Security Analysis of Distance Bounding Protocols

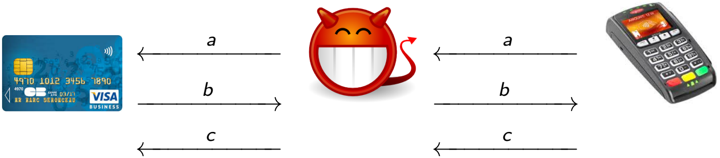
Agnes BRELURUT, Pascal LAFOURCADE, David GERAULT

LIMOS, Université d'Auvergne, France

September 17th 2015

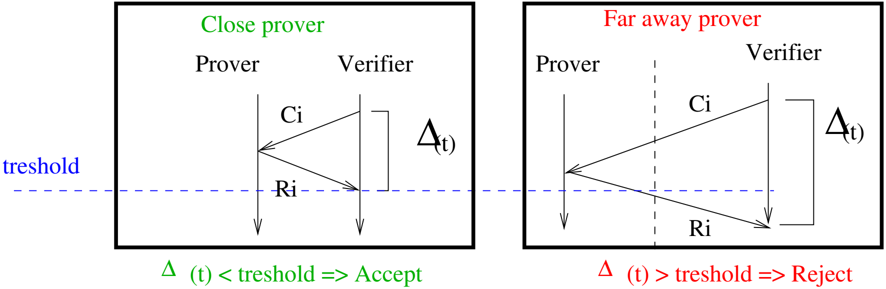
Context

Relay Attacks



Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars,
A. Francillon, 2011

Counter measure : RTT check



Brands & Chaum : Protocol

Verifier V public key : y		Prover P secret key : x
	Initialisation phase	
	$\xleftarrow{\text{commit(m)}}$	$m \xleftarrow{\$} \{0,1\}^n$
	Distance Bounding phase for $i = 1$ to n	
Pick $c_i \in \{0,1\}$		
Start clock	$\xrightarrow{c_i}$	
Stop clock	$\xleftarrow{r_i}$	$r_i := m_i \oplus c_i$
Check timers Δt_i		
	Verification phase	
Check responses	$\xleftarrow{\text{open commitment}}$	
Check signature	$\xleftarrow{\text{Sign}_x(S)}$	$S := c_1 \| r_1 \| ... \| c_n \| r_n$
	$\xrightarrow{\text{Out}_V}$	

Distance Bounding Protocol

Verifier V shared key : x		Prover P shared key : x
	Initialisation phase	
	$\xrightarrow{Messages_V}$	
	$\xleftarrow{Messages_P}$	
	$a = f_x(Messages_V, Messages_P)$	
	Distance Bounding phase	
	for $i = 1$ to n	
Start clock	$\xrightarrow{c_i}$	
Stop clock	$\xleftarrow{r_i}$	$r_i = F(c_i, a_i, x_i)$
	Verification phase	
Check Δt_i, r_i and S	$\xleftarrow{S}$	$S = sign_x(transcript)$

Honest Prover

Mafia Fraud (MF) : an adversary $\mathscr{A}$ tries to prove that a prover P is close to a verifier V.

$$\underbrace{P \leftrightarrow \mathscr{A} \leftrightarrow V}_{\text{far away}}$$

Honest Prover

Mafia Fraud (MF) : an adversary $\mathscr{A}$ tries to prove that a prover P is close to a verifier V.

$$\underbrace{P \leftrightarrow \mathscr{A} \leftrightarrow V}_{\text{far away}}$$

Impersonation Fraud (IF) : an adversary tries to impersonate the prover to the verifier.

$$\mathscr{A} \leftrightarrow V$$

Dishonest Prover

Distance Fraud : a far-away prover P^* tries to prove that he is close to a verifier V.

