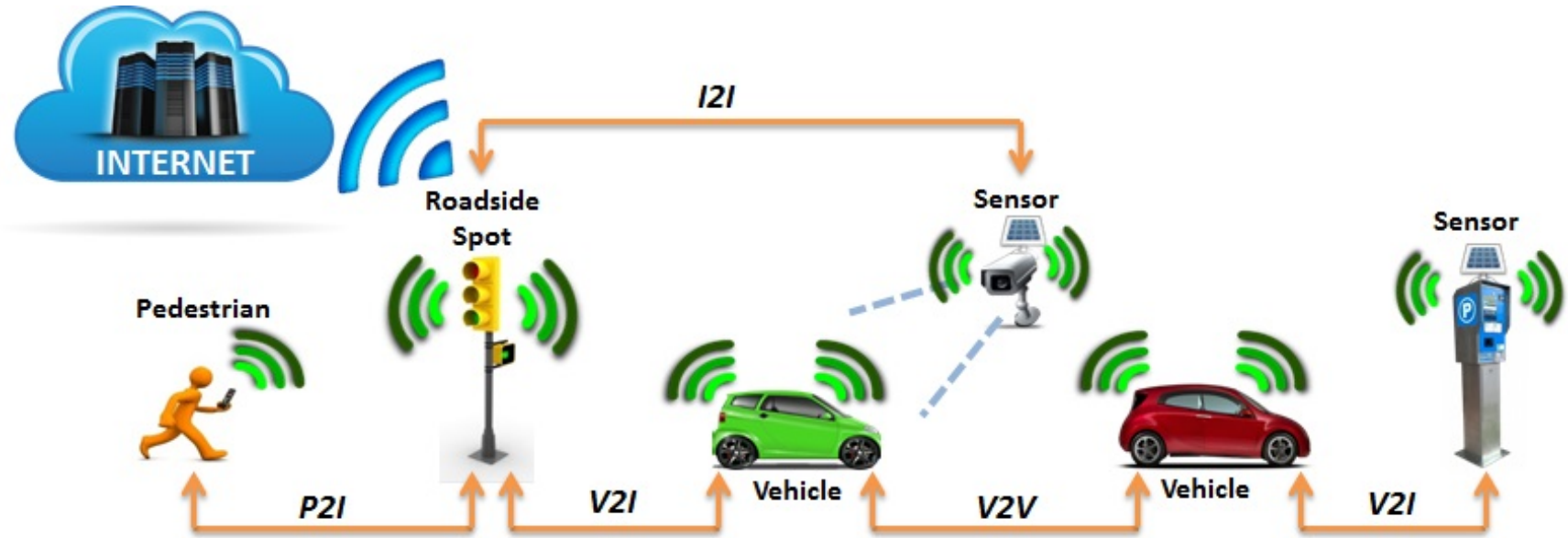
Security in connected autonomous vehiculars

Pascal Lafourcade

7 January 2019

LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

VANET : Vehicular Ad-hoc NETworks



Communications

- V2V: Vehicular to Vehicular
- V2I: Vehicular to Infrastructure
- I2I: Infrastructure to Infrastructure
- P2I: Pedestrian to Infrastructure

Challenges in VANETs

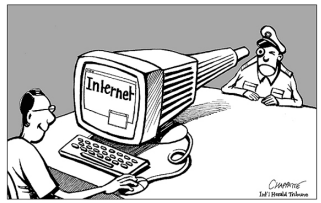
- Mobility
- Connection volatility
- Privacy vs Authentication
- Network scalability
- Bootstrap
- Security

Security Requirements in VANETs

Data exchanged play a VITAL role in traffic safety.

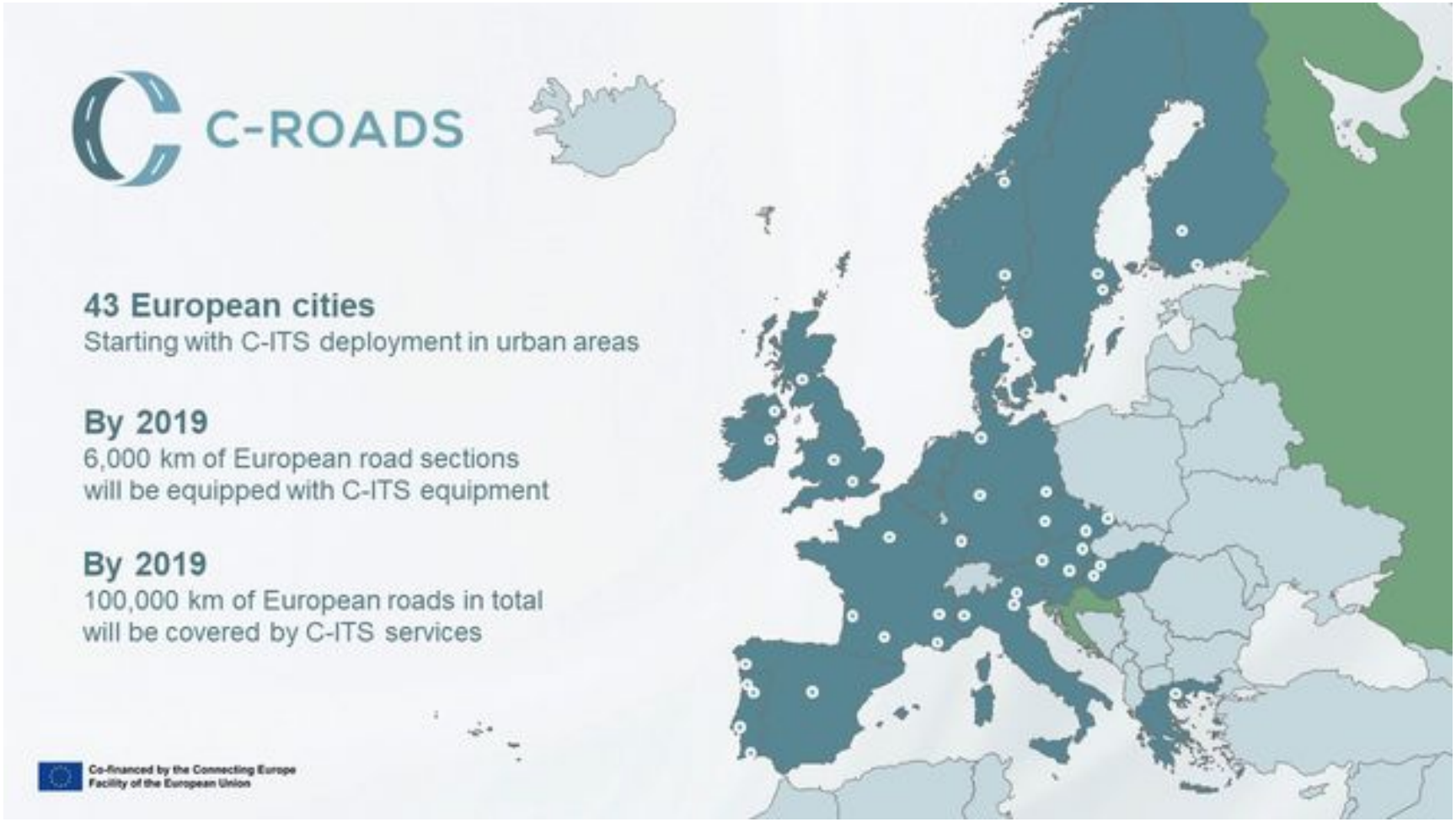
Properties

- Data Integrity
- Data Confidentiality
- Data Privacy
- Authentication
- Non-repudiation
- Avaibility
- Realtime constraints



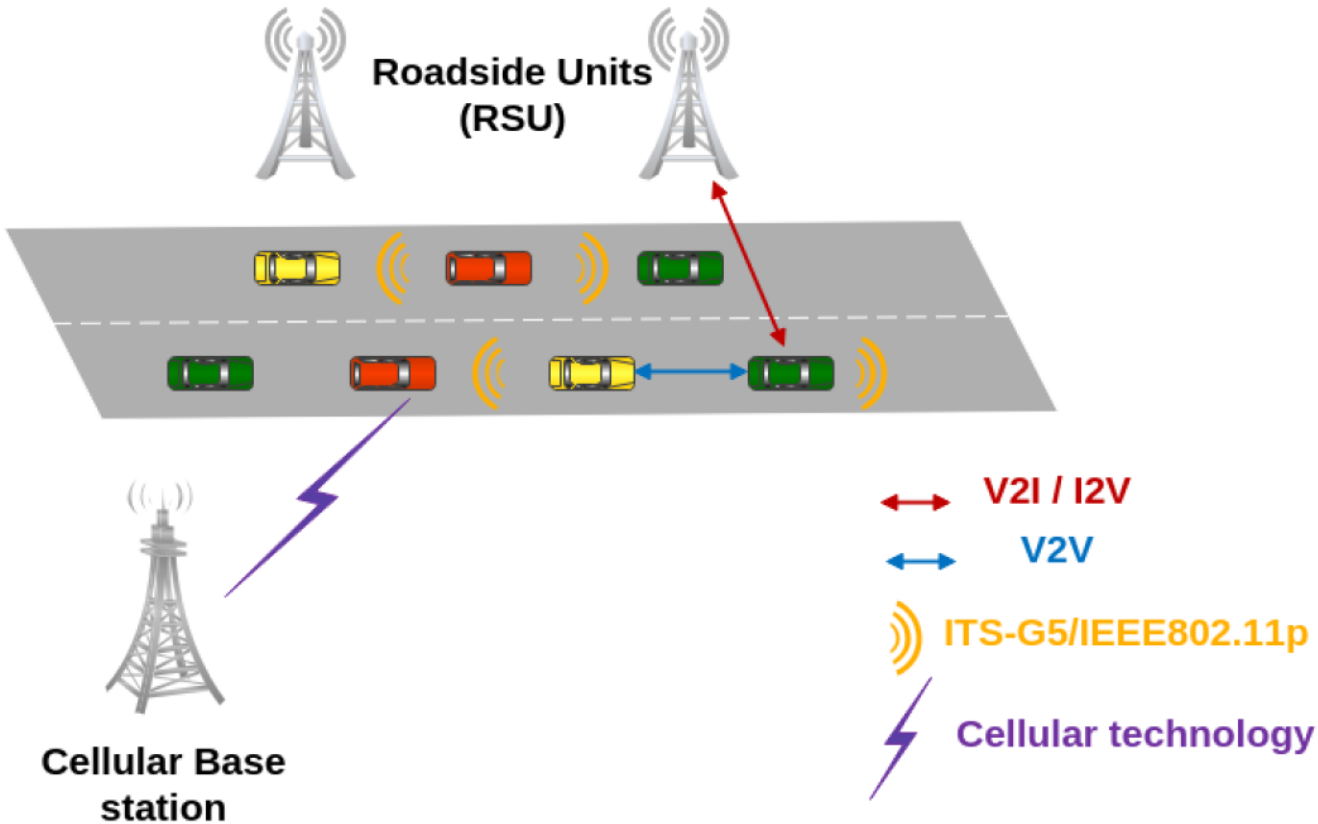
Outline

Outline

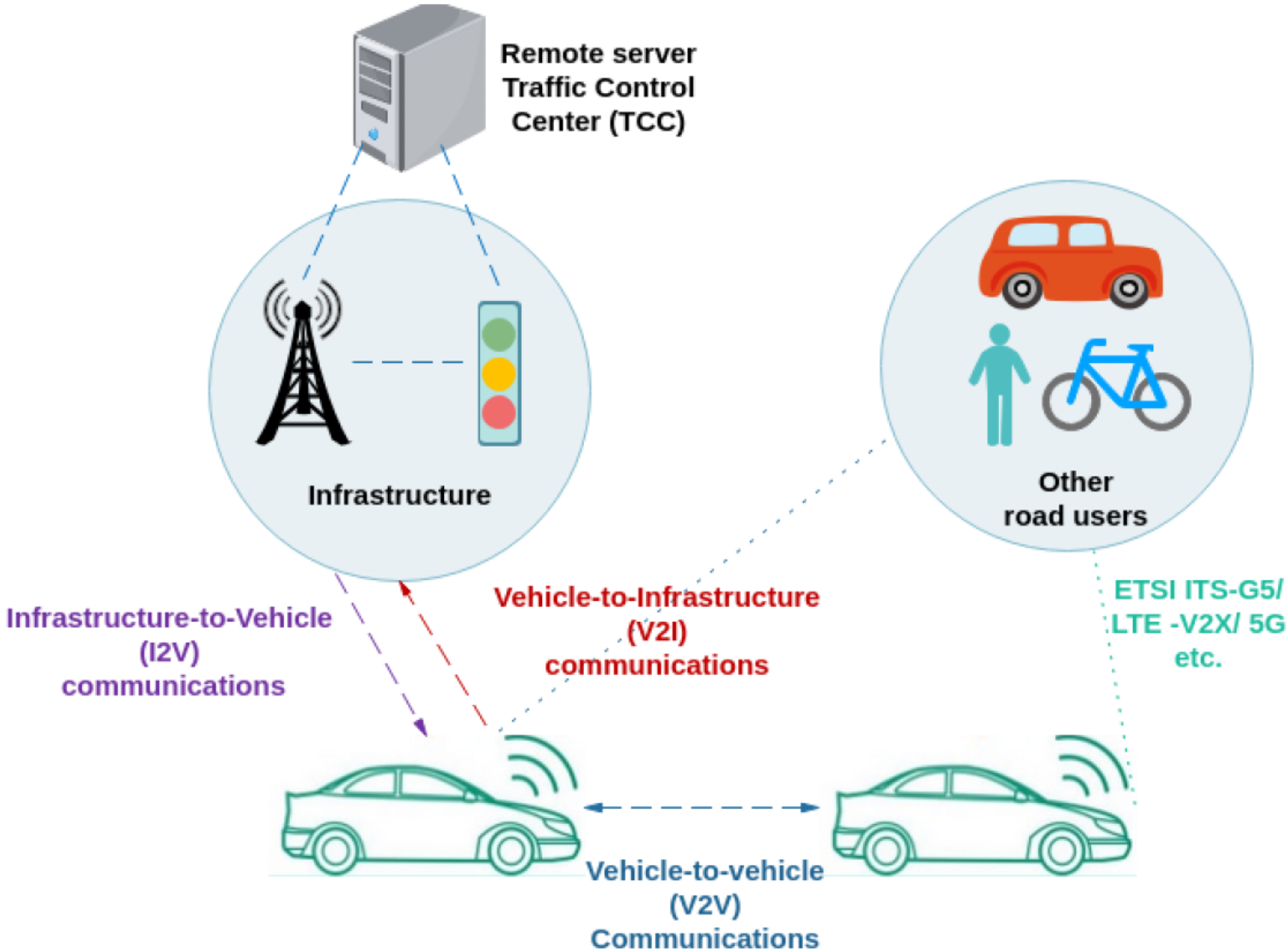

C-ROADS
43 European cities
Starting with C-ITS deployment in urban areas
By 2019
6,000 km of European road sections
will be equipped with C-ITS equipment
By 2019
100,000 km of European roads in total
will be covered by C-ITS services
Co-financed by the Connecting Europe
Facility of the European Union

Cooperative Intelligent Transport Systems (C-ITS)

- C-ITS communications.
- ETSI ITS-G5/Cellular technology.

