4. SECURITE, SURETE ET RISQUES

POSEIDON (2012-2015) integrated security policies for outsourced data

Parties prenantes

Auteurs

Caroline Fontaine (Lab-STICC, CNRS + Télécom Bretagne)

Frédéric Cuppens (Lab-STICC, Télécom Bretagne)

Nora Cuppens-Boulahia (Lab-STICC)

Gouenou Coatrieux (LaTIM, Télécom Bretagne)

David Gross-Amblard (IRISA, Univ. Rennes 1)

Sébastien Gambs (IRISA,Univ. Rennes 1-INRIA)

Nicolas Prigent (IRISA, Supélec)

Partenaires

Context

Outsourced data / Cloud:

- **Various contexts**: outsourced storage and omputation, multimedia content distribution (e.g., Video on Demand), personal data management.
- **Various protagonists**: industry, administration, citizens, social networks .

All of end users are concerned with the same security issues: confidentiality, integrity, authentication, copyright protection, privacy and anonymity. These issues are traditionnally addressed with the help of security and cryptographic mechanisms, e.g. encryption, signature, watermarking, etc.

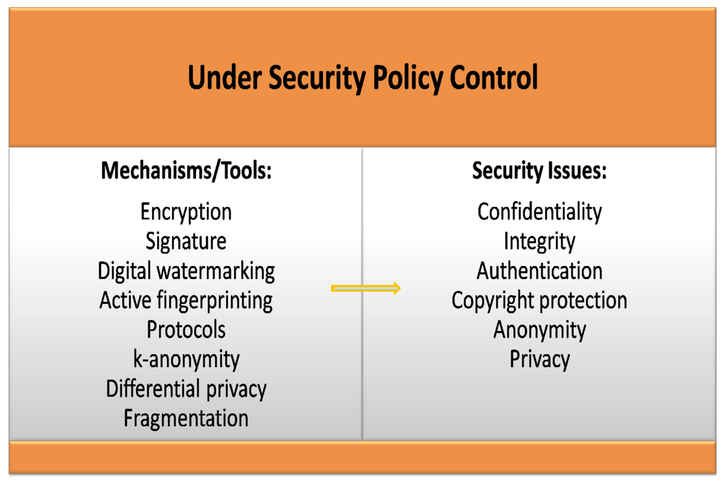
A security policy formalizes the security expectation with respect to the system. It specifies the involved entities, the data and services to protect, the threats. It conditions the actions choices and deployments of the security mechanisms.

While these mechanisms are known to be efficient when used independently, they often have to be combined.

Hence, to ensure a good security level of outsourced data, we need:

1. A **formal expression of the Security Policy**.
2. **Adapted security mechanisms** and a formal expression of the security properties each of them may guarantee.
3. An extension of this formalism to properly state the consequences of the **combination of several such mechanisms**. This is essential to enable an **automated deployment** of the policy: automated selection of the mechanisms depending on the context and related security priorities, automated analysis of possible incompatibilities.

Of course all these formalisms must be compliant with each other.



First Results

- The first track concerns the **study and improvement of security mecanisms** related to data or request privacy in the Cloud. In particular, we focused on the following ones:

  Fully Homomorphic Encryption schemes.

  Anonymous delivery protocol for multimedia content, which enables both privacy and traceability of malicious users.

- The second track focused on the design of a support tool allowing, **for a given security policy, selection of the best mechanism or combination of mechanisms** to enforce this security policy.

- The third track concerns the **adaptation of security solutions to the particular contexts of Cloud and peer-to-peer networks**

Selected publications (more on www.poseidon.cominlabs.ueb.eu)

Recent advances in homomorphic encryption: a possible future for signal processing in the encrypted domain, C. Aguilar-Melchor, S. Fau, C. Fontaine, G. Gogniat, R. Sirdey. IEEE Signal Processing Magazine, Number 2, Volume 30, pp. 108-117 (2013).

Preserving Multi-relational Outsourced databases Confidentiality using Fragmentation and Encryption, Bkakria, A., Cuppens, F., Cuppens-Boulahia, N., Fernandez, J.M., Gross-Amblard, D. Journal of Wireless Mobile Networks, UbiquitousComputing, and Dependable Applications (JoWUA) (2013).

Robust Lossless Watermarking of Relational Databases Based on Circular Histogram Modulation, J. Franco-Contreras, G. Coatrieux, F. Cuppens, N. Cuppens-Boulahia, C. Roux, IEEE Transactions on Information Forensics and Security 9(3): 397-410 (2014)

Contact caroline.fontaine@telecom-bretagne.eu

Site web www.poseidon.cominlabs.ueb.eu

A Joint Watermarking/Encryption Algorithm for Verifying Medical Image Reliability in Both Encrypted and Spatial Domains

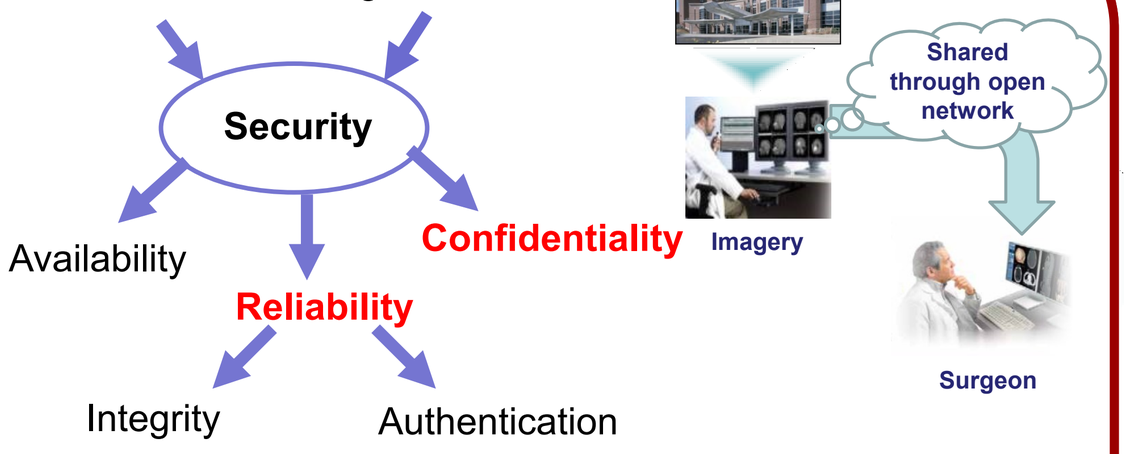
Partners

Authors

Dalel BOUSLIMI
Gouenou COATRIEUX
Michel COZIC
Christian ROUX

MEDICAL DATA PROTECTION

Rules of ethics Legislatives rules



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

Encryption (“a priori” protection) Watermarking (“a posteriori” protection)

Combination

Joint Watermarking/Encryption Algorithm

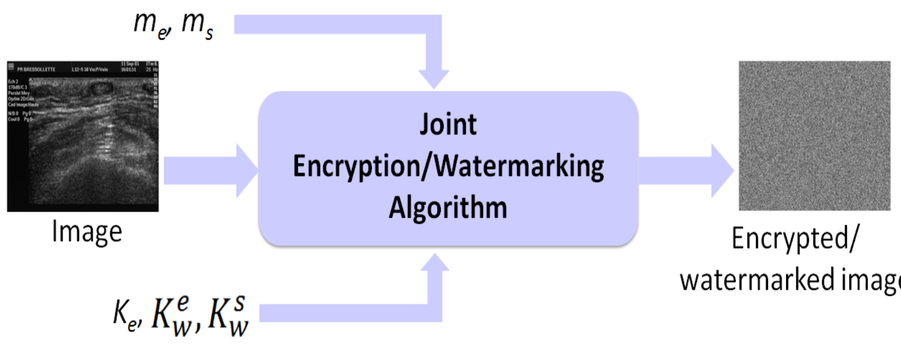
Constraint: interoperability with/transparent to the DICOM standard

⇨ *Use of the AES block cipher in CBC mode.*

SYSTEM ARCHITECTURE

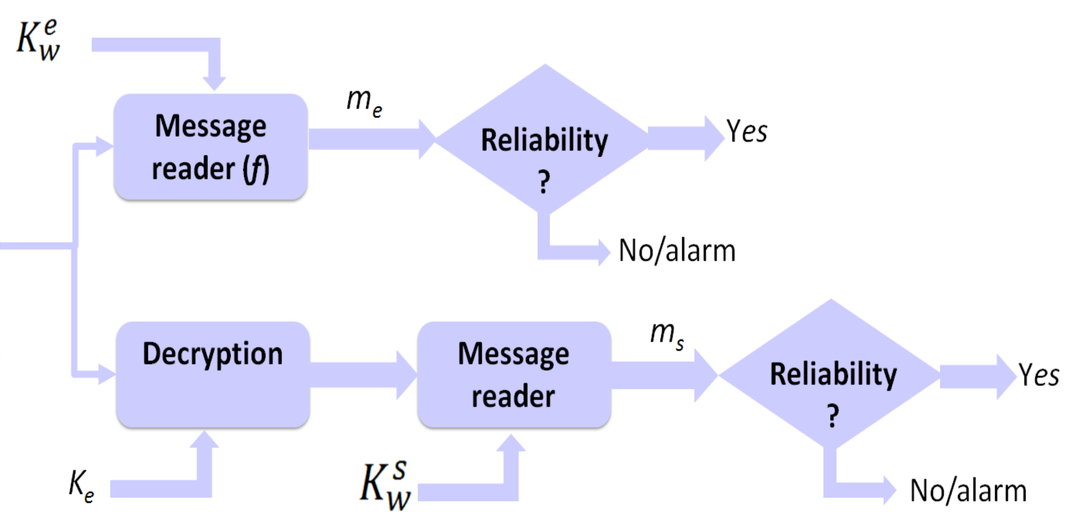
Protection

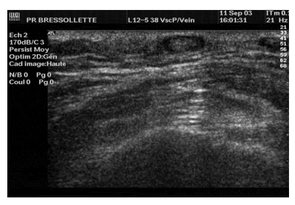
• m_s and m_e : messages available in the spatial and the encrypted domains, respectively.



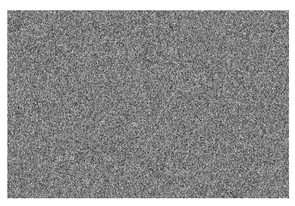
K_w^e, K_w^s : watermarking keys, K_e: encryption key

Verification

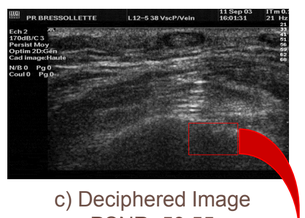




a) Original Image, Entropy=6,76 bits/pixel



b) Joint Watermarked/ ciphered Image



c) Deciphered Image PSNR=53,55

d) Zoom in image difference between (a) and (c)- gray levels values mapped in the range 0-255.

JOINT WATERMARKING/ENCRYPTION

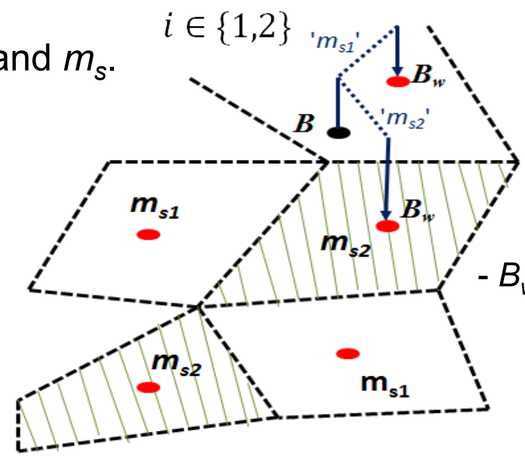
- Modification of the quantization index modulation (QIM):
Disrupt/modulate the image pixels to encode simultaneously m_e and m_s.

-**QIM** : insertion based on codebooks C_{ms_i}, which represents the message m_{si}.

- **QIM/chiffrement** Constitution of sub-codebooks $C_{ms_i me_j}$ according to the AES.

$$C_{m_{si}} = \bigcup_{j=1}^{q} C_{m_{si}m_{ej}} \text{ et } C_{m_{si}m_{ej}} \cap C_{m_{si}m_{ek}} = \emptyset, j \neq k$$

$$C_{ms_i me_j} = \{Y \in C_{ms_i} / \ f(AES(Y, K_e), K_w) = me_j\}$$



$$C_{m_{si}} = \bigcup \emptyset_{m_{si}},$$
$$C_{m_{si}} \cap C_{m_{sj}} = \emptyset, i \neq j$$
$$B_w = \{B_w \in C_{m_{si}} / \|B - B_w\| = \min(\|B - Y\|), Y \in C_{m_{si}}\}$$

- B_w : the watermarked vector B.

EXPERIMENTAL RESULTS

- **Performance Indicators**
  - Image distortion measure: PSNR (dB).
  - Capacity rate (bpp: Bit Per Pixel).
- **100 ultrasound images- 576 × 688 pixels, 8-bit depth.**
  - Capacity rate: 1/16 bpp in each domain.
  - PSNR: greater than 60dB.

CONCLUSION

-The proposed joint encryption/watermarking algorithm guarantees *a priori* as well as *a posteriori* protection.
-The use of the AES in CBC mode makes our method transparent and compliant with the DICOM Standard

- Message insertion introduces very low image distortion.
- **Future works** will focus on making our scheme more robust to attacks like lossy image compression (ex. JPEG),

Contact Gouenou.Coatrieux@telecom-bretagne.eu Site web http://latim.univ-brest.fr/

Lossless Watermarking based on Circular Interpretation of Bijective Transformations for the Protection of Medical Databases

Objectives/Solution/Results: Verify the reliability (authenticity, integrity) of **medical relational databases** / A fragile/robust lossless watermarking algorithm based on a circular interpretation of bijective transformations embedding a message within **numerical data** of a relational database / Our method preserves the value of the database while allowing the embedding of a digital signature or an authentication code for verifying the database integrity and origins (even if the database is modified – traitor tracing).

Parties prenantes

TELECOM Bretagne

Auteurs

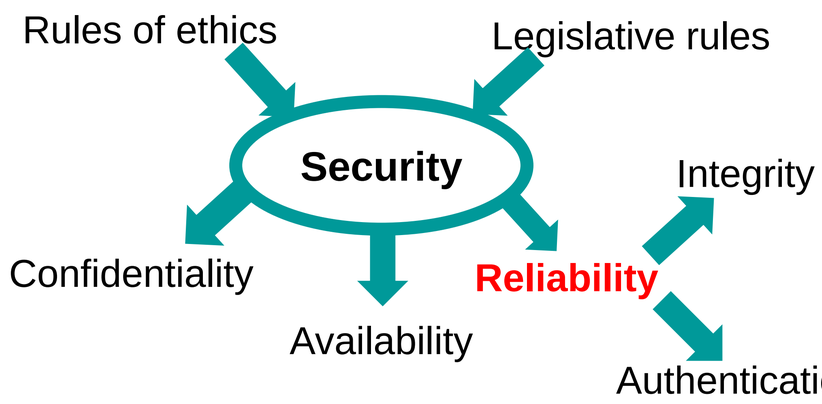
J. Franco-Contreras
G. Coatrieux
N. Cuppens-Boulahia
F. Cuppens
C. Roux

Partenaires

Région Bretagne

1. MEDICAL DATA PROTECTION

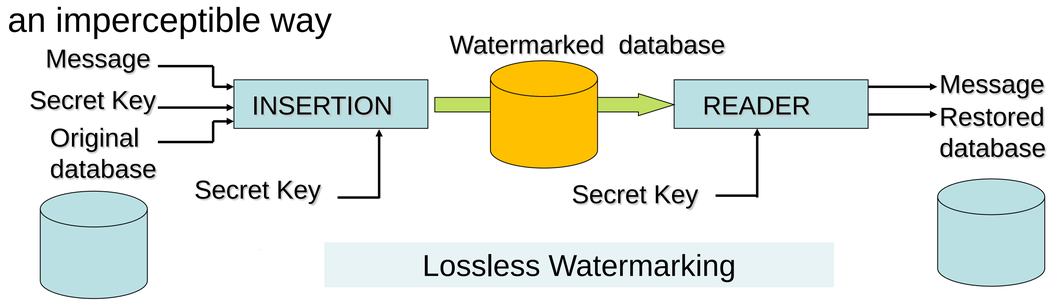
Security Objectives



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

Watermarking

Allows the embedding of a message within a content by modifying its values in an imperceptible way

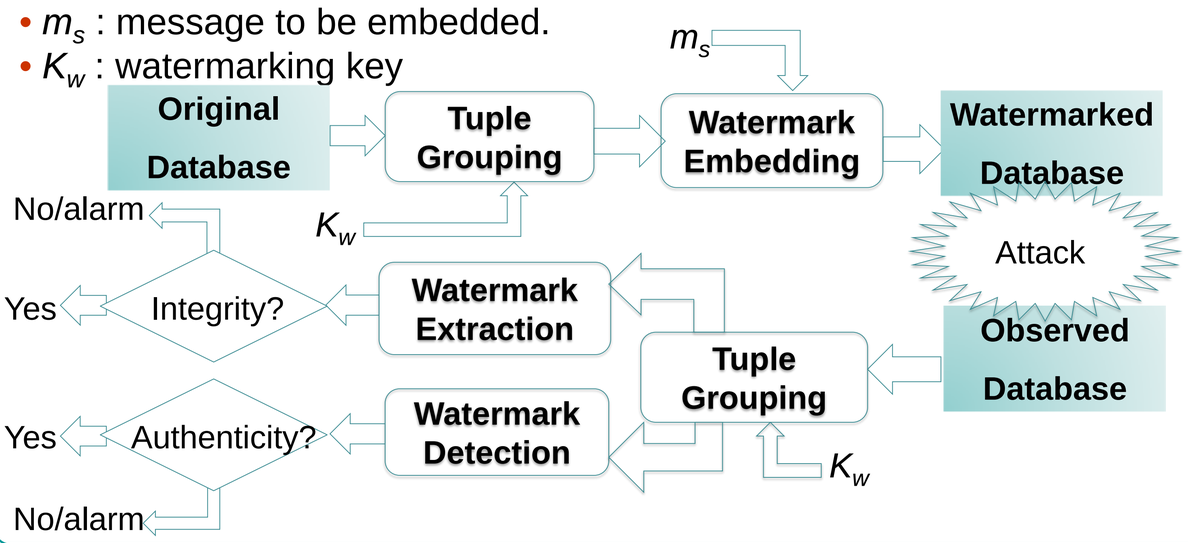


Constraint: Do not perturb the normal interpretation of data

Lossless or reversible property allows watermark removal and exact data restoration.

2. A COMMON DATABASE WATERMARKING CHAIN

- m_s : message to be embedded.
- K_w : watermarking key



Tuple Grouping → Make embedding independent from database storage

- Reorganization of tuples $\{t_u\}_{u=1...Mu}$ in N_g groups depending on their primary key ($t_u.PK$) and a secret watermarking key K_w.
- Each tuple is assigned to the group

$$n_u = H(K_w \mid H(K_w \mid t_u.PK)) \bmod N_g.$$

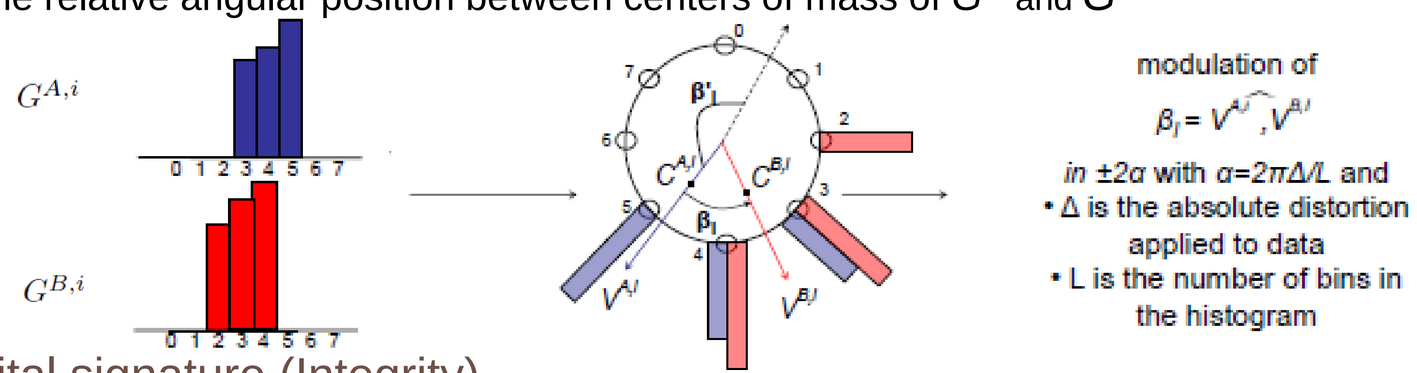
  - H : Cryptographic HASH operation
  - $\mid$: concatenation operation

- One bit is ideally embedded in each group.