$P^* \leftrightarrow V$

Dishonest Prover

Distance Fraud : a far-away prover P^* tries to prove that he is close to a verifier V.

$$P^* \leftrightarrow V$$

Distance Hijacking (DH) : a far-away prover P^* tries to prove that he is close to a verifier V by taking advantage of others provers $P_1, .., P_n$.

$$P^* \leftrightarrow P_1, .., P_n \leftrightarrow V$$

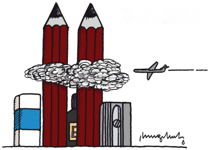
Dishonest Prover

Distance Fraud : a far-away prover P^* tries to prove that he is close to a verifier V.

$$P^* \leftrightarrow V$$

Distance Hijacking (DH) : a far-away prover P^* tries to prove that he is close to a verifier V by taking advantage of others provers $P_1, .., P_n$.

$$P^* \leftrightarrow P_1, .., P_n \leftrightarrow V$$



Terrorist Fraud (TF) : a far-away prover P^* helps an adversary $\mathscr{A}$ to prove that P^* is close to a verifier V without giving $\mathscr{A}$ another advantage.

$$P^* \leftrightarrow \mathscr{A} \leftrightarrow V$$

Motivations

- No exhaustive list of DB protocols.
- No compared or classified.
- No relationship between threat models.

Plan

1. Relations between Model of Threat
2. Attack and defence strategies
3. Conclusion and Perspective

Plan

1. Relations between Model of Threat
2. Attack and defence strategies
3. Conclusion and Perspective

The BMV Model(2013)

Distance Fraud (DF) :

$$P^*(x) \leftrightarrow (P_1(x'), \dots, P'_m(x') \leftrightarrow V_1(y'), \dots, V_m(y') \leftrightarrow) V(y; r_V)$$

Man-In-the-Middle (MiM) :

$$P_1(x), ..., P_m(x) \leftrightarrow \mathscr{A}_1 \leftrightarrow V_1(y), ..., V_z(y)$$
$$P_{m+1}(x), ..., P_l(x) \leftrightarrow \mathscr{A}_2(View_{\mathscr{A}_1}) \leftrightarrow V(y)$$

Collusion Fraud (CF) :

$$P^*(x) \leftrightarrow \mathscr{A}^{\mathrm{CF}} \leftrightarrow V_0(y)$$

- $X \rightarrow Y$ denotes that if the property X is satisfied then Y is also satisfied, an attack on the property Y implies an attack on the property X.

DF **MiM**

DH **CF**

TF MF IF

The BMV Model(2013)

Distance Fraud (DF) :

$$P^*(x) \leftrightarrow (P_1(x'), \ldots, P'_m(x') \leftrightarrow V_1(y'), \ldots, V_m(y') \leftrightarrow) V(y; r_V)$$

Man-In-the-Middle (MiM) :

$$P_1(x), ..., P_m(x) \leftrightarrow \mathscr{A}_1 \leftrightarrow V_1(y), ..., V_z(y)$$
$$P_{m+1}(x), ..., P_l(x) \leftrightarrow \mathscr{A}_2(View_{\mathscr{A}_1}) \leftrightarrow V(y)$$

Collusion Fraud (CF) :

$$P^*(x) \leftrightarrow \mathscr{A}^{\mathrm{CF}} \leftrightarrow V_0(y)$$

- $X \rightarrow Y$ denotes that if the property X is satisfied then Y is also satisfied, an attack on the property Y implies an attack on the property X.

The BMV Model(2013)

Distance Fraud (DF) :

$$P^*(x) \leftrightarrow (P_1(x'), \ldots, P'_m(x') \leftrightarrow V_1(y'), \ldots, V_m(y') \leftrightarrow) V(y; r_V)$$

Man-In-the-Middle (MiM) :

$$P_1(x), ..., P_m(x) \leftrightarrow \mathscr{A}_1 \leftrightarrow V_1(y), ..., V_z(y)$$
$$P_{m+1}(x), ..., P_l(x) \leftrightarrow \mathscr{A}_2(View_{\mathscr{A}_1}) \leftrightarrow V(y)$$

Collusion Fraud (CF) :

$$P^*(x) \leftrightarrow \mathscr{A}^{\mathrm{CF}} \leftrightarrow V_0(y)$$

- $X \rightarrow Y$ denotes that if the property X is satisfied then Y is also satisfied, an attack on the property Y implies an attack on the property X.

