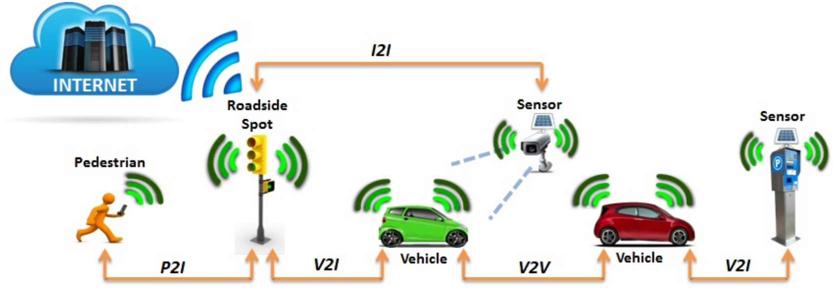
Security and Connected Autonomous Vehiculars

Pascal Lafourcade

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

ESC January 2021

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

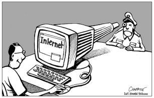
- Mobility
- Connection volatility
- Privacy vs Authentication
- Network scalability
- Bootstrap
- Security

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

C-ROADS & IndID

Distance Bounding

SPADE

- Building Blocks
- Protocol
- Anonymity
- Terrorist Fraud
- Mafia Fraud
- Distance Fraud

Security

Conclusion

Outline

C-ROADS & IndID

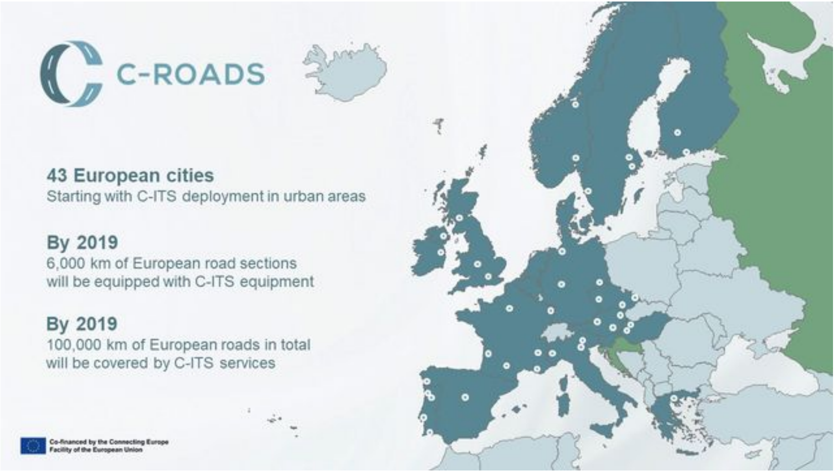
Distance Bounding

SPADE

- Building Blocks
- Protocol
- Anonymity
- Terrorist Fraud
- Mafia Fraud
- Distance Fraud

Security

Conclusion



C-ROADS

43 European cities
Starting with C-ITS deployment in urban areas

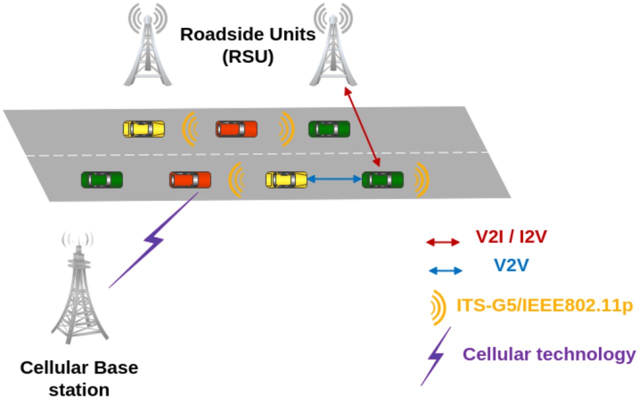
By 2019
6,000 km of European road sections
will be equipped with C-ITS equipment

By 2019
100,000 km of European roads in total
will be covered by C-ITS services

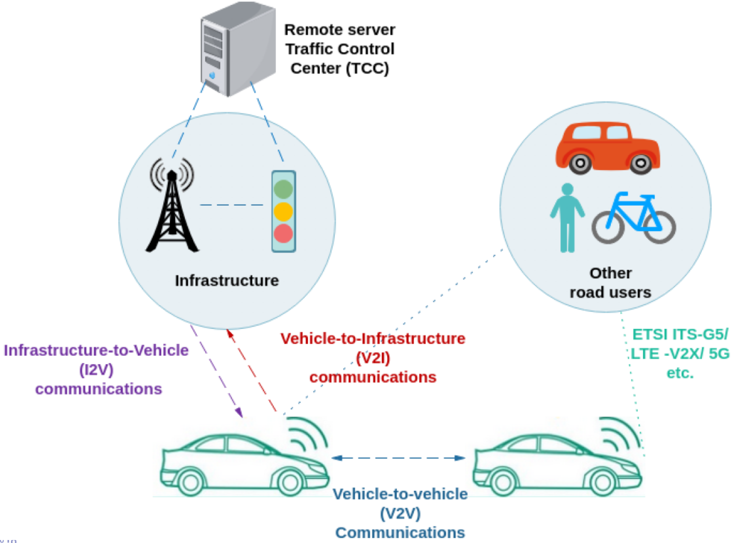
Co-financed by the Connecting Europe
Facility of the European Union

Cooperative Intelligent Transport Systems (C-ITS)

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

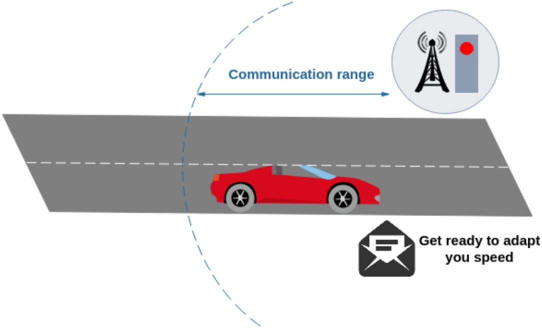


Cooperative Intelligent Transport Systems (C-ITS)