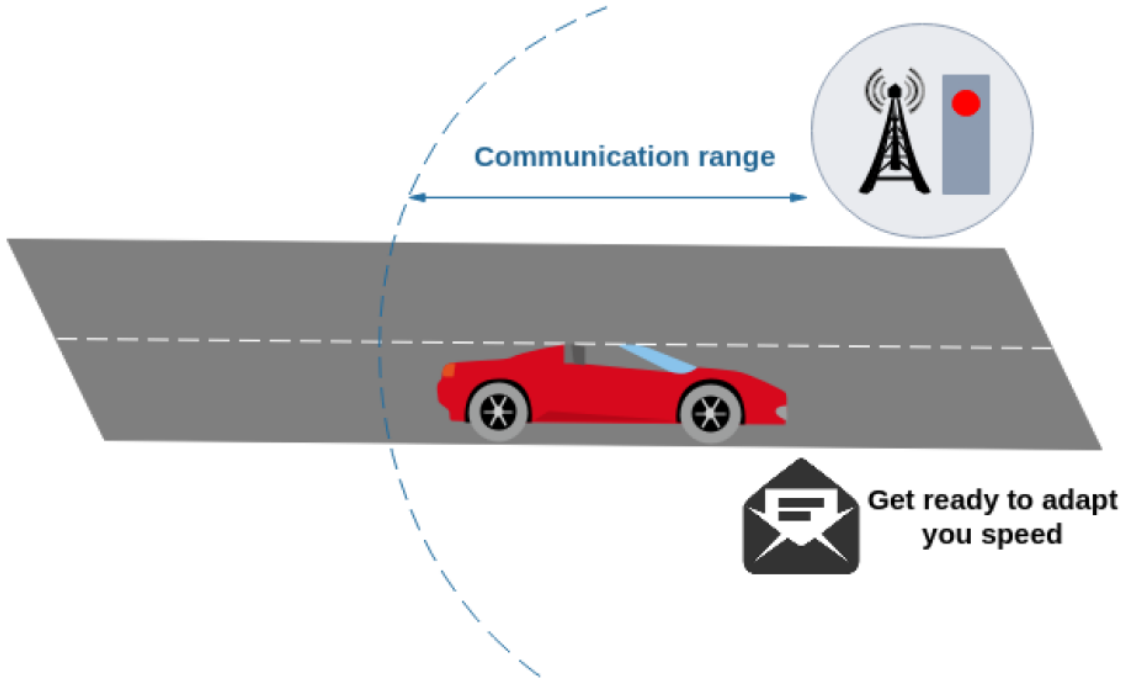


Cooperative Intelligent Transport Systems (C-ITS)

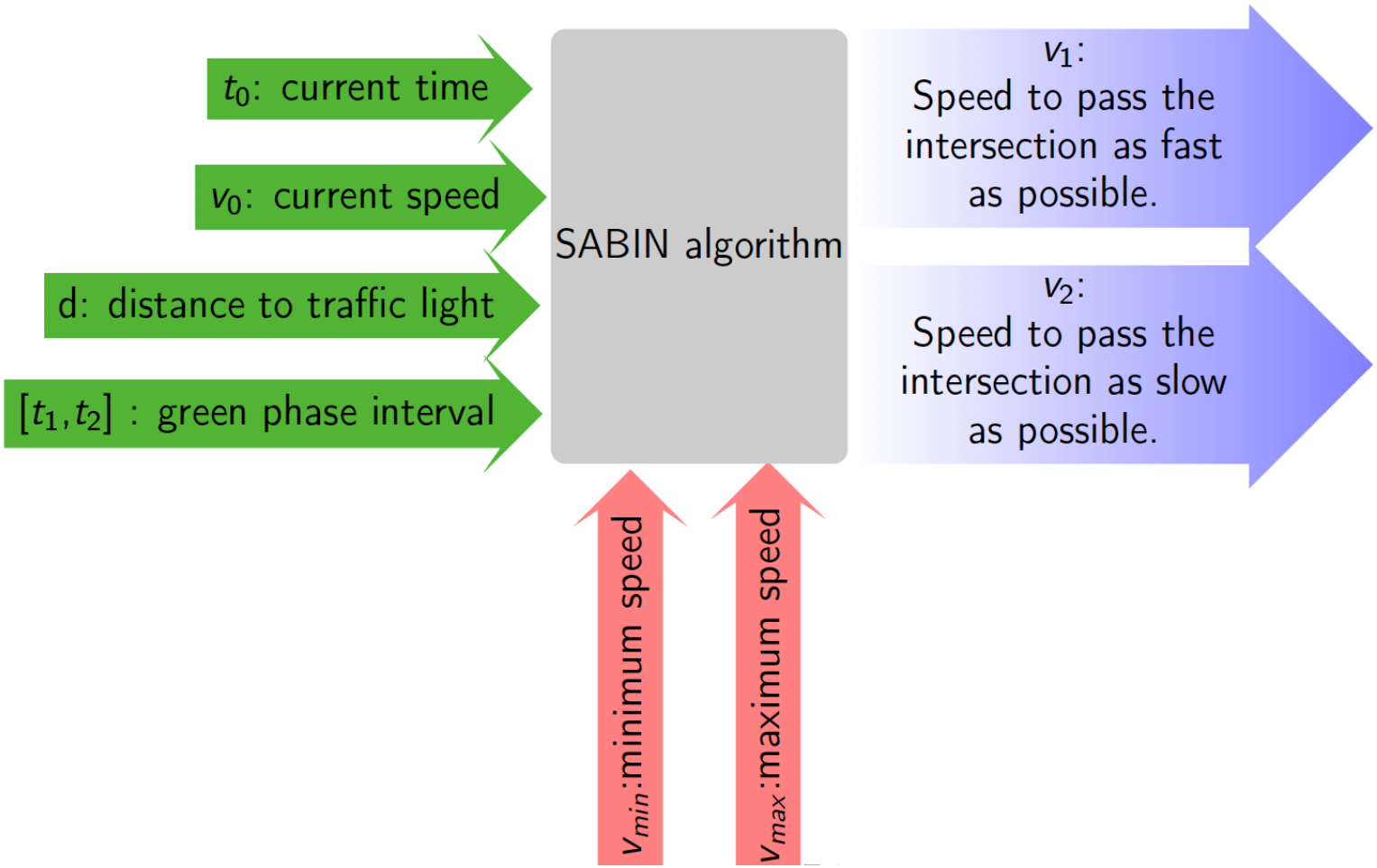


Green Light Optimal Speed Advisory (GLOSA)

A traffic efficiency C-ITS service that uses **Infrastructure-to-vehicle (I2V)** communication mode.



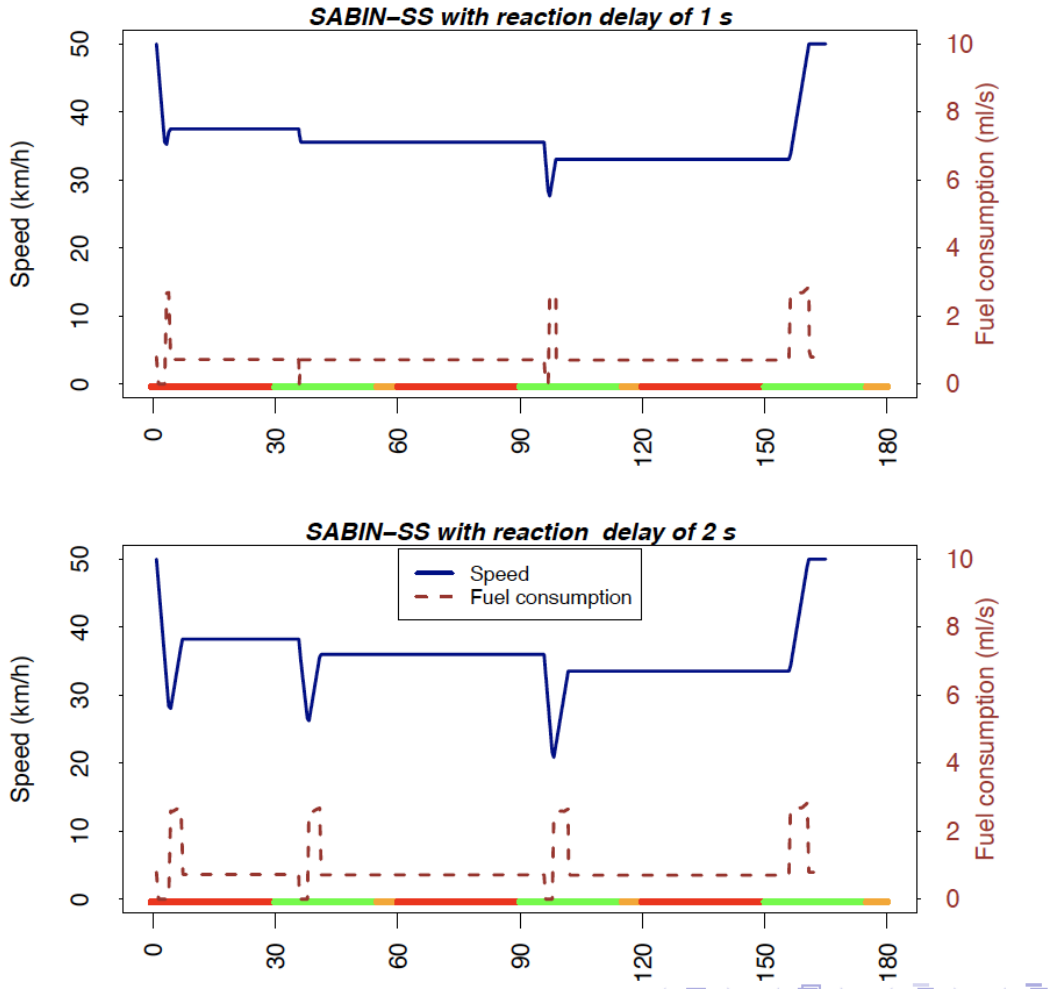
Speed Advisory Boundary fINder (SABIN)



Mouna Karoui, Antonio Freitas, Gérard Chalhoub

LIMOS
LABORATOIRE D'INFORMATIQUE, DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

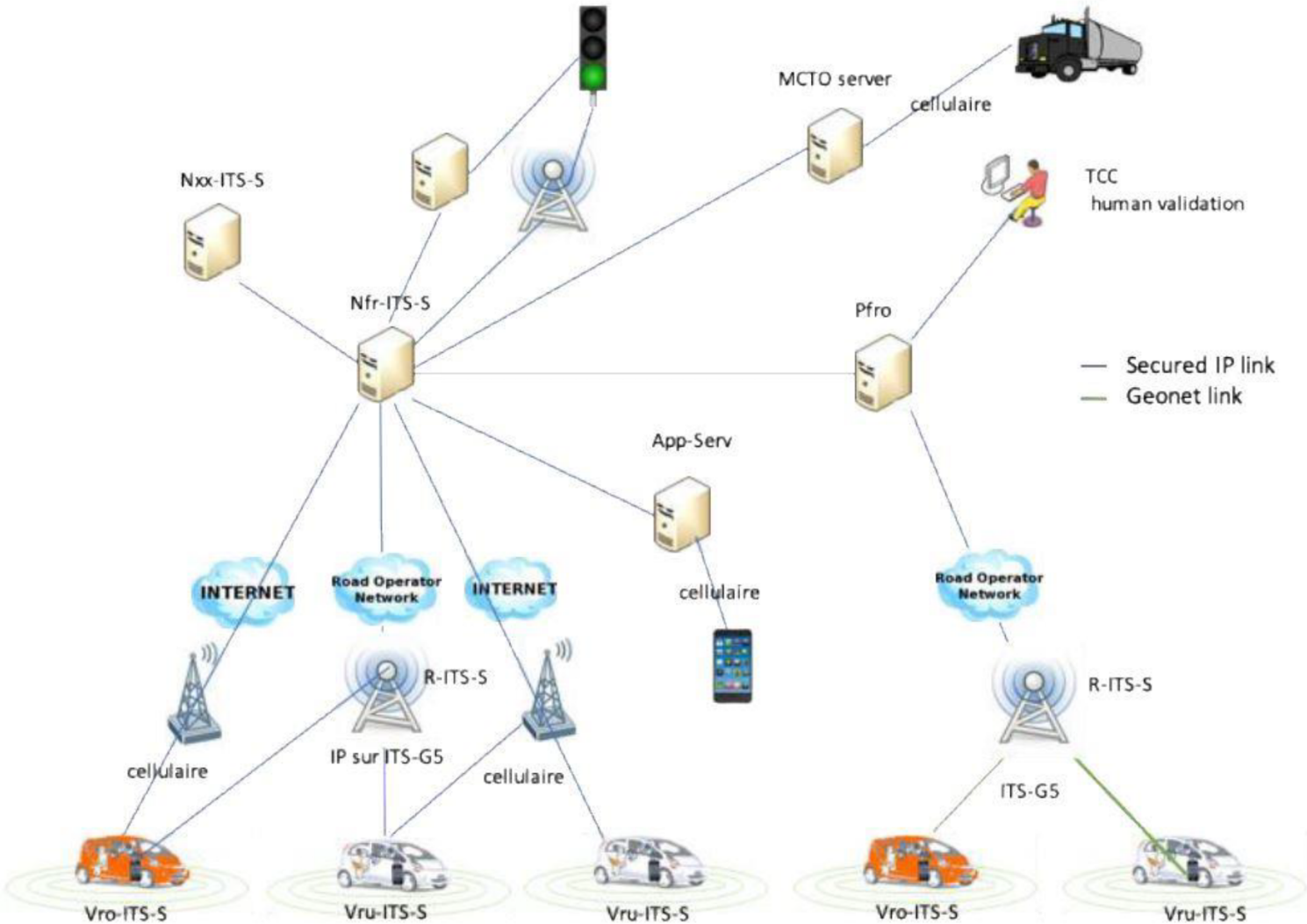
Evaluation of SABIN



Mouna Karoui, Antonio Freitas, Gérard Chalhoub

LIMOS
LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Infrastructure



InDid (2019-2024)

Outline

Clef symétrique

Exemples

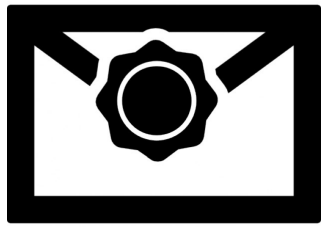
- DES
- AES

Chiffrement à clef publique

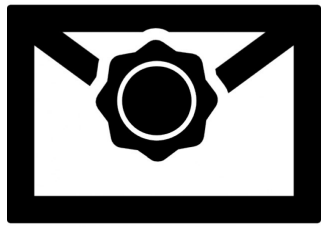
Exemples

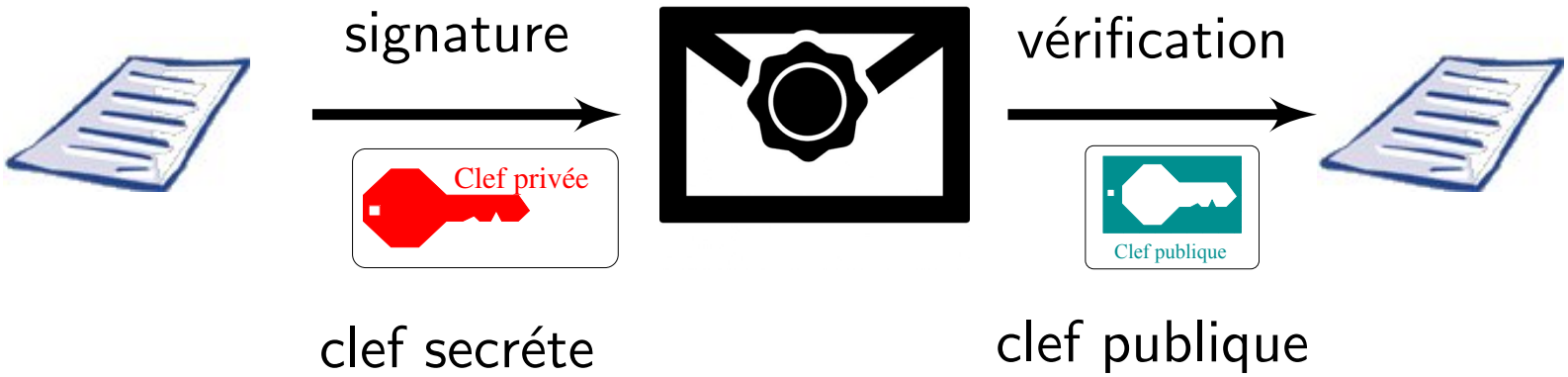
- RSA : $c = m^e \mod n$
- ElGamal : $c \equiv (g^r, h^r \cdot m)$

Signature



Signature





RSA: $m^d \mod n$

PKI : Public Key Infrastructure

- Utiliser des clefs publiques
- Établir une clef symétrique de session
- Confiance
- Certificats
- Authorité de certifications
- Chaîne de confiance

Public Key Infrastructure (PKI)

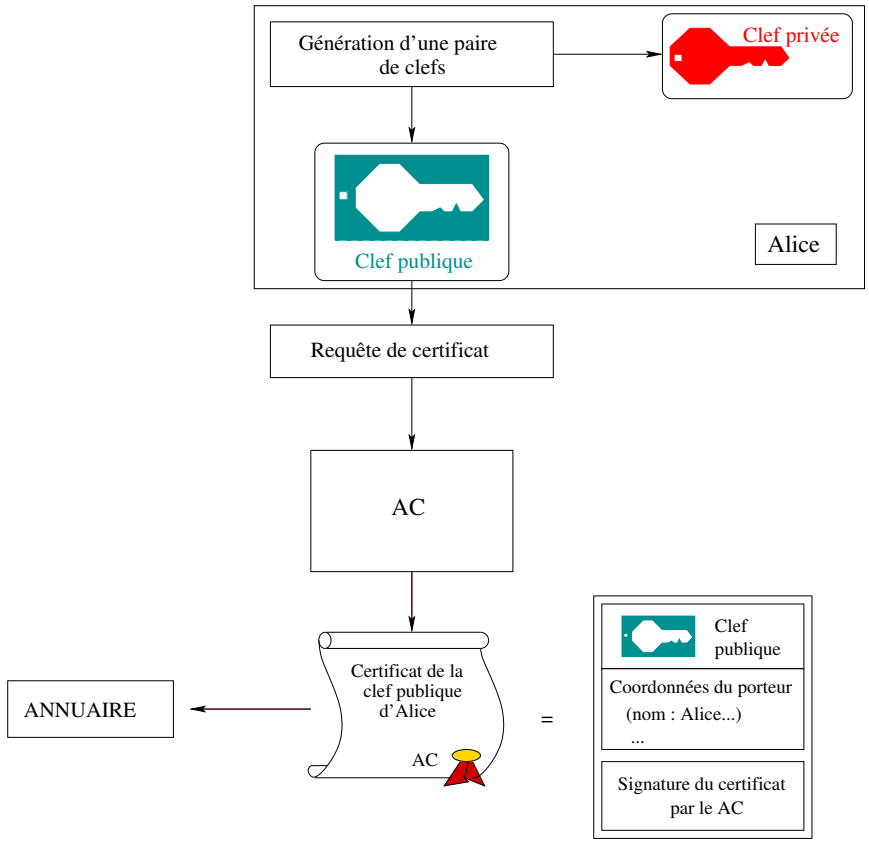
Principales fonctionalités d'une PKI

- Création d'une paire de clef
- Génération d'un certificat
- Remise du certificat au porteur
- Publication des certificats
- Vérification des certificats
- Révocation des certificats (CRL)

