

On the Need for Provably Secure Distance Bounding

Ioane Boureanu

Ecole Polytechnique Fédérale de Lausanne (EPFL)

ESC2013

Outline

- 1 **Topic and Aim**
- 2 **Intro to Distance-Bounding**
 - Distance-Bounding
- 3 **DB Security Threats**
- 4 **Security Flaws**
 - PRF (unfortunate) choices
 - “Unnecessary” PK & Unfortunate Encryption Choices
- 5 **Secure DB?**

Outline

- 1 **Topic and Aim**
- 2 **Intro to Distance-Bounding**
 - Distance-Bounding
- 3 **DB Security Threats**
- 4 **Security Flaws**
 - PRF (unfortunate) choices
 - “Unnecessary” PK & Unfortunate Encryption Choices
- 5 **Secure DB?**

Message

Generic

Many formal and informal security results on distance-bounding (DB) are flawed.

Specific

- The PRF assumption does **NOT** protect against distance fraud or MiM!
- PK-techniques are **NOT** enough against terrorist fraud!
- Certain instances of symmetric encryption schemes used inside DB lead to MiM attacks!

Outline

- 1 Topic and Aim
- 2 Intro to Distance-Bounding**
 - Distance-Bounding
- 3 DB Security Threats
- 4 Security Flaws
 - PRF (unfortunate) choices
 - “Unnecessary” PK & Unfortunate Encryption Choices
- 5 Secure DB?

Distance-Bounding (DB) Protocols

DB Essentials

- introduced by Brands and Chaum in [2]
- **cryptographically enhanced** verification of an upper-bound distance between a prover tag P and a verifier reader V (i.e., attempting to detect delays **and other frauds** in the prover's responses)
- implemented versions of DB protocols have only proven to be efficient in preventing relay attacks [3].

Distance-Bounding (DB) Protocols

Why do we care then?

- see secure remote unlocking (e.g., [5]) \Rightarrow distance-bounding protocols should be designed to resist against more generic attacks
- and formal models and proofs have some shortfalls!

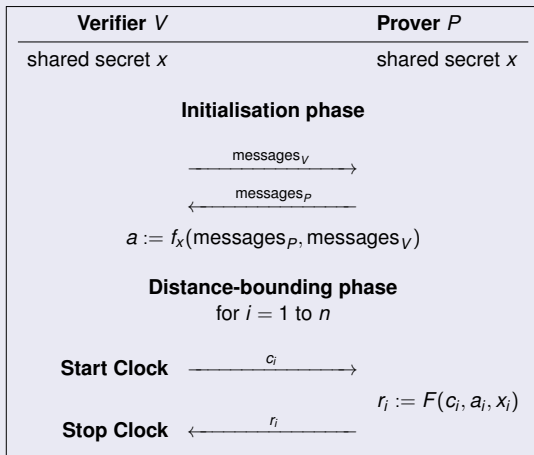
Distance-Bounding (DB) Protocols

Why do we care then?

- see secure remote unlocking (e.g., [5]) \Rightarrow distance-bounding protocols should be designed to resist against more generic attacks
- and formal models and proofs have some shortfalls!

Distance-Bounding (DB) Protocols

An Idea of Most DB (generalising, e.g., [7, 6])



Distance-Bounding (DB) Protocols

- DB relies on a cryptographic exchange, part of which is timed; the round-trip-time is then used to estimate the distance between P and V
- DB is not a service for secure location (i.e., the verifier/reader is not assisted by base stations in his decisions)
- DB should be a secure proximity-identification service, using time-of-flight (ToF) measurements

Outline

- 1 Topic and Aim
- 2 Intro to Distance-Bounding
 - Distance-Bounding
- 3 DB Security Threats**
- 4 Security Flaws
 - PRF (unfortunate) choices
 - “Unnecessary” PK & Unfortunate Encryption Choices
- 5 Secure DB?