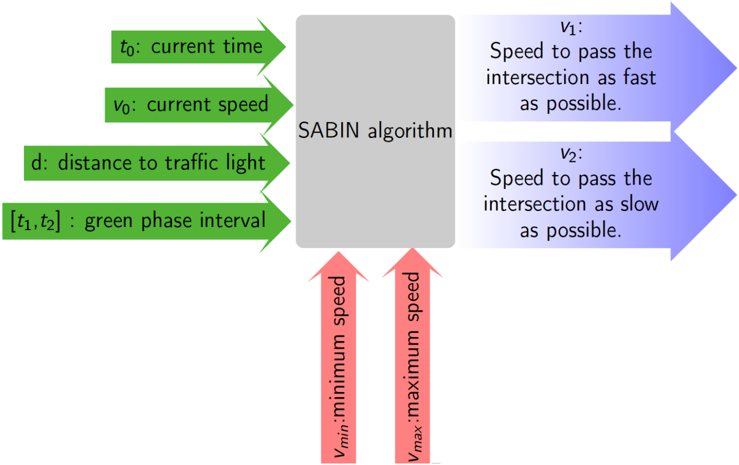


Green Light Optimal Speed Advisory (GLOSA)

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



Speed Advisory Boundary fINder (SABIN)



t_0: current time

v_0: current speed

d: distance to traffic light

$[t_1, t_2]$: green phase interval

SABIN algorithm

v_1: Speed to pass the intersection as fast as possible.

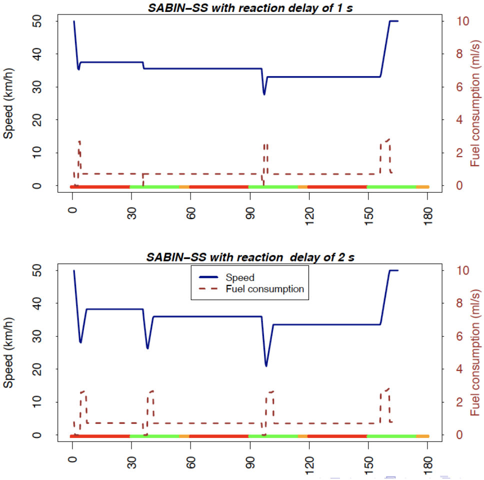
v_2: Speed to pass the intersection as slow as possible.

v_{min}:minimum speed

v_{max}:maximum speed

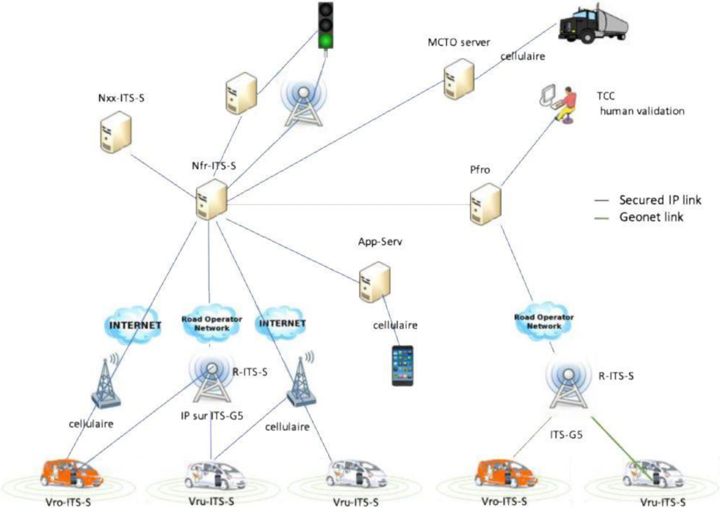
Mouna Karoui, Antonio Freitas, Gérard Chalhoub

Evaluation of SABIN



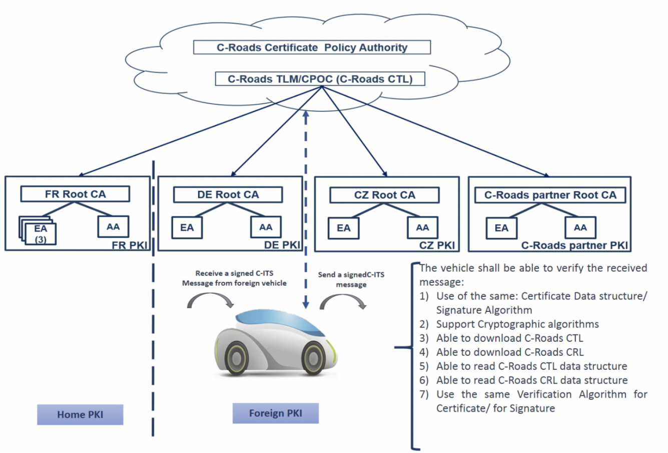
Mouna Karoui, Antonio Freitas, Gérard Chalhoub

Infrastructure



InDid (2019-2024)

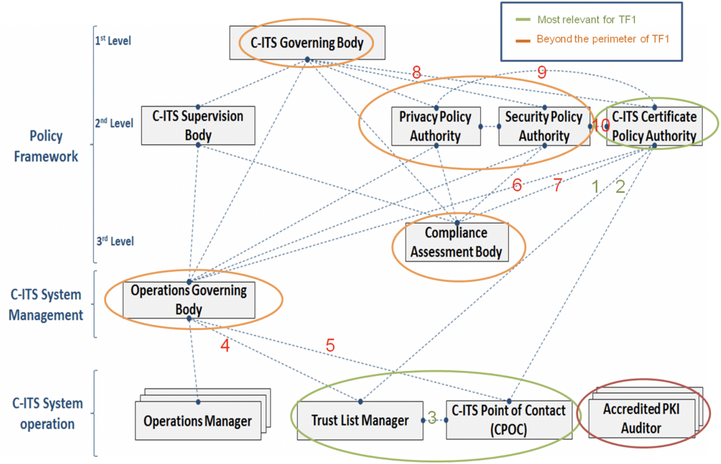
Interoperability


C-Roads Certificate Policy Authority
C-Roads TLM/CPOC (C-Roads CTL)
FR Root CA
EA (3)
AA
FR PKI
DE Root CA
EA
AA
DE PKI
CZ Root CA
EA
AA
CZ PKI
C-Roads partner Root CA
EA
AA
C-Roads partner PKI
Receive a signed C-ITS Message from foreign vehicle
Send a signedC-ITS message
Home PKI
Foreign PKI