3. PROPOSED METHOD

Modulation Principles

- One group is uniformly split into two subgroups ($G^{A,i}$, $G^{B,i}$).
- Histograms for a **numerical attribute** in each subgroup are mapped into a circle
- Modification of the relative angular position between centers of mass of $G^{A,i}$ and $G^{B,i}$



Fragile Embedding → Insertion of a digital signature (Integrity)

$$\beta_i^w = \begin{cases} \beta_i + 2\alpha \text{ if } b=0 \longrightarrow +\Delta \text{ to the values in } G^{A,i} \text{ and } -\Delta \text{ to the values in } G^{B,i} \\ \beta_i - 2\alpha \text{ if } b=1 \longrightarrow -\Delta \text{ to the values in } G^{A,i} \text{ and } +\Delta \text{ to the values in } G^{B,i} \end{cases}$$

- Digital Signature is extracted from the observed database and compared to the one computed from the data.

Robust Embedding → Insertion of an Authentication Pattern (Reliability)

- Same modulation principle but with the insertion of a secret pattern.
- Detection based on correlation (origin) and/or extraction of the pattern (integrity).

*** Special case (Non carriers)**

Groups where $|\beta_i| > 2\alpha$ (as in β'_i) cannot carry information (**non-carriers**) and

$$\beta_i^w = \begin{cases} \beta_i + 2\alpha \text{ if } \beta_i > 0 \\ \beta_i - 2\alpha \text{ if } \beta_i < 0 \end{cases}$$

4. EXPERIMENTAL RESULTS

❖ Experimental Database

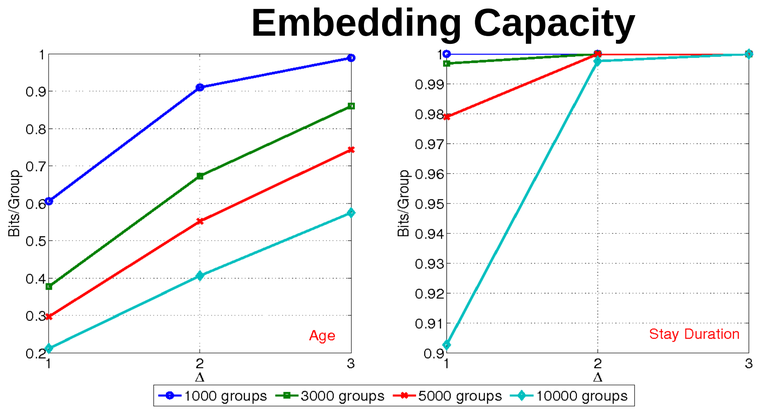
Real medical database related to inpatient stays at the hospital with 1048575 tuples

Id_hospital	Id_patient	age	Stay duration
601433878	7892	29	13
601484325	28653	40	31
601527723	14552	65	4

❖ Fragile Scheme → How much can be embedded

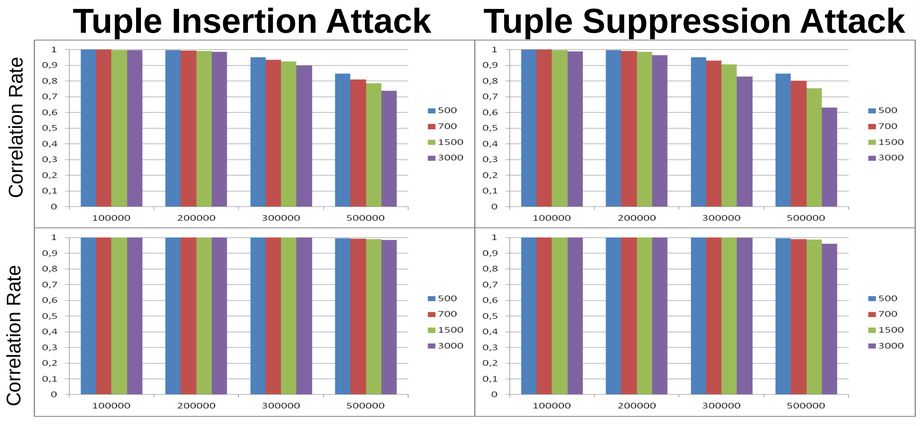
- Three values of Δ=[1,2,3] considered

Embedding Capacity



❖ Robust Scheme

- Att. Age with Δ=3; Att. Stay Duration with Δ=1

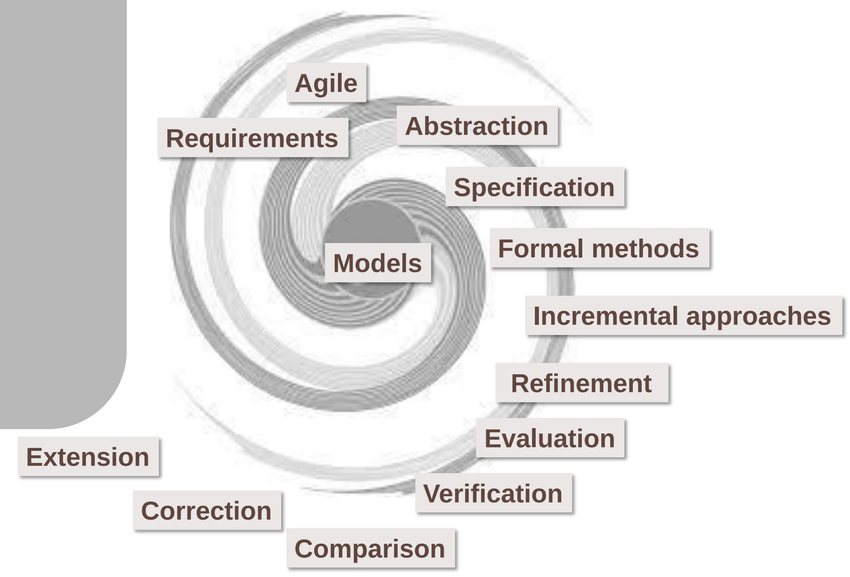


In both cases, results depend on the statistical properties of the attributes, more specifically in their standard deviations.

Contact gouenou.coatrieux@telecom-bretagne.eu
Site web http://latim.univ-brest.fr/

Mars 2014

Incremental development and behavioural verification of reactive systems



Problem

How to assist model development of critical reactive systems?

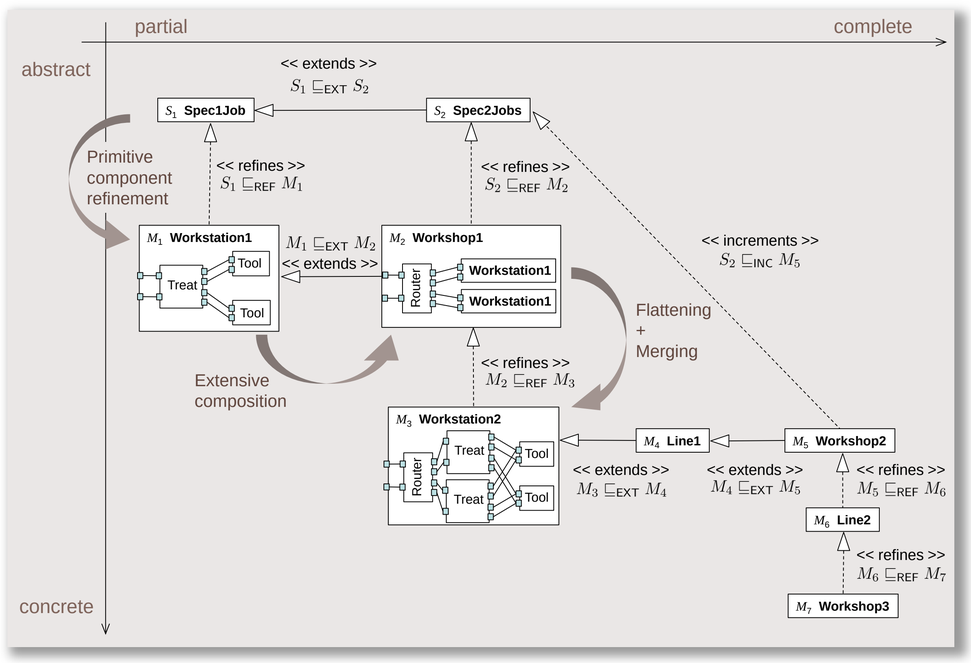
Model engineering is not mature.

- “Engineers don’t know why their system works. [...] They can not be sure a critical system is free of critical errors.” J. Sifakis
- “Today for most software systems, the analogy of building something like a cathedral is no longer a good choice. [...] Requirements change all the time, we need a short time-to-market, we need feed back all the time...” M. Lippert
- “If you want to get it right, be ready to start over at least once.” E.S. Raymond

Need to develop and **verify several** model versions:
from abstract and partial ones,
to detailed and completed ones.

IDF – Incremental Development Framework

Combining model refinements and extensions



Two sets of techniques … to support:

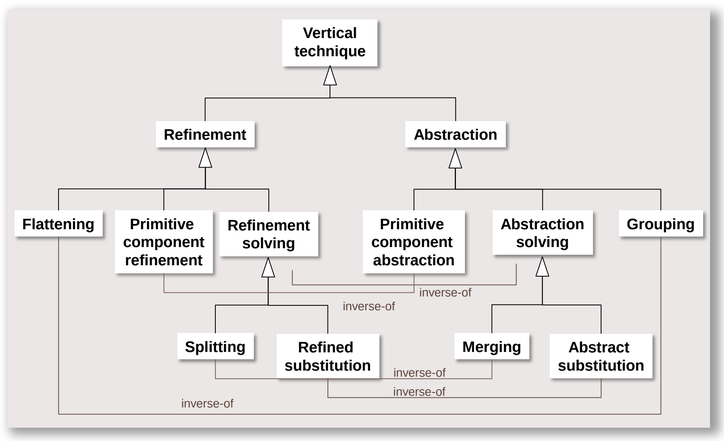
- Construction techniques
- Evaluation techniques

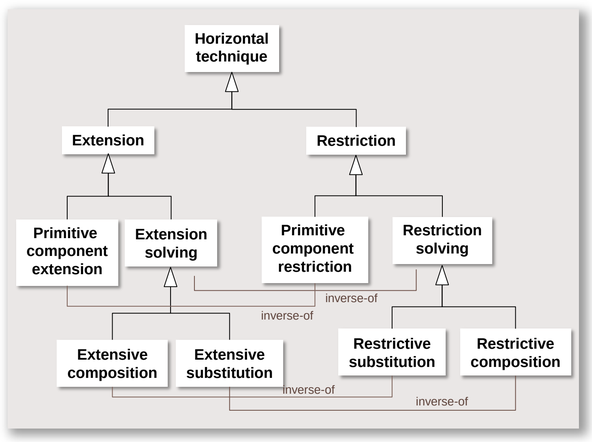
⇒ Incremental development processes

Two axis:

- abstraction level (vertically)
- completion level (horizontally)

Construction techniques





Evaluation techniques

M_2 conf M_1 M_2 is a correct implementation of M_1: M_2 preserves liveness properties of M_1.

$M_1 \sqsubseteq_{INC} M_2$ M_2 increments M_1: any implementation of M_2 is an implementation of M_1.

$M_1 \sqsubseteq_{EXT} M_2$ M_2 extends M_1: M_2 preserves liveness properties of M_1 and has more behaviours.

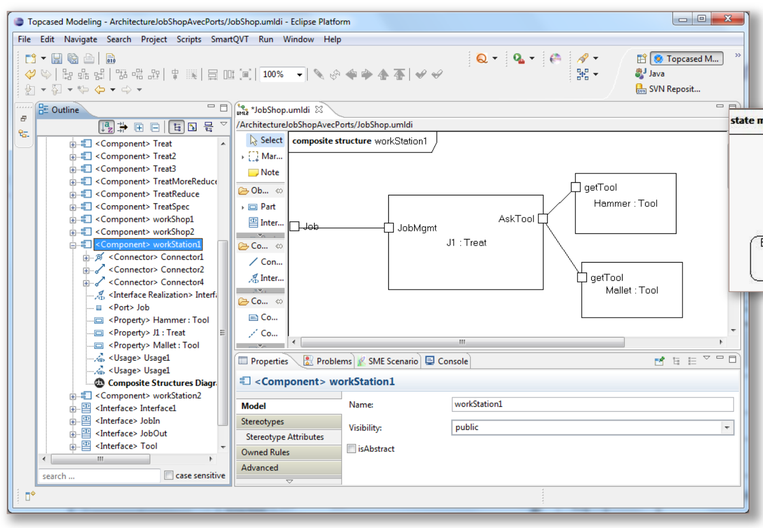
$M_1 \sqsubseteq_{REF} M_2$ M_2 refines M_1: M_2 preserves liveness and safety properties of M_1.

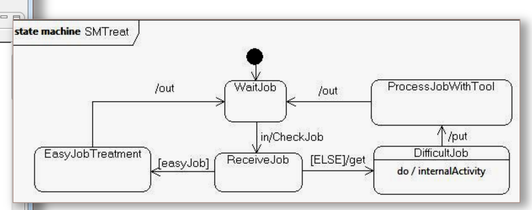
$M_1 \sqsubseteq_{SUB} M_2$ M_2 can substitute M_1: M_2 refines M_1 and can safely replace M_1.

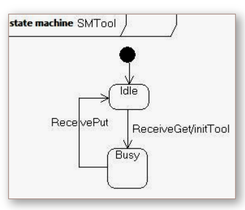
IDCM – Incremental Development of Compliant Models

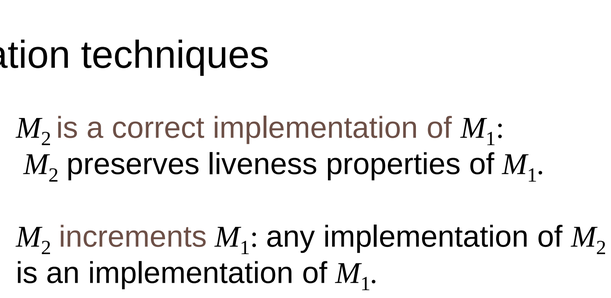
A tool to support IDF

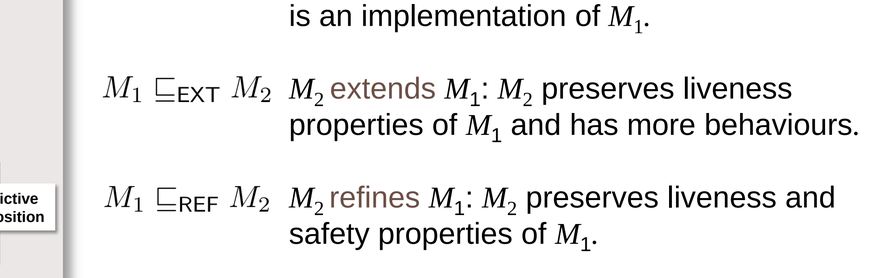
- Transformation of UML models into LTS (Labelled Transition Systems):
  - UML primary components (state machines) and
  - architectures (composite structures).
- Use of CADP (Construction and Analysis of Distributed Processes) features for LTS composition and minimisation
- Implementation of conformance, increment, extension, refinement and substitution relations
- Analysis of models pointing out traces of failure and denied actions whenever relations are not satisfied











Authors

Anne-Lise Courbis
Thomas Lambolais
Hong-Viet Luong
Thanh-Liem Phan

Partners

Christian Percebois

Thérèse Libourel

Contact thomas.lambolais@mines-ales.fr

Web site http://lgi2p.mines-ales.fr

Methodology of system interdependency analysis after a major disruption

Parties prenantes

Auteurs

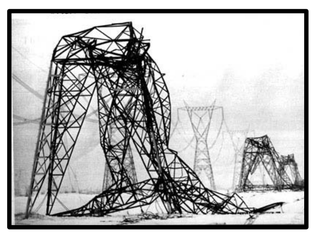
REY Benjamin (EMA)
TIXIER Jérôme (EMA)
DANDRIEUX Aurélia (EMA)
DUSSERRE Gilles (EMA)
LAPEBIE Emmanuel (CEA)

Context

■ Beyond the dramatic deaths, injured people, evacuated families due to the Japan earthquake and tsunami in 2011, another consequence was the destruction of 30% of the electricity production plants. Because of physic interdependencies, many essential activities have been affected by this production disruption (for instances chemical and petrochemical industries) and indirectly the whole country and its population.
Attacks on the World Trade Center in New York in 2001, ice storm in Canada in 1998 are other examples of cascading failures.
It enhances the need for research on the functional and spatial interdependencies in a system (territory, industrial site, organization,…). Project problematic can be formulated in order to answer to this question :

How to assess a major disruption impact in a system (organization, territory,…) composed of several interdependent elements ?

Fukushima Daiichi nuclear plant, 2011, Japan
(origin : SIPA/Ap)



Ice Storm 1998, Canada
(origin : radio-canada website)

Conceptual tools to analyze system interdependencies

What are risk management methodology characteristics about independencies between elements of a system ?

Empirical approach

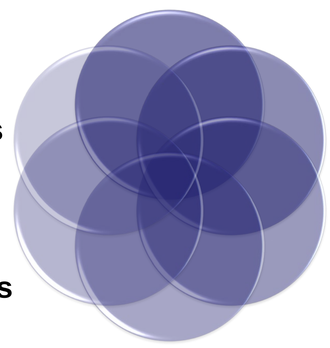
Databases,…
(Pederson and *al*, 2006)
(Yusta et *al.*, 2010)

Physic, geographic, cybernetic, logic
(Rinaldi et *al*., 2001)

Natural hazard, industrial accident, threat

Modeling interdependencies and cascading effects tools

4 Types of Interdependencies



Major disruptions

Predictive approach

Multi-agent system, dynamic system, network theory, petri network, input-output model ,…
(Pederson et *al*, 2006) (Yusta et *al.*, 2010)

Activity sectors Energy, health, food, water, transport, defense, government, telecommunication,…
(SGDN, 2008)

4 Scale levels International, national, regional, local

Physical security, security management,…
(Petit et *al.*, 2011)

Protection

Protection and resiliency measures

Resiliency

Redundancy, stocks, new resources,…
(Petit et *al.*, 2012)

Methodology

Approach

System representation

- Create system typologies of : processes, functions, physic elements, services and constraints

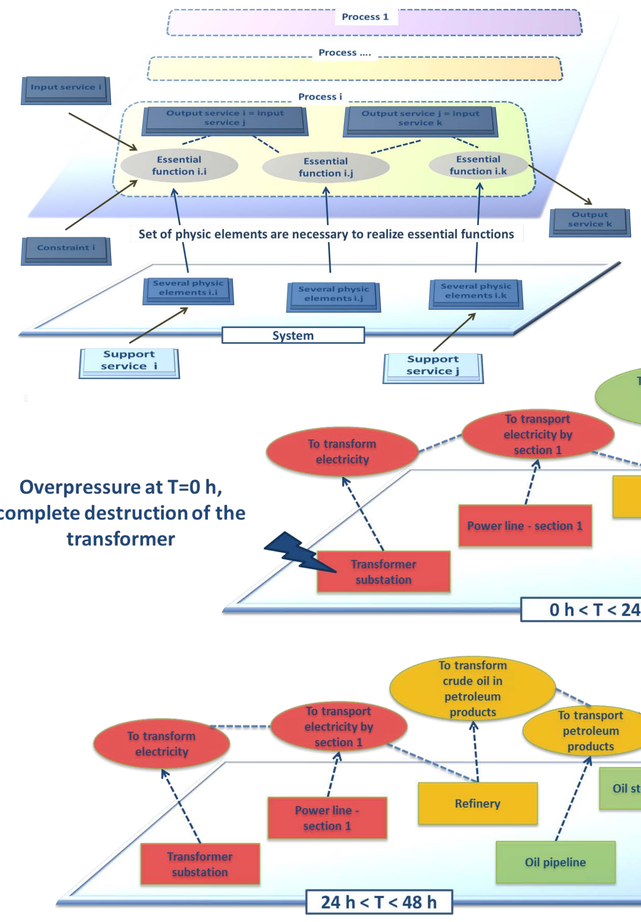
Scenarios building

- Create disruption typology
- Identify fault physic elements and failure functions with their characteristics (maximum capacity, dynamic propagation of a disruption…)

System vulnerability assessment

- Scenario simulation and results :
  1/ service disruption assessment by means of different indexes to define : the number of affected end users, the injured people, …
  2/ to highlight vulnerable elements of the system and define major scenarios

Results



Papers

■ REY B., TIXIER J., BONY-DANDRIEUX A., DUSSERRE G., MUNIER L., LAPEBIE E., (2013), Interdependencies between industrial infrastructures: Territorial vulnerability assessment, Chemical Engineering transactions, vol. 31, 2013

■ M PETIT F., ROBERT B., REY B., 2010, Protection des infrastructures critiques, Les Techniques de l'Ingénieur, Paris: Édition T.I. p.146-152.