Attacks

Distance Fraud:

$$\underbrace{P^* \leftrightarrow V}_{\text{far-away}}$$

- Distance-Bounding Protocols (Extended Abstract). [Brands and Chaum, EUROCRYPT93]
 - the prover is dishonest and far-away, but tries to convince the verifier that he's close [2]

Attacks

Mafia Fraud:

$$\underbrace{P \stackrel{\leftarrow}{\rightleftarrows} \mathcal{A} \stackrel{\leftarrow}{\rightleftarrows} V}_{\text{far-away}}$$

- Major Security Problems with the “Unforgeable” (Feige)-Fiat-Shamir Proofs of Identity and How to Overcome Them [Desmedt SECURICOM 1988]
 - an intruder exploits an honest prover and an honest verifier to show that the latter is close to the former, when this is not the case;

Attacks

MiM Attack:

$$\underbrace{P \rightleftarrows A \rightleftarrows V}_{\text{far-away}}$$

- MiM intruder, in presence of possibly several provers and several verifiers, tries to mount an attack in which he gains the privileges of one of the provers

Attacks

Terrorist Fraud

$$\underbrace{P^* \rightleftarrows A \rightleftarrows V}_{\text{far-away}}$$

- Major Security Problems with the “Unforgeable” (Feige)-Fiat-Shamir Proofs of Identity and How to Overcome Them [Desmedt SECURICOM 1988]
 - a corrupted/coerced prover collaborates with an attacker to prove that the former is close to a far-away verifier
 - the “terrorist” would not disclose his secret key

Other Attacks

Distance Hijacking Fraud

- Distance Hijacking Attacks on Distance Bounding Protocols [Cremers-Rasmussen-Čapkun IEEE S&P 2012]
 - a “mixture” of distance fraud and terrorist fraud
 - a far-away dishonest prover is “abusing” several provers who are close to a verifier V in order to prove that he is close to V

Other Attacks

Distance Hijacking Fraud

- Distance Hijacking Attacks on Distance Bounding Protocols [Cremers-Rasmussen-Čapkun IEEE S&P 2012]
 - a “mixture” of distance fraud and terrorist fraud
 - a far-away dishonest prover is “abusing” several provers who are close to a verifier V in order to prove that he is close to V

Impersonation Fraud

- A Formal Approach to Distance Bounding RFID Protocols [Dürholz-Fischlin-Kasper-Onete ISC 2011]
 - one corrupted prover tries to pass as another prover

Outline

- 1 Topic and Aim
- 2 Intro to Distance-Bounding
 - Distance-Bounding
- 3 DB Security Threats
- 4 **Security Flaws**
 - PRF (unfortunate) choices
 - “Unnecessary” PK & Unfortunate Encryption Choices
- 5 Secure DB?

DB Instability

- most of the (in)security results = attack strategies, **NOT** security proofs in security models
- some security models [4] contain incorrect proofs/arguments:
 - ! replacing a PRF by a random function at a place where the adversary has access to the PRF key or at a place where the PRF key is simultaneously used at other places in the protocol
- other problems (e.g., PK not enough to deter TF & symm. encryptions used inside may lead to MiM attacks)

DB Instability

- most of the (in)security results = attack strategies, **NOT** security proofs in security models
- some security models [4] contain incorrect proofs/arguments:
 - ! replacing a PRF by a random function at a place where the adversary has access to the PRF key or at a place where the PRF key is simultaneously used at other places in the protocol
- other problems (e.g., PK not enough to deter TF & symm. encryptions used inside may lead to MiM attacks)

DB Instability

- most of the (in)security results = attack strategies, **NOT** security proofs in security models
- some security models [4] contain incorrect proofs/arguments:
 - ! replacing a PRF by a random function at a place where the adversary has access to the PRF key or at a place where the PRF key is simultaneously used at other places in the protocol
- other problems (e.g., PK not enough to deter TF & symm. encryptions used inside may lead to MiM attacks)

Trapdoor PRFs in DB

Idea

- out of a PRF \mathcal{G} , construct another PRF \mathcal{F} with $f(\text{trapdoor}) = \text{special_value}$ for $f \in \mathcal{F}$

Trapdoor PRFs in DB

Idea to prove the PRF assumption is not enough for DB

- On the Pseudorandom Function Assumption in (Secure) Distance-Bounding Protocols [Boureau-Mitrokotsa-Vaudenay Latincrypt 2012]
 - out of a PRF \mathcal{G} , construct another PRF \mathcal{F} with $f(\text{trapdoor}) = \text{special_value}$ for $f \in \mathcal{F}$

Trapdoor PRFs in DB

Idea to prove the PRF assumption is not enough for DB

- On the Pseudorandom Function Assumption in (Secure) Distance-Bounding Protocols [Boureau-Mitrokotsa-Vaudenay Latincrypt 2012]
 - out of a PRF \mathcal{G} , construct another PRF \mathcal{F} with $f(\text{trapdoor}) = \text{special_value}$ for $f \in \mathcal{F}$

Result

- distance-frauds exhibited on several DB protocols
- mafia-frauds exhibited on several DB protocols