The vehicle shall be able to verify the received message:

1) Use of the same: Certificate Data structure/ Signature Algorithm
2) Support Cryptographic algorithms
3) Able to download C-Roads CTL
4) Able to download C-Roads CRL
5) Able to read C-Roads CTL data structure
6) Able to read C-Roads CRL data structure
7) Use the same Verification Algorithm for Certificate/ for Signature

PKI Management



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

PKI Security Challenges

- Key management
- Privacy
- Interoperability
- Different countries

Outline

C-ROADS & IndID

Distance Bounding

SPADE

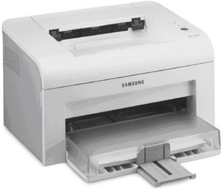
- Building Blocks
- Protocol
- Anonymity
- Terrorist Fraud
- Mafia Fraud
- Distance Fraud

Security

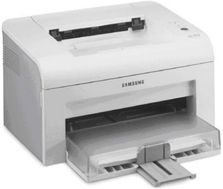
Conclusion

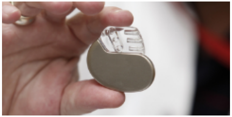
Real attacks on IoT from 2007 ...

Real attacks on IoT from 2007 ...

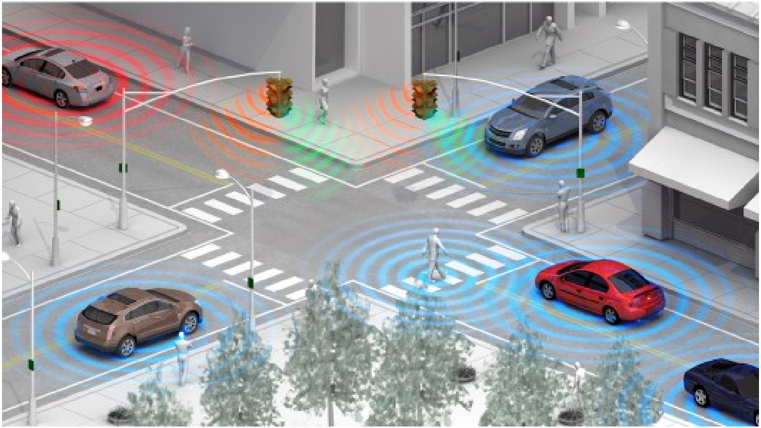


Real attacks on IoT from 2007 ...

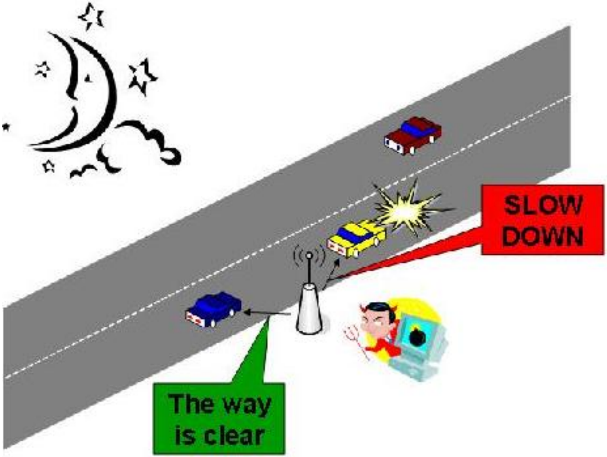




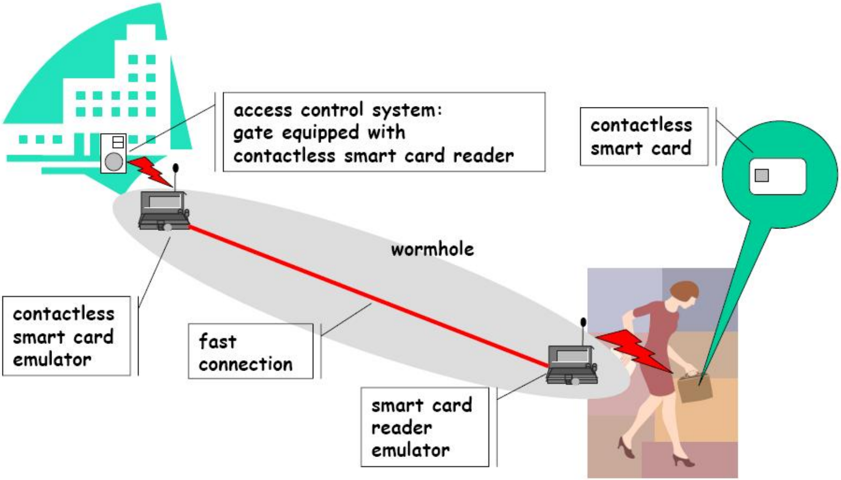
V2V and V2I



Attack on Infrastructure



Wireless communications ⇒ Wormhole Attack



access control system:
gate equipped with
contactless smart card reader

contactless
smart card

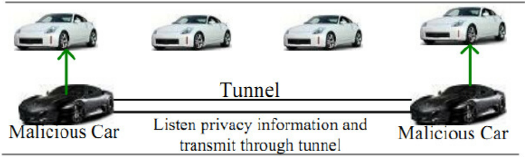
wormhole

contactless
smart card
emulator

fast
connection

smart card
reader
emulator

Wormhole Attack



Proximity Devices Everywhere

What features do we want?