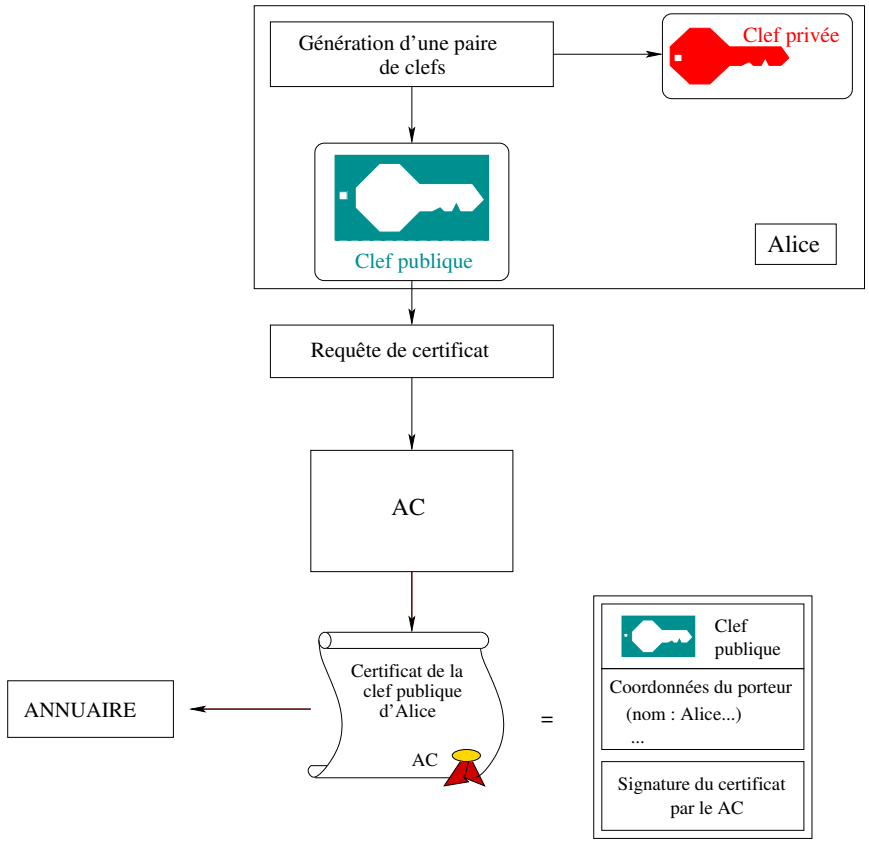
AC : Authorité de Certification

AE : Authorité d'Enregistrement

Public Key Infrastructure (PKI)



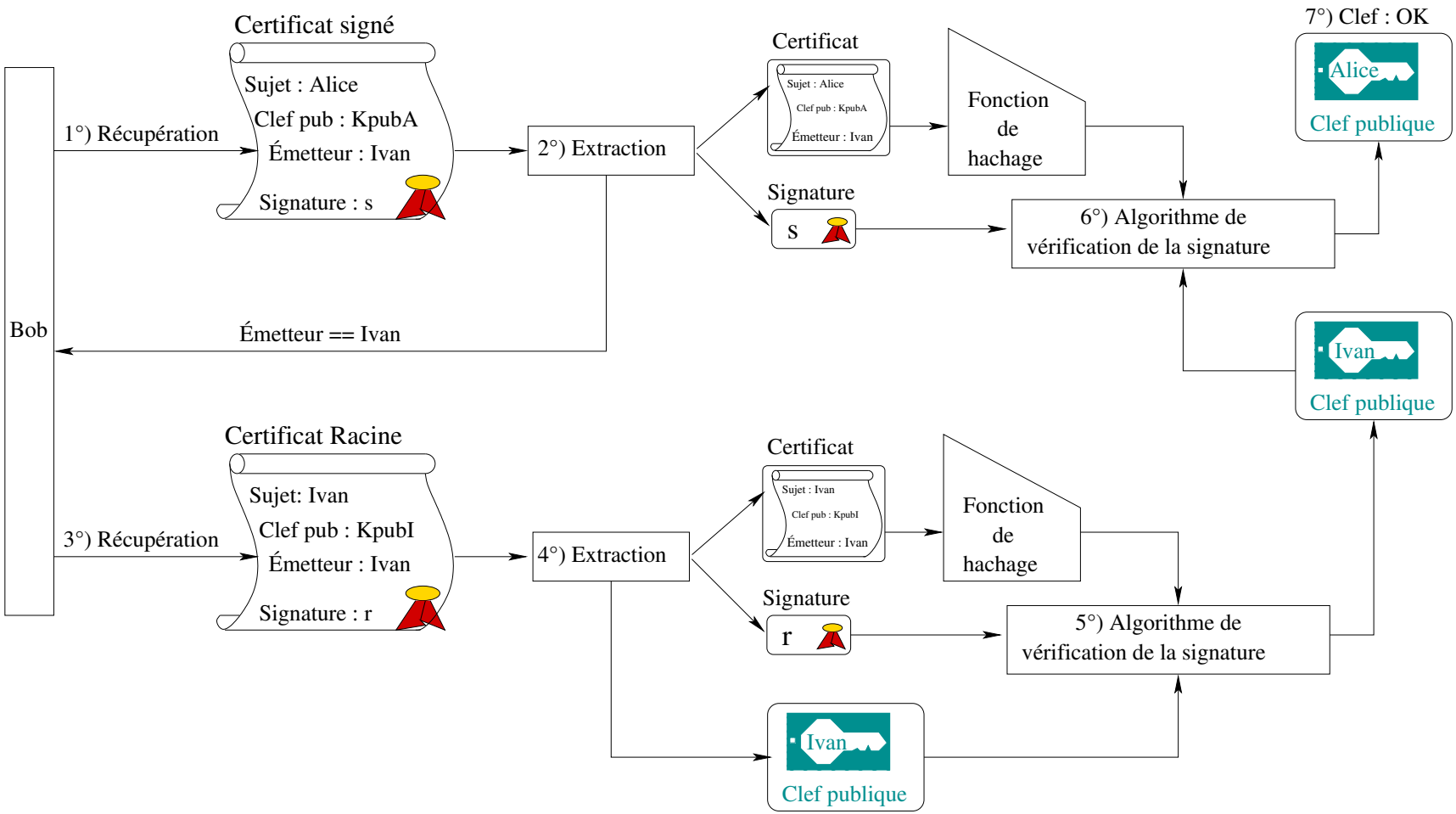
Public Key Infrastructure (PKI)



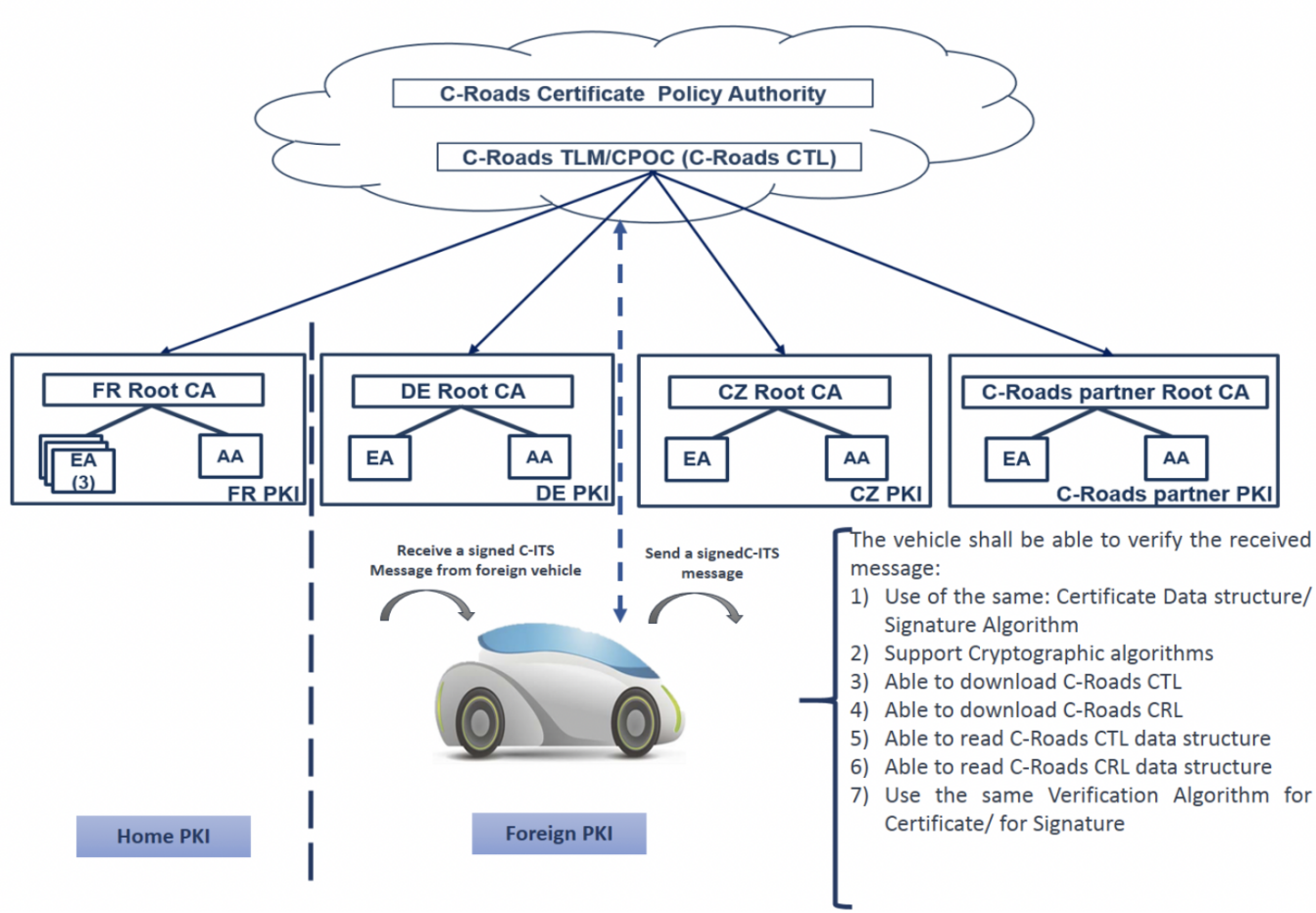
Authentification de l'AC confiance assurée par