Contact benjamin.rey@mines-ales.fr Site web www.mines-ales.fr/

Numérique : Grande échelle et complexité

March 2014

Crisis management training and debriefing

« Improvement of the organizational training and the psychosocial approaches' contribution»

Parties prenantes

MINES Alès

Auteurs

LAPIERRE Dimitri (EMA)
WEISS Karine (Unîmes)
DUSSERRE Gilles (EMA)
BONY-DANDRIEUX Aurélia (EMA)
TENA-CHOLLET Florian (EMA)
TIXIER Jérôme (EMA)

Partenaires

FONDATION TELECOM

INSTITUT CARNOT Télécom & Société numérique

Context

- Feedbacks from the nuclear power plant accident in Fukushima (Japan, 2011) and the explosion of the chemical plant AZF in Toulouse (France, 2001) underline that strategic decision-making is taken in a complex and dynamic environment, characterized by emergency. Improving crisis management of disasters, requires more effective training sessions (i.e. by using simulation game) and methodologies allowing evaluation and debriefing.

Collective failures :

- **Cognitive:** misrepresentation of the situation, *sensemaking* collapse, loss of structuring frame
- **Behavioral:** feelings, lack of understanding, block for acting, non-critical group think, disorientation
- **Organizational:** wrong execution of decisions, coordination collapse, wrong tasks' repartition, leadership deletion, lack of communication, blind support of the procedures

Crisis management's limits

Emergency

- *Collective failures*
- *Maladaptive training for actors*
- *Inexperienced decision makers*

Doubt

Training objectives
- **Facilitate the implementation of learning in real situations**
- **Promote expertise and improve teamwork skills**

Stress

Crisis management improvement

- *Development of non technical skills*
- *Decision-making improvement*
- *Higher organizational reliability*

Ambiguity

Dynamic nature of the event

Time pressure

Resilience capacity

Lack of immersion	Non immersive situation, low feeling of stress, low mediatic pressure, difficulties in mobilizing all actors
Procedural decision-making	Low awareness of the decision-making's models, rigidity of procedural decisions, poor preparation to cope with elements of surprise
Wrong consideration of needs	Few upstream studies for identifying the real needs of participants, similarities between exercises
Psychosocial factors	Low consideration of human and organizational factors, no-promotion of the collective representation of the situation
Debriefing	No clear structuration of debriefing, no match between debriefing animation and trainees' performance and reactions (orchestration level of debriefing)

Methodological elements to improve crisis management training

1. Improve training scenarios

Diversity of crisis situations

CTT
EBAT
Check list
Level adjustment
TADMUS approach
Educational training
Needs adjustments via upstream survey

2. Activate learning levers

Experiential learning

Strength of thinking quickly
Educational leader
CRM Training's tools
Decision making model
Shared Mental Models

Trainings
- EBAT : Event-Based-Approach Training
- CTT : Critical Thinking Training
- CRM : Crew Resource Manager

+ Simulation exercise

Technical skills

Non technical skills

Improvement decision making

3. Assess a group in real time

Skills mobilized

Observation grid
Questionnaire
Check list
Case test

EXTRACT

Phases	Assessment tools
During the exercise	**Check-lists** ▪ Grid of observations adapted from NOTECHS (Non Technical Skills) (objective achievement with the behavior/attitude for each skill) ▪ Grids for group behavior compared to the scenario's' events ▪ Grid of actions to carry out (technical assessment) **Assessment model of the group performance** ▪ Adapted from CRM
After the exercise	**Feedback form** ▪ Self-assessment ▪ Identification of encountered difficulties

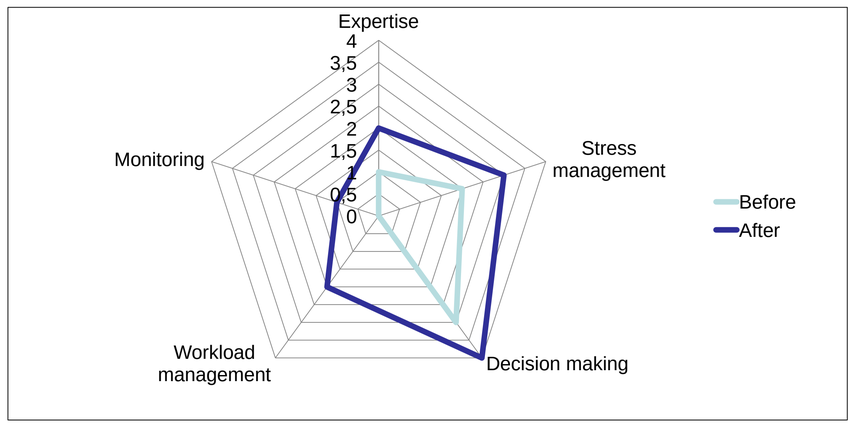
4. Organize the debriefing

Continue learning

Judgment method
Sort of debriefing
Steps'structuring
Orchestration
Feedback

Perspectives

- Index of trainee's ability to cope with crisis situation based on preliminary questionnaire highlighting needs and skills before the training session
- Indexes of monitoring of trainees during the training session to collect real time data (non technical and technical skills, group dynamic, behavior) in order to promote the animation ability
- Assessment tool dedicated to the improvement of debriefing



Collective radar « before / after » training session

Le projet GEPET-Eau

Gestion Efficiente Prédictive ET adaptative de la ressource en Eau des voies navigables dans un contexte de changement climatique

Contexte : Plan National d'Adaptation au Changement Climatique

Constats

- Diminution des ressources en eau
- Augmentation des températures
- Accroissement en fréquence et amplitude des extrêmes

APR 2012 GICC – Projet 2013-2015

- Méthodes d'évaluation des effets directs et indirects
- Réduction de la vulnérabilité aux variations climatiques
- Etude de la résilience aux évènements extrêmes
- Adaptation au changement climatique
- Financement CGDD, DGEC, DGITM

Objectifs

Contributions

- Déterminer les conséquences du changement climatique sur la navigation
- Prédire les conditions exceptionnelles potentielles à partir d'étude sur l'impact du changement climatique
- Disposer d'un modèle générique de la dynamique des voies navigables
- Estimer la résilience des voies navigable - bief Cuinchy-Fontinettes
- Pouvoir disposer, à terme, d'un outil d'aide à la décision

Verrous scientifiques

- Caractériser des scénarios caractéristiques du changement climatique
- Disposer d'un modèle de voies navigables
- Disposer de modèles d'actionneurs (écluses/vannes)
- Etudier la résilience des voies navigables
- Concevoir des stratégies de gestion prédictive
- Proposer une architecture de conduite

Premiers résultats

Architecture de conduite

- Gestion prédictive et adaptative
- Simulation de scénarios extrêmes
- Conception de stratégies de conduite

Modélisation des voies navigables

- « Boîte grise »
- IDZ (Integral Zero Delay)
- IR - Modèle de Résonnance
- Multi-échelle (débit & volume)

Contrôle des voies navigables

- Commande prédictive MPC

Colloque sur le Numérique
Mars 2014

GICC Le programme Gestion et Impacts du Changement Climatique

Parties prenantes

ARMINES

vnf voies navigables de France

Auteurs

K. Horvath
E. Duviella
J. Blesa
L. Rajaoarisoa
S. Lecoeuche
D. Juge-Hubert
K. Chuquet
E. Sauquet
F. Guibert
N. Gaffet

Partenaires

UPC UNIVERSITAT POLITÈCNICA DE CATALUNYA

irstea

AGENCE DE L'EAU ARTOIS PICARDIE

Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE
Direction régionale de l'Environnement, de l'Aménagement et du Logement NORD-PAS-DE-CALAIS

Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE
Ministère de l'Écologie, du Développement durable et de l'Énergie

Contact eric.duviella@mines-douai.fr

Site web http://gepeteau.wordpress.com/
ia.ur.mines-douai.fr

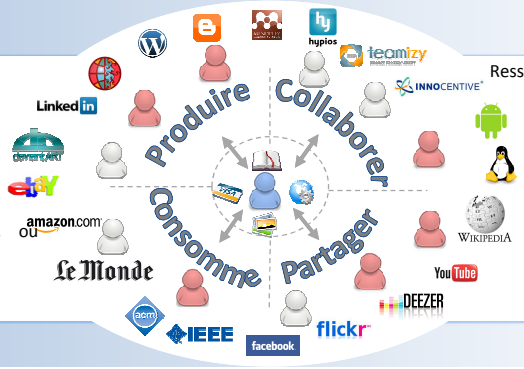
Gestion de la confiance au sein de communautés virtuelles

Réda Yaich, Gauthier Picard, Philippe Jaillon, Olivier Boissier
ISCOD - Institut Henri Fayol
Ecole Nationale Supérieure des Mines de Saint-Etienne, France
Contact : Reda Yaich* (yaich@emse.fr)

Contexte

Les communautés virtuelles :
- Groupes d'entités
- Interagissant via internet
- Partageant des **pratiques, intérêts, valeurs, principes** communs

Leurs objectifs **: production**, **consommation**, **partage, collaboration** autours de ressources (Informations, services, idées, etc.).

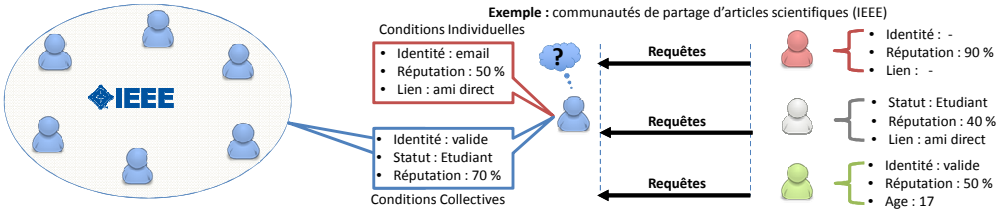


Ressources **sensibles** dont la manipulation comporte un **risque**.

Prise de décision rendue difficile par un contexte :
- **large**
- **distribué**
- **hétérogène**
- **ouvert**
- **décentralisé**
- **dynamique**

La **confiance** est nécessaire pour :
- **maîtriser** le risque
- **réduire** la complexité et l'incertitude

Motivation



Méthode

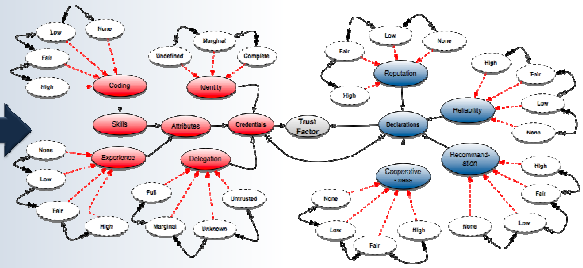
1. Définir un langage de spécification de politiques de confiance **sémantique** et **flexible**.

- **Sémantique** : intelligible par les humains et les agents.
- **Flexible** : dont l'évaluation n'est pas binaire et dont les règles peuvent être modifiées à la volée.

Principe

- ***Une ontologie*** *répertorie les critères de confiance utilisés dans la communauté (ex. Identité, propriétés, et réputation) ainsi que leur domaine de valeurs.*
- *Une politique est spécifiée à partir d'un* ***ensemble*** *de* ***critères de confiance <Type, Valeur, Poids>,*** *Ex. <Réputation, 0.6, 2>.*
- ***La politique est adaptée*** *par l'ajout, la suppression et /ou la modification des critères de confiance.*

Solution

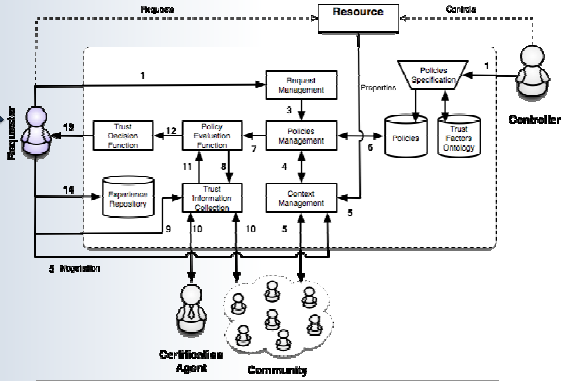


Approche

2. Concevoir un système de gestion de la confiance adaptatif et social

- **Adaptatif** : ajuster au mieux les politiques au contexte métier (risques, opportunités, menaces, etc.)
- **Social :** par articulation des politiques individuelles et collectives.

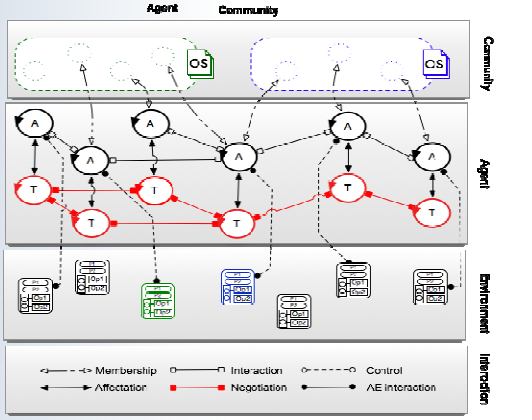
- ***Usage de politiques (expressions en logique pondérée)*** *pour représenter à la fois des politiques individuelles et collectives.*
- ***Usage de métapolitiques (règles ECA)*** *pour adapter et combiner les politiques .*
  - ***E*** *: Evènement du contexte*
  - ***C*** *: Condition de garde*
  - ***A*** *: Une liste d'actions*



3. Implémenter Système de Gestion de la confiance **intelligent** et **autonome** pour adapter, combiner/intégrer et vérifier les politiques de confiance.

- **Intelligent** afin de raisonner sur son contexte (métier et social) et ses politiques.
- **Autonome** afin de prendre des décisions d'adaptation quand c'est nécessaire.

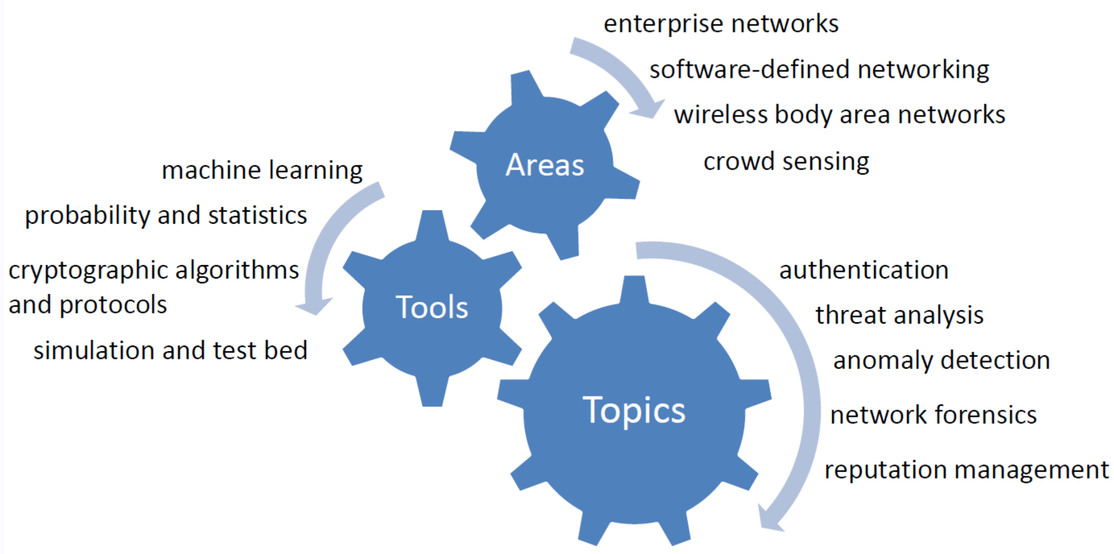
- *Utilisation d'****agents assistants*** *dédiés à la gestion de la confiance.*
- *Pour chaque interaction, l'agent* ***évalue*** *un degré de confiance et* ***recommande*** *à l'utilisateur une décision.*
- *L'agent peut* ***assouplir*** *ou* ***durcir*** *les politiques qu'il utilise en fonction du contexte (métier et social).*



Network Performance and Security

Zonghua Zhang, and Ahmed Meddahi

Research Outline



Challenges

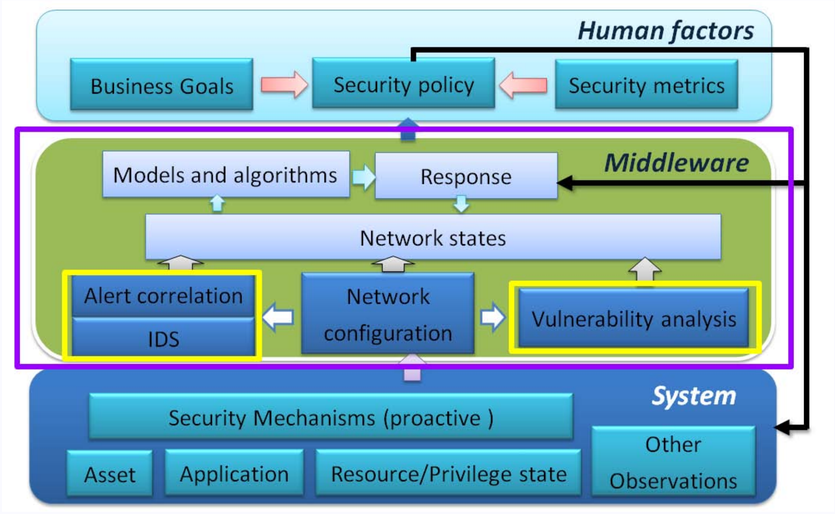
- Building a perfecturly secure system in practice is mission impossible
- The increasing complexity of today's computer and communication systems, and the diversity of networking applications and services lead to the rapid emergence of zero-day vulnerabilities and attacks
- The interactions between system, human, and organization are too complicated to be characterized, modelled, and analyzed
- A prefect in-depth defense line is not available
- ....

We are interested in investigating the significant yet implicit relations between *network performance* (or quality of services) and *security*, designing and developing efficient protocols, models, and algorithms to achieve the best trade-off between expected performance goals and specified security metrics

Selected Research Topics

● Cost-effective security management

Developing adaptive and scalable middleware to enhance *usability*, *effectiveness* and *interoperability* of legacy security mechanisms in enterprise networks. The objective is to assist security administrators in taking optimal security hardening, ranging from vulnerability patching to security mechanism re-configuration and policy enforcement, by leveraging network failure cost resulting from attacks and maintenance cost incurred by defenses. The advent of Software-Defined Network and Cloud Computing has significantly reformed the battlefield between attackers and defenders.



Reference

✓ Shuzhen Wang, Zonghua Zhang, Youki Kadobayashi: Exploring attack graph for cost-benefit security hardening: A probabilistic approach, *Computers & Security* 32: 158-169 (2013) (Details are given below)

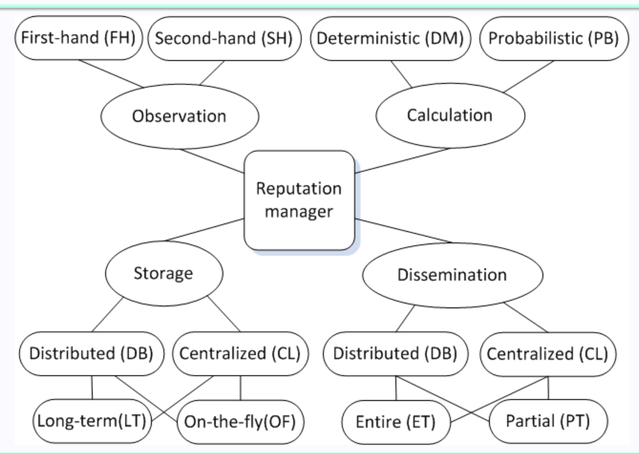
✓ Zonghua Zhang, Farid Naït-Abdesselam, Pin-Han Ho, Youki Kadobayashi: Toward cost-sensitive self-optimizing anomaly detection and response in autonomic networks. *Computers & Security* 30(6-7): 525-537 (2011)

✓ Zonghua Zhang, Pin-Han Ho, Liwen He: Measuring IDS-estimated attack impacts for rational incident response: A decision theoretic approach. *Computers & Security* 28(7): 605-614 (2009)

✓ Zonghua Zhang, Hong Shen: M-AID: An adaptive middleware built upon anomaly detectors for intrusion detection and rational response. *ACM Trans. on Autonomic and Adaptive Systems* 4(4) (2009)

● Reputation and trust management

Designing *privacy-preserving*, *robust* and *light-weight* reputation systems to enhance the quality of services in wireless networks, mobile social networks, and smart city oriented crowd sensing. One of the major aims is to encourage the network entities, varying from static sensors to mobile phone users, to actively contribute their local information for global data processing, knowledge discovery and decision-making.