- Security
- Privacy

Examples of Attacks

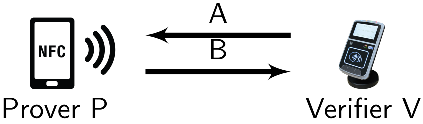
2 VIDEOS

- Public transport tickets
- Car opening

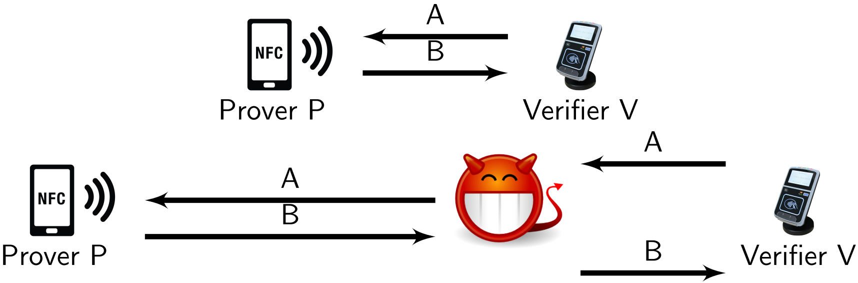
Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars, by Aurélien Francillon, Boris Danev, Srdjan Capkun, NDSS 2011

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

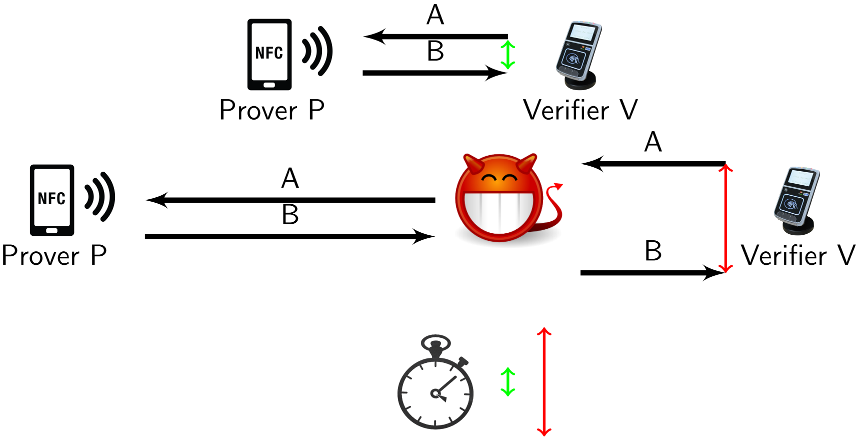
Security: Relay Attacks (Mafia Fraud)



Security: Relay Attacks (Mafia Fraud)

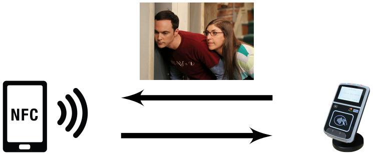


Security: Relay Attacks (Mafia Fraud)



Solution: distance bounding (Brands and Chaum, 1991)