The BMV Model(2013)

Distance Fraud (DF) :

$$P^*(x) \leftrightarrow (P_1(x'), \ldots, P'_m(x') \leftrightarrow V_1(y'), \ldots, V_m(y') \leftrightarrow) V(y; r_V)$$

Man-In-the-Middle (MiM) :

$$P_1(x), ..., P_m(x) \leftrightarrow \mathscr{A}_1 \leftrightarrow V_1(y), ..., V_z(y)$$
$$P_{m+1}(x), ..., P_l(x) \leftrightarrow \mathscr{A}_2(View_{\mathscr{A}_1}) \leftrightarrow V(y)$$

Collusion Fraud (CF) :

$$P^*(x) \leftrightarrow \mathscr{A}^{\text{CF}} \leftrightarrow V_0(y)$$

- $X \rightarrow Y$ denotes that if the property X is satisfied then Y is also satisfied, an attack on the property Y implies an attack on the property X.

The BMV Model(2013)

Distance Fraud (DF) :

$$P^*(x) \leftrightarrow (P_1(x'), \ldots, P'_m(x') \leftrightarrow V_1(y'), \ldots, V_m(y') \leftrightarrow) V(y; r_V)$$

Man-In-the-Middle (MiM) :

$$P_1(x), \ldots, P_m(x) \leftrightarrow \mathscr{A}_1 \leftrightarrow V_1(y), \ldots, V_z(y)$$
$$P_{m+1}(x), \ldots, P_l(x) \leftrightarrow \mathscr{A}_2(View_{\mathscr{A}_1}) \leftrightarrow V(y)$$

Collusion Fraud (CF) :

$$P^*(x) \leftrightarrow \mathscr{A}^{\text{CF}} \leftrightarrow V_0(y)$$

- $X \rightarrow Y$ denotes that if the property X is satisfied then Y is also satisfied, an attack on the property Y implies an attack on the property X.
- $X \dashrightarrow Y$ denotes that an attack on the property Y without sending the secret x implies an attack on the property X.

TF $\dashrightarrow$ DF

- $X \dashrightarrow Y$ denotes that an attack on the property Y without sending the secret x implies an attack on the property X.

Theorem (TF $\dashrightarrow$ DF)

If a protocol is not α-resistant to DF, then there exists an attack of kind TF which succeed with probability at least α.

Proof : If $P^* \longleftrightarrow V$ succeeds, then $P^* \longleftrightarrow \mathscr{A}^{\text{TF}} \longleftrightarrow V$ succeeds with the same probability, if P^* does not transmit his secret and $\mathscr{A}^{\text{TF}}$ simply relays messages. □

TF $\dashrightarrow$ DF

- $X \dashrightarrow Y$ denotes that an attack on the property Y without sending the secret x implies an attack on the property X.

Theorem (TF $\dashrightarrow$ DF)

If a protocol is not α-resistant to DF, then there exists an attack of kind TF which succeed with probability at least α.

Proof : If $P^* \longleftrightarrow V$ succeeds, then $P^* \longleftrightarrow \mathscr{A}^{\text{TF}} \longleftrightarrow V$ succeeds with the same probability, if P^* does not transmit his secret and $\mathscr{A}^{\text{TF}}$ simply relays messages. □

TF $\dashrightarrow$ DF

- $X \dashrightarrow Y$ denotes that an attack on the property Y without sending the secret x implies an attack on the property X.

Theorem (TF $\dashrightarrow$ DF)

If a protocol is not α-resistant to DF, then there exists an attack of kind TF which succeed with probability at least α.

Proof : If $P^* \longleftrightarrow V$ succeeds, then $P^* \longleftrightarrow \mathscr{A}^{\mathrm{TF}} \longleftrightarrow V$ succeeds with the same probability, if P^* does not transmit his secret and $\mathscr{A}^{\mathrm{TF}}$ simply relays messages. □

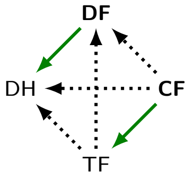
TF $\dashrightarrow$ DF

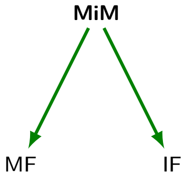
- $X \dashrightarrow Y$ denotes that an attack on the property Y without sending the secret x implies an attack on the property X.

