-v1.0-csd03.pdf

[2] OPNFV, Moon – Security Management Module, Apr 2016. https://wiki.opnfv.org/display/moon/Moon

* We received the best paper award, and selected to present at NFV World Congress 2017

1. Key observations

- Many existing NFV frameworks do not support model-driven NFV orchestration, neither TOSCA data model standard [1]
- The typical NFV orchestrator does not contain the capability of security management

2. Contributions

- We extend the typical NFV orchestrator to have the capability of managing security mechanisms
- We propose a security extension module based on TOSCA data model with security aspect
- We develop a use case of access control by leveraging Moon framework – a well developed security policy engine [2]

3. Security extension for NFV orchestrator

The development of security extension contains three major components:

- TOSCA data model (service template) – our contribution is to extend the typical TOSCA data model with security policy and attribute specification
- NFV orchestrator
- Security extension

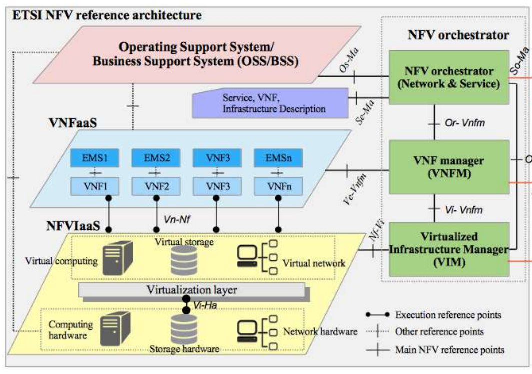


Fig1: Security extension for NFV orchestrator aligned with ETSI NFV MANO

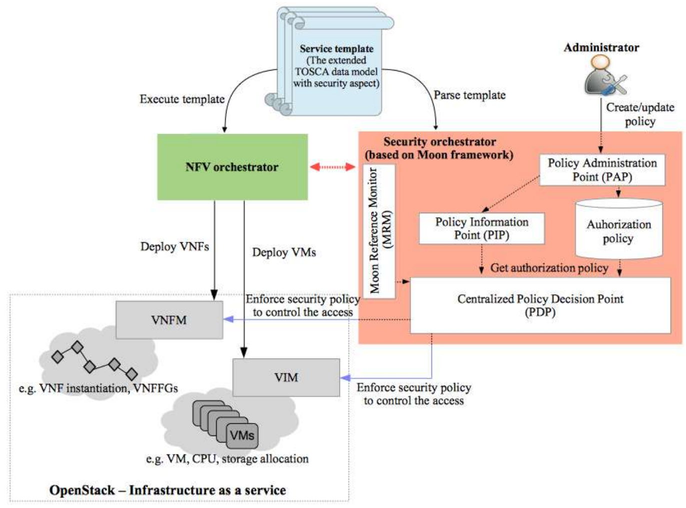


Fig2: The detailed model of security extension of NFV orchestrator, which provides automatic security control, verify security attributes, and enforce security policies

4. Use case: Access control

We develop a realistic use case of access control by extending TOSCA data model with security attributes and policy specification

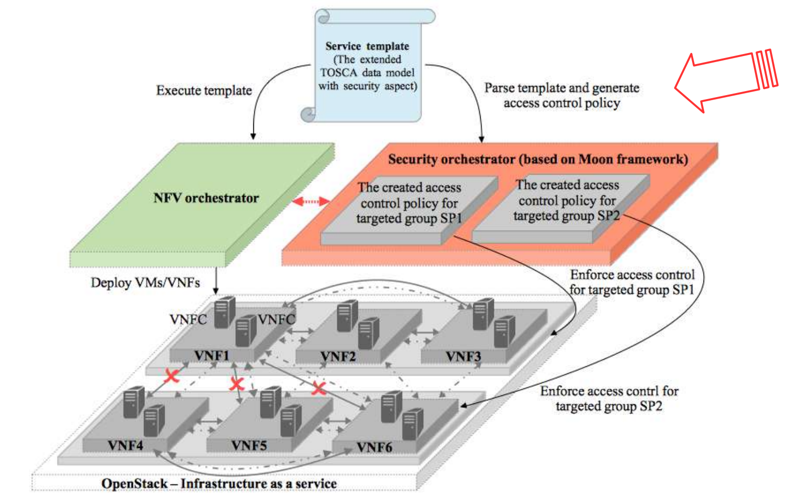


Fig3: Data model of security extension for NFV orchestrator, dotted line represents "no security policy specification", and solid line represents "security policy specification"

Fig4: An example of the extended TOSCA data model with security policy specification (highlighted in yellow)

```
Example
tosca_definitions_version: tosca_simple_profile_for_nfv_1_0
description: example of the extended TOSCA data model
topology_template:
  node_templates:
    VNFC1:
      type: tosca.nodes.Compute
        derived_from: tosca.nodes.Root
      properties:
        num_cpus: 4
        mem_size: 4096 GB
        disk_size: 8GB
        image: vm1.image
    CP1: #logical connection point for this VNFC
      type: tosca.nodes.nfv.CP
        derived_from: tosca.nodes.network.Port
      properties:
        floatingIP: random
      requirements:
        - virtualBinding: VNFC
        - virtualLink: VL
    VL:
      type: tosca.nodes.nfv.VL
        derived_from: tosca.nodes.network.Network
      properties:
         vendor: Fokus
    ... # More VNCF and CP can be created
  node_types:
    VNF1:
      type: tosca.nodes.nfv.VNF
      properties:
        vendor: Fokus
        version: 0.1
        type: server
        floating_ip: 192.168.1.64
      interfaces:
        create: install-server.sh
        start: start-server.sh
        stop: stop-server.sh
      requirements:
        - virtualLink: VL
        - vnfc: VNFC1
    VNF2:
    VNF3:
    VNF4:
    VNF5:
    VNF6:
  Group_Security_Policy:
    SP1:
      type: tosca.groups.nfv
      description: security policy for target group SP1
      targets:
        vnf: [VNF1, VNF2, VNF3]
    SP2:
      type: tosca.groups.nfv
      description: security policy for target group SP2
      targets:
        vnf: [VNF4, VNF5, VNF6]
```

Table1: The extracted data based on the extended TOSCA data model

Nodes	VNF1, IP = 10.0.0.122
	VNF2, IP = 10.0.0.116
	VNF3, IP = 10.0.0.104
	VNF4, IP = 10.0.0.123
	VNF5, IP = 10.0.0.113
	VNF6, IP = 10.0.0.121
Security Policy:	SP1: [VNF1, VNF2, VNF3]
	- Subject: VNF1, Object: VNF2, Access=OK
	- Subject: VNF2, Object: VNF1, Access=OK
	- Subject: VNF1, Object: VNF3, Access=OK
	- Subject: VNF3, Object: VNF1, Access=OK
	- Subject: VNF2, Object: VNF3, Access=OK
	- Subject: VNF3, Object: VNF2, Access=OK
	SP2: [VNF4, VNF5, VNF6]
	- Subject: VNF4, Object: VNF5, Access=OK
	- Subject: VNF5, Object: VNF4, Access=OK
	- Subject: VNF4, Object: VNF6, Access=OK
	- Subject: VNF6, Object: VNF4, Access=OK
	- Subject: VNF5, Object: VNF6, Access=OK
	- Subject: VNF6, Object: VNF5, Access=OK

5. Implementation

- **Service orchestrator**: Heat, as a core part of Openstack platform
- **Security orchestrator**: Parser + Moon policy engine
- **Hardware/CPU specification:**
  - Intel(R) Core(TM) i7-4710HQ CPU @ 2.50GHz + 16 G RAM for Moon framework
  - Intel(R) Core(TM) i5 CPU M 520@ 2.40GHz + 8G RAM for OpenStack
- **Number of deployed VMs:**
  - 6 VNFs (3 VNFs for SP1 + 3 VNFs for SP2