Privacy: Eavesdropper VS Curious Verifier



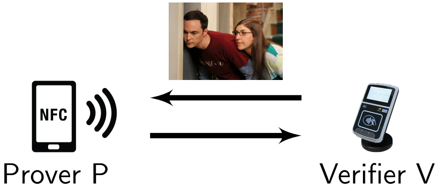
Eavesdropper

Prover P

Verifier V

Privacy: Eavesdropper VS Curious Verifier

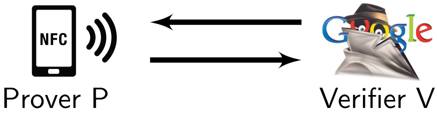
Eavesdropper



Prover P

Verifier V

Curious Verifier

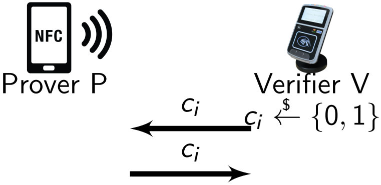


Prover P

Verifier V

Some Naive Examples

Echo protocol



Prover P

Verifier V

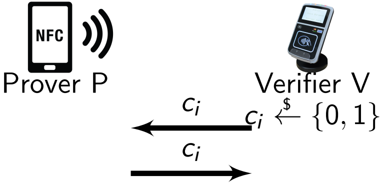
$c_i \xleftarrow{\$} \{0,1\}$

c_i

c_i

Some Naive Examples

Echo protocol



Prover P

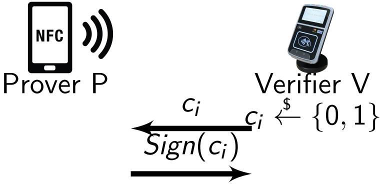
Verifier V

c_i

$c_i \xleftarrow{\$} \{0,1\}$

c_i

Signature



Prover P

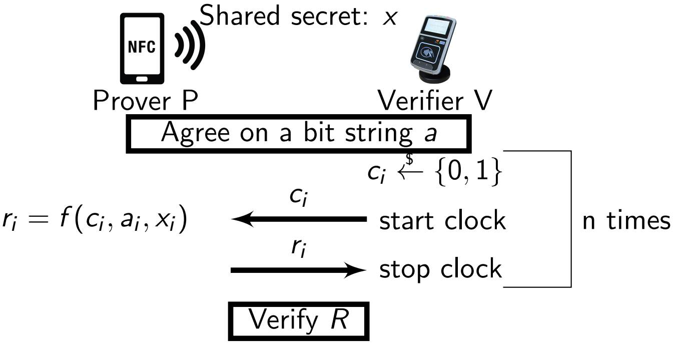
Verifier V

c_i

$c_i \xleftarrow{\$} \{0,1\}$

$Sign(c_i)$

Typical DB protocol



Shared secret: x

Prover P

Verifier V

Agree on a bit string a

$c_i \xleftarrow{\$} \{0,1\}$

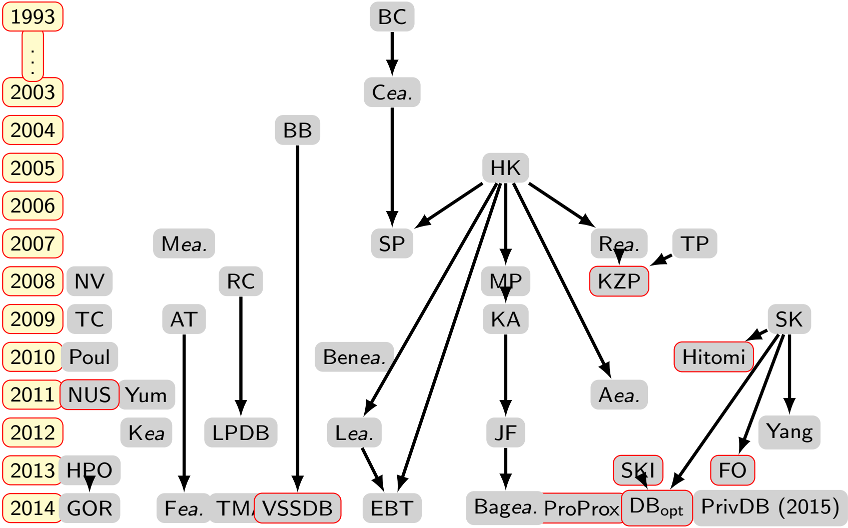
$r_i = f(c_i, a_i, x_i)$ $\xleftarrow{c_i}$ start clock

$\xrightarrow{r_i}$ stop clock

n times

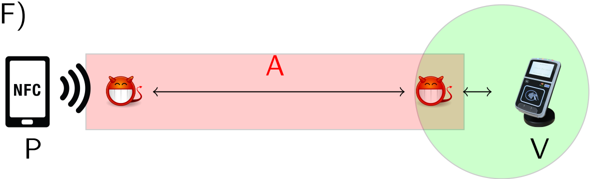
Verify R

Survey : 42 protocols from 1993 to 2015.



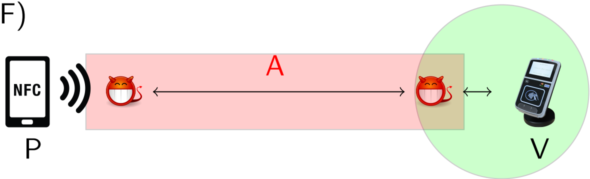
Threats against honest provers

Mafia Fraud (MF)

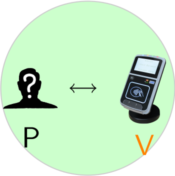


Threats against honest provers

Mafia Fraud (MF)

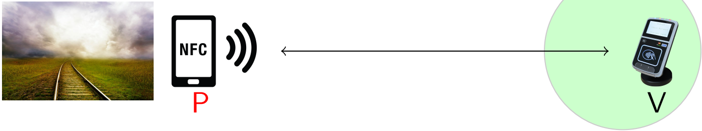


User tracking



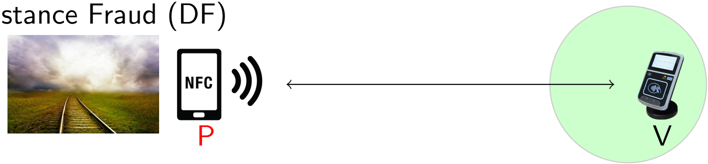
Threats: malicious Provers

Distance Fraud (DF)

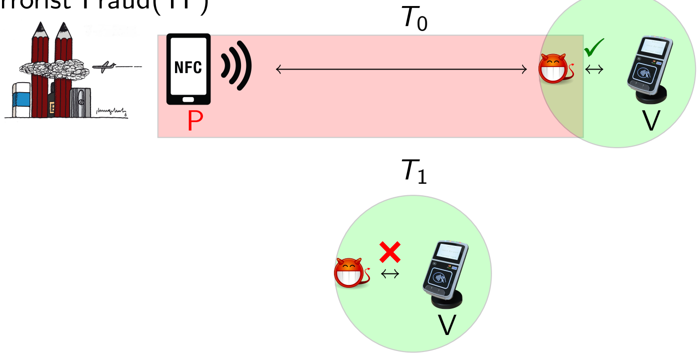


Threats: malicious Provers

Distance Fraud (DF)



Terrorist Fraud(TF)



Outline

C-ROADS & IndID

Distance Bounding

SPADE

- Building Blocks
- Protocol
- Anonymity
- Terrorist Fraud
- Mafia Fraud
- Distance Fraud

Security

Conclusion

SPADE: The intuition

If P exposes his secret key, then V can identify him!
What can he expose then?

- The prover picks a random, one time session key N_P
- Authentication by group signature σ_p on this key
- The prover sends $\{N_P, \sigma_p\}_{\mathrm{pk}_V}$
- He exposes N_P during the protocol

SPADE, building blocks

- A public key encryption scheme PKE
  - IND-CCA2
- A pseudorandom function PRF
  - Unforgeable
  - In the ROM, $\mathsf{PRF}_{\mathsf{sk}}(M) \equiv \mathsf{H}(\mathsf{sk}, M)$
- A revocable group signature scheme PKE
  - Anonymous signature on behalf of the group

SPADE

Prover P	**Verifier** V
$\mathsf{pk}_v, \mathsf{ssk}_p$	$\mathsf{sk}_v, \mathsf{svk}$

SPADE

Prover P		**Verifier** V
$\mathsf{pk}_v, \mathsf{ssk}_p$		$\mathsf{sk}_v, \mathsf{svk}$
	Initialisation	
$N_P \xleftarrow{\$} \{0,1\}^n, \sigma_p = \mathsf{G.sig}_{\mathsf{ssk}_P}(N_P)$	$\xrightarrow{\{N_P,\sigma_p\}_{\mathsf{pk}_V}}$	$N_V \xleftarrow{\$} \{0,1\}^n$
	$\xleftarrow{m,N_V}$	$m \xleftarrow{\$} \{0,1\}^n$