Trapdoor PRFs in DB

Idea to prove the PRF assumption is not enough for DB

- On the Pseudorandom Function Assumption in (Secure) Distance-Bounding Protocols [Boureau-Mitrokotsa-Vaudenay Latincrypt 2012]
 - out of a PRF \mathcal{G} , construct another PRF \mathcal{F} with $f(\text{trapdoor}) = \text{special_value}$ for $f \in \mathcal{F}$

“Formal” Intuition

$$f_k(x) = \begin{cases} \sigma(k, x), & \text{if } x \in \text{correctPad}(k) \\ g_k(x), & \text{otherwise.} \end{cases}$$

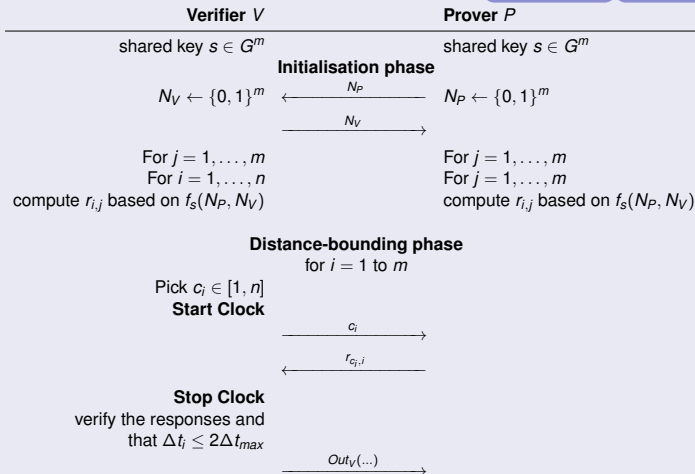
Result

- distance-frauds exhibited on several DB protocols
- mafia-frauds exhibited on several DB protocols

Trapdoor PRFs \Rightarrow DF and MiM Attacks

Example: The TDB [1] Protocol

▶ ||MiM attack) ▶ ||DF attack)



Trapdoor PRFs \Rightarrow DF and MiM Attacks

Frequent Instance of TDB

- $n = k = 3, G = F_2$
- the $3 \times m$ response-matrix of the form:

$$\mathcal{R}_1 = \begin{pmatrix} r_{1,1} & \cdots & r_{1,m} \\ r_{2,1} & \ddots & r_{2,m} \\ s_1 \oplus r_{1,1} \oplus r_{2,1} & \cdots & s_m \oplus r_{1,m} \oplus r_{2,m} \end{pmatrix}$$

Trapdoor PRFs \Rightarrow DF and MiM Attacks

DF Attack on TDB

Let g be a PRF from $\{0, 1\}^{2m}$ to itself.

Take the PRF f as follows:

$$f_s(N_P, N_V) = \begin{cases} s \parallel s, & \text{if } N_P = s \\ g_s(N_P, N_V), & \text{otherwise} \end{cases}$$

Let P^* choose $N_P = s$

\Rightarrow the \mathcal{R}_1 matrix has all its rows equal to s

\Rightarrow for all c_i the response will be the i -th bit of the secret key s

$\Rightarrow P^*$ can win a DF!

!! • the PRF assumption is not enough for the security of the TDB protocols against DF!

Trapdoor PRFs \Rightarrow DF and MiM Attacks

MiM Attack on TDB

Let a $g_s(N_P, N_V) = (\alpha, \beta, \gamma)$ be PRF instance.

Let f be as follows:

$$f_s(N_P, N_V) = \begin{cases} (\alpha, \beta, \gamma, \beta \oplus g_s(\alpha)), & \text{if } N_V \text{ is not of the form} \\ & \bar{\alpha} \parallel (g_s(\bar{\alpha}) \oplus \text{lsb}_{\frac{m}{2}}(s)) \\ & \text{and } (\alpha, \beta, \gamma) = g_s(N_P, N_V) \\ s \parallel s, & \text{if } N_V = \bar{\alpha} \parallel (g_s(\bar{\alpha}) \oplus \text{lsb}_{\frac{m}{2}}(s)), \\ & \text{for some } \bar{\alpha} \end{cases}$$

(cnf. to previous notations, $r_1 = (\alpha, \beta)$ and $r_2 = (\gamma, \beta \oplus g_s(\alpha))$)