- Chaîne de certificats
- Certificat racine ou certificat auto-signé

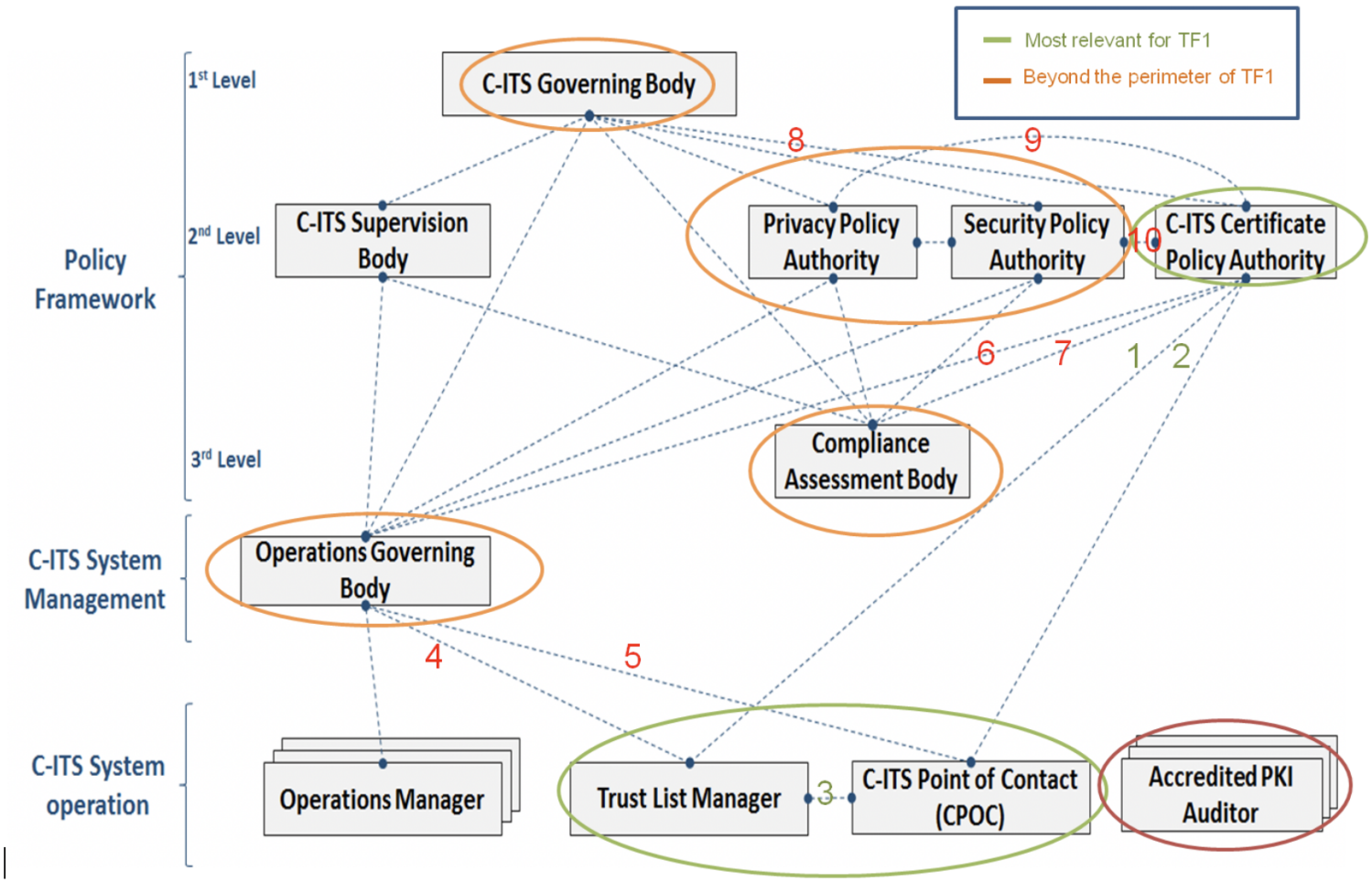
Vérification



Interoperability



PKI Management

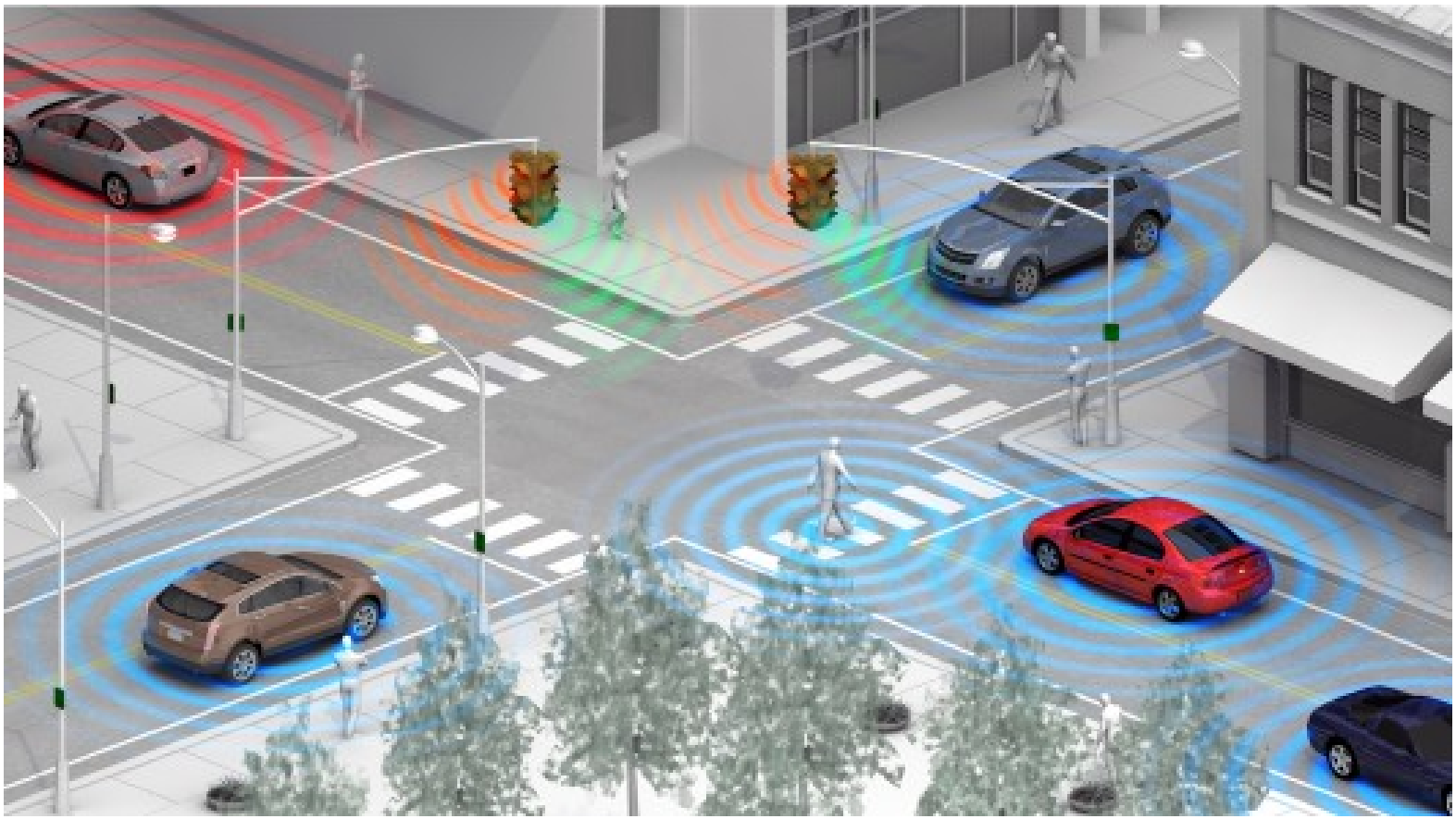


PKI Security Challenges

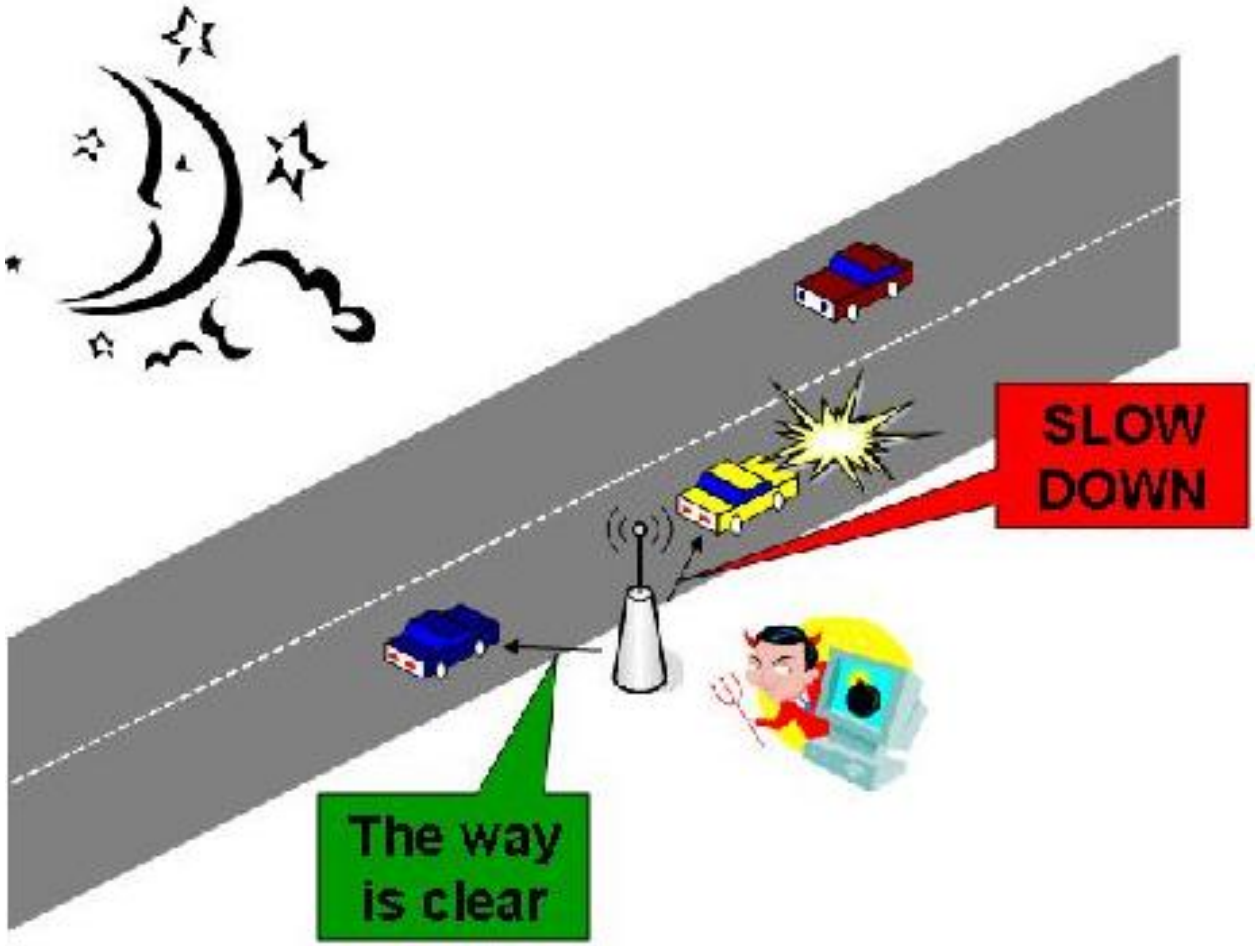
- Key management
- Privacy
- Interoperability
- Different countries

Outline

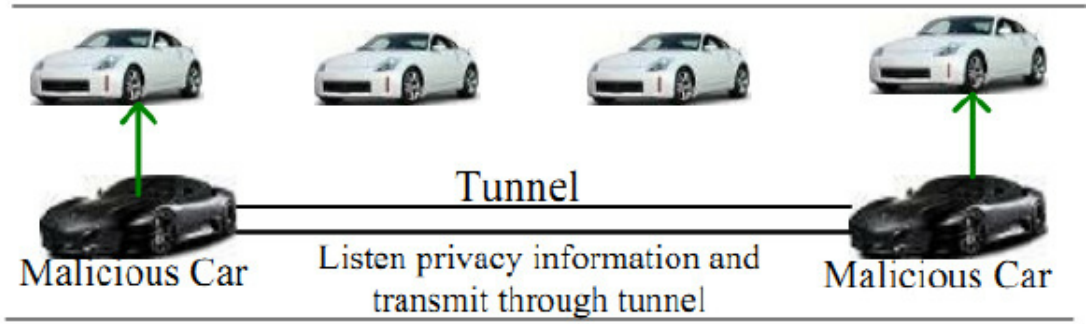
V2V and V2I



Attack on Infrastructure



Wormhole Attack



Proximity Devices Everywhere

What features do we want?

- Security
- Privacy

Examples of Attacks

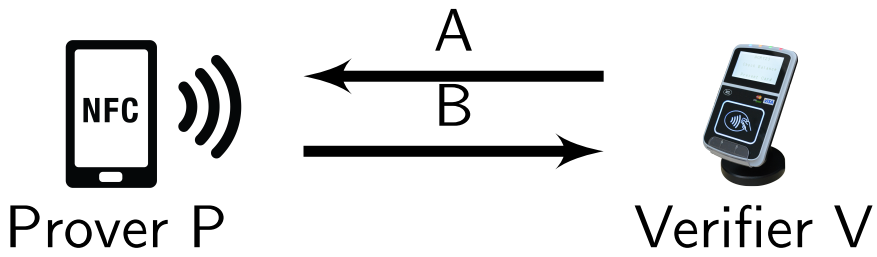
2 VIDEOS

- Achats de tickets de transport
- Ouverture de voiture

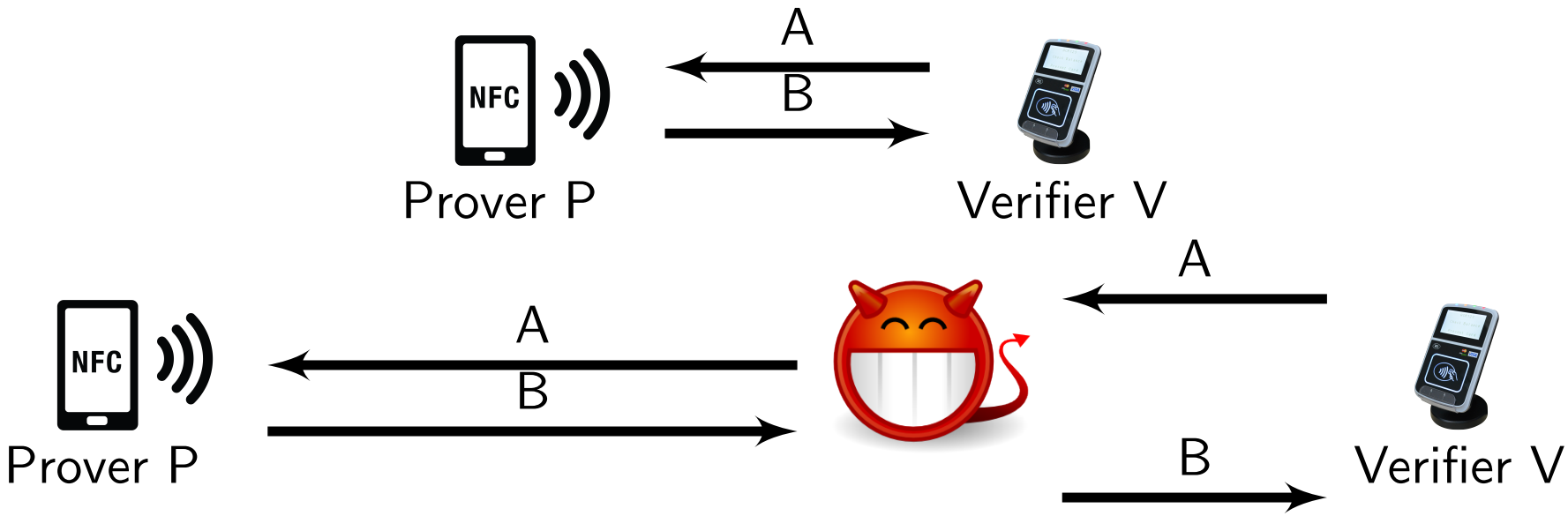
Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars, by Aurélien Francillon, Boris Danev, Srdjan Capkun, NDSS 2011

`https://www.youtube.com/watch?v=bfjMj8fgsBo`

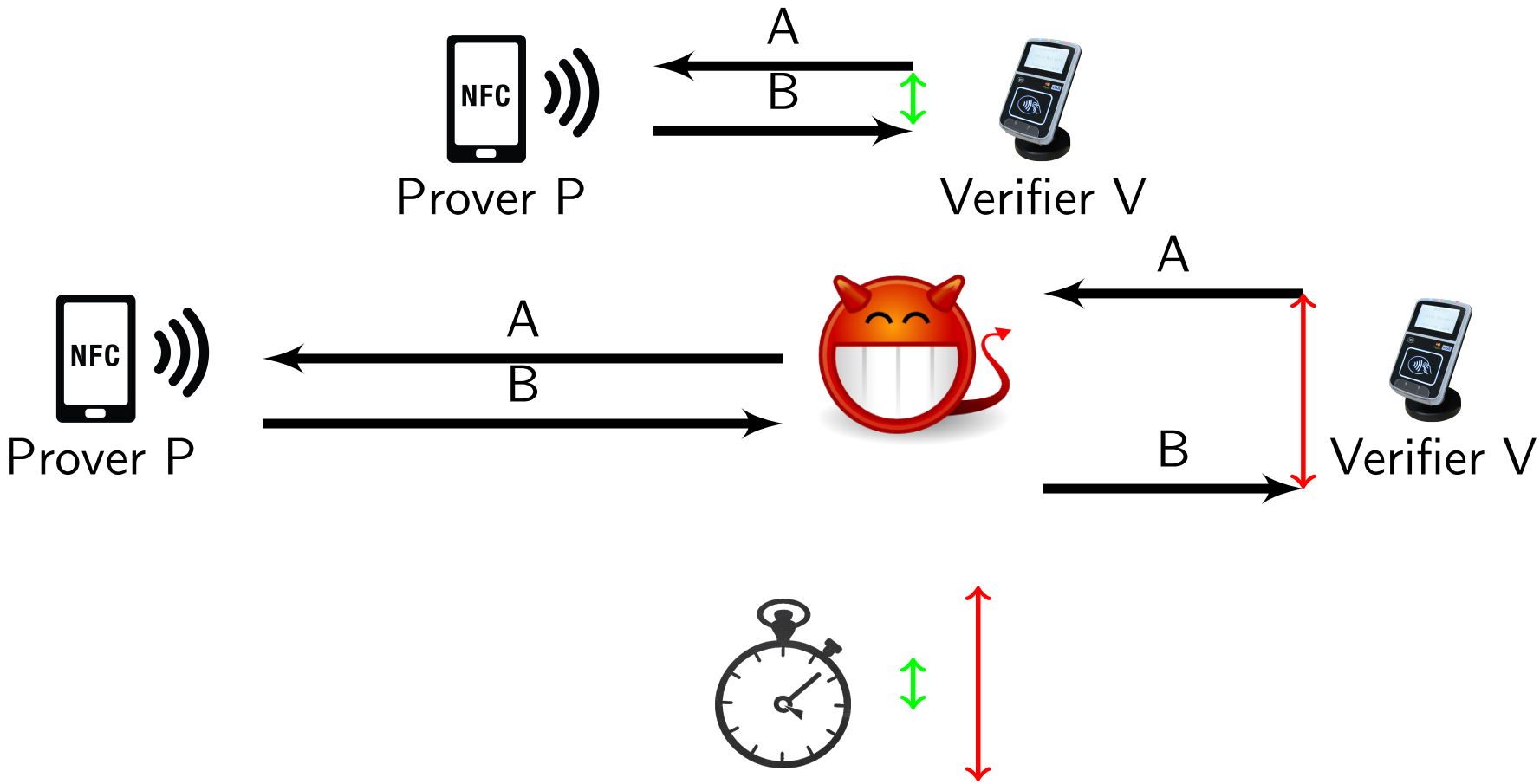
Security: Relay Attacks (Mafia Fraud)



Security: Relay Attacks (Mafia Fraud)

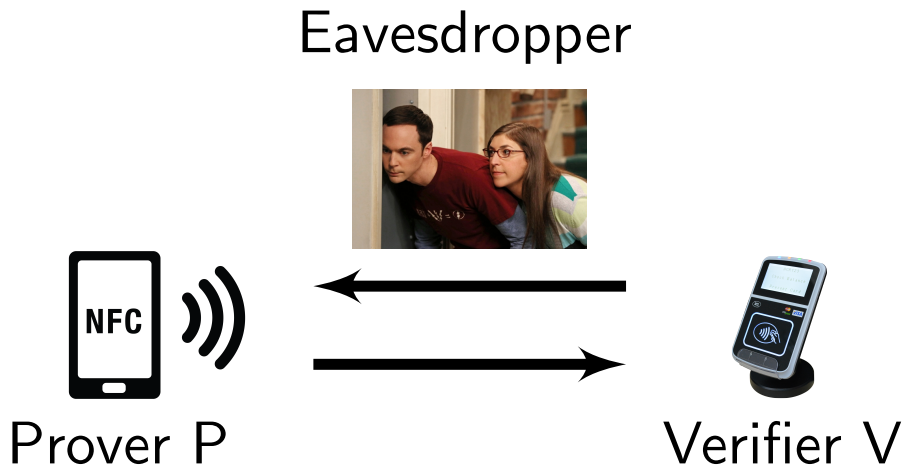


Security: Relay Attacks (Mafia Fraud)

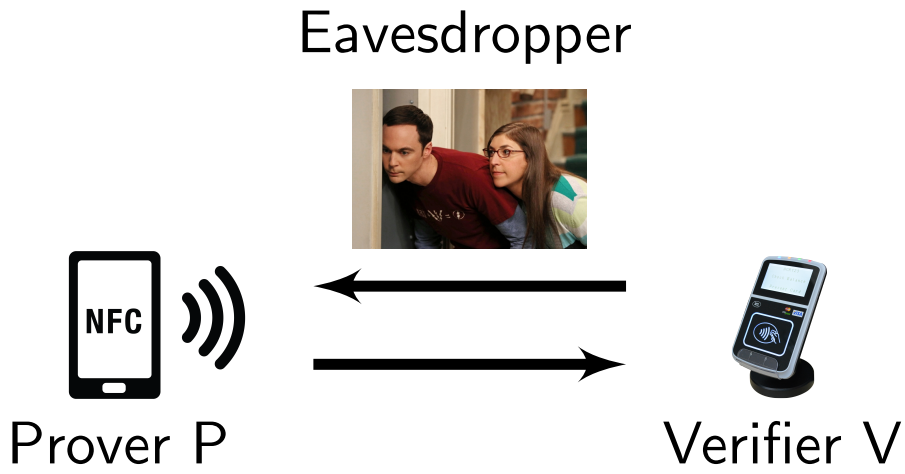


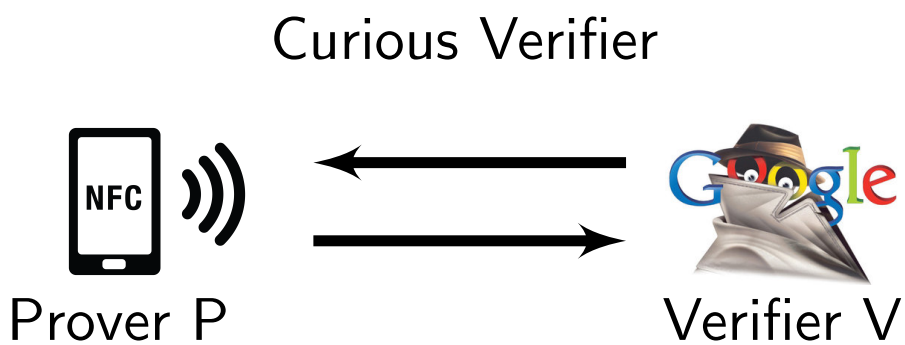
Solution: distance bounding (Brands and Chaum, 1991)