Reference

✓ Zonghua Zhang, Pin-Han Ho, Farid Naït-Abdesselam: RADAR: A reputation-driven anomaly detection system for wireless mesh networks. *ACM Wireless Networks* 16(8): 2221-2236 (2010)

✓ Juan Li, Zonghua Zhang, Weiyi Zhang: MobiTrust: Trust Management System in Mobile Social Computing. in *Proceeding of CIT 2010*: 954-959

✓ Zonghua Zhang, Jingwei Liu, Youki Kadobayashi: STARS: A Simple and Efficient Scheme for Providing Transparent Traceability and Anonymity to Reputation Systems. in *Proceeding of DPM/SETOP 2010*: 170-187

● Privacy-preserving network forensics

Designing *efficient* and *reliable* privacy-preserving methods, algorithms and protocols for forensic analysis on threat data of interest. The purpose is to integrate cross-site encrypted footprints associated with multi-layer observations for manifesting and characterizing attack behavior.

Reference

✓ NECOMA Project (Nippon-European Cyberdefense-Oriented Multilayer threat Analysis, EU FP7) http://www.necoma-project.eu/

✓ Zonghua Zhang, Hong Shen: Constructing Multi-Layered Boundary to Defend Against Intrusive Anomalies: An Autonomic Detection Coordinator. in *Proceedings of IEEE DSN.*

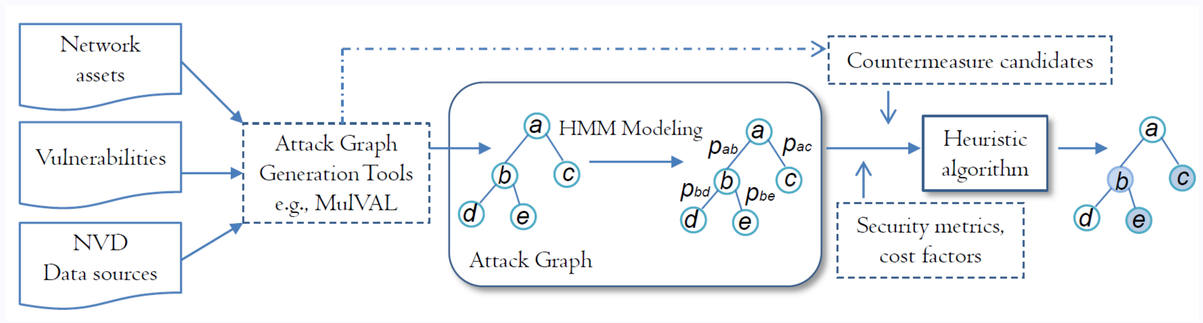
Exploring attack graph for cost-benefit security hardening: a probabilistic approach

● Design Goal

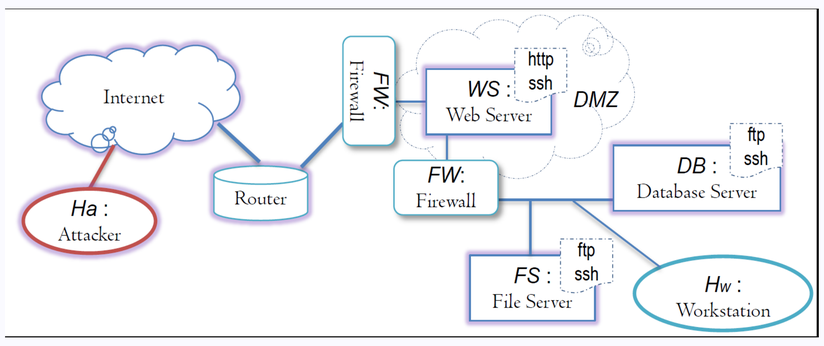
Given a target network and a set of collected observations, how to effectively estimate and predict the implicit system states, subsequently to identify the root causes that may lead to the significant loss of security properties in terms of a set of security metrics, which are specified as security demand and business goal of an organiztaion.

● Design Rationale: Our Approach AG-HMM

- ✓ Commercial/Open source tools are used to identify network vulnerabilities
- ✓ Network assests, vulnerabilities, user priviledges are collected as observations
- ✓ Dependency Attack Graph (AG) is modified and applied to represent observations
- ✓ Hidden Markov Model (HMM) is used to estimate implicit system states based on AG-represented observations
- ✓ System states is quantified as pre-specified security metrics according to a well-defined cost function
- ✓ The observations associated with key system states are removed

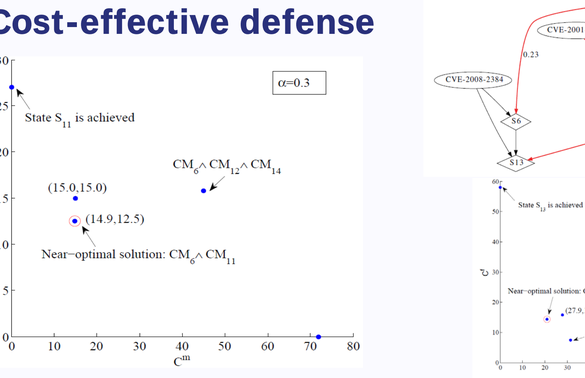


● Example network



Notations	*Network asset*	*Applications*	*Role*
H_a	Attacker	Any	Conducting attacks
H_w	Workstation	Any	Normal activities
WS	Web Server	http, ftp	WWW, database queries
FS	File Server	ftp, ssh	Storing confidential info., etc.
DB	Database Server	ftp, ssh	Storing data accessed via *WS*
FW	Firewall	Loose policies	Traffic filtering and control
IDS	IDS	Signature-based	Intrusion detection and alerts

● Generation of dependency attack graph



● Attack state estimate using Hidden Markov Model

Notation	Countermeasure
CM_1	Disconnect(DB, Internet)
CM_2	Disconnect(FS, Internet)
CM_3	Disconnect(WS, Internet)
CM_4	Patch(DB, CVE-2008-2384)
CM_5	Patch(FS, CVE-2001-0755)
CM_6	Patch(WS, CVE-2006-3747)
CM_7	Patch(H_w, all)
CM_8	Disable(DB, ssh/ftp)
CM_9	Disable(FS, ssh/ftp)
CM_{10}	Disable(WS, ftp)
CM_{11}	Disable(H_w, all)
CM_{12}	Configure(FW)
CM_{13}	Configure(IDS)
CM_{14}	Configure(H_w)

● Cost-effective defense

LIMITED PROOF

GRAPHICAL CODE FOR AUTHENTICATION
INFORMATION THEORETICAL ANALYSIS

School

Authors

Anh Thu PHAN HO
Wadih SAWAYA
Patrick BAS (CNRS)

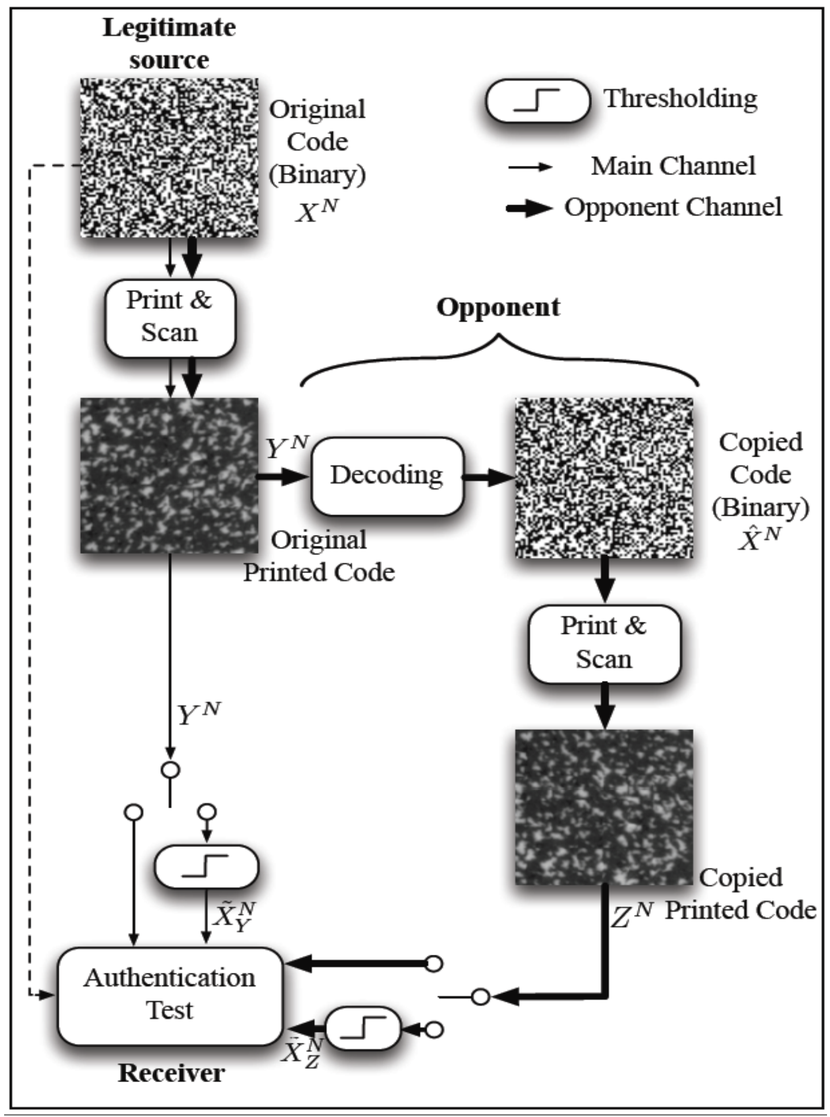
Partner

CONTEXT

- Counterfeiting is rising rapidly in many areas such as food, medicines, cosmetics…
- Fighting against counterfeit by printing a 2D barcode on package of products
- Assuming that printing and acquisition are stochastics and irreversible processes
- Opponent's strategy: generating $\hat{X}^N$ such that Z^N is considered as authentic

OBJECTIVES

- Develop a theoretical authentication model using information theoretic tools
- Extract bounds on the success probabilities of the opponent
- Define the parameters of optimal codes for authentication

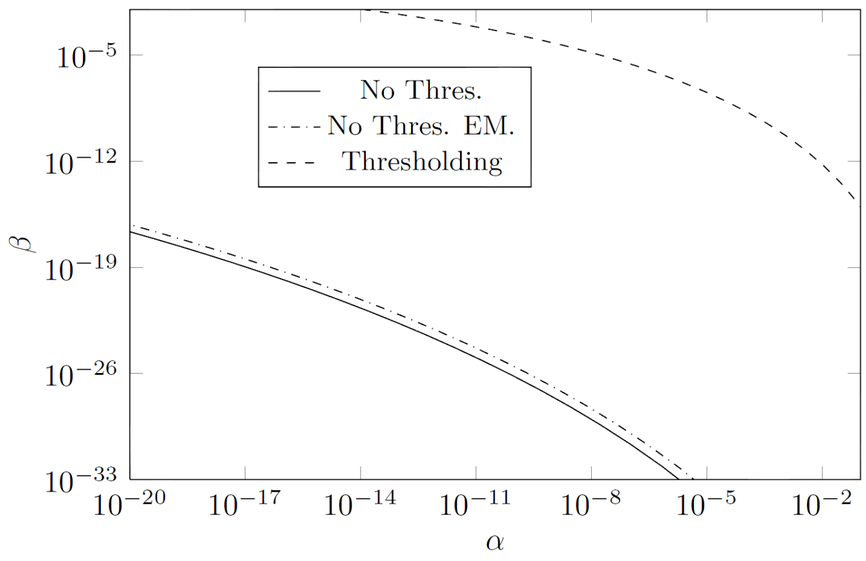


RESULTS

- Gray level observation strategy better than binary thresholding for authentication
- Assuming the models of processes known, using Neyman-Pearson test

$$L = \log \frac{P\left(o^N/x^N,\, H_1\right)}{P\left(o^N/x^N,\, H_0\right)} \underset{H0}{\overset{H1}{\gtrless}} \lambda \text{ where } o^N|H_0 = y^N;\; o^N|H_1 = z^N$$

- Computing false alarm and non detection probabilities
  - ➢ Gaussian aproximation
  - ➢ Chernoff bounds (threshold far away the mean)



PERSPECTIVES

- Authentication for structured codes
- Studying the model of the broadcast channel

REFERENCES

[1] A-T.Phan Ho, B-A. Hoang Mai, W.Sawaya, P.Bas. Document Authentication Using Graphical Codes : Impacts of the Channel Models. In ACM Workshop on Information Hiding and Multimedia Security, Montpellier, France, June 2013

[2] R. G. Gallager. Information theory and reliable communication, volume 15. Willey 1968

Le colloque "Numérique : Grande échelle et complexité"
Mars 2014

Contact phanho@telecom-lille.fr

Site web

RFID, une technologie controversée : entre usages et perception du risque

Objectifs

Un programme de recherche sociologique sur la construction sociale du risque RFID

Analyse des controverses et perceptions du risque en situation

- Analyse de la presse écrite (généraliste et spécialisée, anglophone/francophone, 1990-2010, 100000 articles)
  - Cartographie et chronologie du débat public
  - Identification des acteurs
  - Qualification des risques
- Enquête dans la R&D et production de la RFID
- Ethnographie d'une expérimentation d'usage (santé, DASRI)

Partenaires

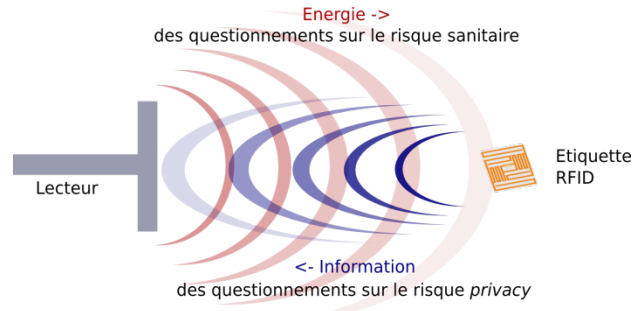
Télécom ParisTech, Dép. SES, DEIXIS-Sophia (leader)
Mines Saint-Etienne, Centre Microélectronique de Provence
Université de Coimbra, OSIRIS, Observatoire sur les Risques

Projets et soutien

Risc - Radiofréquences : Identification des Sources de Controverse. Le cas de la RFID

Trace-De-TIC

Objet de la recherche



Valorisations

Conférence-débat
Télécom ParisTech
14 mars 2014

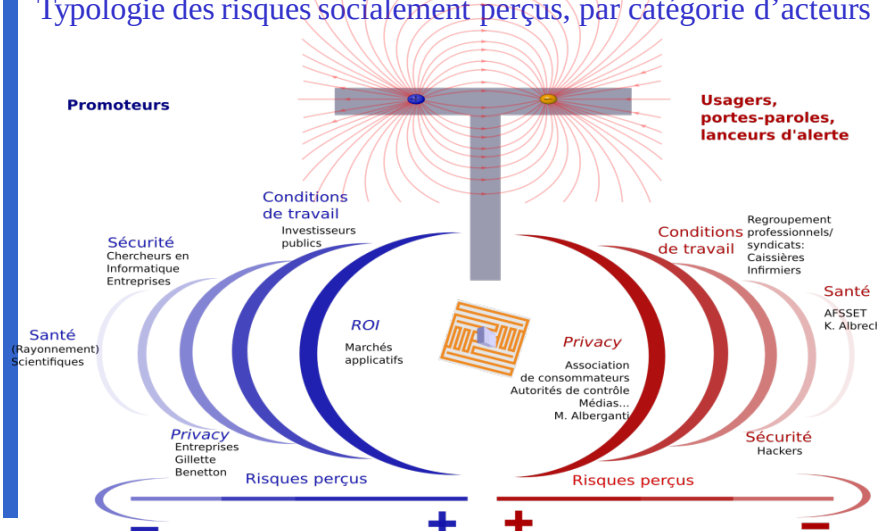
La RFID à l'épreuve de l'innovation responsable

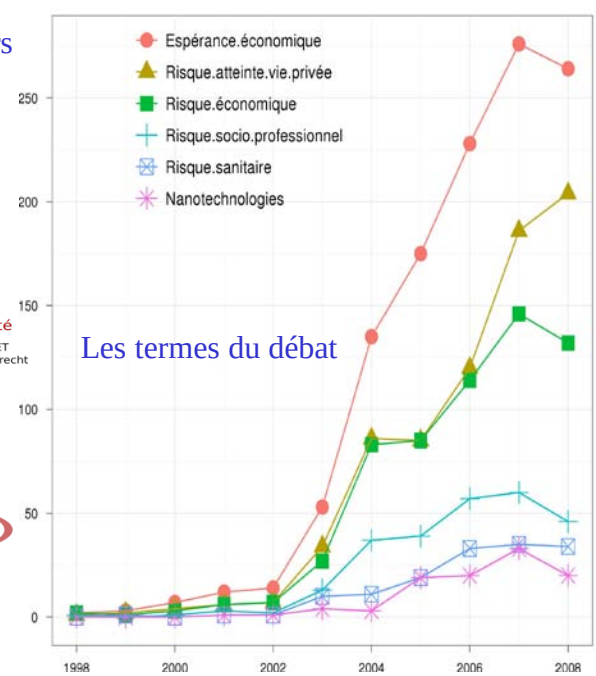
Évaluation d'impact sur la vie privée
gestion de l'exposition humaine
éco-conception et recyclage

Quelles exigences et opportunités pour une approche responsable de l'innovation ?

Quelques résultats de recherche

Typologie des risques socialement perçus, par catégorie d'acteurs





Les termes du débat

Contact : Laura Draetta, TELECOM ParisTech, LTCI/CNRS
+33 (0)4 93 00 84 09 laura.draetta@telecom-parsitech.fr

A Simple Model for Evaluating Secure Key Generation from Random Radio Channels

Institut Mines-Télécom

Auteurs

Taghrid MAZLOUM

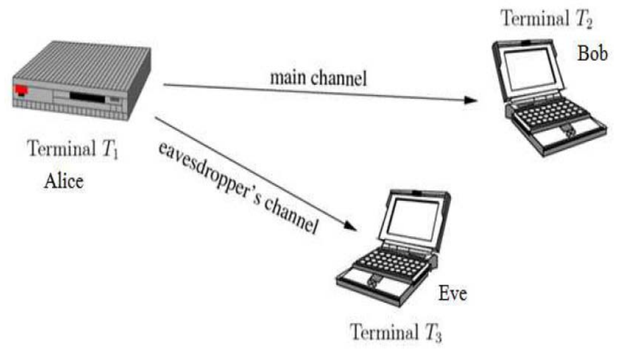
Alain SIBILLE

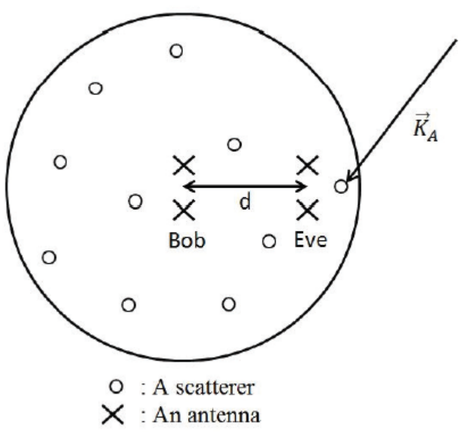
Partenaires

PHYLAWS

Introduction

- Security is a significant challenge in wireless communications. Owing to the public nature of information wireless transmission, an eavesdropper can easily access to the information exchanged between legitimate terminals.
- The widely used method to ensure security is to encrypt and decrypt messages using secret keys. However conventional techniques of generating and distributing such keys may suffer from complexity and high computational cost.
- An alternative solution is physical layer security (PhySec) that designs all kind of security methods which take advantage of the inherent properties of the propagation channel, e.g. noise, interference, and the time-varying nature of fading channels, to provide secure communications.
- We are particularly interested in secret key generation (SKG) achieved by exploiting and invoking radio channel properties, e.g. reciprocity and spatial decorrelation. Legitimate terminals generate independently an identical secret key by observing the same propagation channel considered as a source of randomness. Hence we propose a simple stochastic channel model for which we evaluate the security.