Theorem (TF $\dashrightarrow$ DF)

If a protocol is not α-resistant to DF, then there exists an attack of kind TF which succeed with probability at least α.

Proof : If $P^* \longleftrightarrow V$ succeeds, then $P^* \longleftrightarrow \mathscr{A}^{\mathsf{TF}} \longleftrightarrow V$ succeeds with the same probability, if P^* does not transmit his secret and $\mathscr{A}^{\mathsf{TF}}$ simply relays messages. □



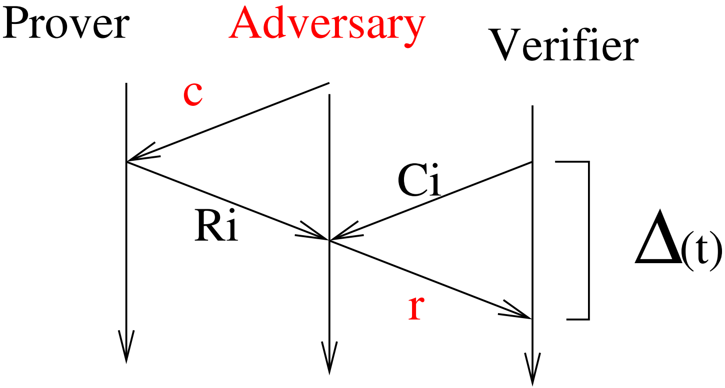


Plan

1. Relations between Model of Threat
2. **Attack and defence strategies**
3. Conclusion and Perspective

Attack Strategies : Mafia Fraud

- Pre ask strategy

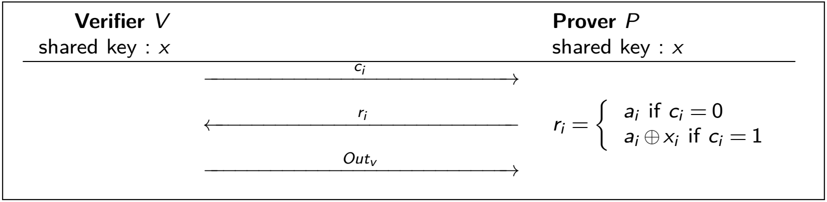


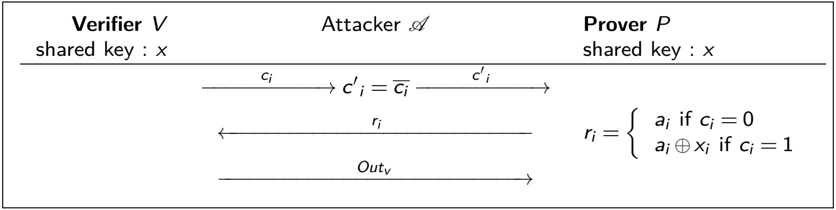
If $c == c_i$*,* $\mathscr{A}$ *knows* r_i*. Else, he has to guess.* $\mathscr{A}$ *wins if he gives a good* r_i *at all rounds*

$\left(\frac{1}{2}\cdot 1+\frac{1}{2}\cdot\frac{1}{2}\right)^n=\left(\frac{3}{4}\right)^n$. Defence : Signature of the transcript

Attack Strategies : Impersonation Fraud

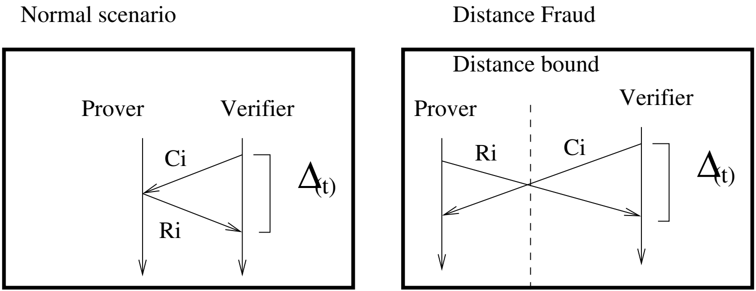
- Key recovery





If $Out_v = 1$, $a_i == a_i \oplus x_i$, so $x_i = 0$. Else, $x_i = 1$. After n executions, $\mathscr{A}$ recovers the whole key ! Defense : The responses can not just be a xor between the key and a one time pad.