Privacy: Eavesdropper VS Curious Verifier



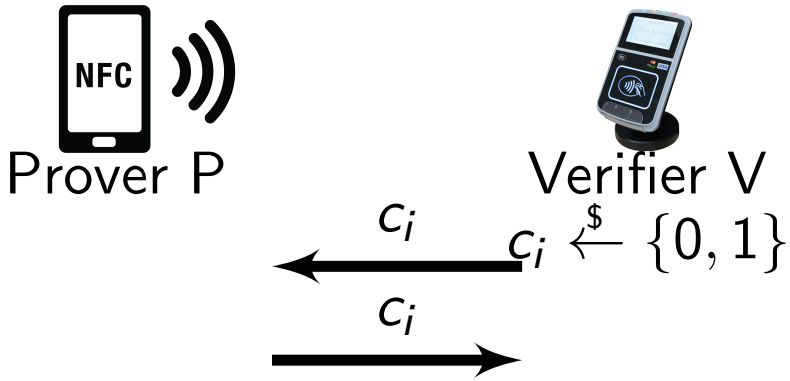
Privacy: Eavesdropper VS Curious Verifier





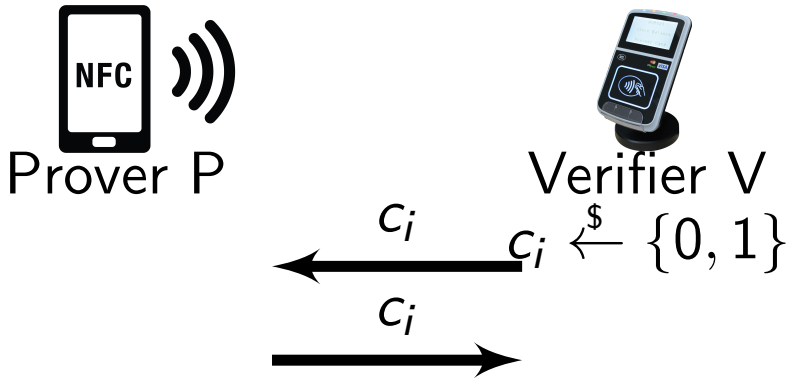
Some Naive Examples

Echo protocol

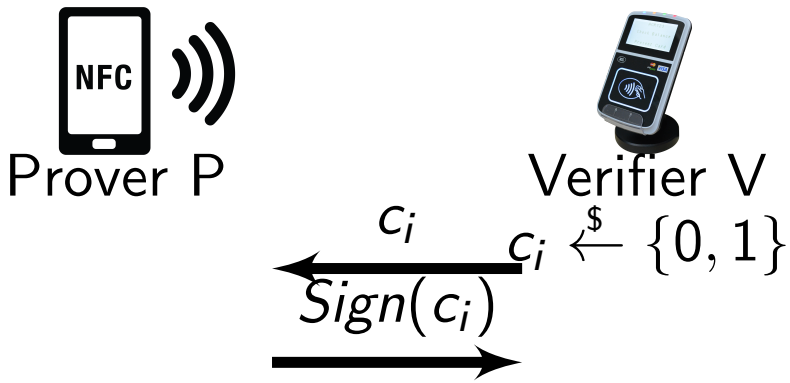


Some Naive Examples

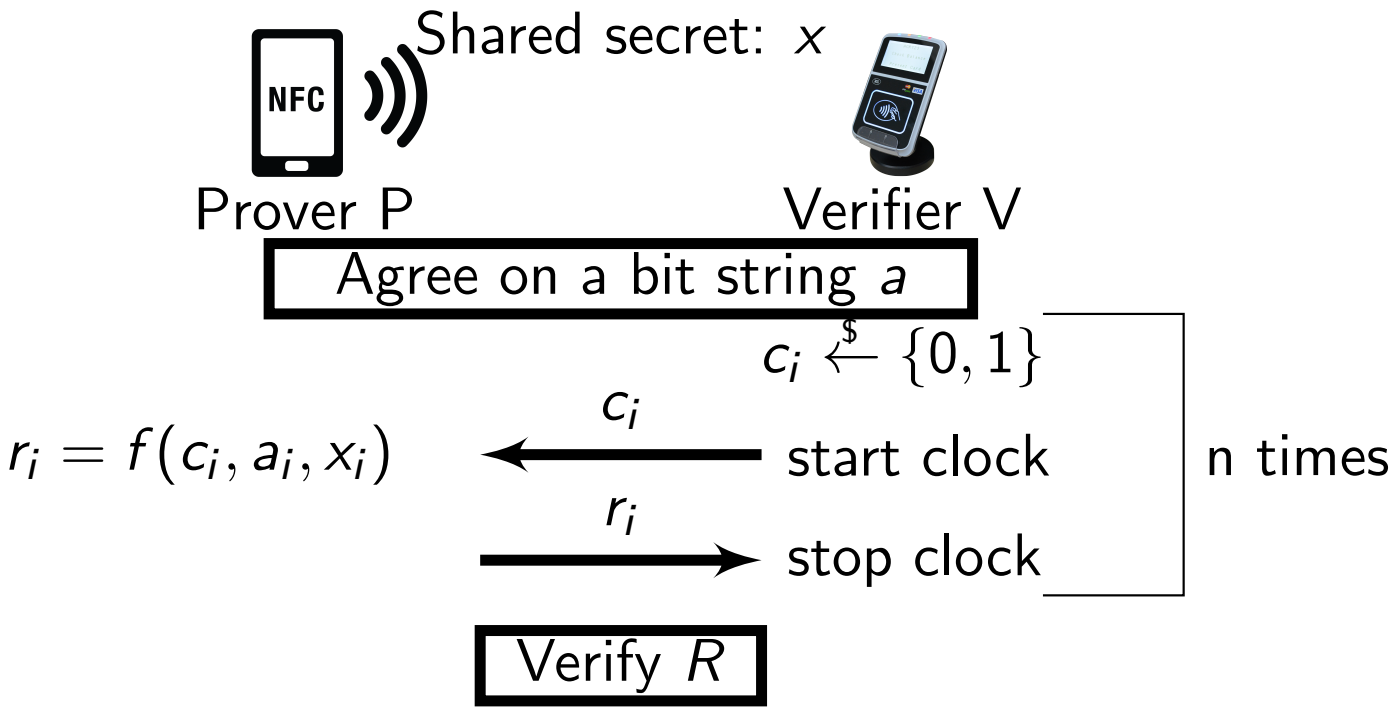
Echo protocol



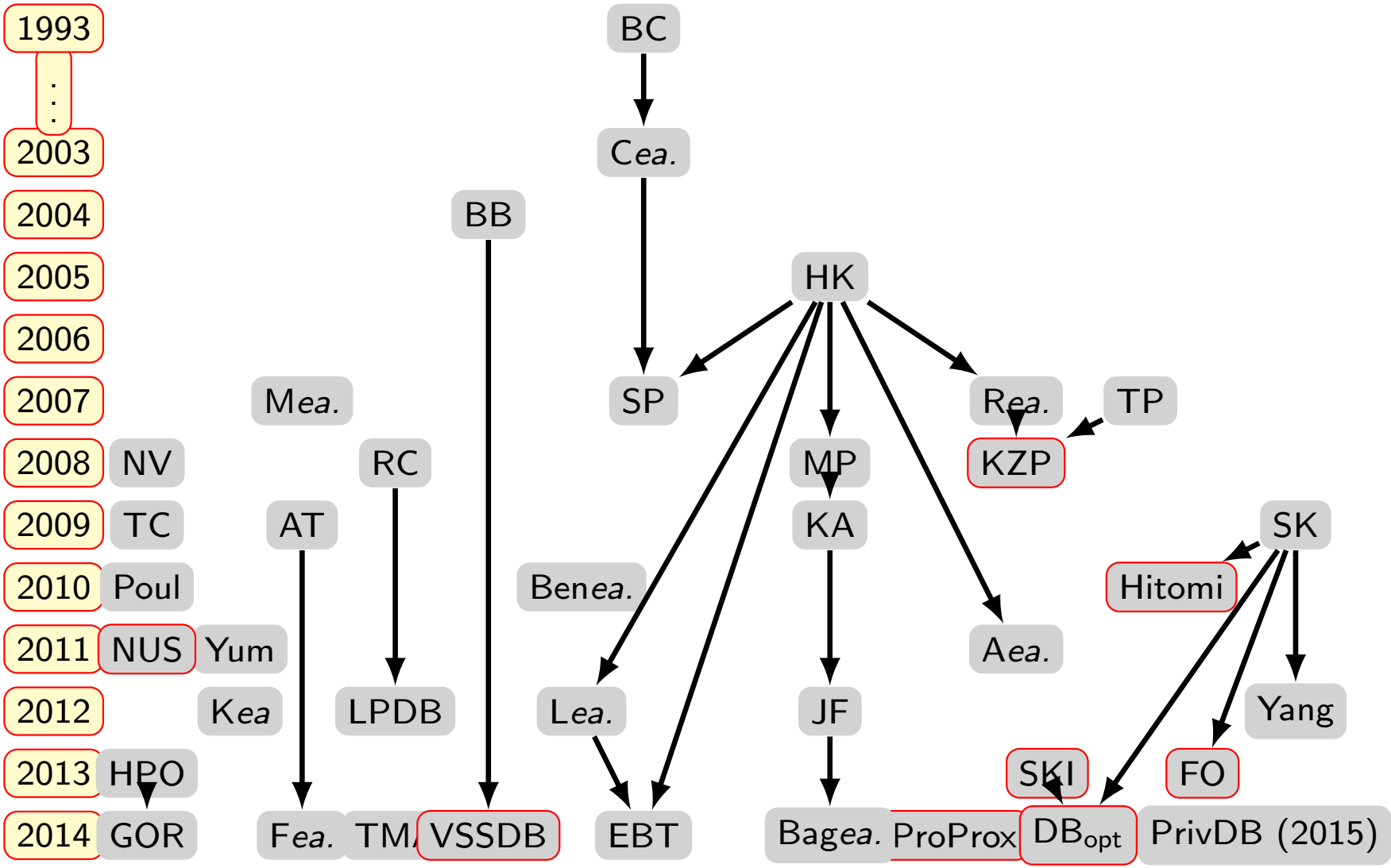
Signature



Typical DB protocol

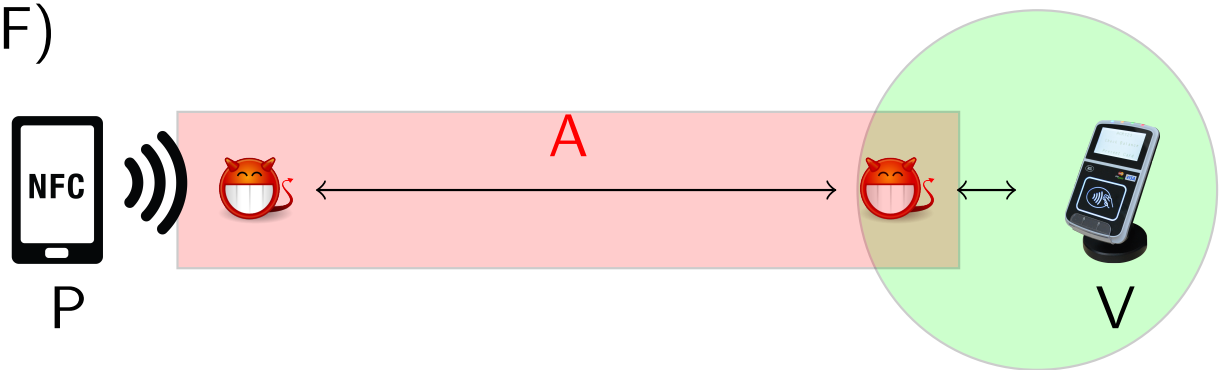


Survey : 42 protocols from 1993 to 2015.



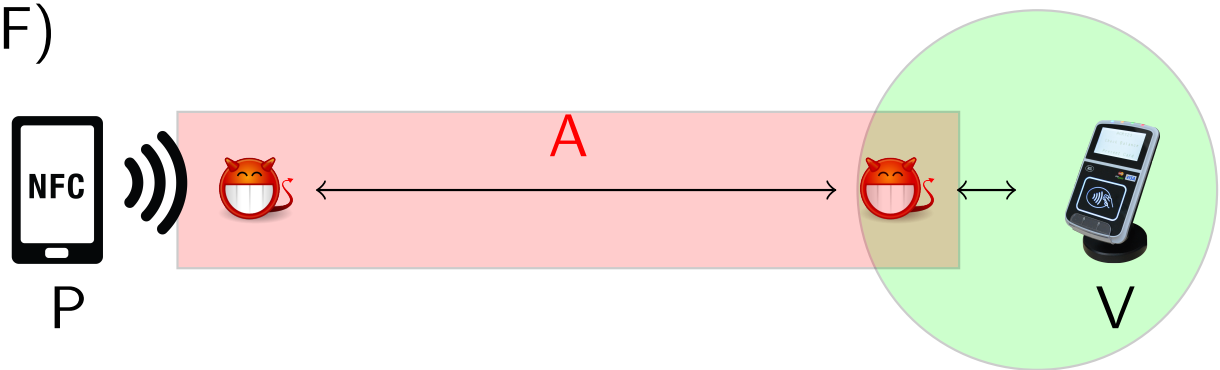
Threats against honest provers

Mafia Fraud (MF)



Threats against honest provers

Mafia Fraud (MF)

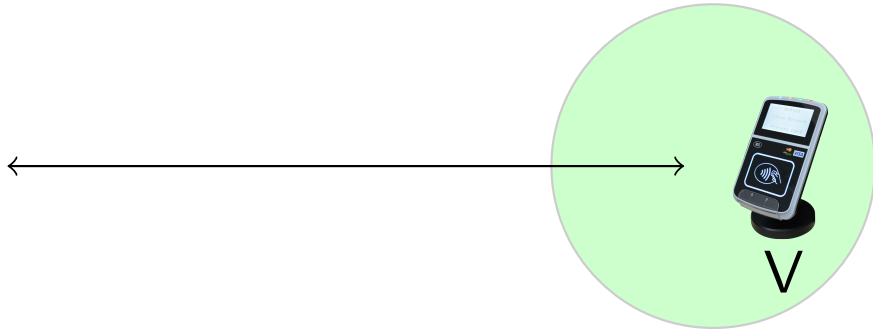


User tracking

Threats: malicious Provers

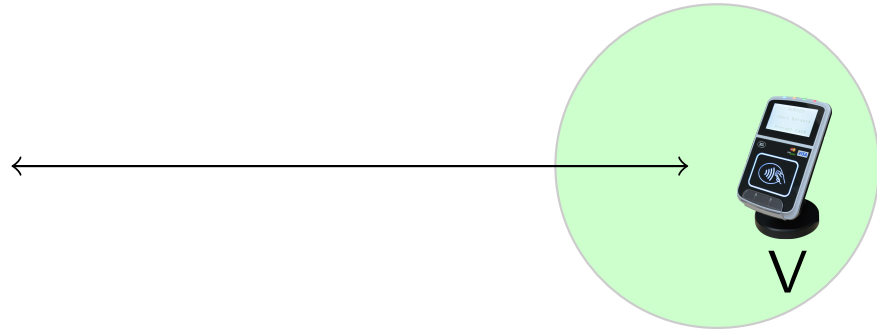
Distance Fraud (DF)

P

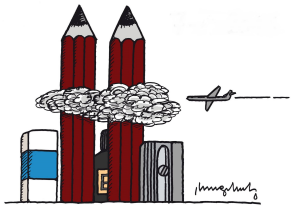


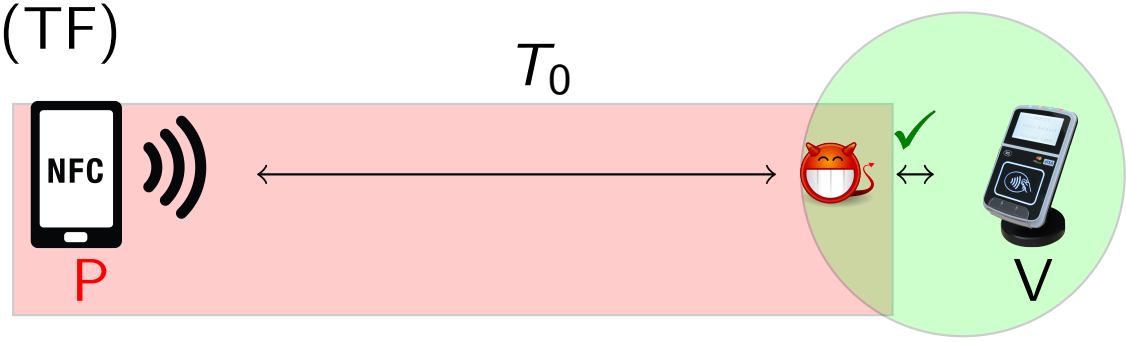
Threats: malicious Provers

Distance Fraud (DF)