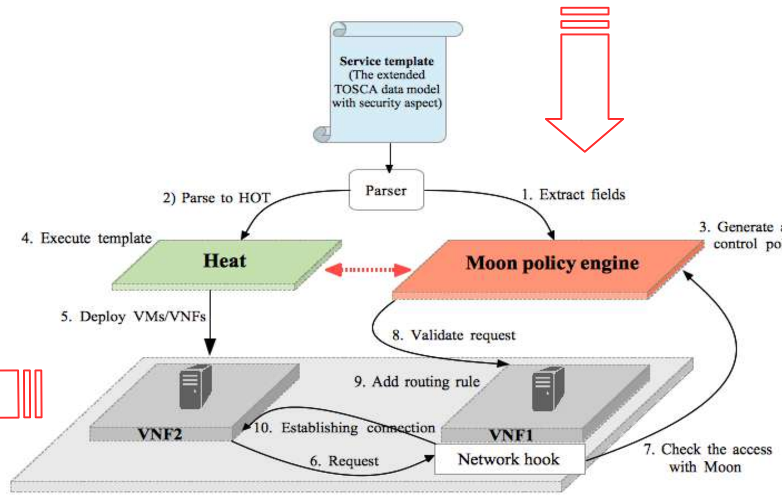


Fig5: The operational flow of security extension for access control

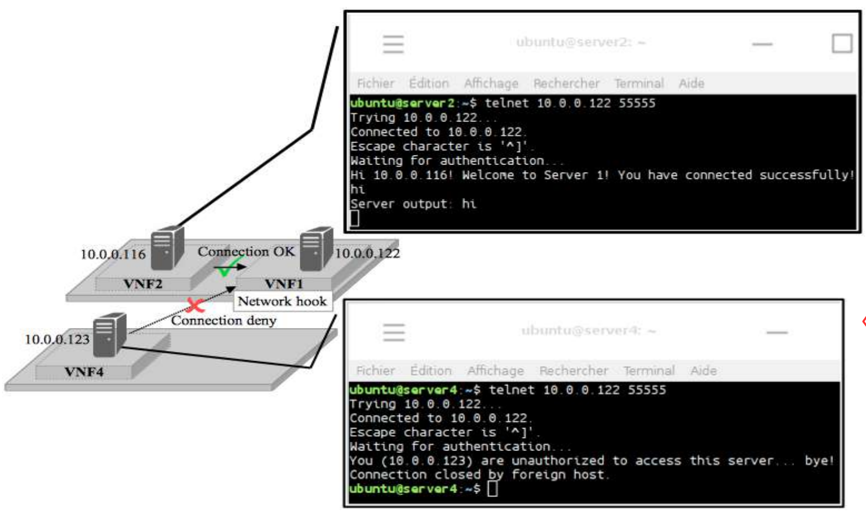


Fig6: A result of testing network connection with Telnel

MINES SAINT-ETIENNE

Institut Mines-Télécom

COGITO

Génération de Code au Runtime pour la Sécurisation de Composants

Parties prenantes

MINES Saint-Étienne

Auteurs

Ecole des Mines de Saint-Etienne
Karim Abdelabtif,
Philippe Jaillon,
Olivier Potin

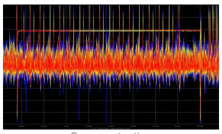
CEA-LIST, CEA-DPACA
Thierno Barry,
Damien Couroussé,
Bruno Robisson

INRIA de Rennes
Hélène Le Bouder,
Jean-Louis Lanet

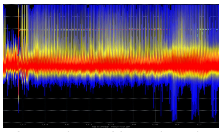
Partenaires

cea tech

Inria



Sans protection



Avec polymorphisme de code

Observation électromagnétique pendant le chiffrement AES

CONTEXTE ET ENJEUX

Ce projet s'intéresse à la sécurisation de composants logiciels dans les systèmes embarqués. Les composants embarqués sont vulnérables aux attaques physiques:

- **les attaques par canaux cachés** sont des attaques passives qui reposent sur l'observation de grandeurs physiques mesurables pendant que le mécanisme sécuritaire attaqué est en fonctionnement, qui permettent par exemple de révéler un secret (par exemple une clé de chiffrement).
- **Les attaques en fautes** sont des attaques actives qui consistent à introduire une erreur pendant que le mécanisme de sécurité s'exécute, afin par exemple de révéler un secret ou à outrepasser les droits d'un utilisateur.
- **La rétro-conception logicielle** permet à un attaquant de se familiariser avec le fonctionnement de la cible d'attaque, afin d'identifier des points de faiblesse et de déterminer un chemin d'attaque.

OBJECTIFS ET METHODES

Le **polymorphisme** de code comme solution innovante pour apporter de la robustesse : pouvoir modifier le **comportement** d'un composant logiciel, sans changer ses **propriétés fonctionnelles**.

- Protection contre le reverse engineering : difficulté de décompilation et de retro-analyse.
- Protection contre les attaques physiques (attaques en fautes, attaques par canaux cachés) : variabilité (spatiale et temporelle) dans l'observation de l'exécution du composant polymorphique.

Mise en œuvre :

deGoal (CEA-LIST) : outil pour la génération de code au runtime, adapté aux contraintes des systèmes embarqués.

Cas d'étude:

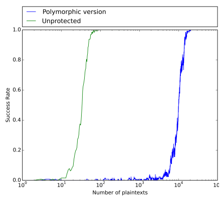
- Fonction de chiffrement AES
- Composant Java Card VerifyPIN (authentification utilisateur)
- Pre-fetch des instructions Java Card

POINTS FORTS

- Légèreté de la solution. Applicable aux systèmes embarqués contraints (< 10kO RAM, <100kO ROM)
- Applicable aux serveurs, plateformes mobiles, etc.
- Compatible avec les protections de l'état de l'art (masking, redondance, etc.)

PERSPECTIVES & MARCHÉS

- IoT / systèmes embarqués enfouis
- General purpose & embedded computing: smartphones, desktop
- Serveurs



Performances

COGITO

Contact : philippe.jaillon@emse.fr , olivier.potin@emse.fr

PROJET FINANCÉ PAR L'ANR - PROJECT FUNDED BY THE ANR

Novembre 2017 Colloque de l'Institut Mines Télécom Paris

TELECOM PARISTECH

Protections against the automotive CAN bus attacks

Khaled karray, Sylvain Guilley, Jean-Luc Danger and Moulay Abdelaziz el Aabid

TELECOM ParisTech – INSTITUT Mines-Télécom; PSA GROUPE

November, 2017

Motivation

1. The Controller Area Network (CAN) is the mostly used communication bus in the automotive domain. The CAN network is not designed with security in mind. E.g., arbitrary read and write accesses are possible.
2. CAN weaknesses when attacker trains (he has access to the CAN network):
   - Protocol Reverse Engineering Attack: an attacker can Read all the frames and reverse the CAN protocol (Message identifiers, message frequencies, etc.).
   - Frame Replay Attack: an attacker can capture, and then replay CAN frames. These CAN frames will be processed by the other ECUs.
   - Frame Injection Attack: an attack can forge CAN frames and inject them into the CAN network. These messages will be processed by other ECUs.
3. Payload protection approaches (confidentiality protection, integrity protection) are not sufficient as the attacker can conduct a payload starvation attack: injection of messages with the right identifiers but with wrong encryption/authentication codes will force the ECU to process the message all the same, hence a possible DoS.

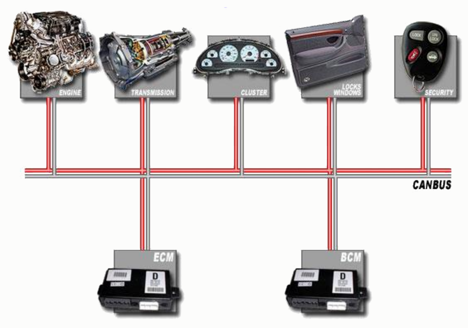
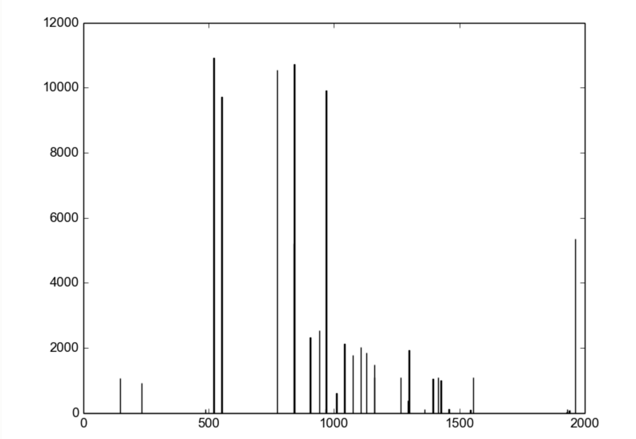


Figure : CAN bus communication between ECUs



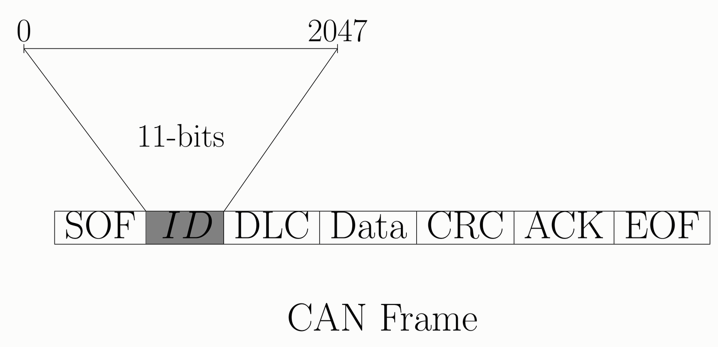


Figure : CAN Identifier Histogram: some identifier are not used

Problem statement

- The goal is to protect the CAN network against *reverse engineering*, *replay* and *injection* attacks
- CAN identifier randomization strategy: the idea is to constantly change the message identifier in a way that the attacker cannot *predict* the next message identifier and cannot *reverse* the CAN protocol.
- The randomization function has to be:
  - Computable
  - Unpredictable
  - Identifier priority preserving
  - Identifier priority preserving in time