SPADE

Prover P — $\mathsf{pk}_v, \mathsf{ssk}_p$

Verifier V — $\mathsf{sk}_v, \mathsf{svk}$

Initialisation

$N_P \xleftarrow{\$} \{0,1\}^n, \sigma_p = \mathsf{G.sig}_{\mathsf{ssk}_P}(N_P) \quad \xrightarrow{\{N_P,\sigma_p\}_{\mathsf{pk}_V}} \quad N_V \xleftarrow{\$} \{0,1\}^n$

$\xleftarrow{m,N_V} \quad m \xleftarrow{\$} \{0,1\}^n$

$a = \mathsf{PRF}_{N_P}(N_V)$

SPADE

Prover P $\mathsf{pk}_v, \mathsf{ssk}_p$		**Verifier** V $\mathsf{sk}_v, \mathsf{svk}$
	Initialisation	
$N_P \overset{\$}{\leftarrow} \{0,1\}^n, \sigma_p = \mathsf{G.sig}_{\mathsf{ssk}_P}(N_P)$	$\xrightarrow{\{N_P,\sigma_p\}_{\mathsf{pk}_V}}$	$N_V \overset{\$}{\leftarrow} \{0,1\}^n$
	$\xleftarrow{m,N_V}$	$m \overset{\$}{\leftarrow} \{0,1\}^n$
	$a = \mathsf{PRF}_{N_P}(N_V)$	
	Distance Bounding	
	for $i = 1$ to n	
		Pick $c_i \in \{0,1\}$
$r_i = \begin{cases} a_i & \text{if } c_i = 0 \\ a_i \oplus {N_P}_i \oplus m_i & \text{if } c_i = 1 \end{cases}$	$\xleftarrow{c_i}$	**Start clock**
	$\xrightarrow{r_i}$	**Stop clock**

SPADE

Prover P $\mathsf{pk}_v, \mathsf{ssk}_p$		**Verifier** V $\mathsf{sk}_v, \mathsf{svk}$
	Initialisation	
$N_P \xleftarrow{\$} \{0,1\}^n, \sigma_p = \mathsf{G.sig}_{\mathsf{ssk}_P}(N_P)$	$\xrightarrow{\{N_P,\sigma_p\}_{\mathsf{pk}_V}}$	$N_V \xleftarrow{\$} \{0,1\}^n$
	$\xleftarrow{m,N_V}$	$m \xleftarrow{\$} \{0,1\}^n$
	$a = \mathsf{PRF}_{N_P}(N_V)$	
	Distance Bounding	
	for $i = 1$ to n	
		Pick $c_i \in \{0,1\}$
$r_i = \begin{cases} a_i & \text{if } c_i = 0 \\ a_i \oplus N_{P\,i} \oplus m_i & \text{if } c_i = 1 \end{cases}$	$\xleftarrow{c_i}$	**Start clock**
	$\xrightarrow{r_i}$	**Stop clock**
	Verification	
		Check timers Δt_i
$\mathcal{T} = \mathsf{PRF}_{N_P}(\mathit{transcript})$	$\xrightarrow{\mathcal{T}}$	Check that $\mathcal{T} = \mathsf{PRF}_{N_P}(\mathit{transcript})$
		If $\#\{i : r_i$ and Δt_i correct$\} = n$ then
	$\xleftarrow{Out_V}$	$Out_V := 1$; else $Out_V := 0$

Security: Main Theorem

Theorem

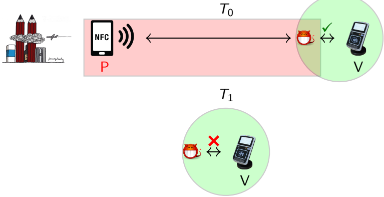
If (i) PKE is IND-CCA2 secure, (ii) G-SIG is unforgeable, unlinkable and revocable and (iii) the challenges are random and independent then SPADE is MF, DF and TF resistant, as well as anonymous and revocable, in the random oracle model.

User tracking

Prover P		**Verifier** V
$\mathsf{pk}_v, \mathsf{ssk}_p$		$\mathsf{sk}_v, \mathsf{svk}$
	Initialisation	
$N_P \xleftarrow{\$} \{0,1\}^n, \sigma_p = \mathsf{G.sig}_{\mathsf{ssk}_P}(N_P)$	$\xrightarrow{\{N_P, \sigma_p\}_{\mathsf{pk}_V}}$	$N_V \xleftarrow{\$} \{0,1\}^n$
	$\xleftarrow{m, N_V}$	$m \xleftarrow{\$} \{0,1\}^n$
	$a = \mathsf{PRF}_{N_P}(N_V)$	

If V can track users, then he can break the unlinkability of the group signature scheme

Security: TF



Prover P		**Verifier V**
$N_P \xleftarrow{\$} \{0,1\}^n$	$\xrightarrow{\{N_P,\sigma_P\}_{\mathsf{pk}_V}}$	$N_V \xleftarrow{\$} \{0,1\}^n$
	$\xleftarrow{m,N_V}$	$m \xleftarrow{\$} \{0,1\}^n$
	$a = \mathrm{PRF}_{N_P}(N_V)$ for $i = 1$ to n	
		Pick $c_i \in \{0,1\}$
$r_i = \begin{cases} a_i & \text{if } c_i = 0 \\ a_i \oplus N_{P_i} \oplus m_i & \text{if } c_i = 1 \end{cases}$	$\xleftarrow{c_i}$	**Start clock**
	$\xrightarrow{r_i}$	**Stop clock**

The accomplice can replay $\{N_P, \sigma_P\}_{\mathsf{pk}_V}$ later: he knows N_P