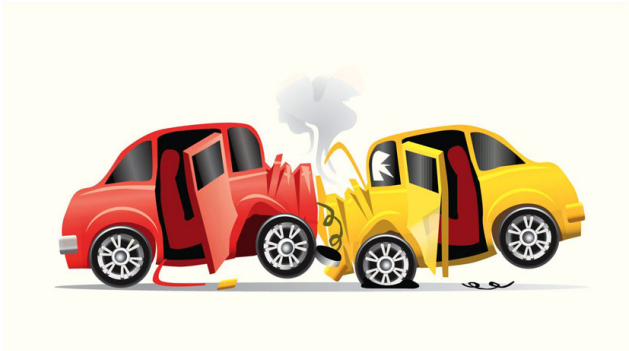
Terrorist Fraud(TF)



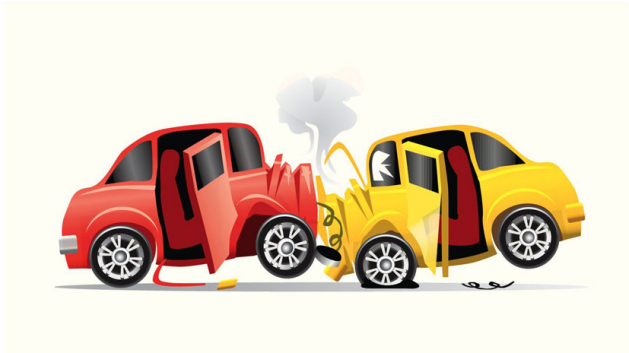


TREAD & SPADE

Outline

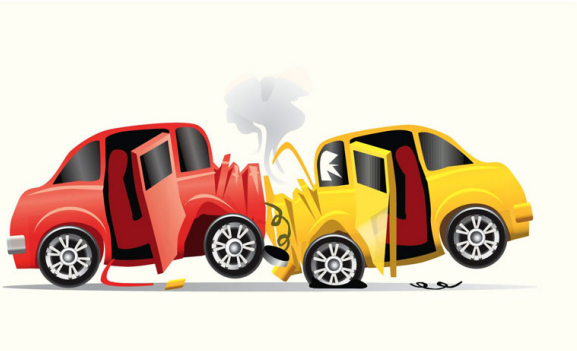



RIP



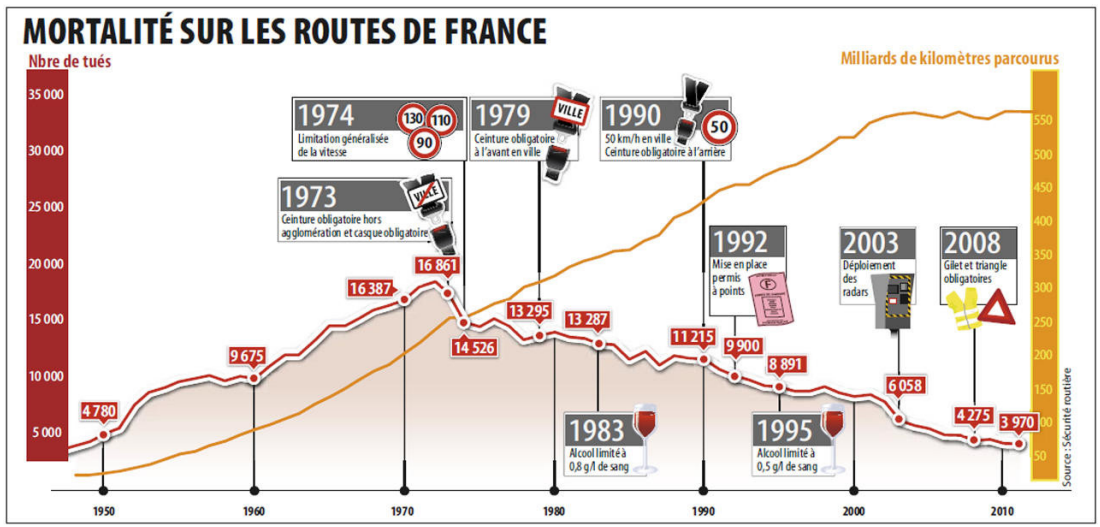

RIP


NON PORT DE LA CEINTURE DE SÉCURITÉ
-4 points
sur le permis de conduire
135 €
Amende forfaitaire
POINTS.12

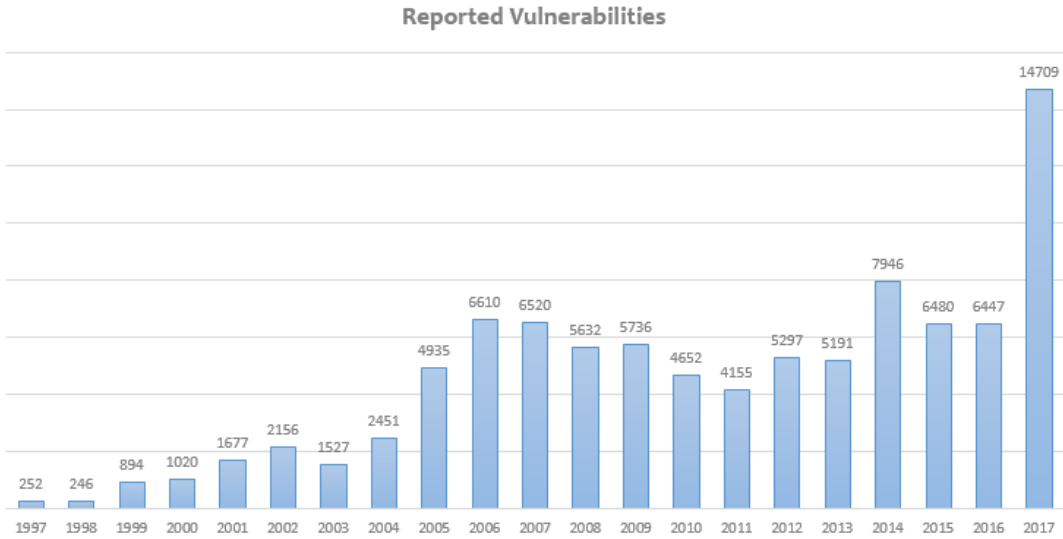


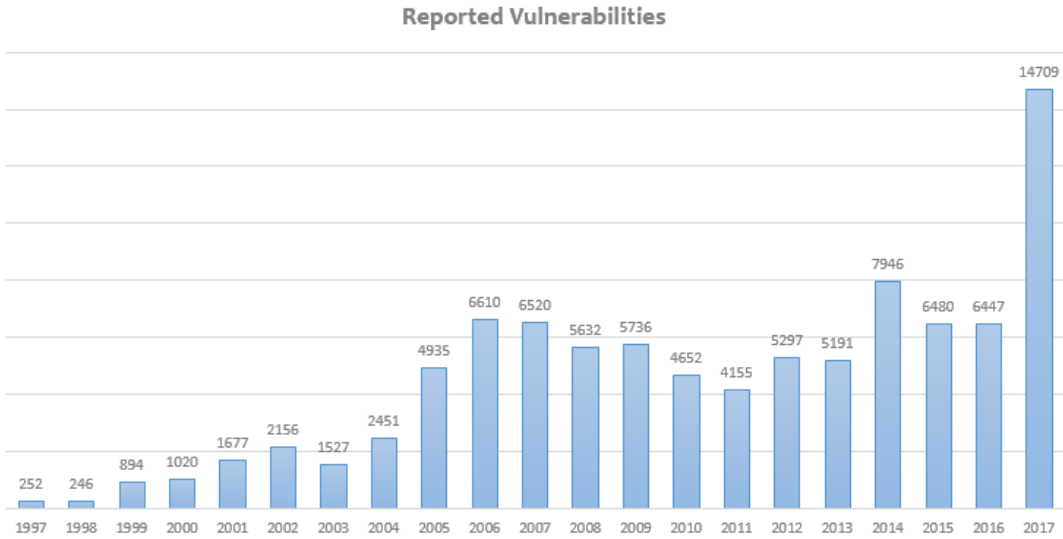

RIP


NON PORT DE LA CEINTURE DE SÉCURITÉ
-4 points
sur le permis de conduire
135 €
Amende forfaitaire
POINTS 12


MORTALITÉ SUR LES ROUTES DE FRANCE
Nbre de tués
Milliards de kilomètres parcourus
35 000
30 000
25 000
20 000
15 000
10 000
5 000
550
500
450
400
350
300
250
200
150
100
50
1974
Limitation généralisée de la vitesse
130
110
90
1979
Ceinture obligatoire à l'avant en ville
VILLE
1990
50 km/h en ville
Ceinture obligatoire à l'arrière
50
1973
Ceinture obligatoire hors agglomération et casque obligatoire
VILLE
1992
Mise en place permis à points
2003
Déploiement des radars
2008
Gilet et triangle obligatoires
4 780
9 675
16 387
16 861
14 526
13 295
13 287
11 215
9 900
8 891
6 058
4 275
3 970
1983
Alcool limité à 0,8 g/l de sang
1995
Alcool limité à 0,5 g/l de sang
1950
1960
1970
1980
1990
2000
2010
Source : Sécurité routière

L'argus


Reported Vulnerabilities
252
246
894
1020
1677
2156
1527
2451
4935
6610
6520
5632
5736
4652
4155
5297
5191
7946
6480
6447
14709
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017

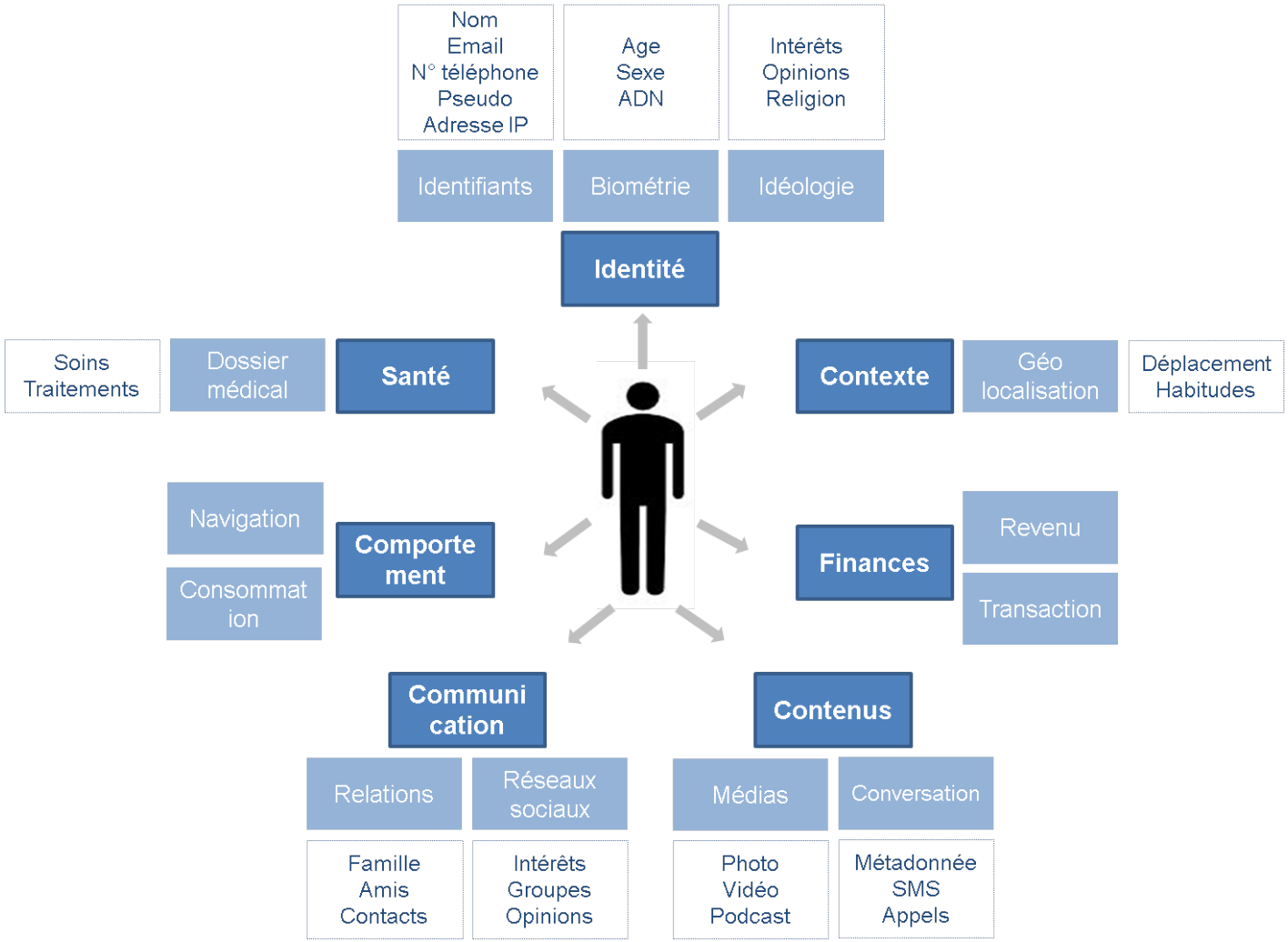


Règlement Général sur la Protection des Données
GDPR : General Data Protection Regulation

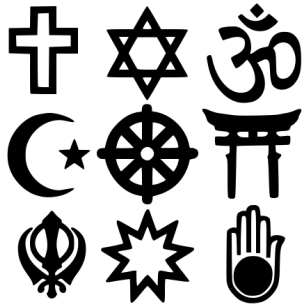
Qui est touché ?

TOUT LE MONDE !

Qu'est-ce qu'une donnée personnelle ?



Qu'est-ce qu'une donnée personnelle **sensible**?



Collecte sans consentement préalable écrit, clair et explicite

Plus de droits pour vos données !

Sanction

Plus de transparence

Droit à l'oubli

Guichet unique

Protection des mineurs

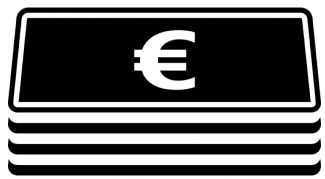
Portabilité

RPGD : en 6 étapes @CNIL

1. Désigner un pilote
2. Cartographier
3. Prioriser
4. Gérer les risques
5. Organiser
6. Documenter

Sanctions

20 millions



ou 4 %

Outline

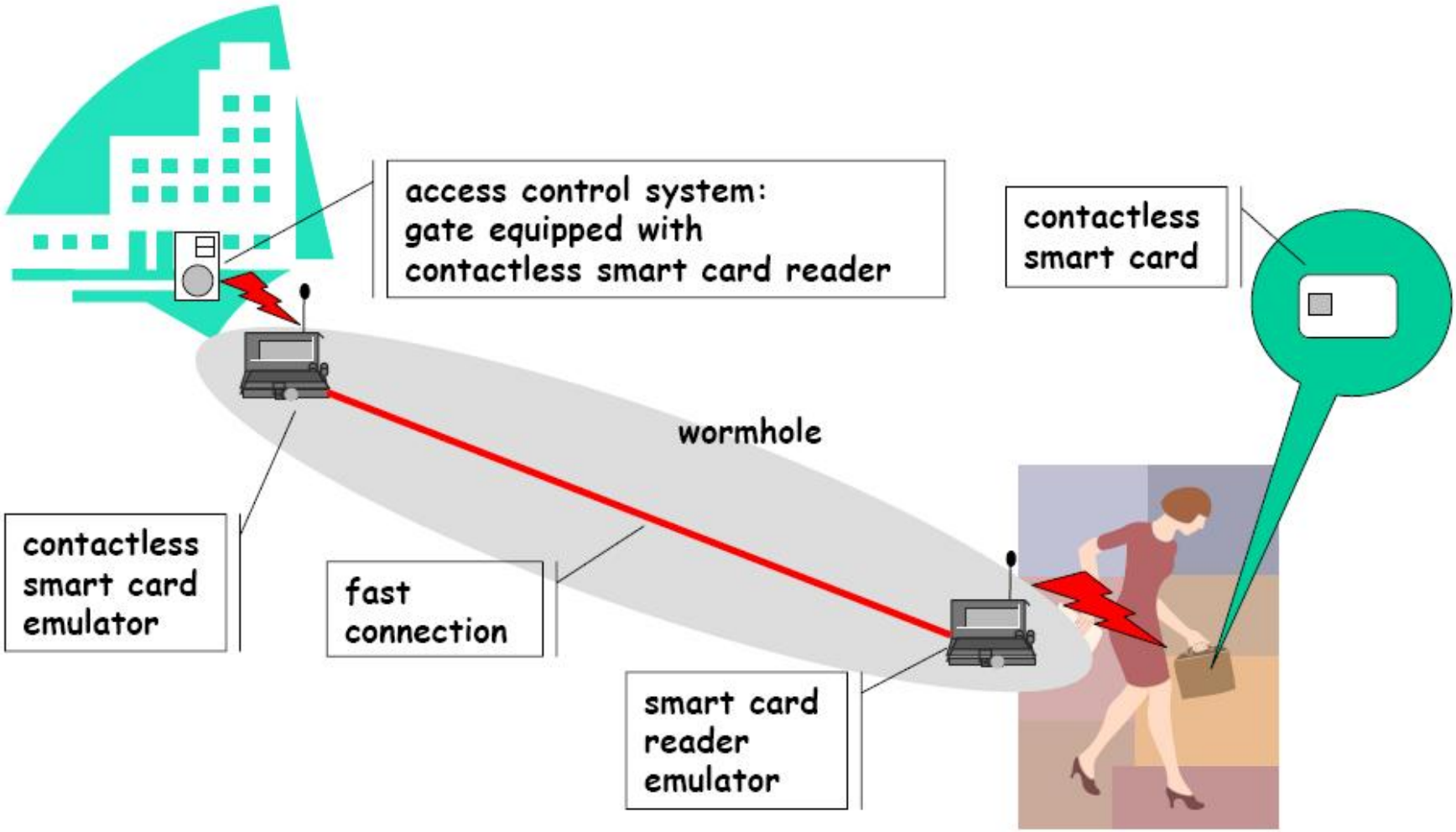
Several Possible Attackers

- Insider vs Outsider
- Active vs Passive
- Local vs Extended
- Single vs Multiple
- Laptop vs Server



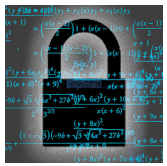



Wormhole Attack



What is cryptography based security?