Attack Strategies : Distance fraud



Two possible responses : if $c_i = 0$, $r_i = a_i$ and if $c_i = 1$, $r_i = b_i$.
$\left(\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2}\right)^n = \left(\frac{3}{4}\right)^n$.

- Defence : The 2 possible responses should be complementary

Attack Strategies : Distance fraud : Example

Let g be a PRF and f a PRF constructed as follows :

$$f_x(M_V, M_P) = \begin{cases} a||a \text{ if } M_P = z \\ g_x(M_V, M_P) \text{ otherwise} \end{cases} \quad f_x \text{ is a PRF.}$$

Verifier V		**Prover** P
shared key : x		shared key : x
	Initialisation phase	
	$\xrightarrow{M_V}$	
	$\xleftarrow{M_P}$	$M_P = z$
	$a\|\|a = f_x(M_V, M_P)$	
	Distance Bounding phase	
	for $i = 1$ to n	
Start clock		
Stop clock	$\xleftarrow{r_i}$	$r_i = \begin{cases} a_i \text{ if } c_i = 0 \\ a_i \text{ if } c_i = 1 \end{cases}$
	$\xrightarrow{c_i}$	
Check Δt_i, r_i		

Defense : The PRF output should not be split in several parts.

Attack Strategies : Terrorist fraud

Verifier V shared key : x	Accomplice $\mathscr{A}$	**Prover** P shared key : x
	Initialisation phase	
	$\xrightarrow{NV}$	
	$\xleftarrow{NP}$	
$a = f_x(NP, NV)$		$a = f_x(NV, NP)$
Stop clock	$\xleftarrow{a}$	
	Distance Bounding phase for $i = 1$ to n	
Start clock	$\xrightarrow{c_i}$	
Stop clock	$\xleftarrow{r_i}$ $r_i = a_i \oplus c_i$	
	Verification phase	
Check Δt_i, r_i and S	$\xleftarrow{S}$	$S = sign_x(transcript)$

P can give a to $\mathscr{A}$ and allow a terrorist fraud with success probability 1, since a does not link any information about the secret key. Defense : Making the responses related to the key

Improvements of Attacks : TF, IF, DH

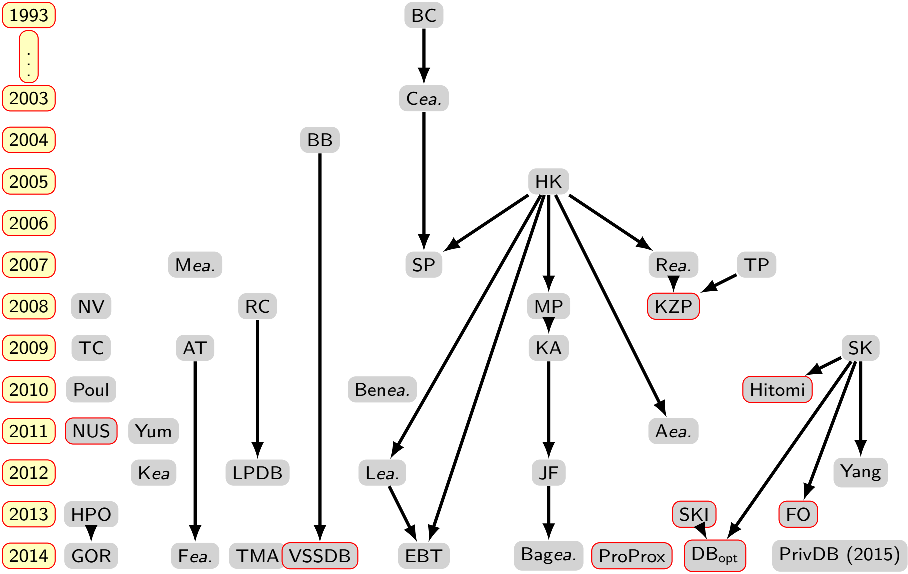
IF : Threat model few considered.
Exhaustive research on the key.
$\left(\frac{1}{2}\right)^s$, where s is the size of the key.