The Backdoor

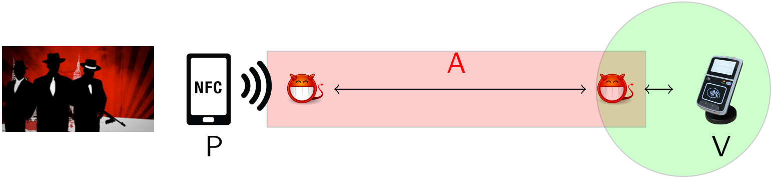
The backdoor helps the accomplice recover the missing bits

$$\xrightarrow{\{N_P,\sigma_p\}_{\mathsf{pk}_V},N'_P} \quad \text{if } d_H(N_P, N'_P) > t \text{ then abort}$$

$$\xleftarrow{N_P}$$

- Trick for the proof
- Slightly lowers MF resistance
- Can adjust t

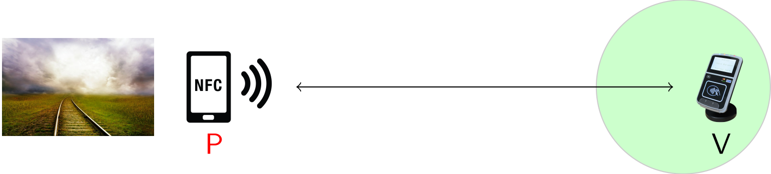
Security: MF

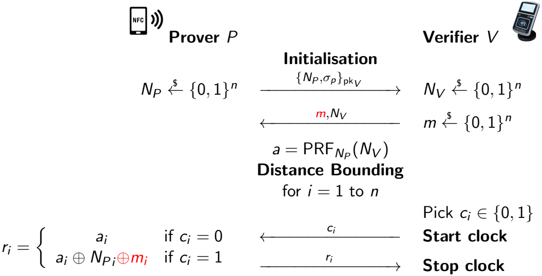


Prover P		Verifier V
	for $i = 1$ to n	
		Pick $c_i \in \{0,1\}$
$r_i = \begin{cases} a_i & \text{if } c_i = 0 \\ a_i \oplus N_{P\,i} \oplus m_i & \text{if } c_i = 1 \end{cases}$	$\xleftarrow{c_i}$	**Start clock**
	$\xrightarrow{r_i}$	**Stop clock**
		Check timers Δt_i
	Verification	
$\mathcal{T} = \mathrm{PRF}_{N_P}(\mathit{transcript})$	$\xrightarrow{\mathcal{T}}$	Check that $\mathcal{T} = \mathrm{PRF}_{N_P}(\mathit{transcript})$

A wrong challenge guess is detected!

Security: DF





Prover P | **Verifier** V

Initialisation

$$N_P \xleftarrow{\$} \{0,1\}^n \quad \xrightarrow{\{N_P,\sigma_P\}_{\mathrm{pk}_V}} \quad N_V \xleftarrow{\$} \{0,1\}^n$$

$$\xleftarrow{m, N_V} \quad m \xleftarrow{\$} \{0,1\}^n$$

$$a = \mathrm{PRF}_{N_P}(N_V)$$

Distance Bounding

for $i = 1$ to n

Pick $c_i \in \{0,1\}$

$$r_i = \begin{cases} a_i & \text{if } c_i = 0 \\ a_i \oplus N_{P_i} \oplus m_i & \text{if } c_i = 1 \end{cases} \quad \xleftarrow{c_i} \quad \textbf{Start clock}$$

$$\xrightarrow{r_i} \quad \textbf{Stop clock}$$

The mask m ensures that $r_i^0 \neq r_i^1$ for ≈ half the rounds

Outline

C-ROADS & IndID

Distance Bounding

SPADE

- Building Blocks
- Protocol
- Anonymity
- Terrorist Fraud
- Mafia Fraud
- Distance Fraud

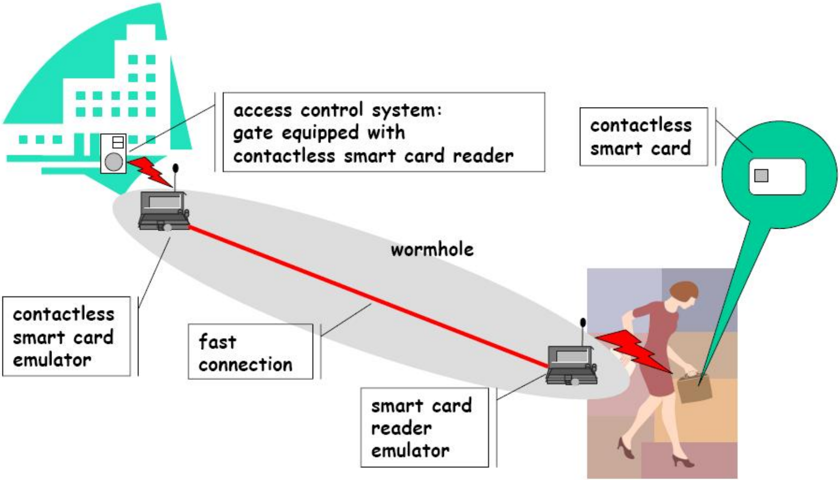
Security

Conclusion

Several Possible Attackers

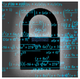
- Insider vs Outsider
- Active vs Passive
- Local vs Extended
- Single vs Multiple
- Laptop vs Server

Wormhole Attack



What is cryptography based security?

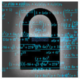
Cryptography:



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

What is cryptography based security?

Cryptography:



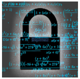
- Primitives: RSA, Elgamal, AES, DES, SHA-3 ...
- Protocols: Distributed Algorithms

Properties:

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

What is cryptography based security?

Cryptography:



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

Properties:

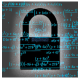
- Secrecy,
- Authentication,
- Privacy
- Non Repudiation ...