Proposed solutions : exploit the sparse distribution of the CAN identifiers

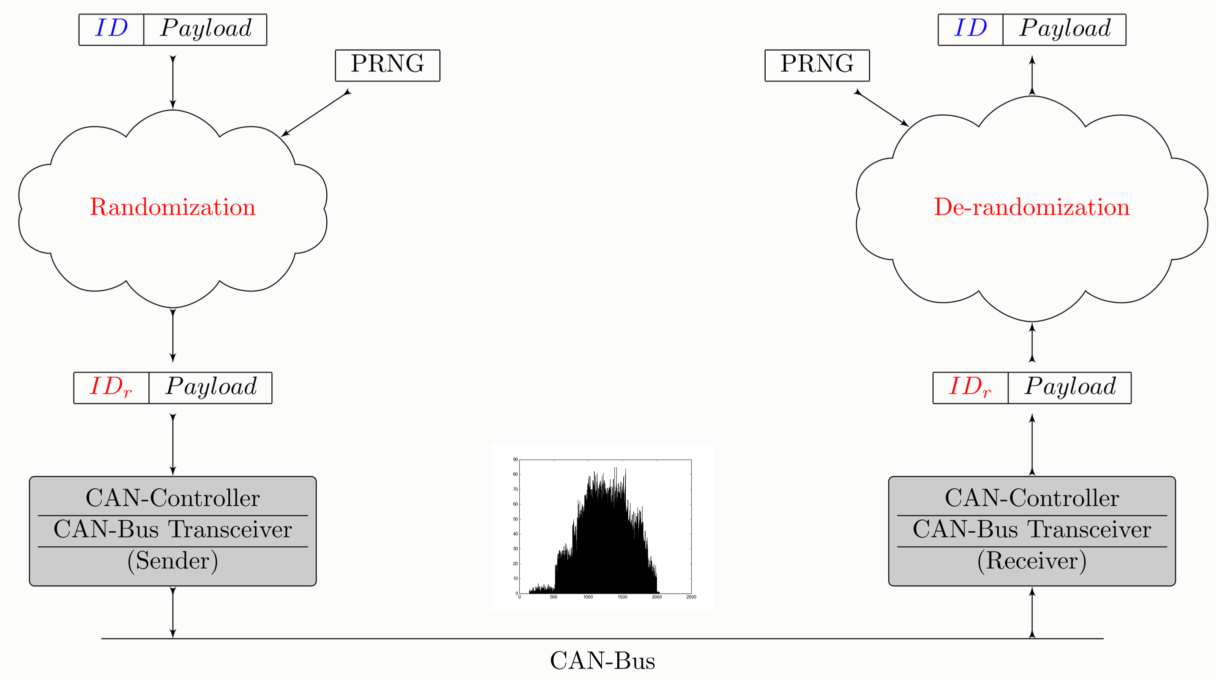


Figure : Randomization Principle: Software layer

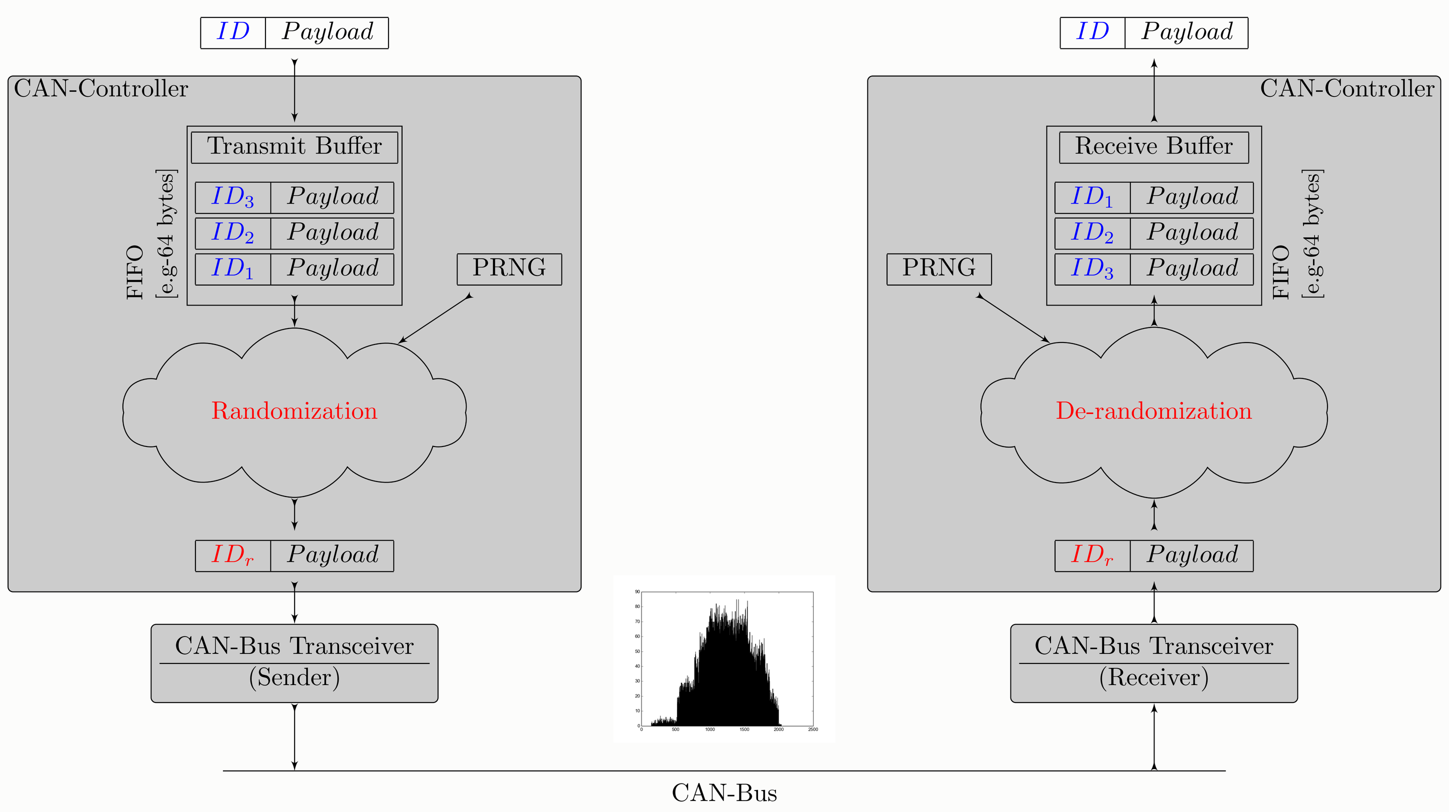
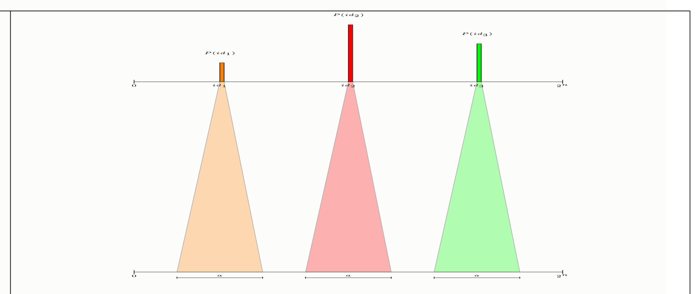
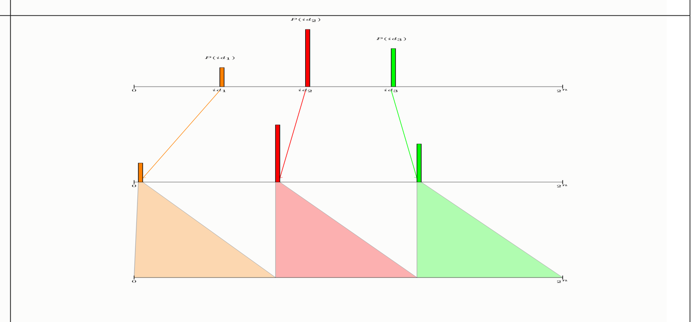
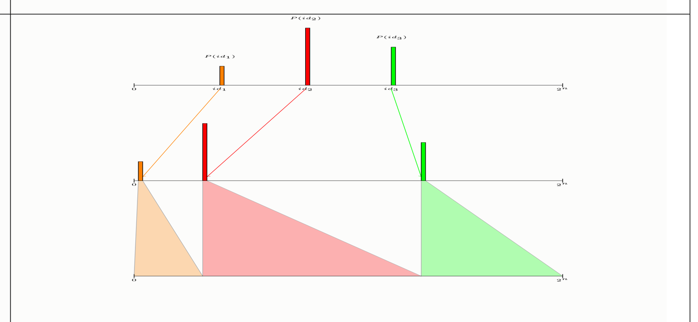
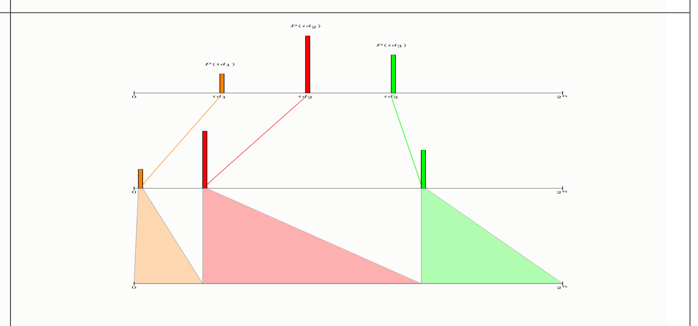
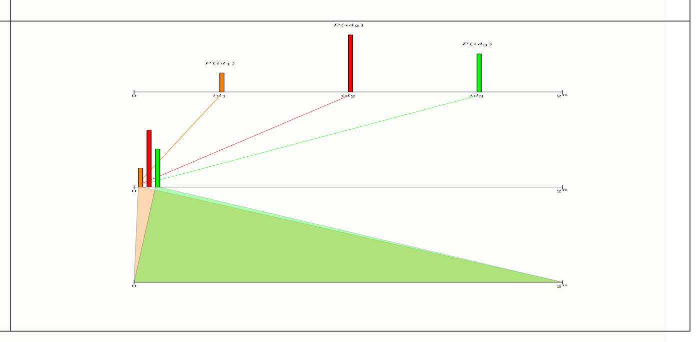