SKG through a simple channel model

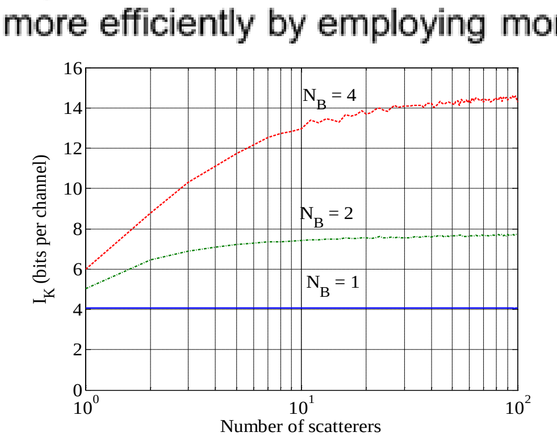
Description of the channel model

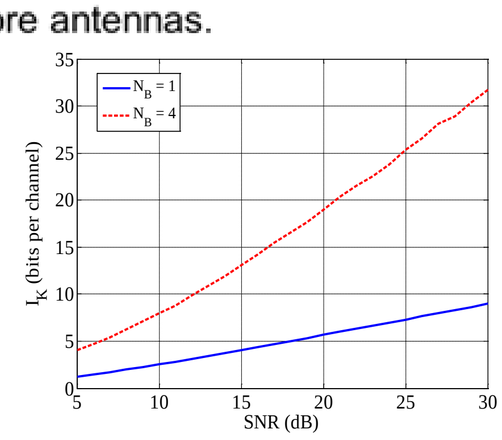
- In the literature, the security is evaluated for a worst-case scenario where one legitimate user, i.e. Alice or Bob, and the eavesdropper Eve are sufficiently close to each other. However, in order to explore more realistic scenarios, we propose a simple 2-D geometry-based stochastic channel model to study the effect of the lack of spatial stationarity between Bob and Eve on the SKG.
- We model a macroscopic environment by uniformly distributing scatterers within a disc around Bob. Eve is located at a distance *d* from Bob. They both are equipped with either single or multiple omnidirectional antennas. The transmitter Alice is assumed far away from the disc.
- The complex channel gain connecting Alice antenna with the *m*th antenna at Bob/Eve side can be defined as:

$$h_m = \sum_{l=1}^{N_S} \frac{\beta_l}{d_l} \exp\left\{j\left(K.d_{ml} + \overrightarrow{K_A}.\overrightarrow{r_l}\right)\right\}$$

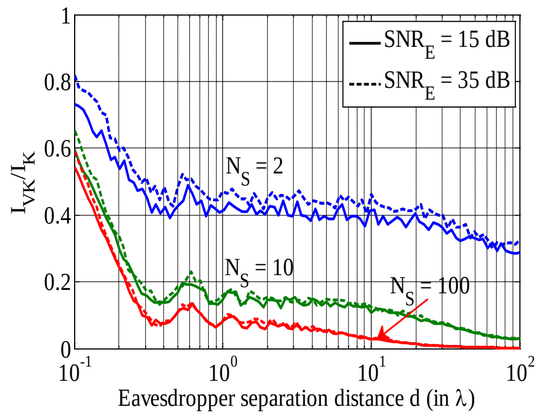
SKG evaluation

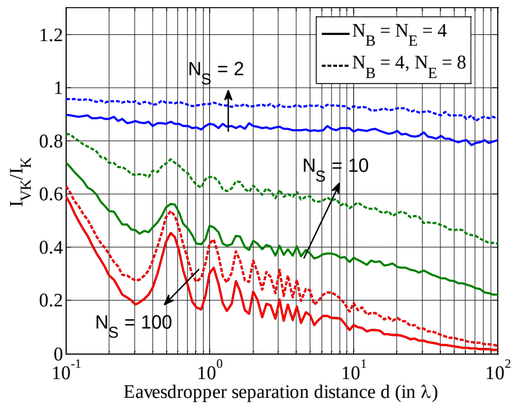
- I_K is the maximum number of bits that can be extracted from the reciprocal propagation channel. By increasing the spatial diversity of the channel, i.e. by employing multiple antennas, I_K increases especially for rich scattered channels and for higher SNR.
- Eve is able to know some bits of I_K. Therefore we define the vulnerable key bits I_{VK} as the number of bits leaked to Eve. The security is improved for rich scattered channels and for large separation distance Bob/Eve. Eve degrades the security by either increasing her SNR or more efficiently by employing more antennas.





The improvement of I_K with respect to the channel richness in scatterers, to the number of antennas and also to the SNR





The relative vulnerable key bits I_{VK}/I_K vs. Eve separation distance for either larger SNR or employing more antennas

Conclusion

- A simple channel model exploring the macroscopic variation between Bob and Eve is investigated in SKG context.
- The confidentiality is achieved owing to the spatial decorrelation between the legitimate channel and that measured by Eve, especially in rich scattered channels for large separation distance Bob/Eve where they both do not share a common stationarity region.
- Exploiting the degrees of freedom of multiple antennas improve the security by increasing I_K leading to generate more secure key bits. Unfortunately, it also helps Eve to gather more information about the shared key.

Contact {Taghrid.mazloum, alain.sibille}@telecom-paristech.fr Site web www.telecom-paristech.fr

Pseudonym update for privacy in cooperative V2X systems

Parties prenantes

TELECOM ParisTech

RENAULT

Auteurs

Rim Moalla, TPT.
Houda Labiod, TPT.
Brigitte Lonc, Renault.

Partenaires

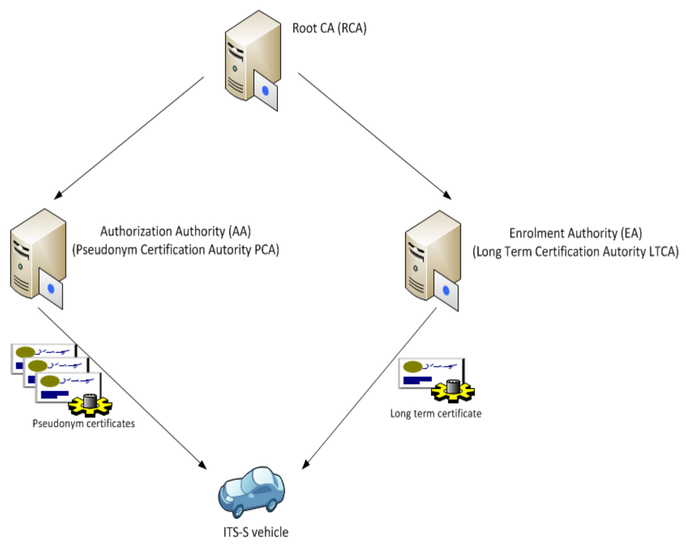
FONDATION TELECOM

INSTITUT CARNOT Télécom & Société numérique

Problem statement

Context

- Privacy is a complex requirement in V2X systems as we have to identify stations and to protect personal data.
- Several solutions are proposed to provide privacy: Anonymous certificates, group signature and pseudonyms certificates.
- Car2Car consortium and standardization organizations choose pseudonyms solution where ITS-S vehicle has two types of certificates: short term certificates named pseudonyms certificates and long term certificate.
- Pseudonyms certificates change frequently and consequently have to be updated.
- We consider pseudonyms certificates update over-the-air using the unsecure G5 (IEEE 802.11p) media.

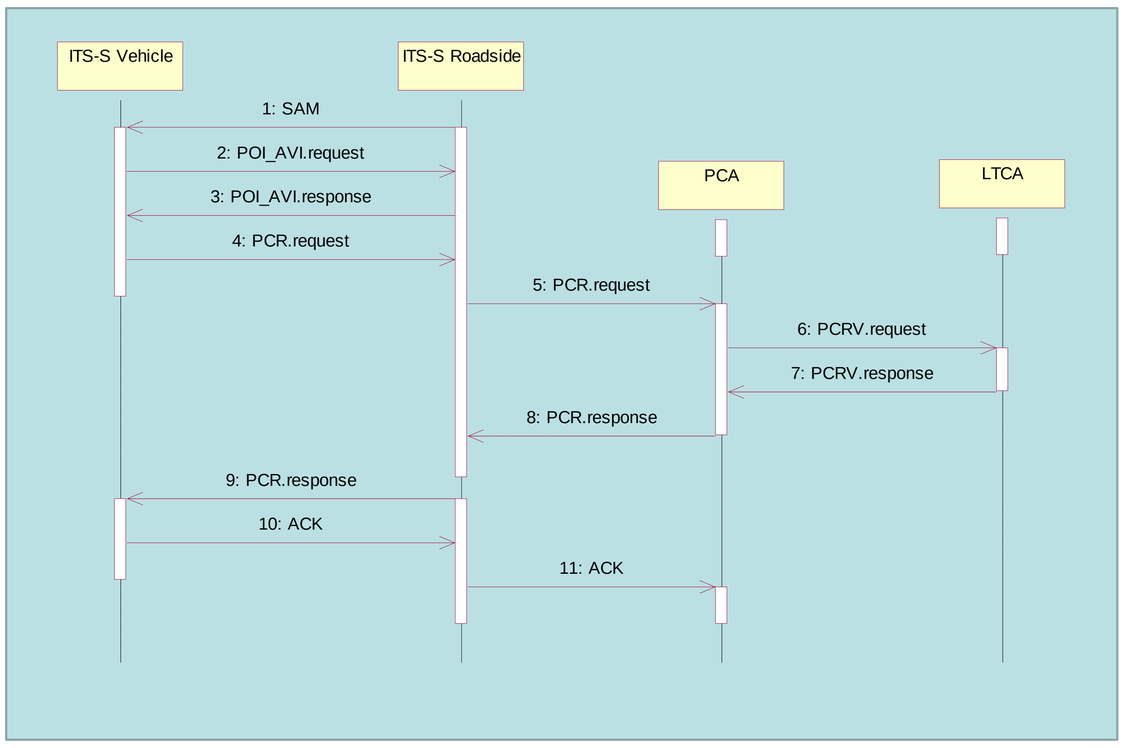


Requirements

- ITS-S vehicle has to transmit sensitive data to the PCA without conveying them to an intermediary node such as ITS-S roadside.
- ITS-S vehicle has to prove to the intermediary node that is authorized to establish communication with PCA.
- ITS-S roadside is required to prove its legitimacy to the PCA by providing that it is authorized to act on behalf of the ITS-S vehicle.

Proposed protocol

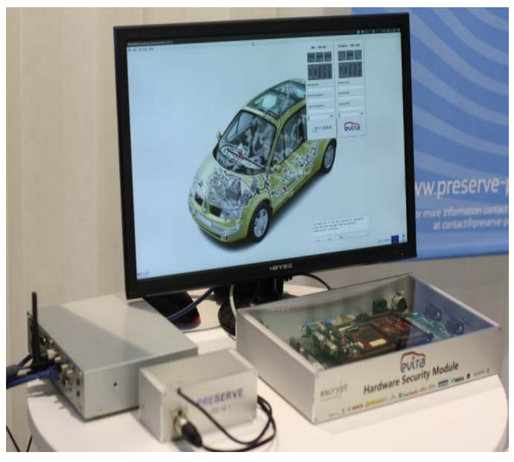
- Is composed by two phase: phase I covers service discovery and session key establishment and phase II for certificate update.
- Enables vehicle to securely update its certificates from a roadside unit (over G5).
- Considers performance, scalability and cost issues.



Pattent submitted in July 2013

Implementation

- We integrate security services into Score@F platform.
- Cryptographic operations are based first on Java crypto library and then on FP7 PRESERVE security solution.
- We evaluated during last tests session on September 2013:
  - Signature generation duration
  - Signature verification duration
  - Pseudonyms change strategies



Validation

- Score@F/ PRESERVE Workshop , NRIA-Rocquencourt, September2013
- Journée Mobilité 2.0, Satory, February 2014

Contact rim.moalla@telecom-paristech.fr Site web

Modeling and Characterization of Physically Unclonable Functions

*

Parties prenantes

TELECOM ParisTech

LABORATOIRE Hubert CURIEN UMR • CNRS • 5516 • ST-ETIENNE

Authors

PhD student :
Zouha Cherif Jouini
Supervisors:
Jean-Luc Danger
Lilian Bossuet

Partners

orange™

Physically Unclonable Functions

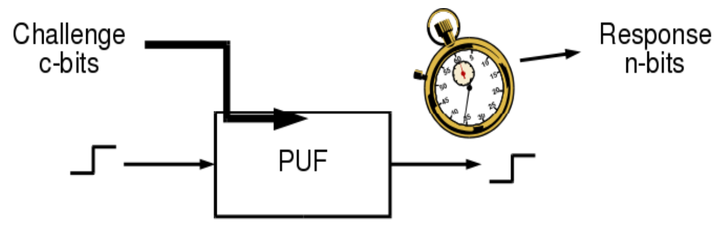
- It returns a signature intrinsic to a circuit (a fingerprint).

Applications

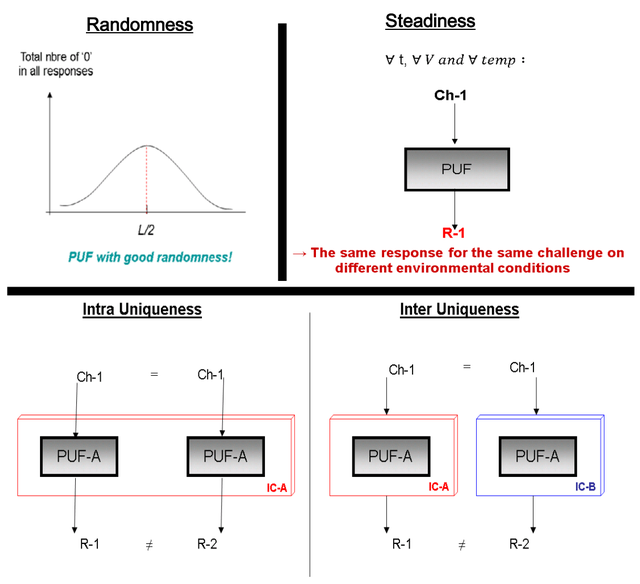
- Authentication of Integrated Circuits.
- Generation of cryptographic keys.

Types

- Silicon: Easy to implement : Arbiter PUF, Ring-Oscillator PUF, SRAM PUF, etc.
- Non silicon: Coating PUF, Optical PUF, etc.



Our Contributions



1- PUF characterization method

Principle

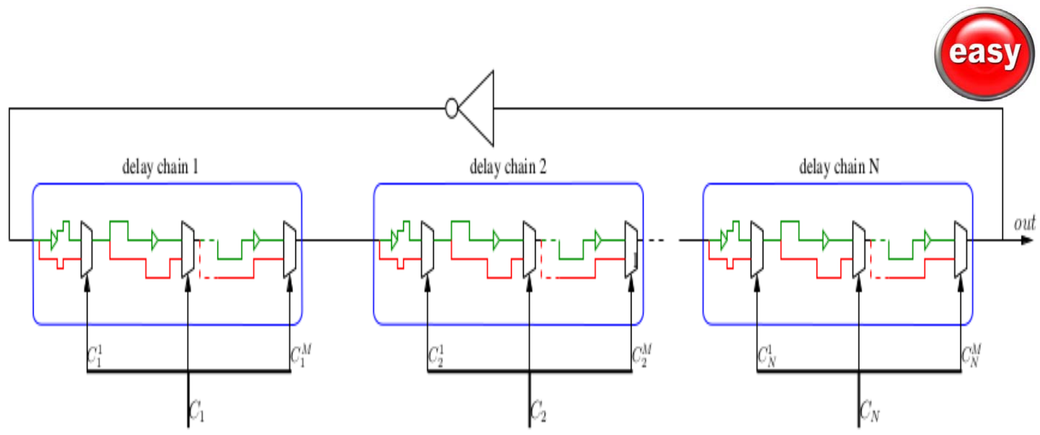
- Used to evaluate silicon PUFs (specially delay PUFs).
- Takes advantage of the physical characteristics of the PUF structures.

Performance Indicators

- Randomness
- Uniqueness
- Steadiness

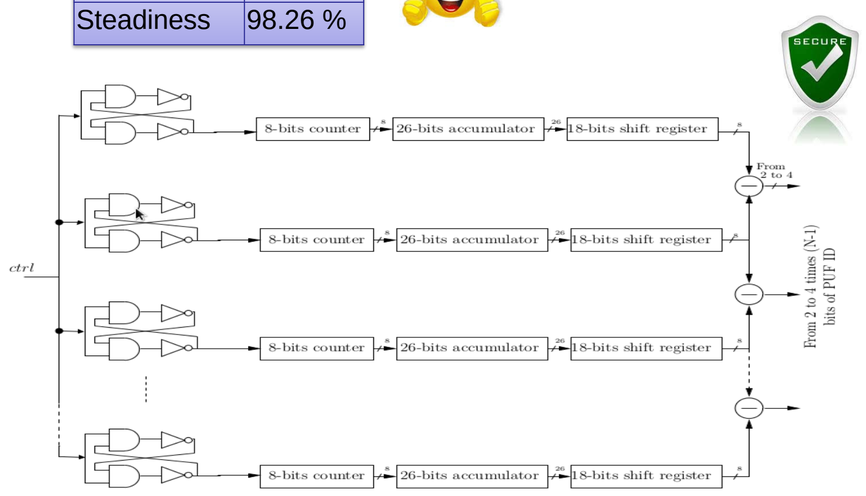
2- Loop PUF

- Silicon delay based PUF.
- Easy to implement :
  - ➢ No hard routing and placement constraints.



Performance Results

Randomness	98.97 %
Uniqueness	89.21 %
Steadiness	98.26 %



3- TERO PUF

- Silicon Ring-Oscillator based PUF.
- Not sensitive to locking phenomenon.

Performance Results

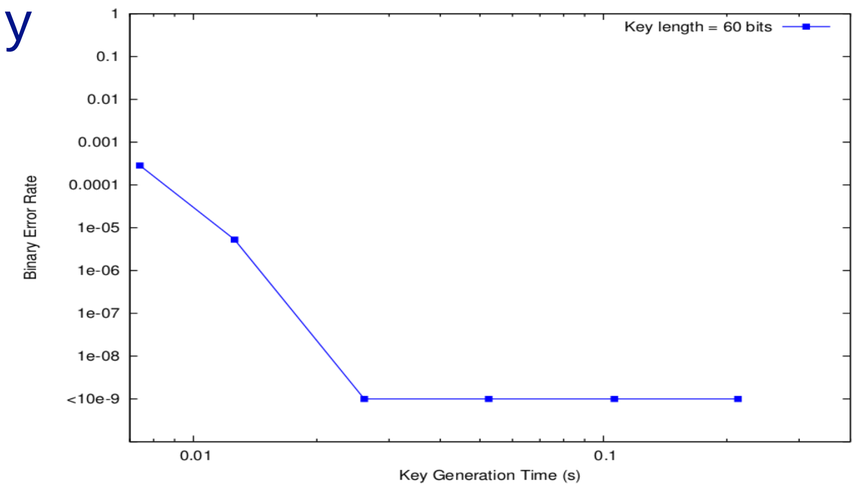
Randomness	98.61 %
Uniqueness	98.54 %
Steadiness	97.25 %

4- Loop PUF-based cryptographic key

Principle

- Smart selection of challenges.
- Increasing the number of tests.
- Unreliable bit identification.
- Key correction procedure.

➡ BER = 10-9 - 10ms - 101 slices in Xilinx FPGA.



* http://www.newelectronics.co.uk/electronics-news/puffin-aims-to-protect-against-identity-theft/45139

Contact Zouha.cherif@telecom-paristech.fr

Drone for Humanitarian Operations

Visit our website and have a look at our videos at, http://drone4u.eurecom.fr

Institutions

Authors

Tullio Joseph Tanzi (Télécom ParisTech)

tullio.tanzi@telecom-paristech.fr

Ludovic Apvrille (Télécom ParisTech)

Jean-Luc Dugelay (EURECOM)

Claire Migliaccio (LEAT)

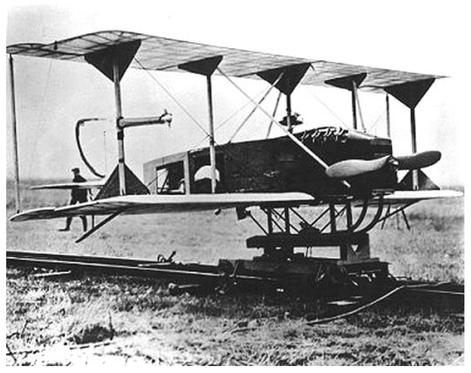
Julien Morel (Télécom ParisTech)

Franck Guarnieri (Mines ParisTech)

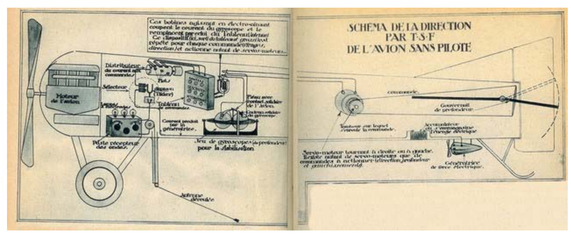
Partners

Main characteristics of drones

- **Unmanned** Aerial Vehicle: Drones can perform some specific missions with no on-board pilot;
- **Self-flying**: Autonomous fly is usually limited to reach a specific location given by GPS. More advanced autonomous functionalities can help in a decision process to react against unpredicted situations;
- **Reusable** and **reconfigurable**: Drones can be used for diverse missions, and can be appropriately customized.