Trapdoor PRFs \Rightarrow DF and MiM Attacks

MiM Attack on TDB



- STEP 1: the attacker \mathcal{A} impersonates first V to P
 - ★ \mathcal{A} sends an arbitrary N_V , so P calculates some subsecret vectors $(\alpha', \beta', \gamma', \psi')$ for $(\alpha, \beta, \gamma, \beta \oplus g_s(\alpha))$
 - ★ \mathcal{A} sends many challenges equal to 1, $c_i = 1$, e.g., for $i \in \{1, \dots, \frac{m}{2}\}$
 $\Rightarrow \mathcal{A}$ gets the first half of the first subsecret-vector
 $r_1 = (\alpha, \beta)$, i.e., \mathcal{A} obtains α
 - ★ \mathcal{A} sends P many challenges equal to 3, some $c_i = 3$
 \Rightarrow responses to the latest challenges are equal to
 $r_1 + r_2 + s = (\alpha, \beta) \oplus (\gamma, \beta \oplus g_s(\alpha)) \oplus s = (\alpha \oplus \gamma, g_s(\alpha)) \oplus s$
 $\Rightarrow \mathcal{A}$ knows $g_s(\alpha) \oplus \text{lsb}_{\frac{m}{2}}(s)$
 $\Rightarrow \mathcal{A}$ can form $N'_V = \alpha \parallel (g_s(\alpha) \oplus \text{lsb}_{\frac{m}{2}}(s))$

Trapdoor PRFs \Rightarrow DF and MiM Attacks

MiM Attack on TDB



- STEP 2: the attacker \mathcal{A} impersonates again V to P
 - ★ \mathcal{A} makes this new session' N_V equal to N'_V above
 - ★ injecting any challenges to the prover, \mathcal{A} knows (due to the built-in PRF) that P 's responses are the bits of s

\Rightarrow \mathcal{A} will eventually learn the whole of the secret key and he will be subsequently able to impersonate this prover in any circumstance.
- !! ● the PRF assumption is not enough for the security of the TDB protocols against MiM!

Other Results based on Programmed PRFs

- On the Pseudorandom Function Assumption in (Secure) Distance-Bounding Protocols

[Boureau-Mitrokovska-Vaudenay Latincrypt 2012]

protocol	distance fraud	man-in-the-middle attack
TDB Avoine-Lauradoux-Martin [ACM WiSec 2011]	✓	✓
Dürholz-Fischlin-Kasper-Onete [ISC 2011]	✓	–
Hancke-Kuhn [Securecomm 2005]	✓	–
Avoine-Tchamkerten [ISC 2009]	✓	–
Reid-Nieto-Tang-Senadji [ASIACCS 2007]	✓	✓
Swiss-Knife Kim-Avoine-Koeune- Standaert-Pereira [ICISC 2008]	–	✓

“Unnecessary” PK & Unfortunate Encryption Choices

The Bussard-Bagga (BB) Protocols

[Bussard-Bagga IFIP SEC 2005]

Verifier

public key: y

Prover

secret key: x

initialization phase

pick $k, v, v', e = \text{Enc}_k(x), e = (ux - k) \bmod p - 1$

$Z_{k,i} = \text{commit}(k_i, v_i)$

$z_{e,i} = \text{commit}(e_i, v'_i)$

where $\text{commit}(b, v) = g^b h^v \bmod p$ with g, h of \mathbf{Z}_p^* and

$z = \text{comm}((k + e) \bmod (p - 1), v)$; $z = \prod_i (z_{k,i} z_{e,i})^{2^{i-1}}$, $v = \sum_i (v_i + v'_i) 2^{i-1}$

← z_k, z_e

distance bounding phase

for $i = 1$ to n

pick c_i

start clock

stop clock

→ c_i

← r_i

$$r_i = \begin{cases} k_i & \text{if } c_i = 0 \\ e_i & \text{if } c_i = 1 \end{cases}$$

termination phase

check openable commitments

check timers

← γ

$$\gamma_i = \begin{cases} v_i & \text{if } c_i = 0 \\ v'_i & \text{if } c_i = 1 \end{cases}$$

← PoK(x)...