Figure : Randomization Principle: Hardware layer

IA-C: IA-CAN [software] state-of-the-art	$f: [0,2^a-1] \times [2^a,2^n-1] \rightarrow [0,2^n-1]$; $r, id \rightarrow id_{MSB(n-a)} + id_{LSB(a)} \oplus r$	
EI: Equal Intervals [software] New	$Map: [0,2^n-1] \rightarrow [0,2^n-1]$; $id_i \rightarrow i \times Max(1, \lfloor \frac{1}{N} \rfloor)$ $f_r: [0,2^n-1] \rightarrow [0,2^n-1]$; $id_i \rightarrow Map(id_i) + r_{[0, Max(1, \lfloor \frac{1}{N} \rfloor)]}$	
FI: Frequency Intervals [software] New	$Map: [0,2^n-1] \rightarrow [0,2^n-1]$; $id_{i+1} \rightarrow id_i + Max(1, \lfloor \frac{2^n \times f_i}{\sum_{j=1}^{N} f_j} \rfloor)$ $f_r: [0,2^n-1] \rightarrow [0,2^n-1]$; $id_i \rightarrow Map(id_i) + r_{[0, Max(1, \lfloor \frac{2^n \times f_i}{\sum_{j=1}^{N} f_j} \rfloor)]}$	
DFI: Dynamic Frequency Intervals [software] New	$M = m_{1 \leq i,j \leq N} = P(id_j^{t+1}/id_i^t)$: Identifier transition matrix At instant t : id_k was received: $Map^{t+1}: [0,2^n-1] \rightarrow [0,2^n-1]$; $id_{i+1} \rightarrow id_i + Max(1, \lfloor \frac{2^n \times m_{k,i}}{\sum_{j=1}^{N} m_{k,j}} \rfloor)$ $f_r^{t+1}: [0,2^n-1] \rightarrow [0,2^n-1]$; $id_i \rightarrow Map^{t+1}(id_i) + r_{[0, Max(1, \lfloor \frac{2^n \times m_{k,i}}{\sum_{j=1}^{N} m_{k,j}} \rfloor)]}$	
AM: Arithmetic Masking [hardware] New	$Map: [0,2^n-1] \rightarrow [0,N-1]$; $id_i \rightarrow i$ $f_r: [0,2^n-1] \rightarrow [0,2^n-1]$; $id_i \rightarrow Map(id_i) + r_{[0,2^n-N]}$	

Results: Comparison between different randomization strategies

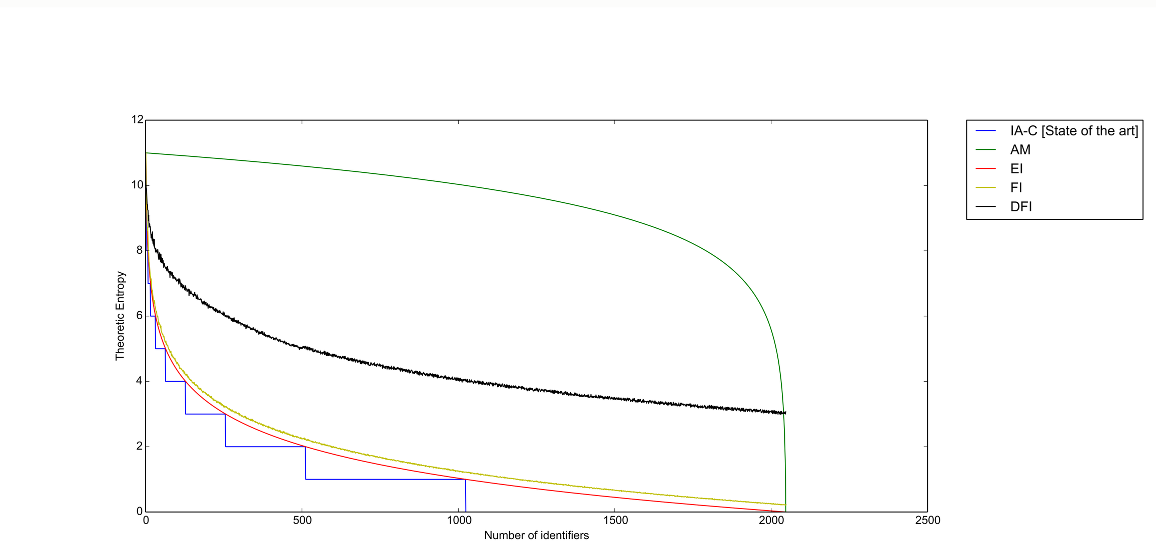


Figure : Conditional entropy $H = f(N)$ [Prediction]: Replay & Injection attacks

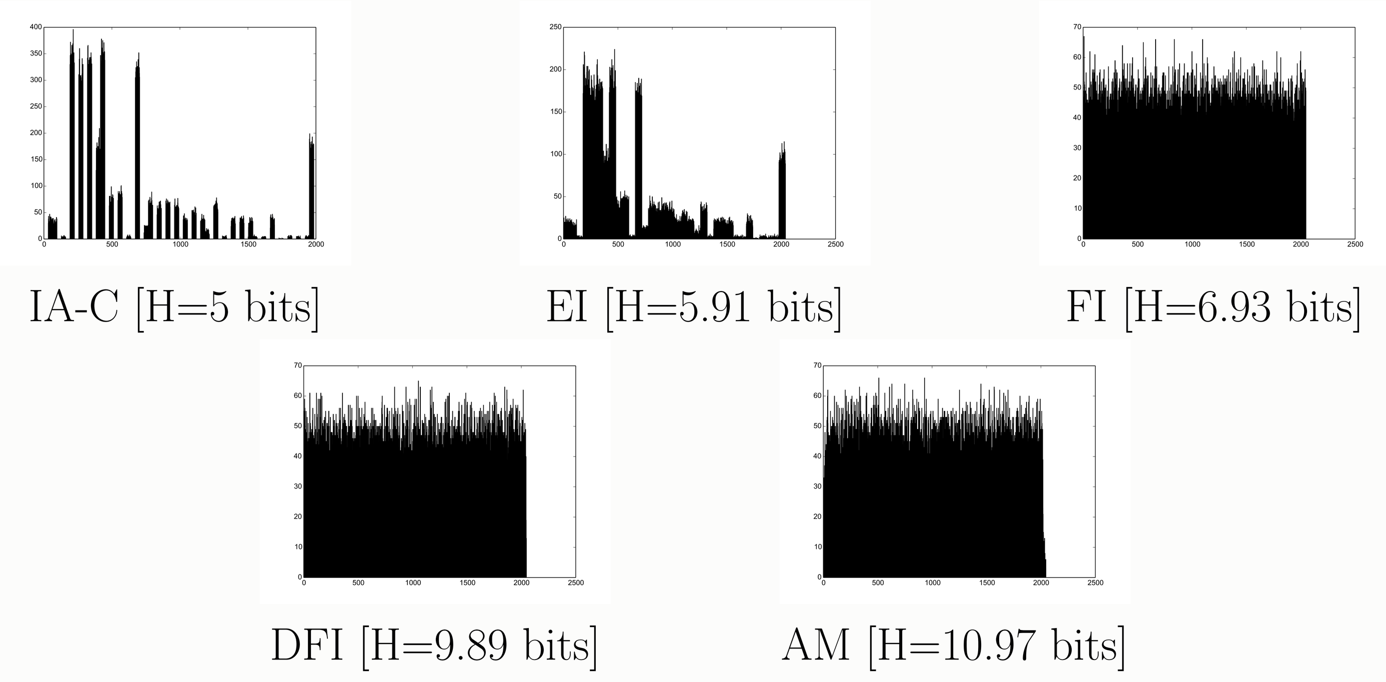


Figure : Identifier histogram after randomization [N=34]

Conclusion:

- Advantage: It is clear that the proposed solution performs better than state-of-the-art solutions from security point of view. The entropy is used as a metric for comparison.
- Limitations: Solutions that perform the best have to be implemented on the hardware level which requires a modification of the standard itself. Application level solutions are limited.

contact : firstname.lastname@telecom-paristech.fr, firstname.lastname@mpsa.com

TELECOM SUDPARIS

Evaluation de la vie privée dans les bases de données basée sur la métrique Discrimination Rate

TELECOM SudParis
INSTITUT Mines-Télécom

université PARIS-SACLAY

cnrs

Auteurs

Louis Philippe SONDECK,
Maryline LAURENT,
Vincent FREY

Partenaires

orange™

Résumé

Nous évaluons de façon précise le degré d'anonymisation d'une base de données en fonction des attaques connues. Notre évaluation est basée sur la métrique Discrimination Rate (DR).

La métrique Discrimination Rate (DR)

Description: Le DR mesure la capacité des attributs clés (Y1, Y2, …, Yn) à raffiner (identifier) les outputs de l'attribut sensible X. Les outputs de X représentent l'ensemble de sujets à protéger (anonymity set). Les valeurs du DR varient entre 0 et 1, proportionnellement à la capacité d'identification.

$$DR_X(Y_1, Y_2, ..., Y_n) = 1 - \frac{H(X|Y_1, Y_2, ..., Y_n)}{H(X)}$$

Nous évaluons la capacité de chaque attribut dans la Table Originale 1 à identifier un sujet dans cette table. Par exemple, DR(Salary) = 1 car chaque sujet possède un salaire différent.