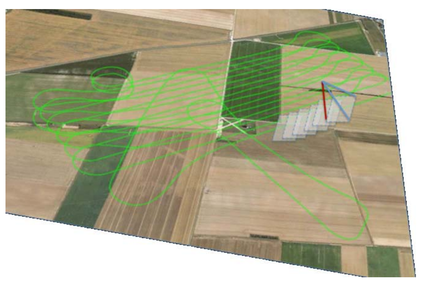


Hewitt-Sperry Automatic Airplane 1910



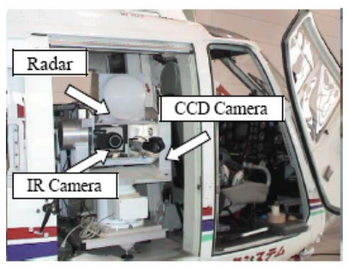
"Avion sans pilote« , by Maurice Percheron [Lectures pour tous, février 1923].

Drones for assisting disasters

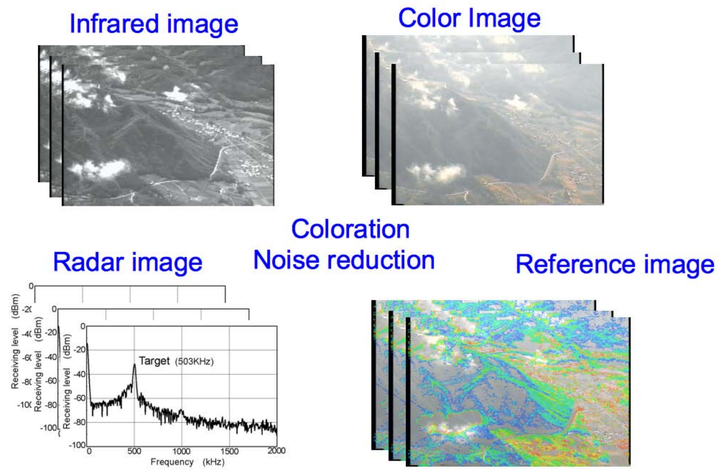


3D Reconstruction

- Spatial **coverage**:
  - Scanning a given area to establish an overview map of emergency;
- **Image processing**:
  - Detecting groups with a fast classification (e.g., adults vs children)
  - 3D reconstruction to allow drones to navigate autonomously with cameras
- **Specialized** on-board devices and **sensors**:
  - Detecting signals attached to wireless networks (e.g., mobile phones) so as to drive rescuers to areas where they are more likely to find persons.
- etc.

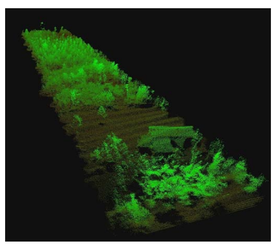


Non conventional payload



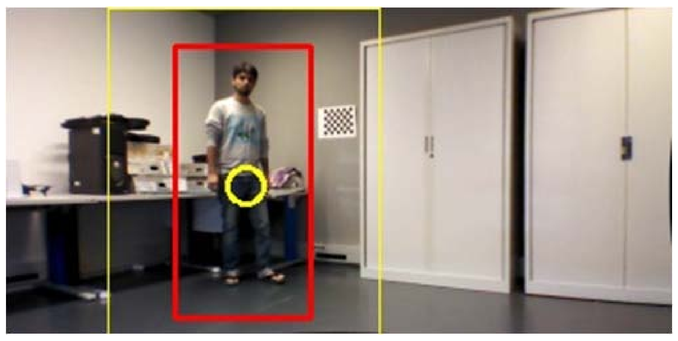
Embedded electronic and software architecture

- Cameras,
- Lidars,
- Low cost and efficient processing units (e.g., parallella ...)



LIDAR Image

UAV cluster



People detection and tracking

Summary

- Designing a civil drone to assist disasters;
- "Smart drone": Autonomous drone with some standalone capacities to make decisions;
- Safety and security are taken into account at design stage.
- Integration of complex sensors;
- Handling complex national and international rules and policies;
- Societal impacts, including privacy preservation.

TTool — An open source toolkit provided by

Colloque l'Institut Mines-Télécom , "Numérique : Grande échelle et complexité"

26 et 27 mars 2014

Formally Proved Security of Assembly Code Against Leakage

Pablo RAUZY
Sylvain GUILLEY

Institut MINES-TELECOM,
TELECOM-ParisTech,
CNRS LTCI (UMR 5141).
Paris, France

Context: countermeasures

	Hardware	Software
Masking	***	***
Hiding (dual-rail)	***	*few works!*

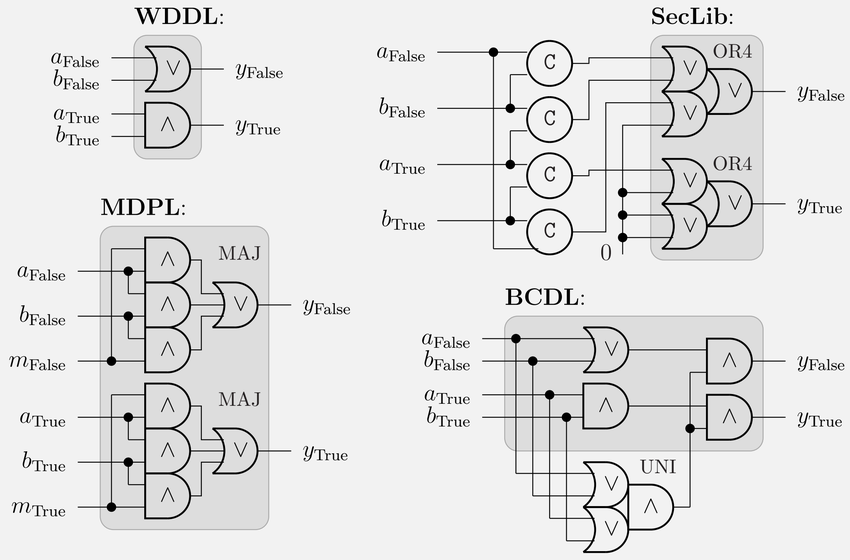
Problems of masking in software

- Lots of entropy (*not available on resource-constrained devices*)
- Structural vulnerability: existence *high-order* attacks

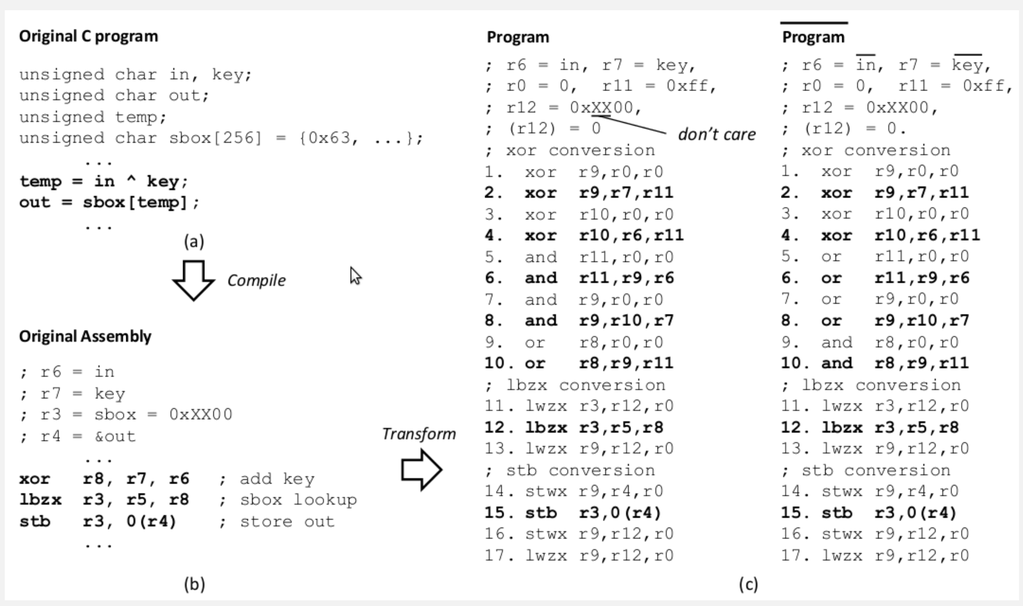
Dual-rail in software: opportunities

- No need for entropy
- Provable correction of leakage-free (with a finite number of *physical* hypotheses, to do by pre-characterization)

State-of-the-art about dual-rail in hardware [DGBN09]



State-of-the-art: mixed HW/SW, *e.g.*, dual-rail instruction set [CSS13]

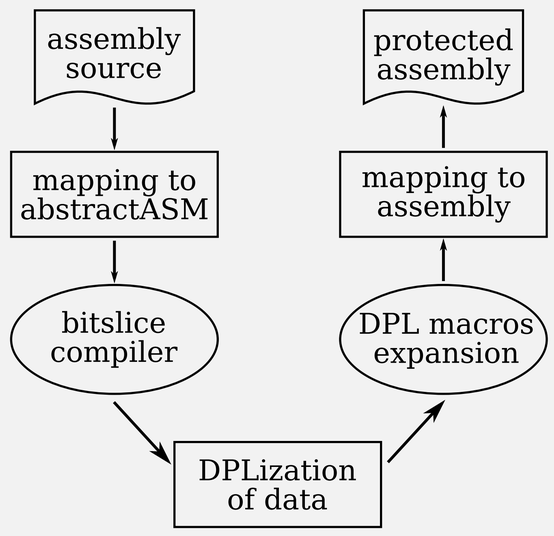


Courtesy of Zhimin Chen and Patrick Schaumont ECE Department, Virginia Tech Blacksburg VA 24061, USA

An example of Virtual Secure Circuit (VSC):

(a) `KeyAddition` and `SubBytes` operations in C code;
(b) Compiled assembly code;
(c) Converted VSC assembly code.

Pure software dual-rail: design flow



DPL: **D**ual-**R**ail with **P**recharge

Macro for Boolean operation *op*

```
r1 ← r0          mov r1 r0
r1 ← a           mov r1 a
r1 ← r1 ∧ 3      and r1 r1 #3
r1 ← r1 ≪ 1      shl r1 r1 #1
r1 ← r1 ≪ 1      shl r1 r1 #1
r2 ← r0          mov r2 r0
r2 ← b           mov r2 b
r2 ← r2 ∧ 3      and r2 r2 #3
r1 ← r1 ∨ r2     orr r1 r1 r2
r3 ← r0          mov r3 r0
r3 ← op[r1]      mov r3 !r1,op
 d ← r0          mov d r0
 d ← r3          mov d r3
```

Cost on PRESENT [BKL+07] case-study

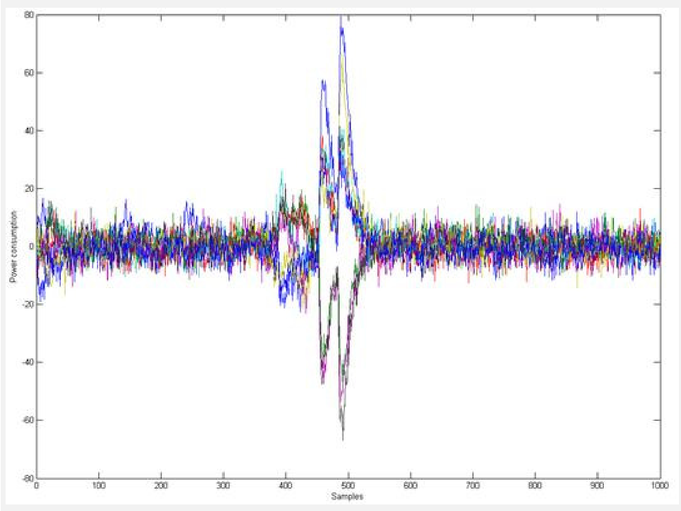
	cycle count	code size*	RAM words*
state-of-the-art	11342	1000	18
bitsliced	6473	1194	144
DPL protected	182572	2674	192

* The state-of-the-art code size and RAM words are given for encryption + decryption, while ours are for encryption only. Code size and RAM words are given in bytes.

Optimizations (still with formal proof of correction)

- The existence of non-sensitive signals (*e.g.*, the selection of key size); or loop counters;
- The limited data range of some variables, that makes some parts of the code use constant variables;
- The possibility to go from one macro to the other through register, thereby saving time from the memory transfers;
- The possibility to merge instructions given certain patterns;
- The use of architecture-specific intructions not included in our abstractASM.

Leakage analysis (physical part)

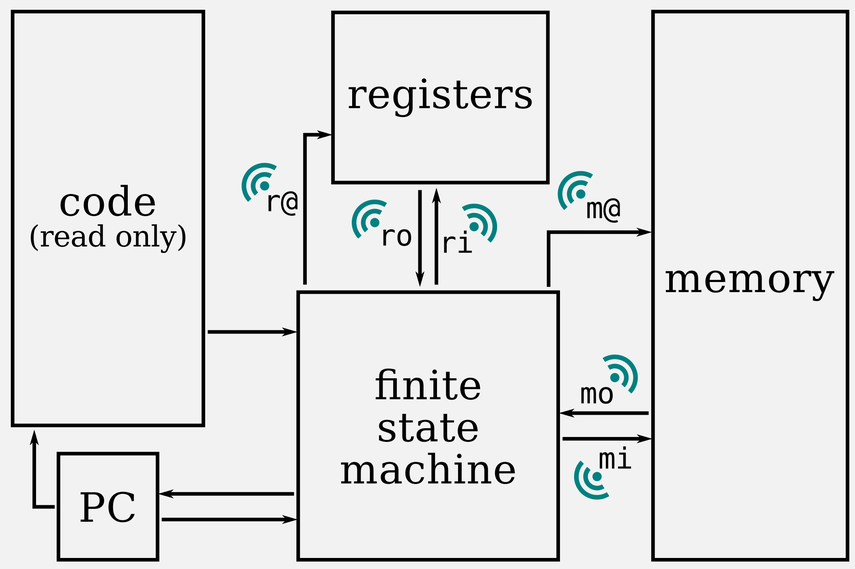


Verifications:
- indistinguishable resources
- for data and addresses

Tools:
- profiling
- linear regression

Stochastic characterization [SLP05] of every bit in a general purpose CPU.

Leakage analysis (formal part)



Verification:

- Leakage: **Hamming distance** of values, **should be constant**
- **Symbolic execution** to check this constantness property

References

[BKL+07] Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and Charlotte Vikkelsoe. PRESENT: An Ultra-Lightweight Block Cipher. In *CHES*, volume 4727 of *LNCS*, pages 450–466. Springer, September 10-13 2007. Vienna, Austria.

[CSS13] Zhimin Chen, Ambuj Sinha, and Patrick Schaumont. Using Virtual Secure Circuit to Protect Embedded Software from Side-Channel Attacks. *IEEE Trans. Computers*, 62(1):124–136, 2013.

[DGBN09] Jean-Luc Danger, Sylvain Guilley, Shivam Bhasin, and Maxime Nassar. Overview of Dual Rail with Precharge Logic Styles to Thwart Implementation-Level Attacks on Hardware Cryptoprocessors, — *New Attacks and Improved Counter-Measures* —. In *SCS*, IEEE, pages 1–8, November 6–8 2009. Jerba, Tunisia. DOI: 10.1109/ICSCS.2009.5412599.

[SLP05] Werner Schindler, Kerstin Lemke, and Christof Paar. A Stochastic Model for Differential Side Channel Cryptanalysis. In LNCS, editor, *CHES*, volume 3659 of *LNCS*, pages 30–46. Springer, Sept 2005. Edinburgh, Scotland, UK.

Maximizing the success of a side-channel attack

Institut Mines-Télécom

Authors

Annelie Heuser

Sylvain Guilley

Olivier Rioul

Télécom ParisTech / Institut Mines-Télécom / CNRS LTCI

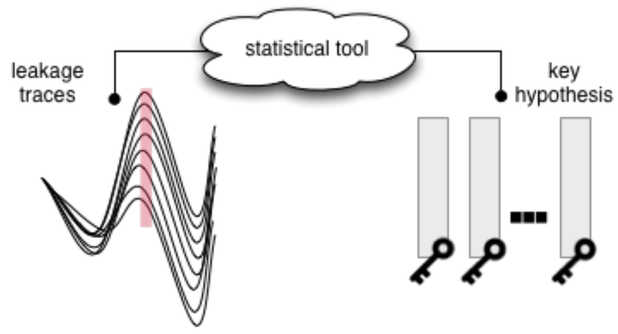
Annelie Heuser is a recipient of the Google Europe Fellowship in Privacy.

State of the Art

✧ What distinguishes known distinguishers, in terms of distinctive features?

✧ Given a side-channel context, what is the best distinguisher amongst all known ones?

- Distinguishers were chosen as (arbitrary) **statistical tools** (correlation, difference of means, linear regression, etc.)
- [1] highlights that proposed distinguishers behave **equivalent** when using the same leakage model, only "statistical artifacts" can explain different behavior [2]
- The **estimation** of the statistical tools (esp. mutual information) is very crucial and effective on the success [3]

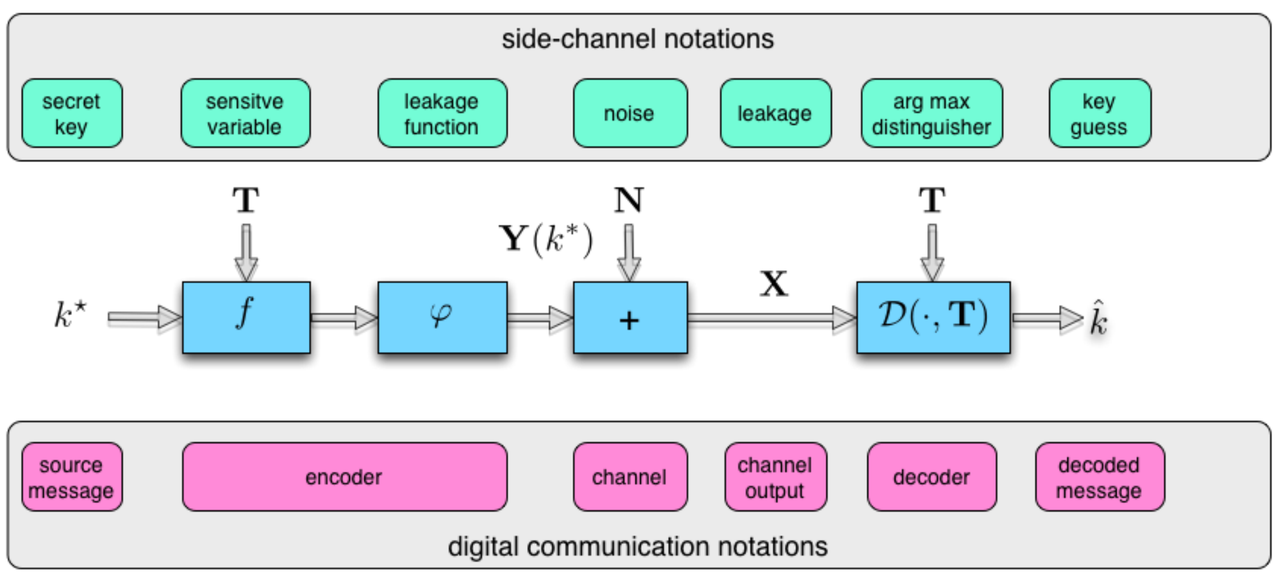


[1] Doget, Prouff, Rivain, and Standaert, JCEN, 2011
[2] Mangard, Oswald, and Standaert. IET, 2011
[3] Prouff and Rivain, IJACT, 2010.
[4] Heuser, Rioul, and Guilley, under submission

Side-channel analysis as a communication problem [4]

✧ Given a side-channel scenario, what is the best distinguisher, amongst all possible ones?