DH : Threat model few considered.
P^* hopes that P responds correctly to V.
$\left(\frac{1}{2}\right)^n$, where n is the number of round in the DB phase.

TF : P^* gives responses to $\mathscr{A}$. So, TF mainly filled with 1.

Survey

- 42 protocols from 1993 to 2015.



Survey

- 82 improvements = 28 DH + 10 DF + 0 MF + 30 IF + 1 MiM + 13 TF/CF.

Survey

- 82 improvements = 28 DH + 10 DF + 0 MF + 30 IF + 1 MiM + 13 TF/CF.
- 9 survivors : no attacks with probability of success at 1.

Survey

- 82 improvements = 28 DH + 10 DF + 0 MF + 30 IF + 1 MiM + 13 TF/CF.
- 9 survivors : no attacks with probability of success at 1.

Protocols	Success Probability						
	DH	**DF**	MF	IF	**MiM**	TF	**CF**
KZP (2008)	$(\frac{1}{2})^n$	$(\frac{3}{4})^n$ [8]	$(\frac{1}{2})^n$ [8]	$(\frac{1}{2})^s$	$(\frac{1}{2})^n$ [8]	$(\frac{3}{4})^v$ [8]	$(\frac{3}{4})^v$ [8]
Hitomi (2010)	$(\frac{1}{2})^n$ [5]	$(\frac{3}{4})^n$	$(\frac{1}{2})^n$ [9]	$(\frac{1}{2})^n$	$(\frac{1}{2})^n$ [9]	$(\frac{3}{4})^v$ [9]	$(\frac{3}{4})^v$ [9]
NUS (2011)	$(\frac{1}{2})^n$	$(\frac{3}{4})^n$ [1]	$(\frac{1}{2})^n$ [7]	$(\frac{1}{2})^n$ [7]	$(\frac{1}{2})^n$ [7]	$(\frac{3}{4})^v$	$(\frac{3}{4})^v$
SKI_{pro} (2013)	$(\frac{1}{2})^n$	$(\frac{3}{4})^n$ [2]	$(\frac{2}{3})^n$ [2]	$(\frac{1}{2})^s$	$(\frac{2}{3})^n$ [2]	$(\frac{5}{6})^v$ [3]	$(\frac{5}{6})^v$ [3]
Fischlin & Onete (2013)	$(\frac{1}{2})^n$	$(\frac{3}{4})^n$ [10]	$(\frac{3}{4})^n$ [10]	$(\frac{1}{2})^{2s}$	$(\frac{3}{4})^n$ [10]	$(\frac{3}{4})^v$ [10]	$(\frac{3}{4})^v$ [10]
DB1 (2014)	$(\frac{1}{t})^n$	$(\frac{1}{t})^n$ [4]	$(\frac{1}{t})^n$ [4]	$(\frac{1}{2})^s$	$(\frac{1}{t})^n$ [4]	$(\frac{t-1}{t})^v$ [4]	$(\frac{t-1}{t})^v$ [4]
DB2 (2014)	$(\frac{1}{2})^n$	$\left(\frac{1}{\sqrt{2}}\right)^n$ [4]	$(\frac{1}{2})^n$ [4]	$(\frac{1}{2})^s$	$(\frac{1}{2})^n$ [4]	$\left(\frac{1}{\sqrt{2}}\right)^v$ [4]	$\left(\frac{1}{\sqrt{2}}\right)^v$ [4]
ProProx (2014)	$(\frac{1}{2})^{n \cdot s}$	$\left(\frac{1}{\sqrt{2}}\right)^{ns}$ [11]	$(\frac{1}{2})^{ns}$ [11]	$(\frac{1}{2})^s$ [11]	$(\frac{1}{2})^{ns}$ [11]	$\left(\frac{1}{\sqrt{2}}\right)^{ns}$ [11]	$\left(\frac{1}{\sqrt{2}}\right)^{ns}$ [11]
VSSDB (2014)	$(\frac{1}{2})^n$	$(\frac{3}{4})^n$ [6]	$(\frac{1}{2})^n$ [6]	$(\frac{1}{2})^{2s}$ [6]	$(\frac{1}{2})^n$ [6]	$(\frac{3}{4})^v$ [6]	$(\frac{3}{4})^v$ [6]