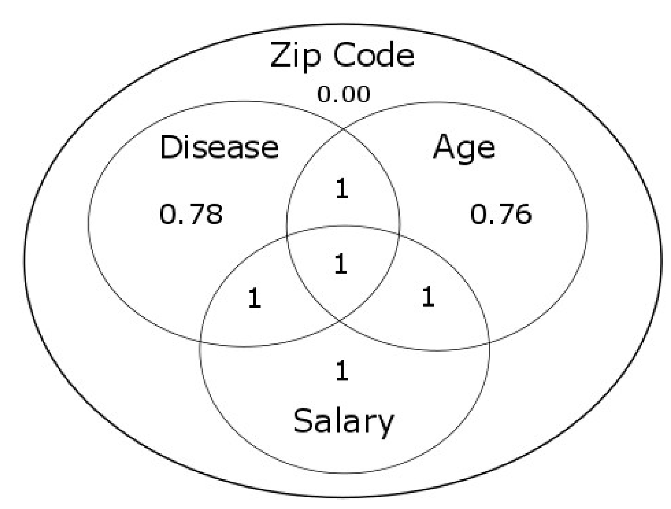


Table Originale 1

	ZIP Code	Age	Salary	Disease
1	35502	22	4K	colon cancer
2	35502	22	5K	stomach cancer
3	35502	22	6K	lung cancer
4	35502	45	7K	stomach cancer
5	35502	63	12K	diabetes
6	35502	40	9K	aids
7	35502	35	8K	aids
8	35502	35	10K	flu
9	35502	32	11K	lung cancer

Table Originale 2

	Age	Disease
1	22	lung cancer
2	22	lung cancer
3	22	lung cancer
4	45	stomach cancer
5	63	diabetes
6	40	flu
7	35	aids
8	35	aids
9	32	diabetes

Méthode

Nous nous proposons d'anonymiser les tables originales (1 & 2) avec une 3-diversification et une 3-anonymisation. Nous évaluons ensuite ces techniques en fonction des attaques connues (*attaque sur l'identité, attaque sur les attributs*).

Tables après 3-anonymisation (Table Originale 2)

Table 1

Age	Age*
22	2*
22	2*
22	2*
45	≥ 40
63	≥ 40
40	≥ 40
35	3*
35	3*
32	3*

Table 2

Age*	Disease
2*	lung cancer
2*	lung cancer
2*	lung cancer
≥ 40	stomach cancer
≥ 40	diabetes
≥ 40	flu
3*	aids
3*	aids
3*	diabetes

Table après 3-diversification (Table Originale 1)

Table 3

	Age*	Disease
1	2*	colon cancer
2	2*	stomach cancer
3	2*	lung cancer
4	≥ 40	stomach cancer
5	≥ 40	diabetes
6	≥ 40	aids
7	3*	aids
8	3*	flu
9	3*	lung cancer

Description des attaques

Attaque sur l'identité: reflète la capacité pour un attaquant de **retrouver l'identité réelle d'un individu** à partir de la table anonymisée, dans notre cas, d'associer une valeur particulière de **Age* (Table 2)** à une valeur particulière de **Age (Table 1).**

Attaque sur les attributs: reflète la capacité pour un attaquant de **gagner de l'information dans une table anonymisée,** dans notre cas, d'associer (dans les **Tables 2 et 3**), une valeur particulière de **Age*** à une valeur particulière de **Disease.**

Résultats

Evaluation des attaques dans les Tables 2 et 3

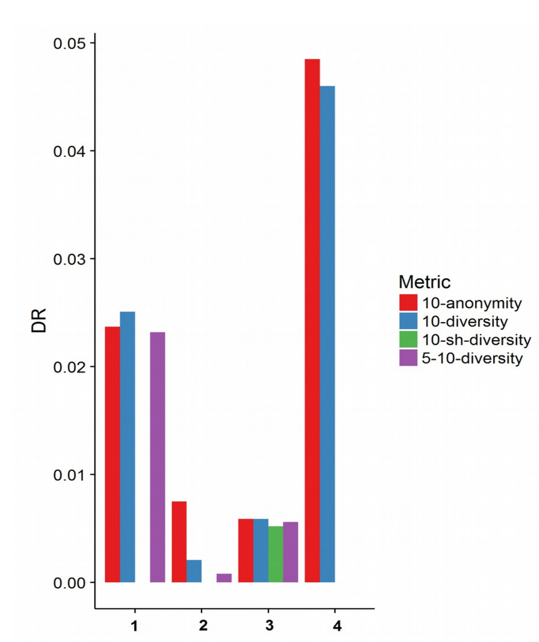
Evaluation de l'attaque sur l'identité (Table 2)

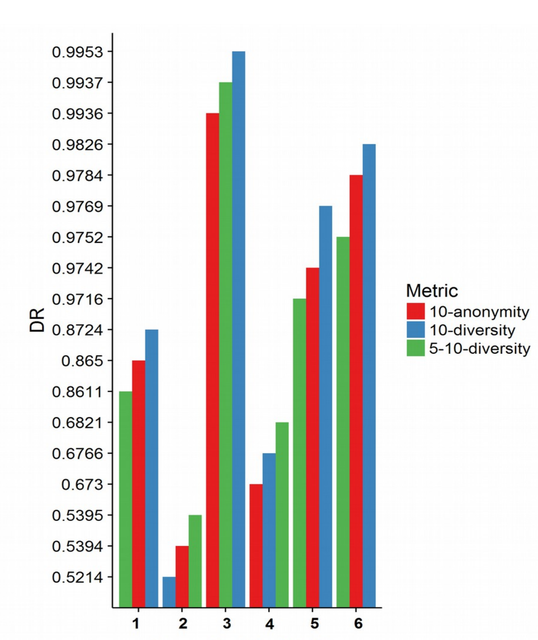
X	Y	$DR_X(Y)$
Age	2*	1
Age	3*	0.87
Age	≥ 40	0.78
Age	Age*	0.65

Evaluation de l'attaque sur les attributs (Tables 2 et 3)

X	Y	$DR_X(Y)$
k-anonymity Table		
Disease	2*	1
Disease	≥ 40	0.70
Disease	3*	0.83
Disease	Age*	0.52
l-diverse Table		
Disease	2*	0.78
Disease	≥ 40	0.78
Disease	3*	0.78
Disease	Age*	0.36

Expérimentation sur données réelles





Expérimentation:
Basée sur des données d'un recensement Américain contenant **plus de 30 000 observations**. Les données ont été **anonymisées** puis évaluées avec notre algorithme implémenté en langage **R en** fonction de l' **attaque sur les attributs**

Observation:
Nous **soulignons certaines incohérences**. Par exemple, pour certaines valeurs, **la k-anonymisation est meilleure que la l-diversification.**

Colloque IMT Cybersécurtié

Novenbre 2017

Contact lpsondeck@hotmail.com

Site web

Sécurité et déploiement de réseaux virtuels répartis

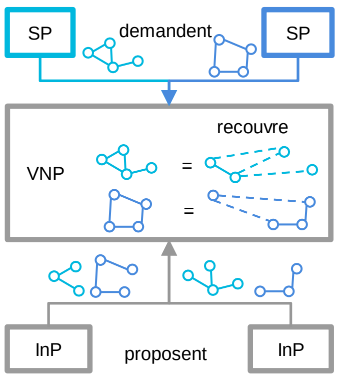
Pour établir la confiance entre les fournisseurs d'infrastructure et de service

Parties prenantes

Auteurs

François Boutigny
Hervé Debar
Gregory Blanc
Antoine Lavignotte
Stéphane Betgé-Brezetz
Ion Popescu

Partenaires

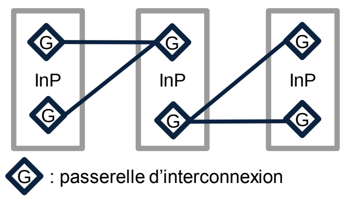


Entités et opérations du modèle

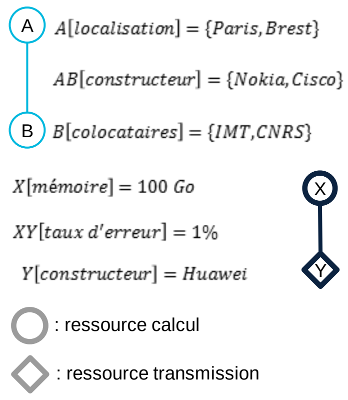
Modélisation des acteurs et relations de confiance

La place du fournisseur de réseaux virtuels

- **Fournisseurs d'infrastructure** *(InP)* – Possède des ressources informatiques (calcul, transmission de données), et cherche à les louer.
- **Fournisseurs de service** *(SP)* – Préfère louer des ressources plutôt que d'en posséder, afin de délivrer son service.
- **Fournisseur de réseaux virtuels** *(VNP)* – Établit un réseau virtuel distribué sur plusieurs infrastructures pour le compte d'un fournisseur de service.
- Les SP comptent sur le VNP pour sélectionner les « bons » InP.
- Le VNP compte sur l'honnêteté des InP.
- Les InP comptent sur le VNP
  - Pour ne pas divulguer leurs informations.
  - Pour que la concurrence soit juste.
- Les InP refusent d'exposer la topologie de leur infrastructure.