- Idea: Translate the problem of side-channel analysis into a problem of communication theory ➔ derive **optimal distinguisher**: maximize the success rate
- Leakage model is known to the attacker (**Theorem 1**)
  - Only statistical noise
  - Optimal decoding rule $\arg\max_k \Big(\mathbb{P}\{k\} \cdot p(\mathbf{x}|\mathbf{y}(k))\Big)$ (template attack, profiling is possible)
  - The optimal distinguisher only depends on the noise distribution (e.g., Laplacian, uniform, Gaussian)
- Leakage model is partially unknown to the attacker (**Theorem 2**)
  - Statistical and epistemic noise
  - Leakage arises due to a weighted sum of bits, where the weights follow a normal distribution



Theorem 1: optimal distinguisher when the leakage model is known

If the leakage arises from $X = Y(k^\star) + N$ *with known leakage model* $Y(k) = \varphi(f(k, T))$ *then the optimal distinguishing rule are*

- *Gaussian noise distribution:* $\mathcal{D}^{M,G}_{opt}(\mathbf{x}, \mathbf{t}) = \arg\max_k \ \langle \mathbf{x}|\mathbf{y}(k)\rangle - \frac{1}{2}\|\mathbf{y}(k)\|_2^2$,
- *Uniform noise distribution:* $\mathcal{D}^{M,U}_{opt}(\mathbf{x}, \mathbf{t}) = \arg\max_k \ -\|\mathbf{x} - \mathbf{y}(k)\|_\infty$,
- *Laplace noise distribution:* $\mathcal{D}^{M,L}_{opt}(\mathbf{x}, \mathbf{t}) = \arg\max_k \ -\|\mathbf{x} - \mathbf{y}(k)\|_1$.

Theorem 2: optimal distinguisher when the leakage model is partially unknown

Let $\mathbf{Y}_{\boldsymbol{\alpha}}(k) = \sum_{j=1}^{n} \alpha_j [f(\mathbf{T}, k)]_j$, $\mathbf{Y}_j(k) = [f(\mathbf{T}, k)]_j$ *and* $\mathbf{X} = \sum_{j=1}^{n} \alpha_j [f(T, k^\star)]_j + N$ *with* $N \sim \mathcal{N}(0, \sigma^2)$. *Assuming weights are independently deviating normally from the Hamming weight model, then the optimal distinguishing rule is*

$$\mathcal{D}^{\alpha,G}(\mathbf{x}, \mathbf{t}) = \arg\max_k \ (\gamma\langle \mathbf{x}|\mathbf{y}(k)\rangle + \mathbf{1})^t \cdot (\gamma Z(k) + I)^{-1} \cdot (\gamma\langle \mathbf{x}|\mathbf{y}(k)\rangle + \mathbf{1}) - \sigma_\alpha^2 \ln\det(\gamma Z(k) + I) \ ,$$

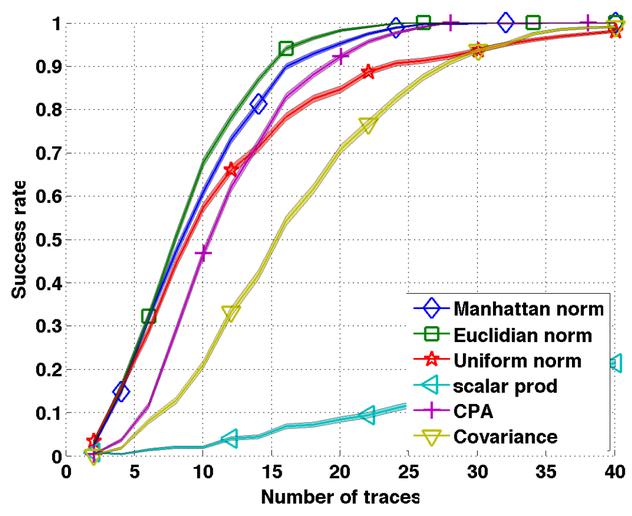
where $\gamma = \frac{\sigma_\alpha^2}{\sigma^2}$ *is the* **epistemic-to-stochastic-noise-ratio** *(ESNR).*

Correlation

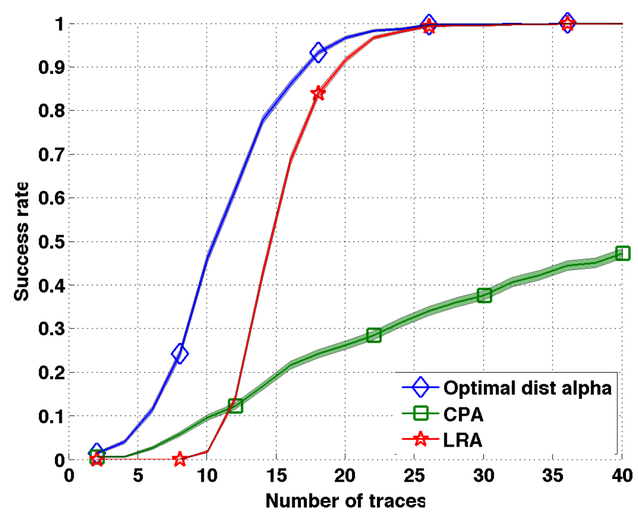
Covariance

Linear regression

Our novel **optimal** distinguishers **outperform** all state-of-the-art distinguishers depending on statistical tools in terms of the **success rate**!



Known model



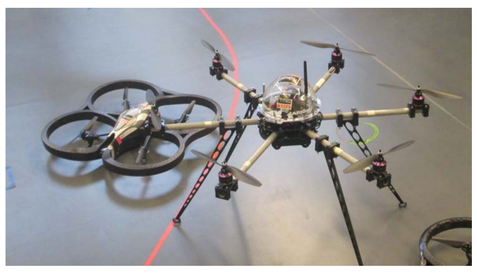
Partially unknown model

Contact annelie.heuser@telecom-paristech.fr Site web perso.telecom-paristech.fr/heuser

SysML-Sec: Capturing and Formally Proving Safety and Security Properties

Handling risk in safety-critical systems

- Automotive systems, avionics systems, nuclear power plants . . .
  - Digital car:
    - Security of over-the-air firmware updates, car control by malware [Koscher 2010], Autonomous vehicle safety (e.g., Google car)
    - Car navigation data spoofing [Andrea et al. 07]
  - Drones:
    - Sensitive data protection and communications security and safety
    - Autonomous support system: security and safety (hijacking, secure data fusion and interpretation, fault-tolerant attitude self-control)



Our proposal for security: SysML-Sec ...

- Objective: bring together system engineers and security experts
- Model-Driven Engineering from requirements to code generation
- Centered around a security-aware HW/SW partitioning
- Formal safety and security proofs
- Free software (TTool)

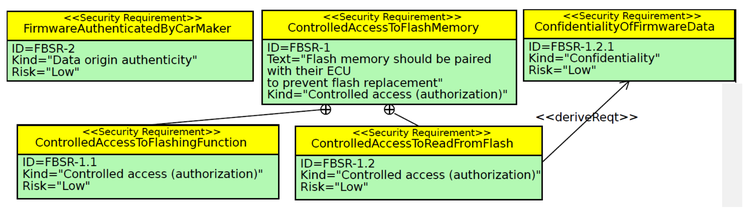
... Integration with safety models ongoing

TTool

An open source toolkit provided by

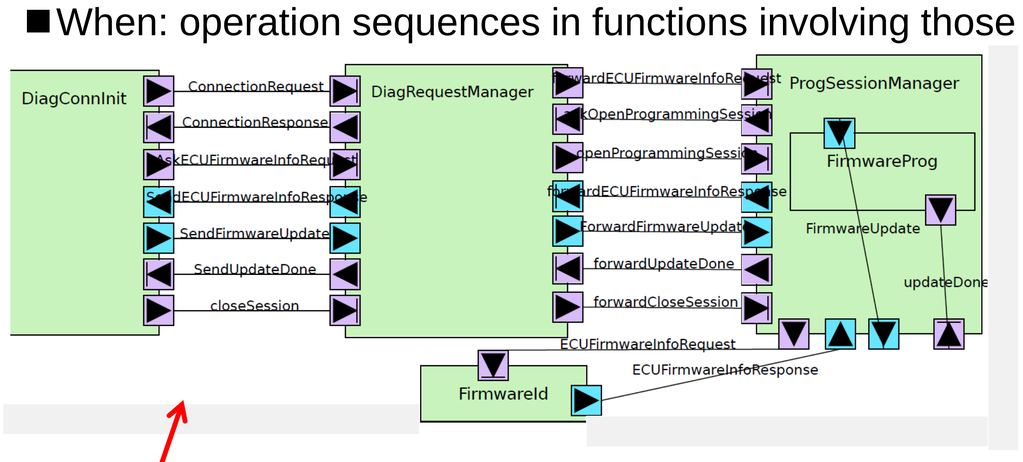
Requirements

- Who and why: stakeholders and security goals



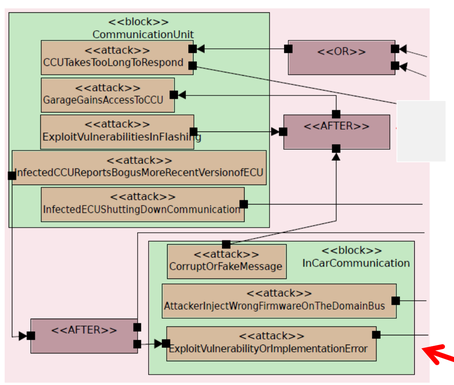
Application

- When: operation sequences in functions involving those assets



Attacks

- Who and Why: attackers, their capabilities, and objectives (risk analysis)

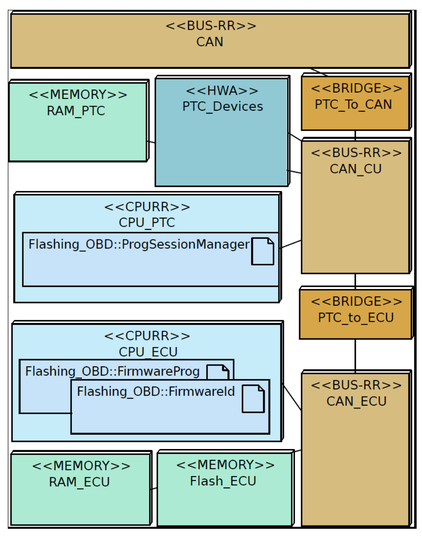


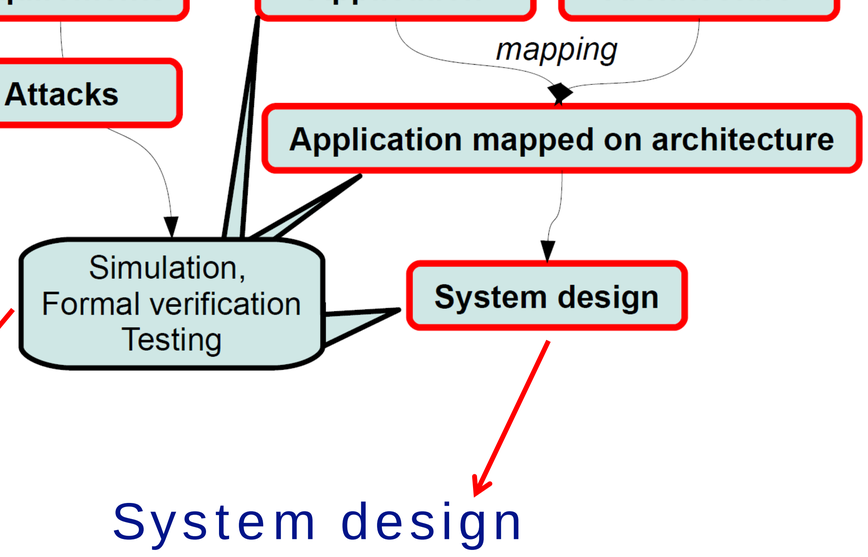
Architecture

- What: assets to be protected

Mapping

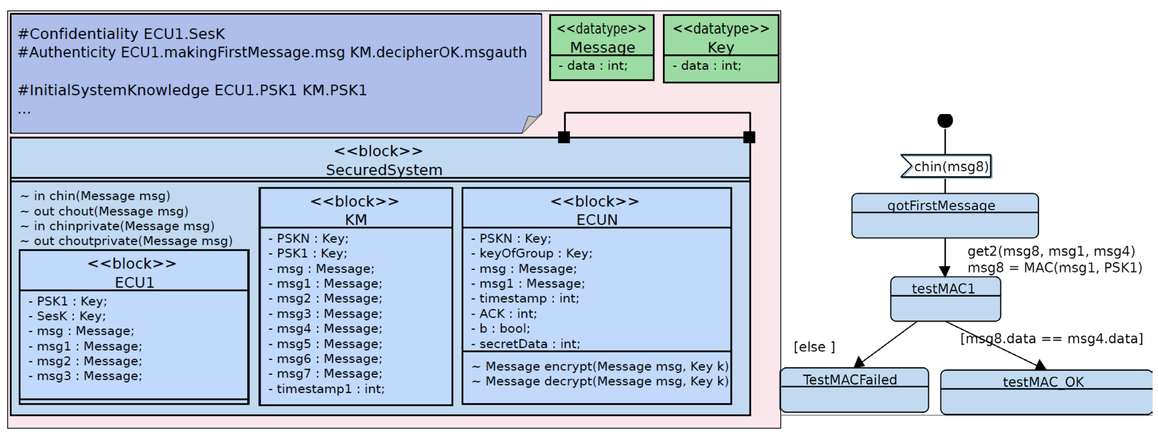
- Where: mapping of functions over architecture assets





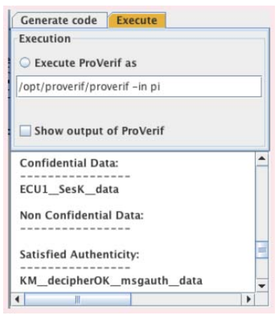
System design

- How: security objectives due to architecture (e.g., network topology, process isolation, etc.)



Formal verification

- Proof based on ProVerif
  - Authenticity, confidentiality
- Press-button approach from TTool



Authors

Ludovic Apvrille (Télécom ParisTech)

Ludovic.Apvrille@telecom-paristech.fr

Yves Roudier (EURECOM)

Tullio Joseph Tanzi (Télécom ParisTech)

Franck Guarnieri (Mines ParisTech)

Partners

Institutions: Télécom ParisTech, EURECOM, Mines ParisTech

Partners: Fondation Télécom, Institut Carnot Télécom & Société numérique

Circuits pour la Sûreté de Fonctionnement

Parties prenantes

Auteurs

Lirida Naviner, Jean-François Naviner, Hervé Petit

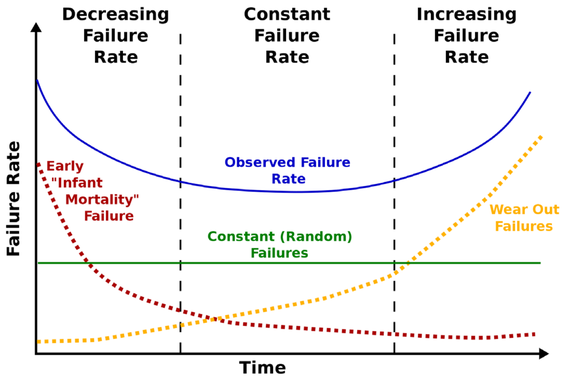
Doctorants : A. Ben Dhia, T. An, K. Liu, S. Sarrazin, C. Bottoni, B. Coeffic, N. Jovanovic, Y. Wang

Post-docs : M. Slimani, H. Cai, M. Costa

Partenaires

SURETE DE FONCTIONNEMENT

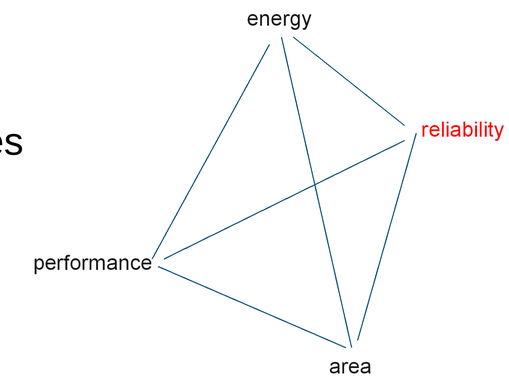
Contexte



- Technologie nanométrique et forte densité d'intégration (Loi de Moore)
- Circuits complexes et performants, mais vulnérables
- Augmentation du nombre de fautes
- Baisse du rendement de fabrication et de la fiabilité
- Industrie électronique « fabless »

Enjeux

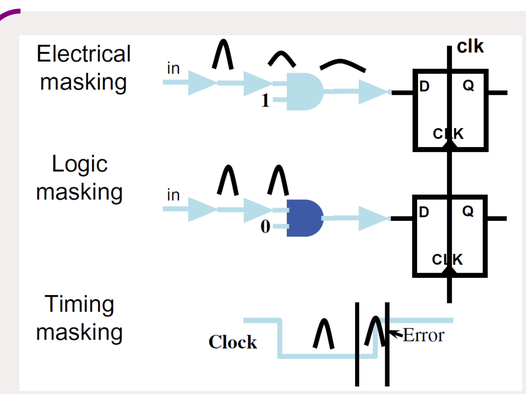
- Conception de systèmes électroniques sûrs et économiquement viables
- Intégration de la fiabilité dans le flot de conception
- Analyse et amélioration de la tolérance aux fautes

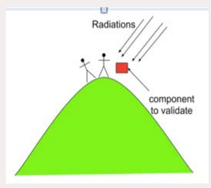


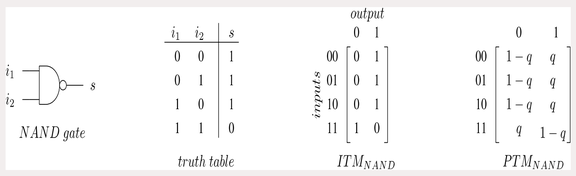
FAUTES TRANSITOIRES ET INTERMITTENTES

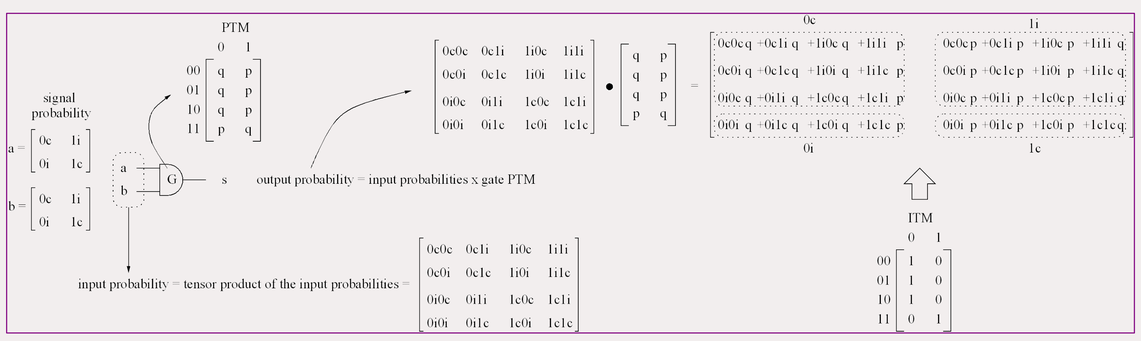
Rayonnement, Variabilité

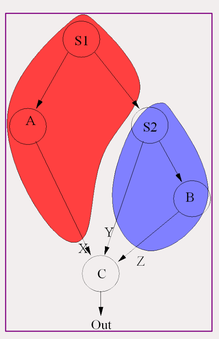
- Analyse de masquage logique
- Test en ligne (fautes de délai)
- Injection de fautes (FIFA)
- Analyse et compensation du bruit
- Durcissement sélectif
- Processeurs tolérants