Plan

1 Relations between Model of Threat

2 Attack and defence strategies

3 Conclusion and Perspective

Conclusion and Perspective

- The **relationship** between threats models.
- Identify more easily the properties of a DB protocols.
- Compilation and classification of **42 protocols**.
- **Graph of dependency**.
- **82 improvements** of attacks.
- **9 still secure** protocols.
- **Tool box :** strategies of attack/defense.

Conclusion and Perspective

- The **relationship** between threats models.
- Identify more easily the properties of a DB protocols.
- Compilation and classification of **42 protocols**.
- **Graph of dependency**.
- **82 improvements** of attacks.
- **9 still secure** protocols.
- **Tool box :** strategies of attack/defense.

Futur works :

- Formal verification.
- Best protocol design.

Thanks for your attention !

Questions ?

References I

Mohammad Reza Sohizadeh Abyaneh.
Security analysis of two distance-bounding protocols.
CoRR, abs/1107.3047, 2011.

Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay.
Practical & provably secure distance-bounding.
IACR Cryptology ePrint Archive, 2013 :465, 2013.

Ioana Boureanu, Aikaterini Mitrokotsa, and Serge Vaudenay.
Towards secure distance bounding.
In *Fast Software Encryption - 20th International Workshop, FSE 2013*, pages 55–67, Singapore, March 2013.

Ioana Boureanu and Serge Vaudenay.
Optimal proximity proofs.
In *Information Security and Cryptology - 10th International Conference, Inscrypt 2014, Beijing, China, December 13-15, 2014, Revised Selected Papers*, pages 170–190, 2014.

References II

Cas Cremers, Kasper Bonne Rasmussen, Benedikt Schmidt, and Srdjan Capkun.
Distance hijacking attacks on distance bounding protocols.
In *IEEE Symposium on Security and Privacy*, 2012.

Sébastien Gambs, Marc-Olivier Killijian, Cédric Lauradoux, Cristina Onete, Matthieu Roy, and Moussa Traoré.
VSSDB : A Verifiable Secret-Sharing and Distance-Bounding protocol.
In *International Conference on Cryptography and Information security (BalkanCryptSec'14)*, Istanbul, Turkey, October 2014.

Ali Özhan Gürel, Atakan Arslan, and Mete Akgün.
Non-uniform stepping approach to rfid distance bounding problem.
In *Proceedings of the 5th International Workshop on Data Privacy Management, and 3rd International Conference on Autonomous Spontaneous Security*, DPM'10/SETOP'10, pages 64–78, Berlin, Heidelberg, 2011. Springer-Verlag.

References III

Gaurav Kapoor, Wei Zhou, and Selwyn Piramuthu.
Distance bounding protocol for multiple RFID tag authentication.
In *2008 IEEE/IPIP International Conference on Embedded and Ubiquitous Computing (EUC 2008), Shanghai, China, December 17-20, 2008, Volume II : Workshops*, pages 115–120, 2008.

Pedro Peris-Lopez, Julio César Hernández Castro, Juan M. Estévez-Tapiador, and Jan C. A. van der Lubbe.
Shedding some light on RFID distance bounding protocols and terrorist attacks.
CoRR, abs/0906.4618, 2009.

Serge Vaudenay.
On modeling terrorist fraud.
In *Provable security - 7th International Conference, ProvSec 2013, Melaka, Malaysia, October 23-25, 2013, Proceedings*, pages 1–20, 2013.

Serge Vaudenay.
Proof of proximity of knowledge.
IACR Cryptology ePrint Archive, 2014 :695, 2014.

References IV