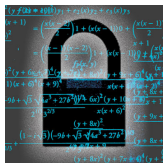
Cryptography:



- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocols: Distributed Algorithms

What is cryptography based security?

Cryptography:



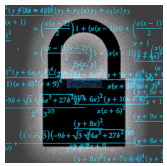
- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocols: Distributed Algorithms

Properties:

- Secrecy,
- Authentication,
- Privacy
- Non Repudiation ...

What is cryptography based security?

Cryptography:



- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocols: Distributed Algorithms

Properties:

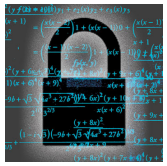
- Secrecy,
- Authentication,
- Privacy
- Non Repudiation ...

Intruders:

- Passive, active
- CPA, CCA ...

What is cryptography based security?

Cryptography:



- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocols: Distributed Algorithms

Properties:

- Secrecy,
- Authentication,
- Privacy
- Non Repudiation ...

Intruders:

- Passive, active
- CPA, CCA ...

Designing **secure** cryptographic protocols is **difficult**

Is it preserving your privacy?

Is it preserving your privacy?

4096 RSA encryption

Is it preserving your privacy?

4096 RSA encryption

Environs 60 températures possibles: 35 ... 41

Is it preserving your privacy?

4096 RSA encryption

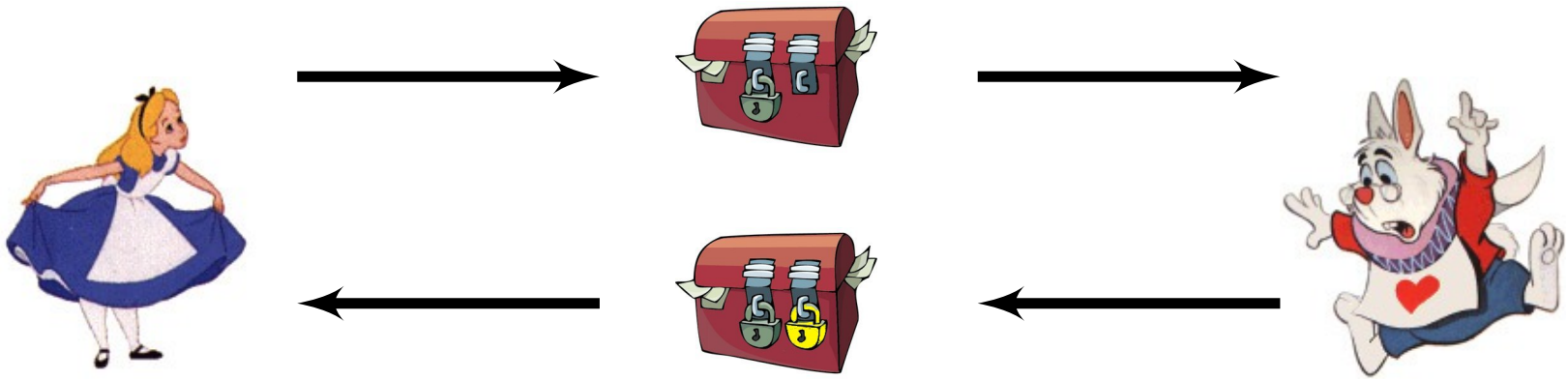
Environs 60 températures possibles: 35 ... 41

$$\{35\}_{pk}, \{35, 1\}_{pk}, ..., \{41\}_{pk}$$

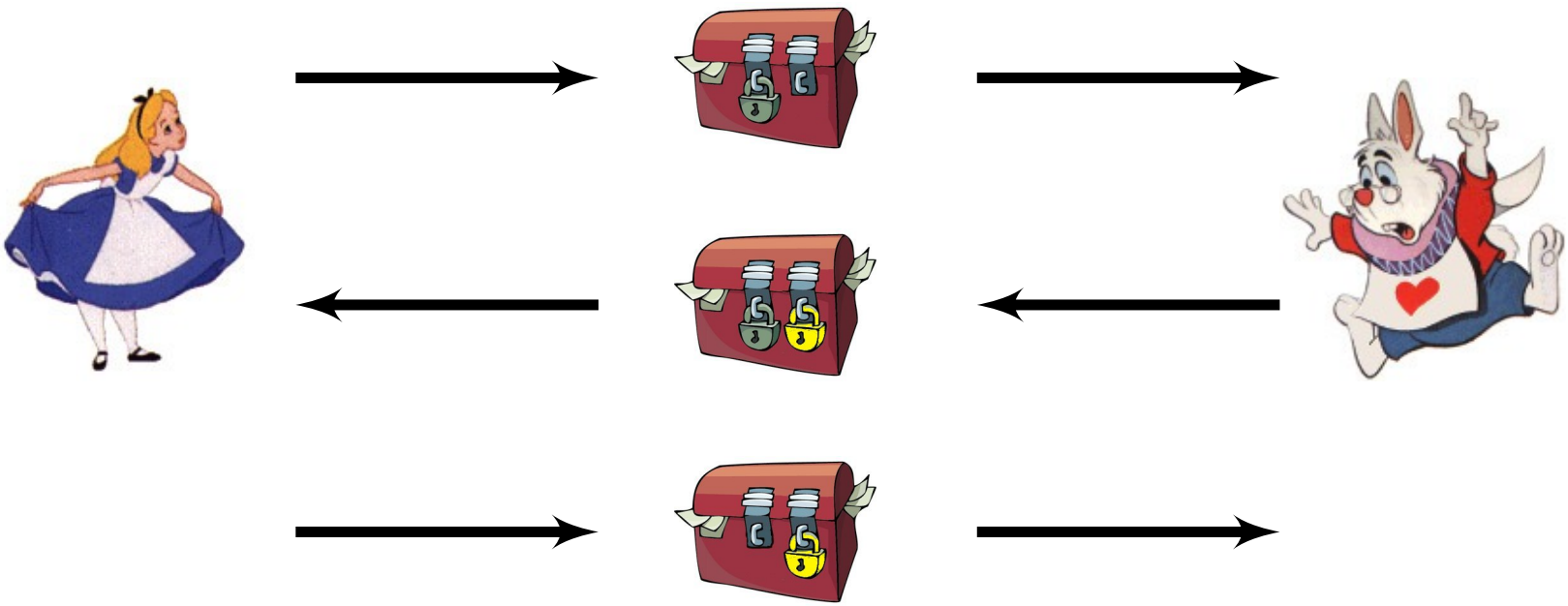
3-pass Shamir

3-pass Shamir

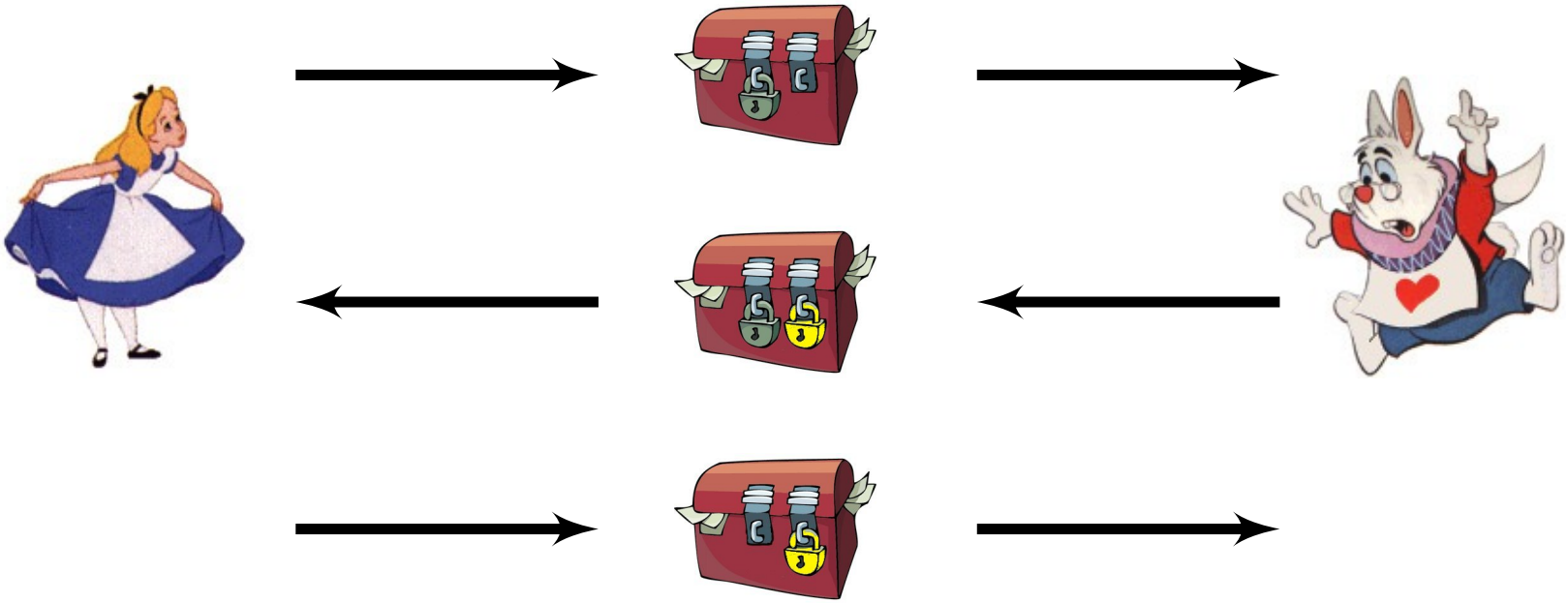
3-pass Shamir



3-pass Shamir



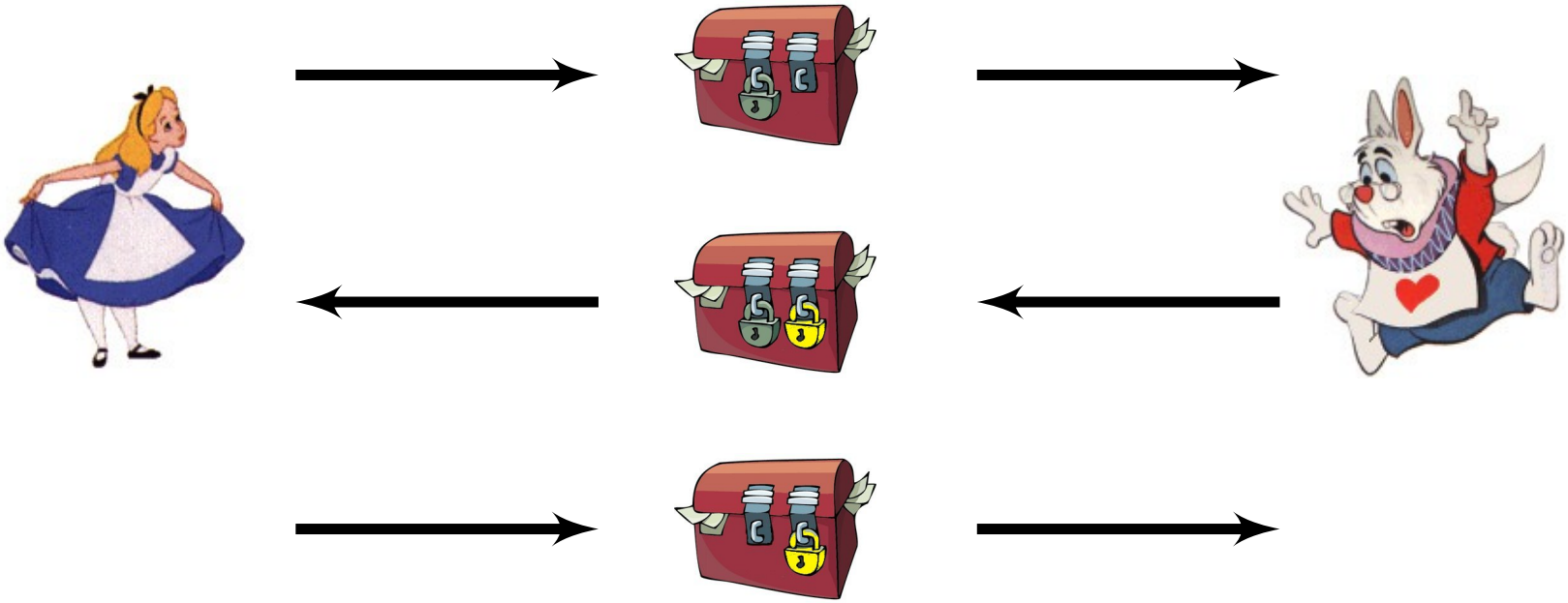
3-pass Shamir



Abstract Representation

$$1 \quad A \quad \rightarrow \quad B \quad : \quad \{m\}_{K_A}$$

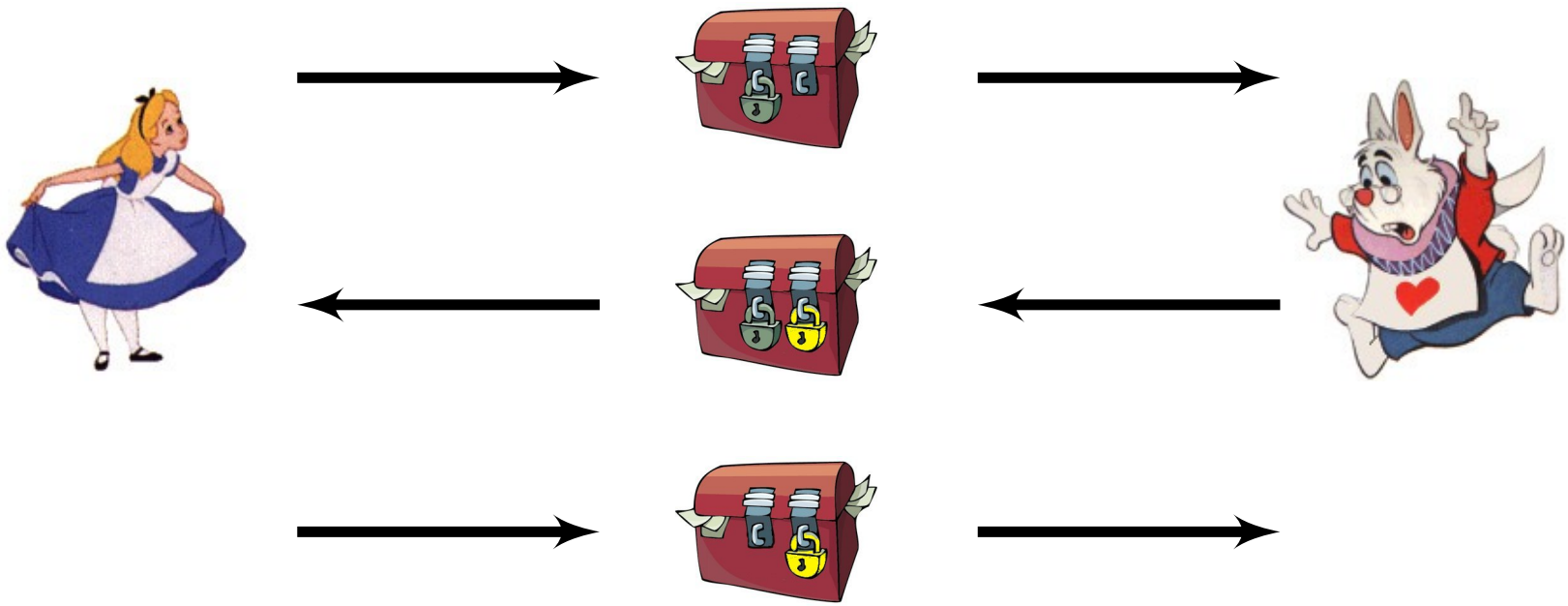
3-pass Shamir



Abstract Representation

$$
\begin{array}{llcll}
1 & A & \rightarrow & B & : \{m\}_{K_A} \\
2 & B & \rightarrow & A & : \{\{m\}_{K_A}\}_{K_B}
\end{array}
$$