État de la connaissance du fournisseur de réseaux virtuels

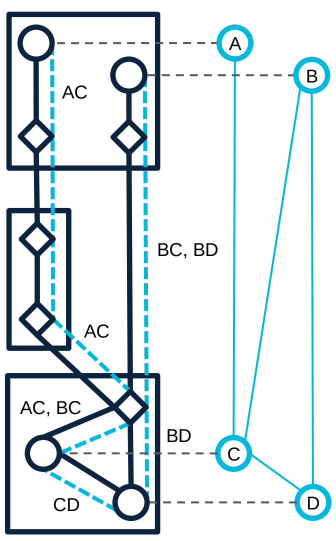


Exemples de demande et d'offre

Application des politiques de sécurité des SP et des InP

Trouver l'équilibre entre la demande et l'offre

- Les ressources sont pourvues **d'attributs**:
  - Contraintes de sécurité sur les ressources demandées.
  - Propriétés, disponibilité sur les ressources offertes.
  - *Exemples*: **localisation** géographique, **constructeurs** d'un commutateur, **fonctions** de sécurité, **colocataires** autorisés, **taux d'erreur** sur un lien.
- Les InP appliquent leur propre **politique de sécurité**:
  - Obligation/interdiction sur la demande.
  - En cas de conflit, rejet de la demande.



Exemple d'allocation de ressources plus générale que l'état de l'art [1] (vue globale)

Allocation des ressources réparties sur plusieurs infrastructures

Optimiser les couts selon deux perspectives

- Les InP veulent maximiser leurs revenus
  - Héberger le plus de SP possibles, ou le plus de ressources demandées
- Les SP veulent minimiser leurs dépenses
  - Sélectionner des InP et des interconnexions les moins couteuses
- Résolution hybride [1]
  - Un SP envoie une demande au VNP
  - Le VNP transmet aux InP
  - Les InP renvoient des propositions conformes (et maximisées)
  - Le VNP minimise le cout (chiffré)

[1] T. Mano, T. Inoue, D. Ikarashi, K. Hamada, K. Mizutani, and O. Akashi, "Efficient Virtual Network Optimization Across Multiple Domains Without Revealing Private Information," *IEEE Transactions on Network and Service Management*, vol. 13, no. 3, pp. 477–488, Sep. 2016.

Contact : francois.boutigny@telecom-sudparis.eu

Institut Mines-Télécom

Detection of Attacks against Cyber-Physical Systems

Parties prenantes

TELECOM SudParis

CHAIRE CYBER CNI Sécurité des infrastructures critiques

Auteurs

Jose Rubio Hernan
Joaquin Garcia-Alfaro

1. Context

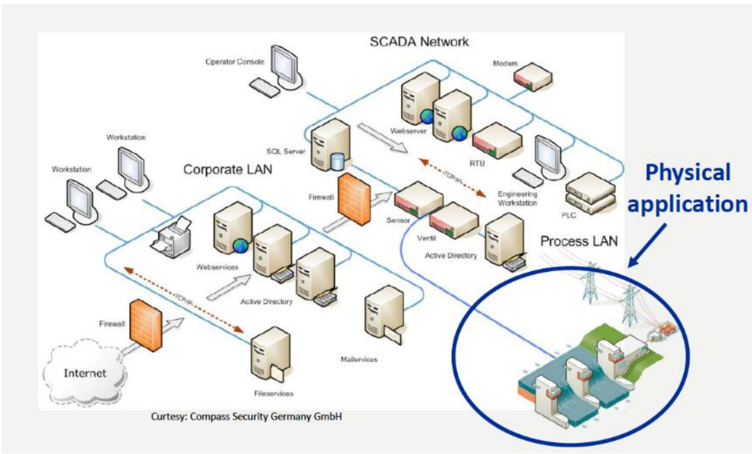
- Cyber-Physical Systems & SCADA (Supervisory Control and Data Acquisition) technologies
- Real-time systems that centrally monitor & control remote equipment



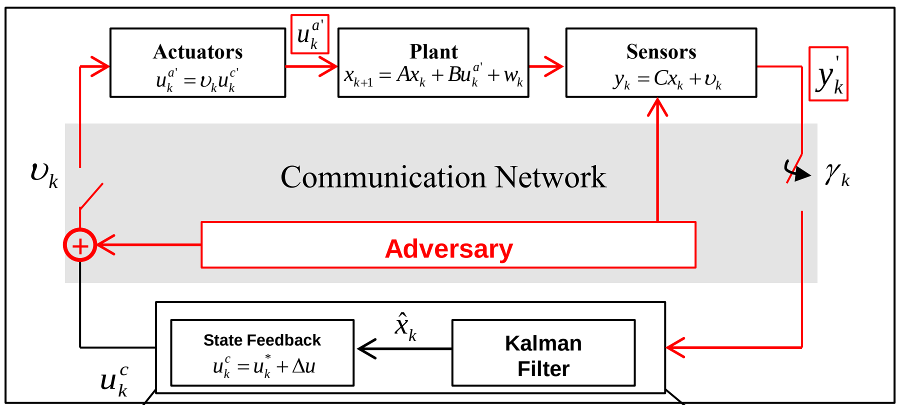
DCS (Distributed Control Systems)


ICS (Industrial Control Systems)

Cyber-Physical Systems



Source: Hacking Chemical Plants for Competition and Extortion, by Krotofil and Larsen, DefCon23, 2015.



The Detector value : $g_t = \sum_{i=t-w+1}^{t} (y_i - C\hat{x}_{i|i-1})^T P^{-1} (y_i - C\hat{x}_{i|i-1})$

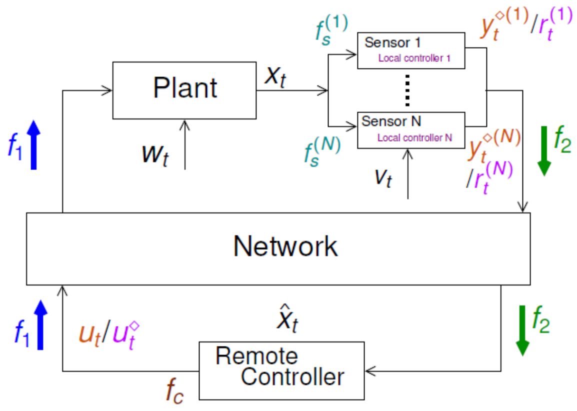
The residue : $r_t = y_t - C\hat{x}_{t|t-1}$

The watermark : $\Delta u \in R^{\rho}$

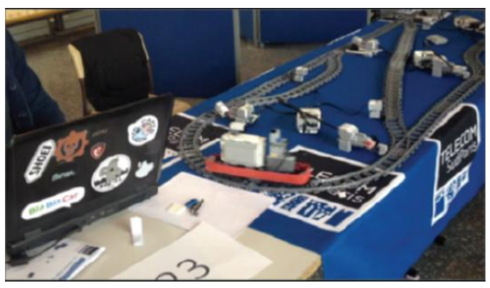
Source: Mo & Sinopoli. Secure Control against Replay Attacks. 2009.

2. Security Analysis

- **Cyber vs. Cyber-Physical Adversaries**
  - Non-parametric vs. parametric Cyber-Physical Adversaries
- **Detection strategies**
  - Single-watermark detector: $\Delta u_t \in R^{\rho}$
  - Multi-watermark detector: $\Delta u_t^{(i)} \in R^{\rho} \quad i \in I = \{0,1,\ldots,N-1\}$
  - Distributed detector:



	Watermark Detectors	Distributed Detector
Detector Ratio	12.00%	75.25%
Detection Time	6.08s	6.20s
False Negatives	88.60%	38.66%
False Positives	1.35%	5.23%



Cyber-Physical System Testbeds at Telecom SudParis (cf. **http://j.mp/TSPScada**)

3. Simulation & Testbed

Strategy	Features	Scope	Impact
Single-watermark detector	▪ Centralized ▪ Stationary watermark	Replay attacks	Performance
Multi-watermark detector	▪ Centralized ▪ Non Stationary watermark	Replay attacks & Non-parametric cyber-physical attacks	Performance
Distributed detector	▪ Decentralized ▪ Non Stationary watermark	Integrity attacks	Performance & Detection time