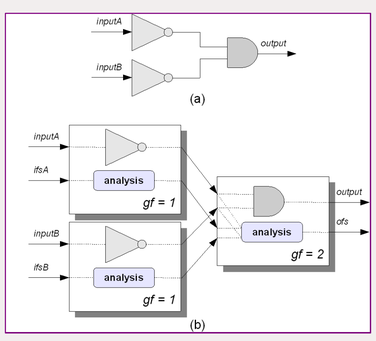


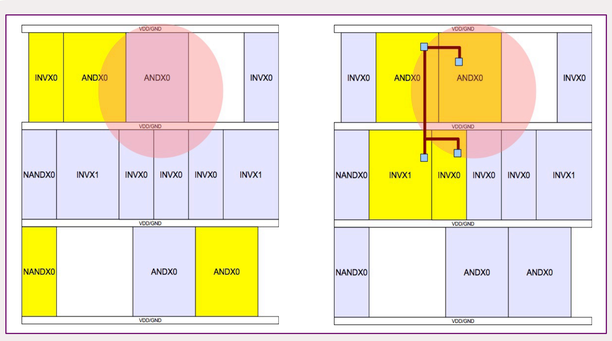


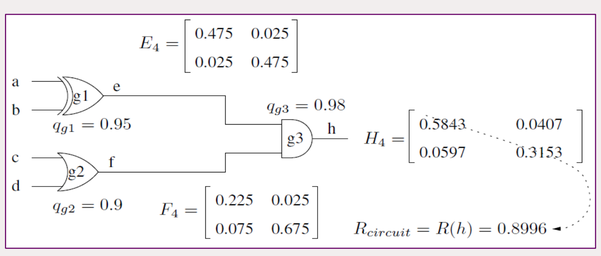


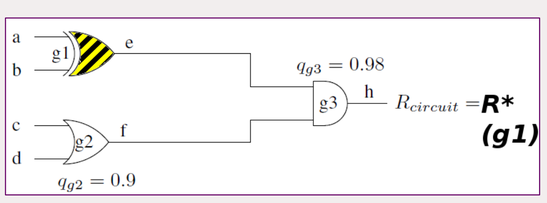








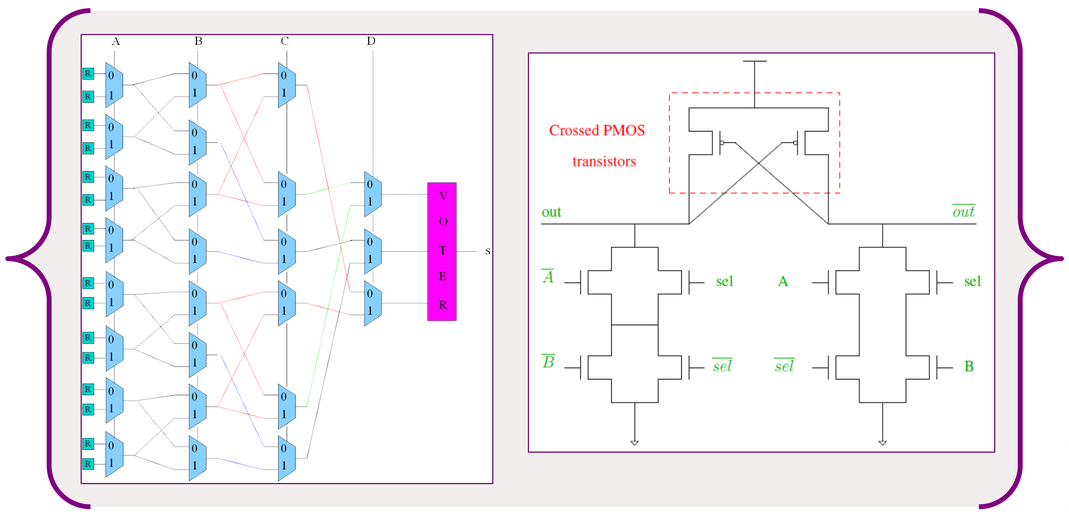




FAUTES PERMANENTES

Défauts de fabrication, Vieillissement

- Durcissement des blocs de base du FPGA
- Architectures robustes: Cross logic, DCVS
- Emulation/injection de défauts et analyse du taux de masquage



Numérique : Grande échelle et complexité

Paris, le 27 mars 2014

Contact lirida.naviner@telecom-paristech.fr

Site web nanoelec.wp.mines-telecom.fr

A geometrical model for selecting optimal countermeasures against multiple attack scenarios

Institut Mines-Télécom

Samovar UMR 5157

Authors

- Gustavo GONZALEZ GRANADILLO
- Hervé DEBAR
- Grégoire JACOB

RST Department

MOTIVATION

- Cyber-attacks are more sophisticated and complex.
- Challenges in the detection and reaction process.
- Huge amount of information from different sources.
- Current solutions do not provide a comprehensive impact analysis of attacks and countermeasures.
- Need of a model to evaluate complex and multiple attack scenarios.

RESULTS

- Quantitative model for evaluating, ranking, and selecting optimal countermeasures.
- Process to evaluate combinations of countermeasures, and select the one with the highest index.
- Deployment of the cost sensitive model over real attack scenarios provided by industrial partners.
- Geometrical model that represents the volume of systems, attacks, and countermeasures based on user accounts, channels, and resources.
- Impact evaluation and graphical representation of multiple attacks and countermeasures.

Context/funding

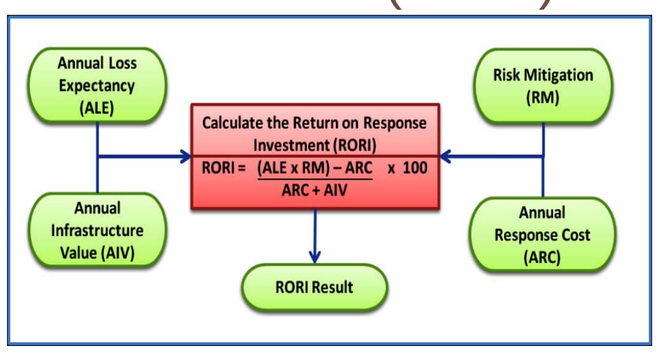
MASTF

SEVENTH FRAMEWORK PROGRAMME

ADAX

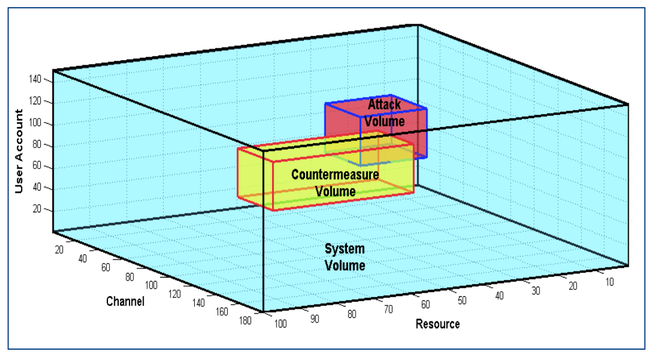
PROPOSAL

Return On Response Investment (RORI)



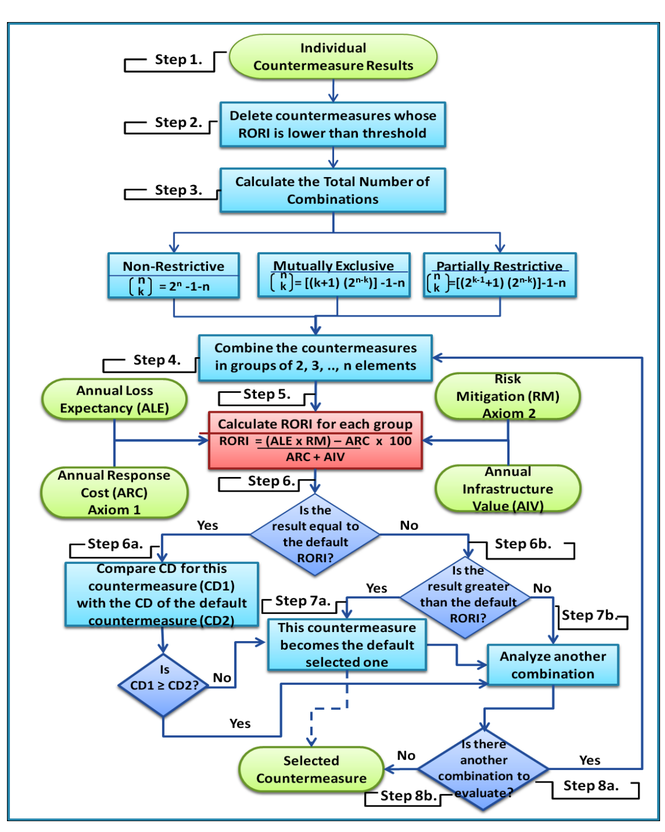
- **ALE:** Annual impact cost obtained in the absence of security countermeasures.
- **AIV:** Fixed costs expected on the system due to services, renting, and equipment maintenance.
- **RM:** Risk mitigation level associated to a particular countermeasure.
- **ARC:** Annual response cost incurred by implementing a new security action.

Attack Volume Model



- **System Volume:** Maximal space a given system is exposed to attackers.
- **Attack Volume:** Portion of the system that is targeted by a given attack based on the vulnerabilities it can exploit.
- **Countermeasure Volume:** Level of action a security solution has on a system over a given attack.

Countermeasure Selection Process

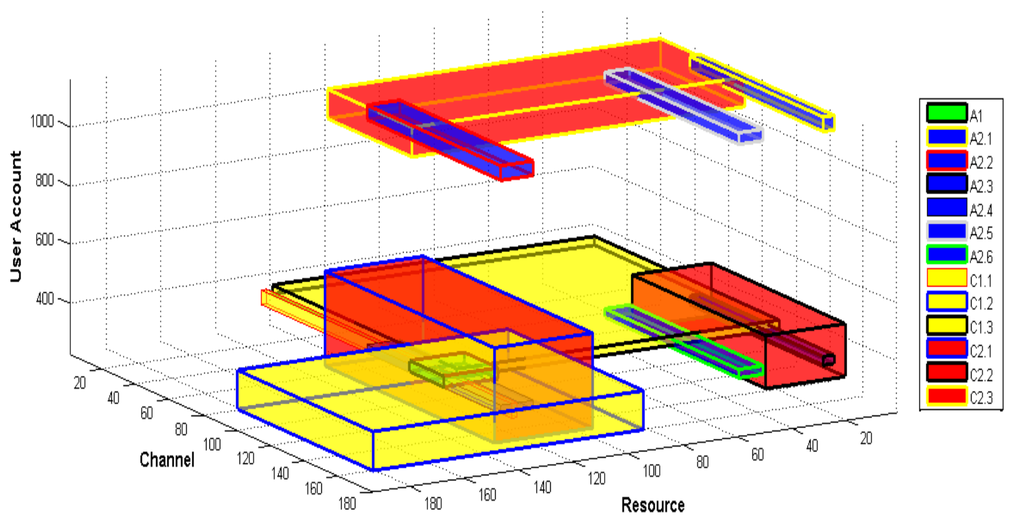


EXAMPLE

Multiple attacks detected at Telecom SudParis, France

Element	User Account	Channel	Resource	Volume (units^3)
System	U1:U3691	Ch1:Ch4512	R1:R993	430,106,901,440
Attack 1	U340:U377	Ch100:Ch120	R110:R130	904,932
Attack 2	U320:U349& U1110:U1159	Ch70:Ch149	R5:R9& R31:R40& R115:R127	8,380,800
CM 1.1	U300: U349	Ch1: Ch149	R121: R123	1,206,900
CM 1.2	U301: U433	Ch100: Ch179	R94: R193	57,456,000
CM 1.3	U330: U360	Ch1: Ch110	R1: R119	25,411,320
CM 2.1	U229: U550	Ch50: Ch110	R94: R130	35,124,840
CM 2.2	U270: U449	Ch70: Ch149	R1: R30	56,052,000
CM 2.3	U1030: U1130	Ch40: Ch90	R1: R123	14,551,218

Graphical representation of attacks and countermeasures



ITEA 2

INFORMATION TECHNOLOGY FOR EUROPEAN ADVANCEMENT

Contact gustavo.gonzalez_granadillo@ telecom-sudparis.eu

Site web www.telecom-sudparis.eu

Preuve formelle de la sécurité d'une application ferroviaire de signalisation en modes nominal et dégradés

Parties prenantes

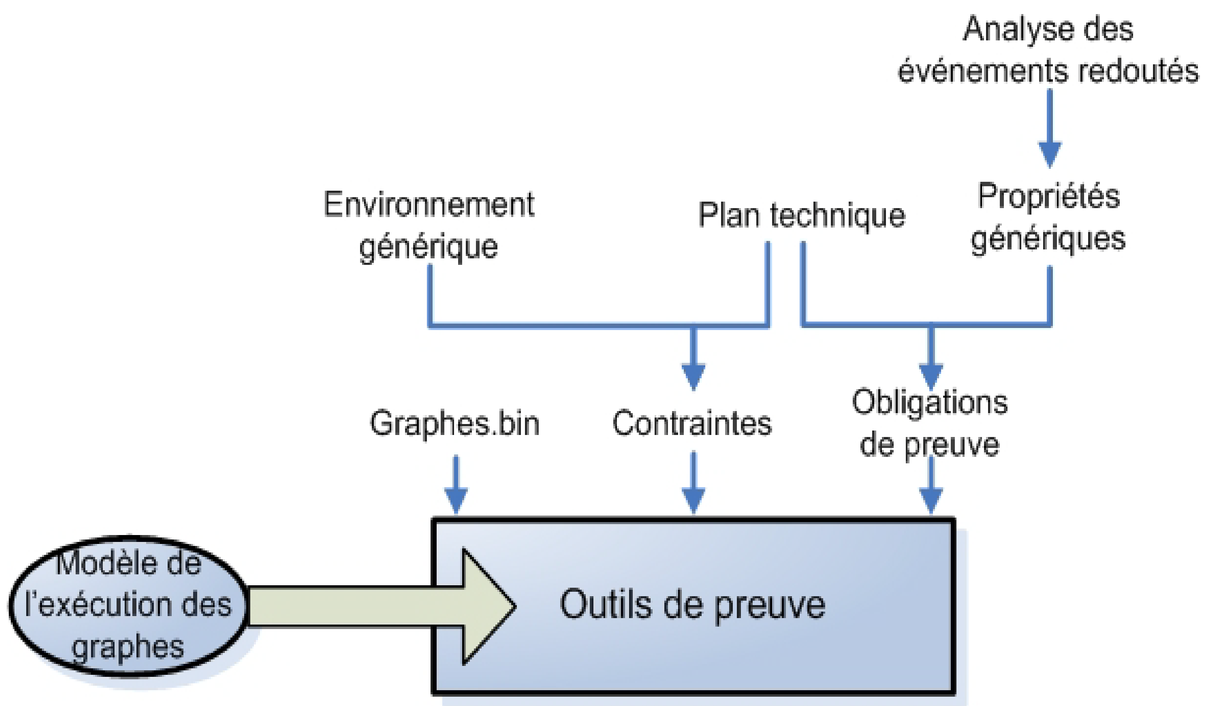
Auteurs

Amel Mammar (TSP)
Jean-Marc Mota (Thalès)

Approche générale par la preuve

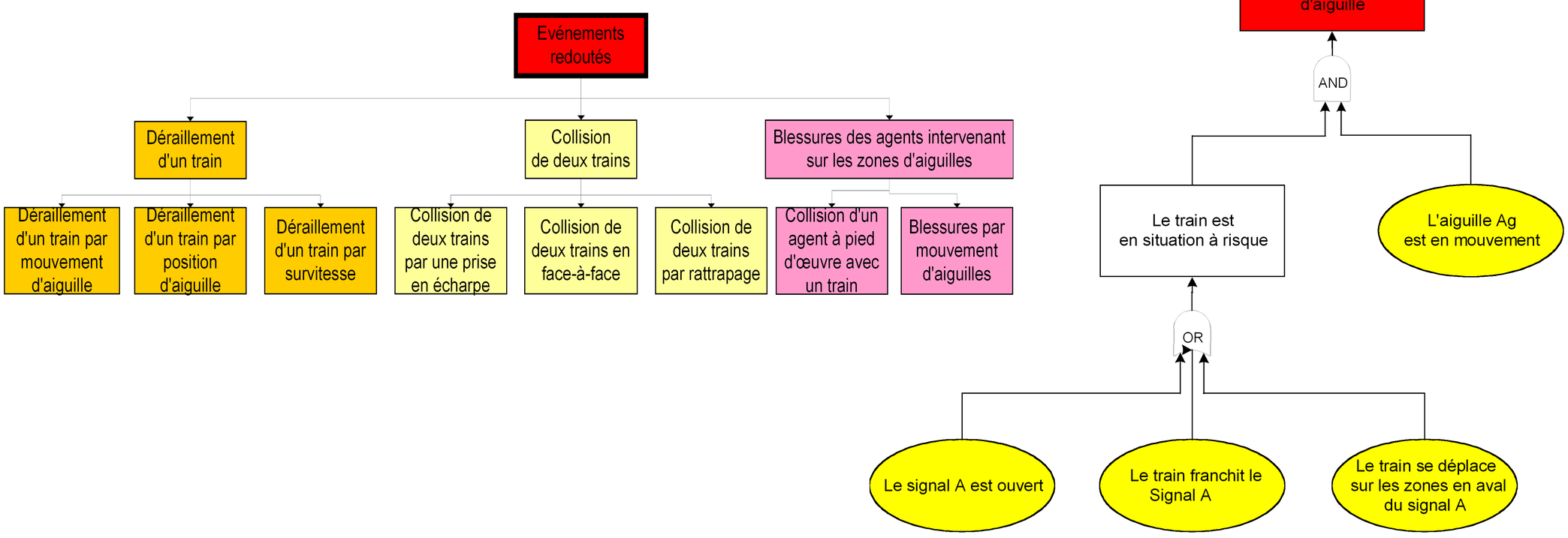
Objectifs

- Définir les différents scénarios menant aux situations redoutées
- Prendre en compte les défaillances possibles des éléments matériels
- Modéliser les scénarios par des propriétés de sécurité

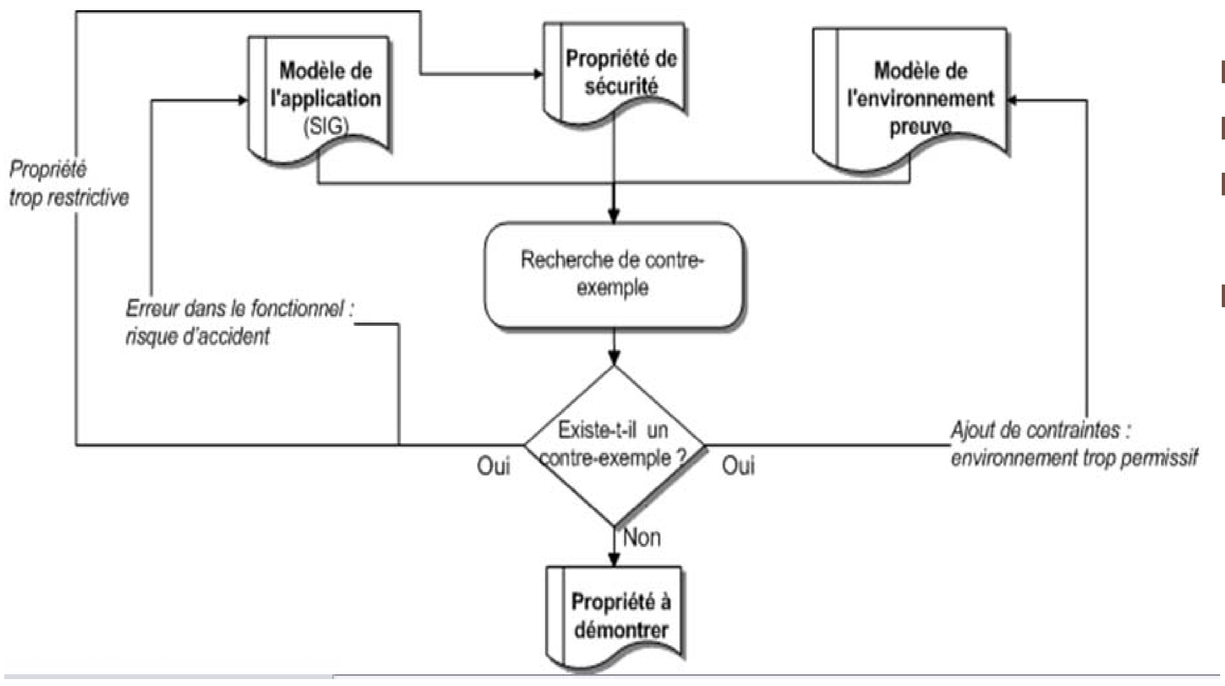


Analyse des événements redoutés

- Utilisation des arbres de fautes
- Démarche par raffinement d'événements



Preuve et modélisation de l'environnement par recherche de contre-exemples



- Une aiguille ne peut être simultanément à droite et à gauche
- Une aiguille ne change pas de position sans être commandée
- Une aiguille a besoin d'au moins deux cycles pour passer d'une position droite (resp. gauche) à une position gauche (resp. droite)
- Les actions de l'agent à pied d'œuvre sont conformes à la sécurité (modes dégradés)

colloque Institut Mines-Télécom "Numérique : Grande échelle et complexité"

Mars 2014

Contact amel.mammar@telecom-sudparis.eu Site web www. -public.it-sudparis.eu/~mammar_a/