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

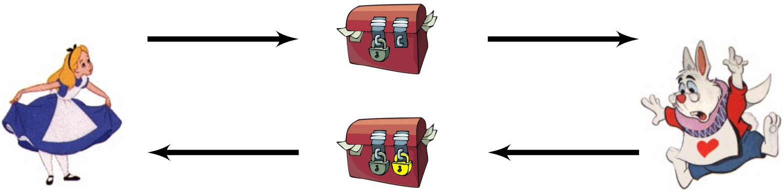
Environs 60 températures possibles: 35 ... 41

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

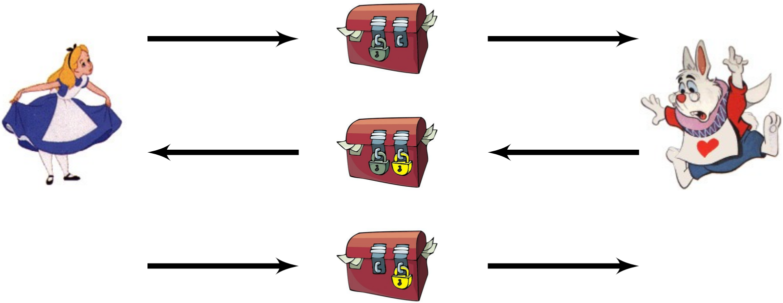
3-pass Shamir

3-pass Shamir

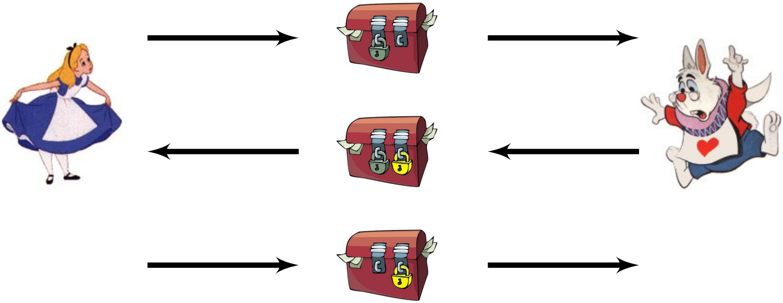
3-pass Shamir



3-pass Shamir



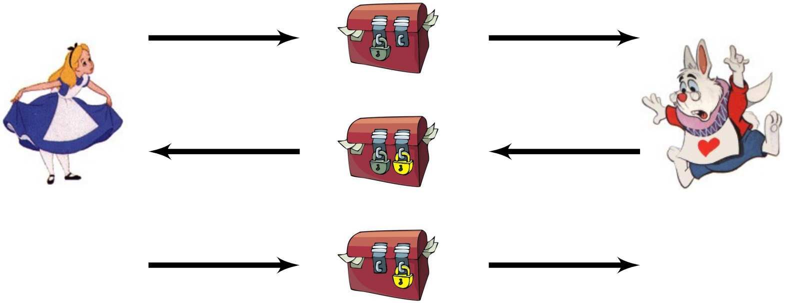
3-pass Shamir



Abstract Representation

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

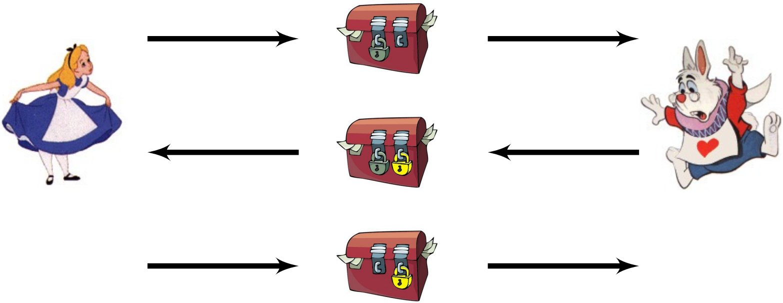
3-pass Shamir



Abstract Representation

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

3-pass Shamir

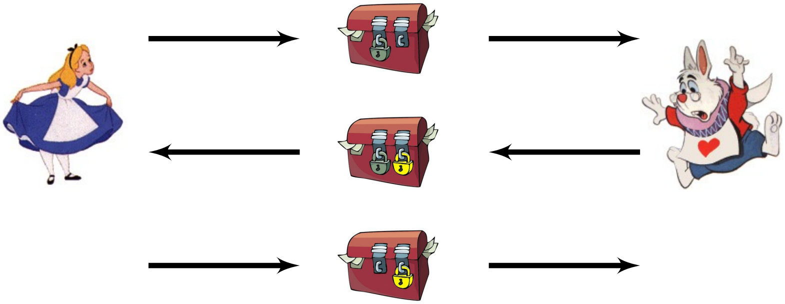


Abstract Representation

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

Commutative Encryption

3-pass Shamir



Abstract Representation

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

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
- $x \oplus y = y \oplus x$
  Commutativity
- $x \oplus 0 = x$ **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
- $x \oplus y = y \oplus x$
  Commutativity
- $x \oplus 0 = x$ **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

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

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

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

Passive attacker :

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

Second Example

Needham Schroeder Key Echange 1976

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

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

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

- 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

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

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

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

Broken 17 years after, by G. Lowe

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

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

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

Cryptography is not sufficient !

Example : Needham Schroeder Key Echange

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

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

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

Broken 17 years after, by G. Lowe

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

Computer-Aided Security

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.

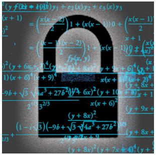
GOAL : A tool is finding flaws or establishing their correctness.

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

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

Formal Verification Approaches

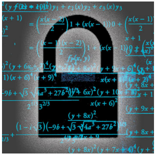
Designer



Attacker

Formal Verification Approaches

Designer

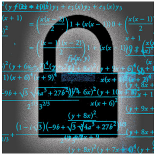


Attacker

Security Team

Formal Verification Approaches

Designer



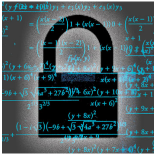
Attacker

Give a proof

Security Team

Formal Verification Approaches

Designer



Attacker

Give a proof

Find a flaw

Security Team

Applications

Outline

C-ROADS & IndID

Distance Bounding

SPADE

- Building Blocks
- Protocol
- Anonymity
- Terrorist Fraud
- Mafia Fraud
- Distance Fraud

Security

Conclusion

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 ⇒ Security

Thanks for your attention

Questions ?

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