Contact: jose.rubio_hernan@telecom-sudparis.eu & jgalfaro@ieee.org

User centred privacy and security in the cloud

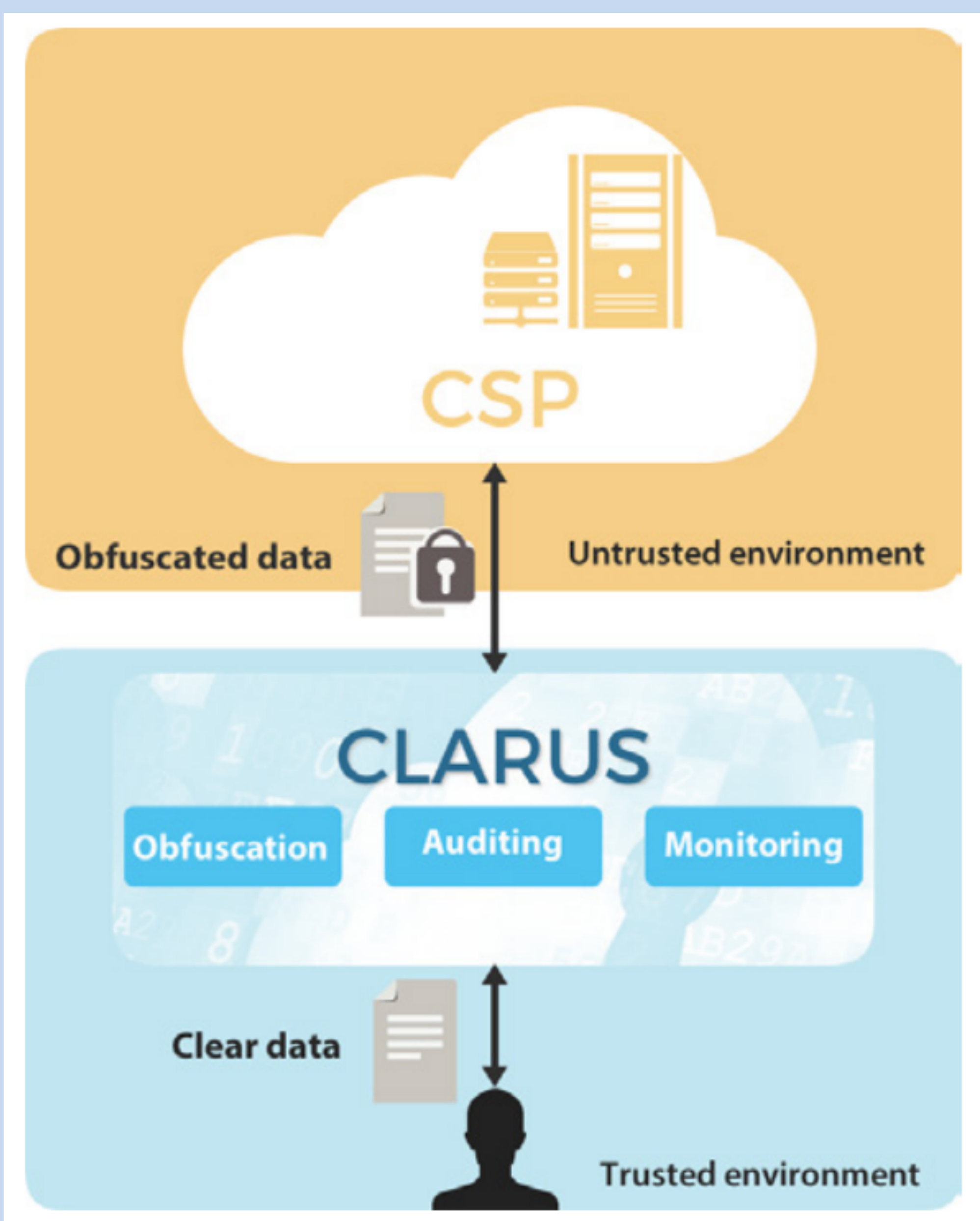
CLARUS has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 644024

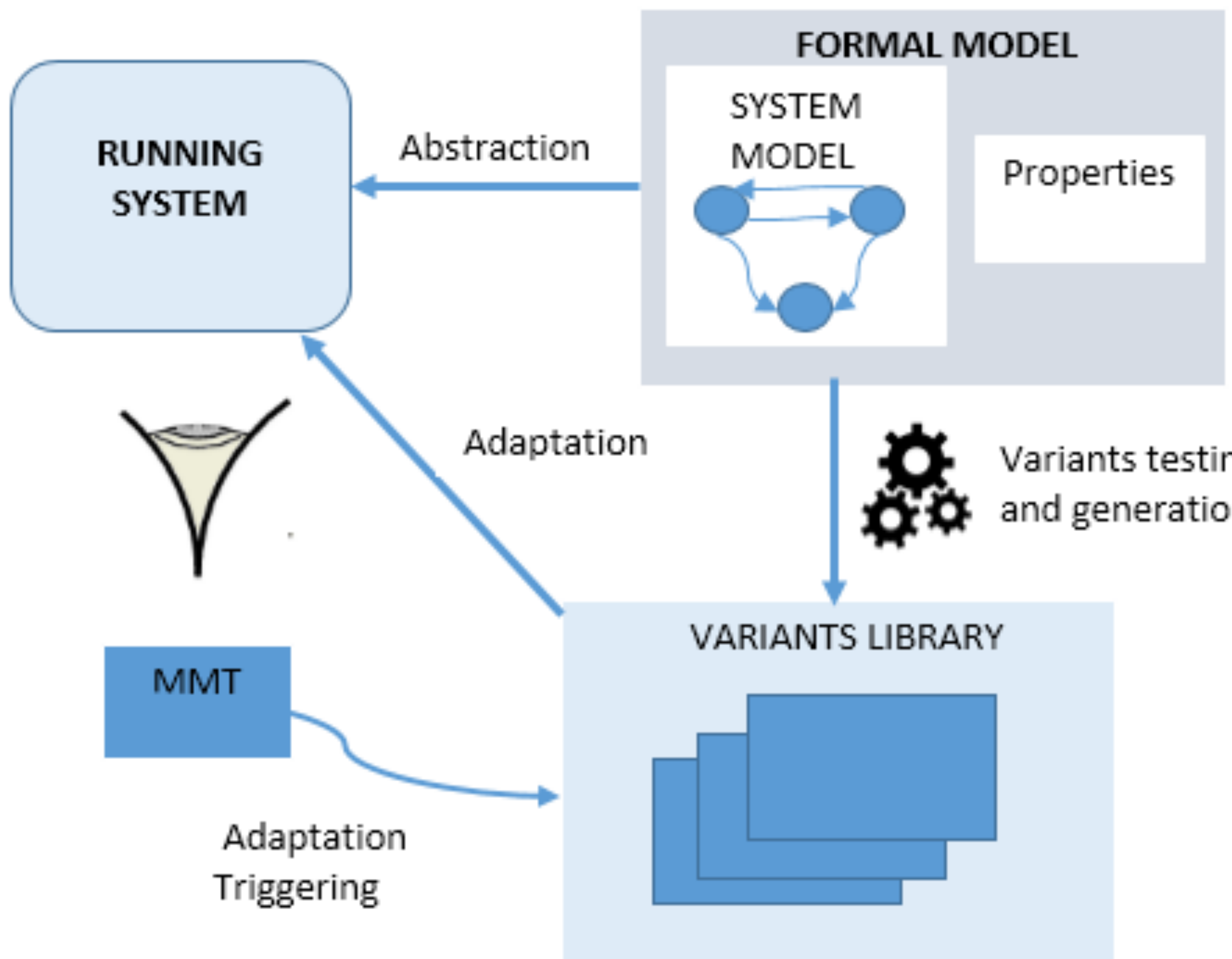
Attack Tolerant Cloud

The cloud has become an established and widespread paradigm. This success is due to the gain of flexibility and savings provided by this technology. However, the main obstacle to full cloud adoption is security. The cloud, as many other systems taking advantage of the Internet, is also facing threats that compromise data confidentiality and availability. The main innovation of this thesis is the design and the implementation of a framework for cloud systems, tolerant to attacks, which can continue to deliver its services even when after a successful attack, and can be able to recover quickly, in the context of the H2020 CLARUS project.

CLARUS focuses on providing solutions to the usual security and privacy threats that affect cloud computing and hinder a franker migration by end users. The CLARUS solution is envisioned as a proxy located in a domain trusted by the end user (e.g., a server in his/her company's intranet, a plug-in in the user's device) that implements security and privacy-enabling features towards the cloud service provider.
To do so, CLARUS relies and innovates on the current state of the art on:

- functionality-preserving cryptography,
- data anonymization,
- and splitting techniques ,
- Attack tolerance.





Proposed framework

Definition

A distributed system is attack tolerant if there is a possibility in which that system can continue to function properly with minimal degradation of performance, even if the presence of a malicious attacker is detected.

Approach

We investigate attack tolerance at the design and specification phase. We create a formal model of the system, derive one or some other models from the first one. We verify that the new models satisfy the global security properties of the system and finally generate source code according to the chosen model that face to the potential new attacks. When an attack is detected, we replace the running implementation by a secure one.

Instanciation

The framework has been instantiated as follows:

- A Model-based approach in which we derive several variants models of the core model and tested that approach with a web application [1]. Brute-force attack was carried out.
- A Diversity-based approach in which we directly generate variants of the core model to reduce the of the first method. The use-case was a Web service [2] and [3] because Cloud applications are usually Web services. DDoS attack was performed.

Results

The experiments revealed that:

- Attack tolerance is effective with the two approaches,
- The replacement of the components induces little performance overheads (~5 - 10 %),
- Attack tolerance is transparent to the Users.

We plan to extend the framework to micro-services in the Cloud with metaprogramming.

Georges Ouffoué, Ph. D. Student

Paris-Saclay University
LRI

Dr Fatiha zaïdi, Principal Advisor

Paris-Saclay University
LRI

Prof Ana Cavalli, Advisor

Telecom SudParis
Samovar

References

1. Georges Ouffoué, Fatiha Zaïdi, Ana R. Cavalli, Mounir Lallali : Model-Based Attack Tolerance. WAINA 2017
2. Georges Ouffoué, Fatiha Zaïdi, Ana R. Cavalli, Mounir Lallali :How Web Services Can Be Tolerant to Intruders through Diversification ? ICWS 2017
3. Georges Ouffoué, Fatiha Zaïdi, Ana R. Cavalli, Mounir Lallali : An Attack Tolerance Framework for Web Services. SCC 2017