3-pass Shamir

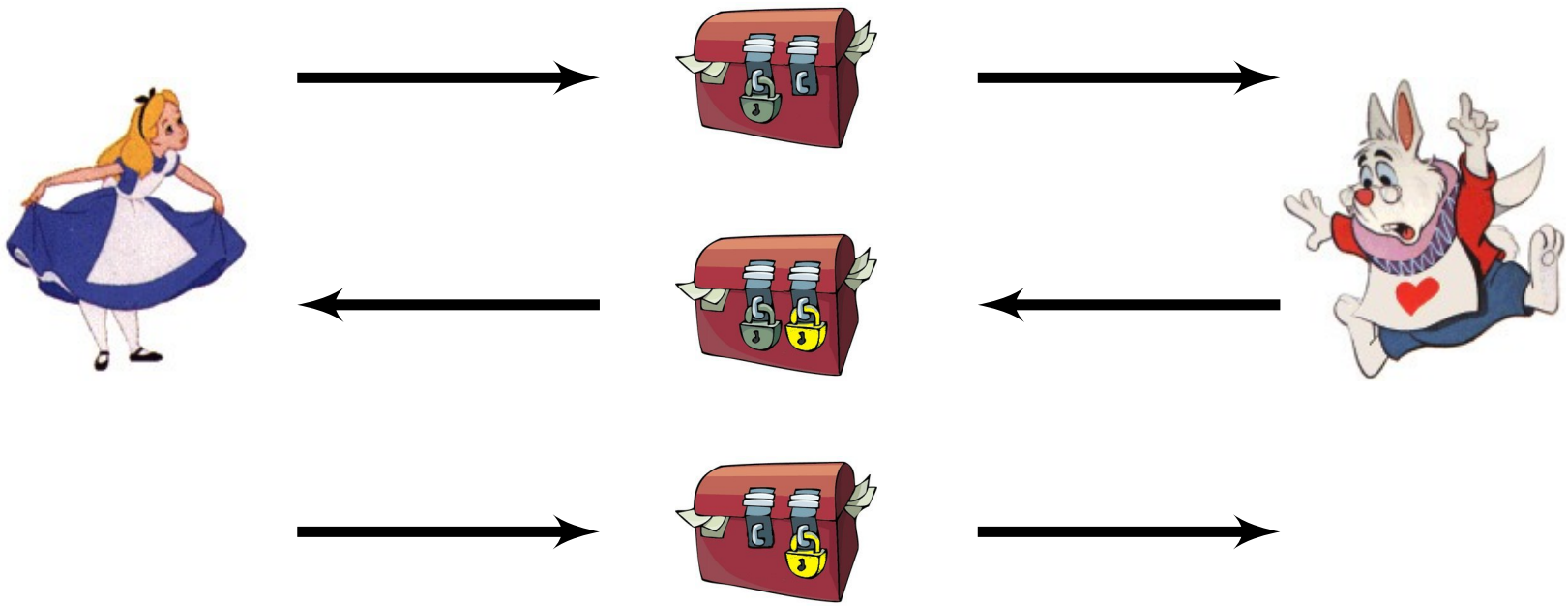


Abstract Representation

$$
\begin{array}{llcll}
1 & A & \rightarrow & B & : \quad \{m\}_{K_A} \\
2 & B & \rightarrow & A & : \quad \{\{m\}_{K_A}\}_{K_B} = \{\{m\}_{K_B}\}_{K_A}
\end{array}
$$

Commutative Encryption

3-pass Shamir



Abstract Representation

$$
\begin{array}{llcll}
1 & A & \rightarrow & B & : \{m\}_{K_A} \\
2 & B & \rightarrow & A & : \{\{m\}_{K_A}\}_{K_B} = \{\{m\}_{K_B}\}_{K_A} \\
3 & A & \rightarrow & B & : \{m\}_{K_B}
\end{array}
$$

Commutative Encryption

Logical Attack on Shamir 3-Pass Protocol (I)

Perfect encryption one-time pad (Vernam Encryption)

$\{m\}_k = m \oplus k$

XOR Properties (ACUN)

- $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ **A**ssociativity
- $x \oplus y = y \oplus x$ **C**ommutativity
- $x \oplus 0 = x$ **U**nity
- $x \oplus x = 0$ **N**ilpotency

Logical Attack on Shamir 3-Pass Protocol (I)

Perfect encryption one-time pad (Vernam Encryption)

$$\{m\}_k = m \oplus k$$

XOR Properties (ACUN)

- $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ **A**ssociativity
- $x \oplus y = y \oplus x$ **C**ommutativity
- $x \oplus 0 = x$ **U**nity
- $x \oplus x = 0$ **N**ilpotency

Vernam encryption is a commutative encryption :

$$\{\{m\}_{K_A}\}_{K_I} = (m \oplus K_A) \oplus K_I = (m \oplus K_I) \oplus K_A = \{\{m\}_{K_I}\}_{K_A}$$

Logical Attack on Shamir 3-Pass Protocol (II)

Perfect encryption one-time pad (Vernam Encryption)

$$\{m\}_k = m \oplus k$$

Shamir 3-Pass Protocol

$$\begin{array}{llll} 1 & A & \rightarrow & B : \quad m \oplus K_A \\ 2 & B & \rightarrow & A : \quad (m \oplus K_A) \oplus K_B \\ 3 & A & \rightarrow & B : \quad m \oplus K_B \end{array}$$

Passive attacker :

$$m \oplus K_A \qquad m \oplus K_B \oplus K_A \qquad m \oplus K_B$$

Logical Attack on Shamir 3-Pass Protocol (II)

Perfect encryption one-time pad (Vernam Encryption)

$$\{m\}_k = m \oplus k$$

Shamir 3-Pass Protocol

$$\begin{array}{llll} 1 & A & \rightarrow & B : \quad m \oplus K_A \\ 2 & B & \rightarrow & A : \quad (m \oplus K_A) \oplus K_B \\ 3 & A & \rightarrow & B : \quad m \oplus K_B \end{array}$$

Passive attacker :

$$m \oplus K_A \oplus m \oplus K_B \oplus K_A \oplus m \oplus K_B = m$$

Necessity of Tools to Analyze Cryptographic Protocols

- Protocols are small recipes.
- Non trivial to design and understand.
- The number and size of new protocols.
- Out-pacing human ability to rigourously analyze them.

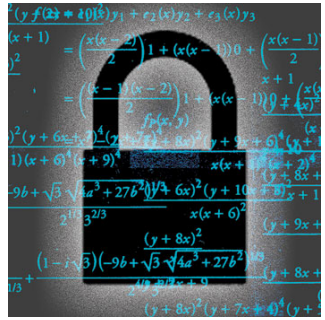
GOAL : A tool is finding flaws or establishing their correctness.

- completely automated,
- robust,
- expressive,
- and easily usable.

Existing Tools: AVISPA, Scyther, Proverif, Tamarin ..

Formal Verification Approaches

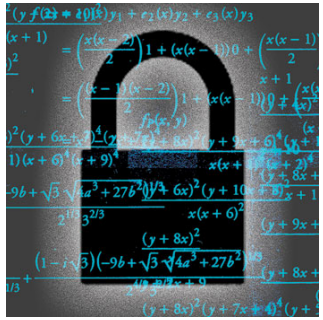
Designer



Attacker

Formal Verification Approaches

Designer

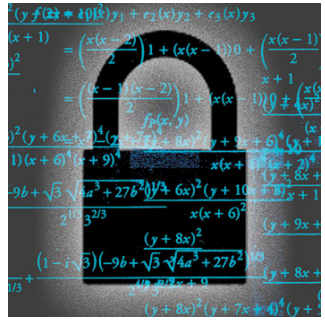


Attacker

Security Team

Formal Verification Approaches

Designer



Attacker

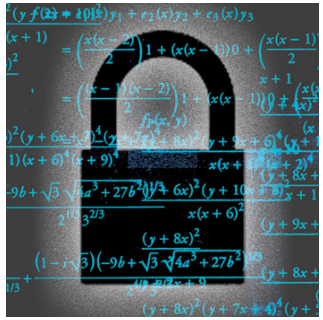
Give a proof

Security Team

LIMOS
LABORATOIRE D'INFORMATIQUE,
DE MODÉLISATION ET D'OPTIMISATION DES SYSTÈMES

Formal Verification Approaches

Designer



Attacker

Give a proof

Find a flaw

Security Team

Applications

Outline

Things to bring home

Several **challenges** in VANETs, specially in **security**:

- Connected Vehicule will be subject to more and more attacks
- Security should be taken into account
- Distance Bounding can help also in Vehicule context
- Designing secure protocols is difficult
- Formal methods are useful for designing secure protocols




Protocol + Properties + Intruder $\Rightarrow$ Security

Thanks for your attention

Questions ?

Second Example

Needham Schroeder Key Echange 1976

$$A \rightarrow B : \{A, N_A\}_{Pub(B)}$$

$$B \rightarrow A : \{N_A, N_B\}_{Pub(A)}$$

$$A \rightarrow B : \{N_B\}_{Pub(B)}$$

- Use cryptography
- Small programs
- Distributed

Cryptography is not sufficient !

Example : Needham Schroeder Key Echange

$$A \rightarrow B : \{A, N_A\}_{Pub(B)}$$

$$B \rightarrow A : \{N_A, N_B\}_{Pub(A)}$$

$$A \rightarrow B : \{N_B\}_{Pub(B)}$$

Cryptography is not sufficient !

Example : Needham Schroeder Key Echange

$$A \to B : \{A, N_A\}_{Pub(B)}$$

$$B \to A : \{N_A, N_B\}_{Pub(A)}$$

$$A \to B : \{N_B\}_{Pub(B)}$$

Broken 17 years after, by G. Lowe

$$A \to I : \{A, N_A\}_{Pub(I)} \qquad I \to B : \{A, N_A\}_{Pub(B)}$$

$$A \leftarrow I : \{N_A, N_B\}_{Pub(A)} \qquad I \leftarrow B : \{N_A, N_B\}_{Pub(A)}$$

$$A \to I : \{N_B\}_{Pub(I)} \qquad I \to B : \{N_B\}_{Pub(B)}$$

Cryptography is not sufficient !

Example : Needham Schroeder Key Echange

$$A \to B : \{A, N_A\}_{Pub(B)}$$

$$B \to A : \{N_A, N_B\}_{Pub(A)}$$

$$A \to B : \{N_B\}_{Pub(B)}$$

Broken 17 years after, by G. Lowe

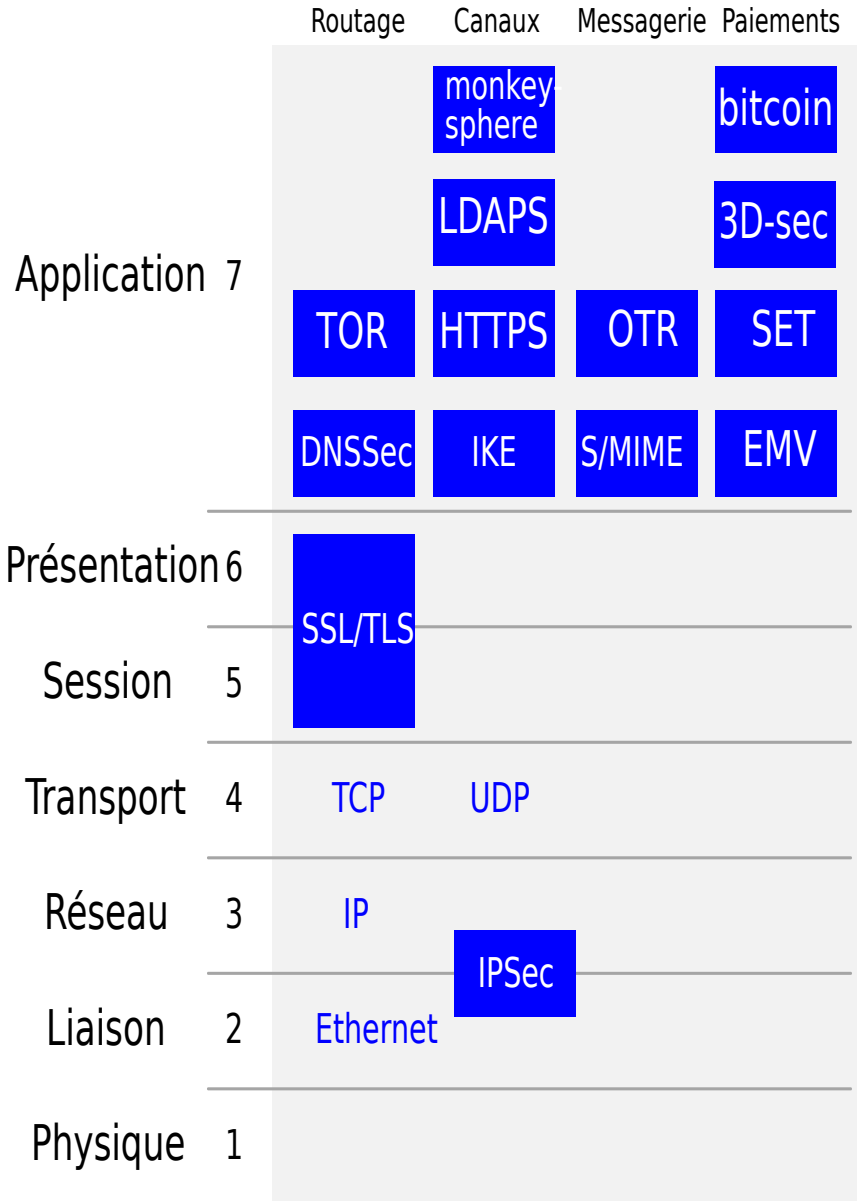
$$A \to I : \{A, N_A\}_{Pub(I)} \qquad I \to B : \{A, N_A\}_{Pub(B)}$$

$$A \leftarrow I : \{N_A, N_B\}_{Pub(A)} \qquad I \leftarrow B : \{N_A, N_B\}_{Pub(A)}$$

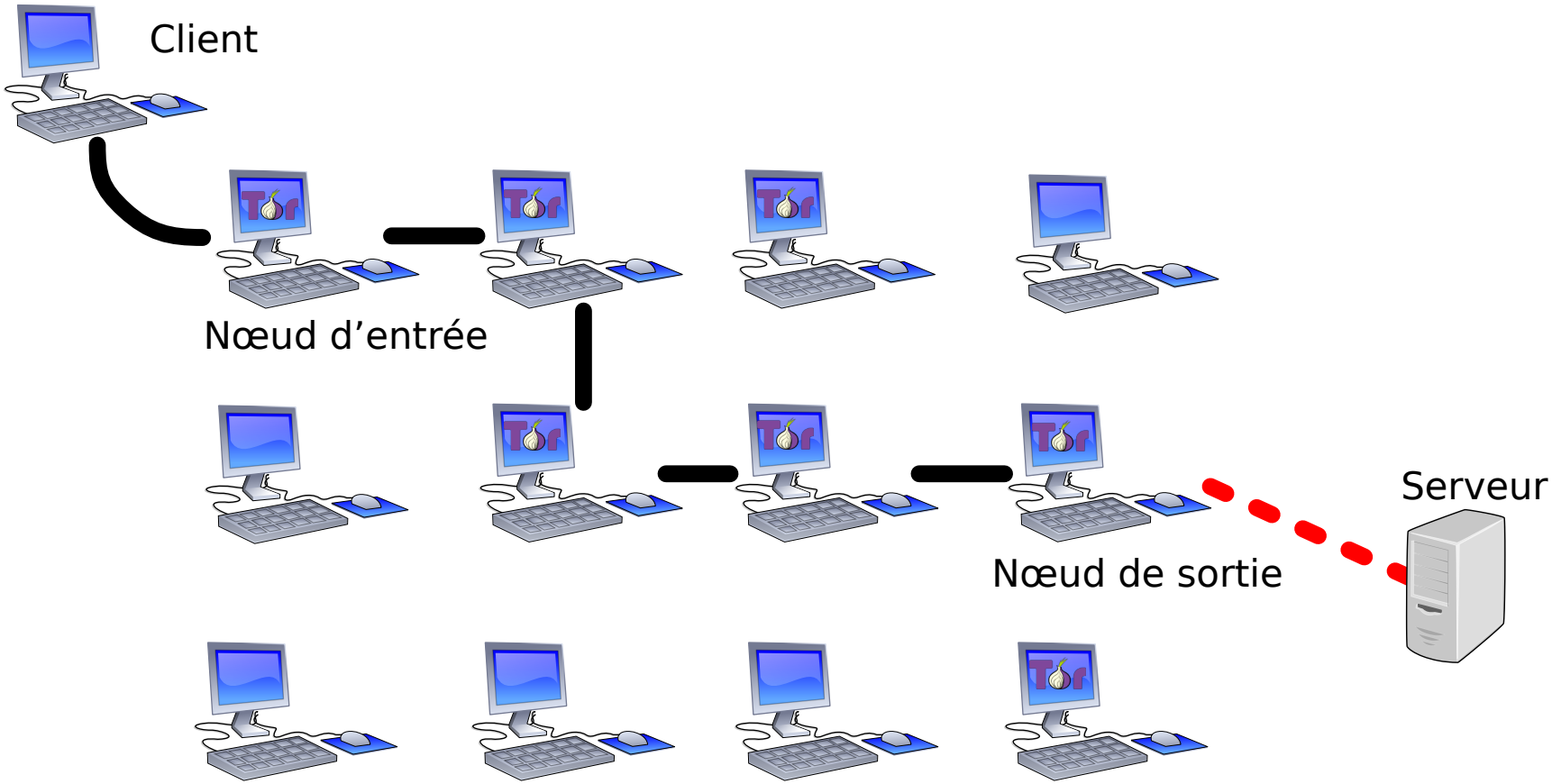
$$A \to I : \{N_B\}_{Pub(I)} \qquad I \to B : \{N_B\}_{Pub(B)}$$

Computer-Aided Security

Applications



Application : The Onion Router



https://www.torproject.org

Application : Tor