Institut Mines-Télécom

ArOMA: An SDN-based Autonomic DDoS Mitigation Framework

Parties prenantes

TELECOM SudParis

Une école de l'IMT

S@movar UMR 5157

Auteurs

Rishikesh Sahay
Gregory Blanc
Zonghua Zhang
Hervé Debar

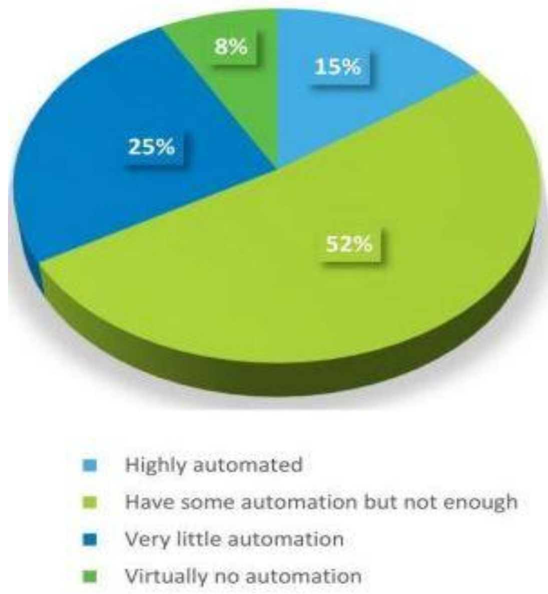
Partenaires

NECOMA

SUPER CLOUD

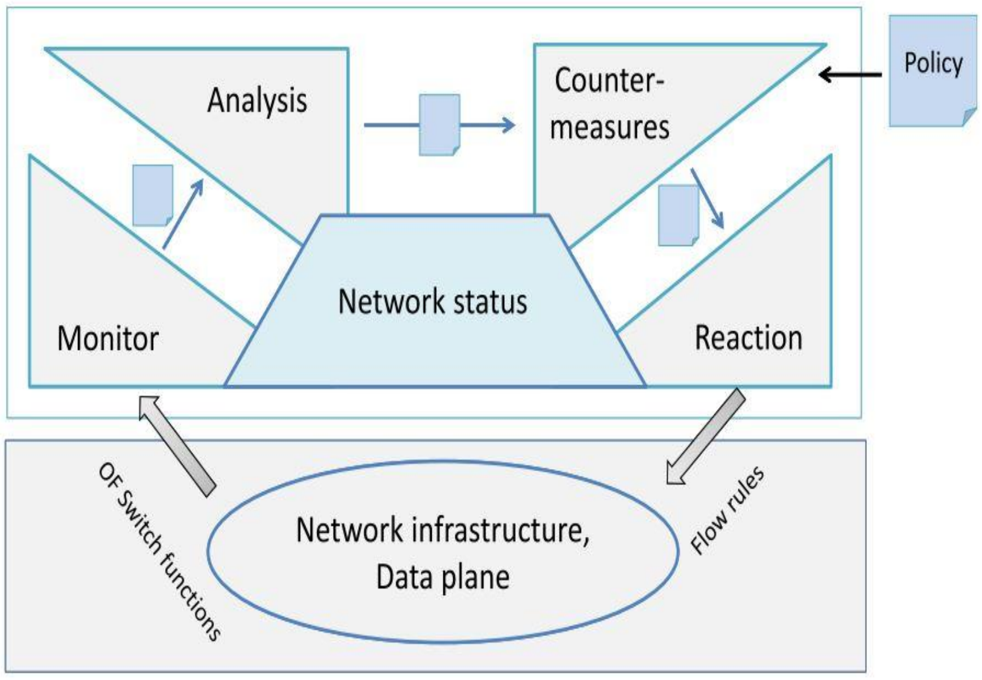
Motivation

- Defense requires manual configuration of devices

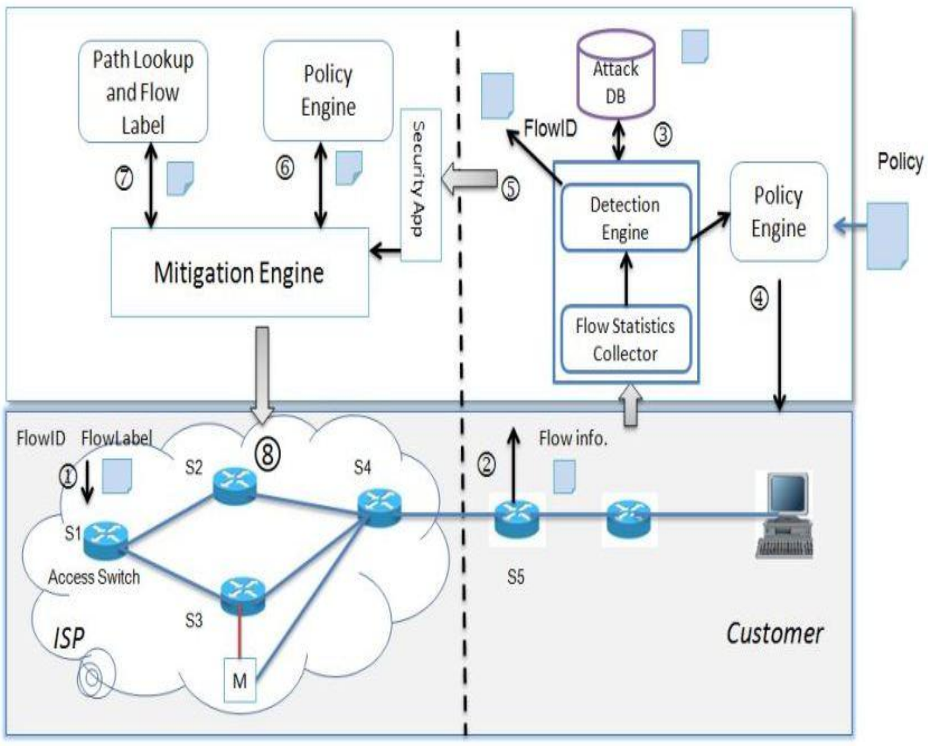


Source: The State of Automation in Security. AlgoSec, 2016.

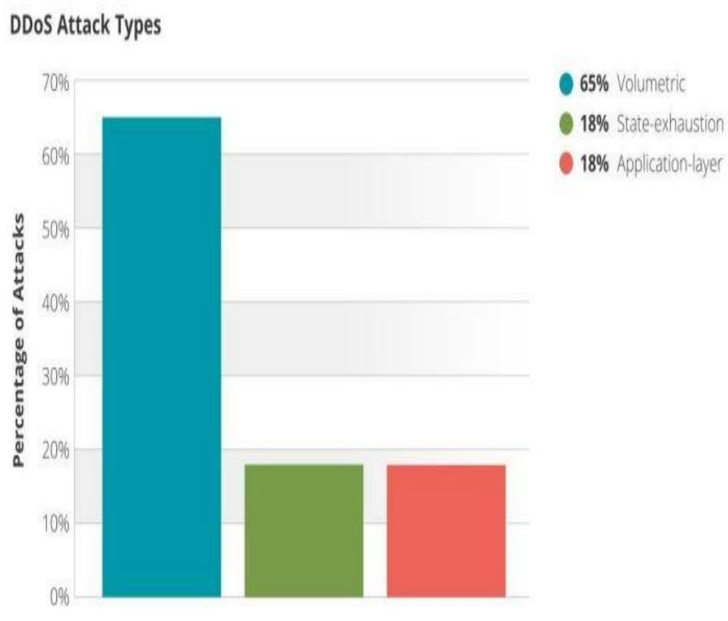
Approach



ArOMA: Autonomic Mitigation Framework

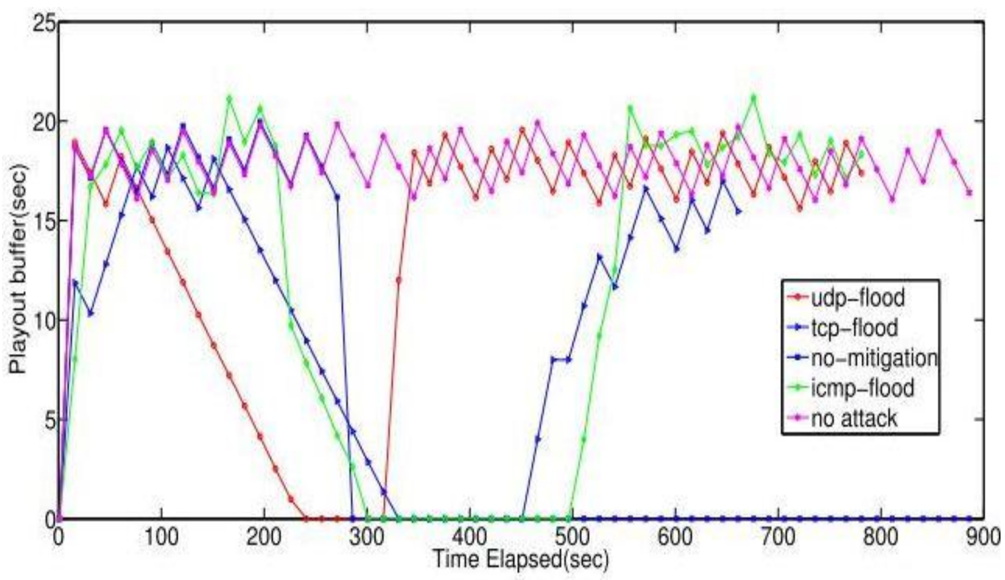


Main Attack Vector



Source: Worldwide Infrastructure Report. Arbor Networks, 2017.

Result: Time to Rebuffer



Conclusion

- The framework provides collaborative and automated attack mitigation between Internet Service Provider (ISP) and its customer
- Main DDoS attack vectors are analyzed
- Experimentation has been run on a physical testbed using SDN switches. The goal was to protect a video streaming provider
- During no attack playout buffer was maintained above 15 seconds
- During attack playout buffer became empty and client was not able to play the video
- When the mitigation started it took 10 to 15 seconds for the playout buffer to return to the normal level

Contact : rishikesh.sahay@telecom-sudparis.eu

Novembre 2015 Colloque de l'Institut Mines Télécom Paris