← Out_v

On the Instances & Follow-ups of Bussard-Bagga

- BB instances to protect against terrorist fraud
 - addition modulo $p - 1$ DBPK-Log:
$$\text{Enc}_k(x) = x - k \bmod p - 1$$
 - modular addition with random factor DBPK-Log:
$$\text{Enc}_k(x; u) = (u, ux - k \bmod p - 1)$$
- BB's “children”

On the Instances & Follow-ups of Bussard-Bagga

- BB instances to protect against terrorist fraud
 - **addition modulo $p - 1$ DBPK-Log:**
 $\text{Enc}_k(x) = x - k \bmod p - 1$
 - modular addition with random factor DBPK-Log:
 $\text{Enc}_k(x; u) = (u, ux - k \bmod p - 1)$
- BB's “children”

On the Instances & Follow-ups of Bussard-Bagga

- BB instances to protect against terrorist fraud
 - **addition modulo $p - 1$ DBPK-Log:**
 $\text{Enc}_k(x) = x - k \bmod p - 1$
 - **modular addition with random factor DBPK-Log:**
 $\text{Enc}_k(x; u) = (u, ux - k \bmod p - 1)$
- BB's “children”
 - e.g., Reid *et al.* protocol with $\text{Enc}_k(x)$ as per the above

On the Instances & Follow-ups of Bussard-Bagga

- BB instances to protect against terrorist fraud
 - **addition modulo $p - 1$ DBPK-Log:**
$$\text{Enc}_k(x) = x - k \bmod p - 1$$
 - **modular addition with random factor DBPK-Log:**
$$\text{Enc}_k(x; u) = (u, ux - k \bmod p - 1)$$
- BB's “children”
 - e.g., Reid *et al.* protocol with $\text{Enc}_k(x)$ as per the above

On the Instances & Follow-ups of Bussard-Bagga

- BB instances to protect against terrorist fraud
 - **addition modulo $p - 1$ DBPK-Log:**
 $\text{Enc}_k(x) = x - k \bmod p - 1$
 - **modular addition with random factor DBPK-Log:**
 $\text{Enc}_k(x; u) = (u, ux - k \bmod p - 1)$
- BB's “children”
 - e.g., Reid *et al.* protocol with $\text{Enc}_k(x)$ as per the above

TF on BB (Cont'd)

- it succeeds with prob. $\frac{1}{2}$ (or even 1 if the verifier allows an error in the first round)
- the proof-of-knowledge is zero-knowledge and x is not used anywhere else \Rightarrow the adversary learns no information about $x \Rightarrow$ it is a valid terrorist fraud
- it can be transformed in a DF
 - P^* can take $k_i = e_i, i = 2, \dots, m$
 - if x is even, P^* can select $k = e = \frac{x}{2}$ and $u = 1$ and we have $r_i = k_i = e_i$ for every i .
 - if x is odd, P^* can select $k = \frac{x-1}{2}, e = \frac{x+1}{2}$, and $u = 1$ so that $r_i = k_i = e_i$ for $i \geq 2$.



“Unnecessary” PK & Unfortunate Encryption Choices

MiM Attacks on Bussard-Bagga’s “Children”

- The Bussard-Bagga and Other Distance-Bounding Protocols under Man-in-the-Middle Attacks [Bay-Boureau-Mitrokotsa-Spulber-Vaudenay Inscrypt 2012]
- MiM attacks, exploiting the different instantiations of the symmetric encryption inside Bussard-Bagga’s followers, e.g., in Reid *et al.*

▶ [||later>](#)

Outline

- 1 Topic and Aim
- 2 Intro to Distance-Bounding
 - Distance-Bounding
- 3 DB Security Threats
- 4 Security Flaws
 - PRF (unfortunate) choices
 - “Unnecessary” PK & Unfortunate Encryption Choices
- 5 Secure DB?

Problem 1: Integrate Time in the Communication Model

- all communication are subject to a transmission speed limit!
- information is broadcast, local on a growing sphere
- adversary is also local (maybe several adversaries)
- adversary can impersonate and change the message destination
- honest people only see messages for which they are destinator
- all communication is subject to random noise with caveat:
 - adversary sees message with no noise (better equipment)
 - if time allows, honest participants see message with no noise (error correction)

Problem 1: Integrate Time in the Communication Model

- all communication are subject to a transmission speed limit!
- information is broadcast, local on a growing sphere
- adversary is also local (maybe several adversaries)
- adversary can impersonate and change the message destination
- honest people only see messages for which they are destinator
- all communication is subject to random noise with caveat:
 - adversary sees message with no noise (better equipment)
 - if time allows, honest participants see message with no noise (error correction)

Problem 1: Integrate Time in the Communication Model

- all communication are subject to a transmission speed limit!
- information is broadcast, local on a growing sphere
- adversary is also local (maybe several adversaries)
- adversary can impersonate and change the message destination
- honest people only see messages for which they are destinator
- all communication is subject to random noise with caveat:
 - adversary sees message with no noise (better equipment)
 - if time allows, honest participants see message with no noise (error correction)

Problem 1: Integrate Time in the Communication Model

- all communication are subject to a transmission speed limit!
- information is broadcast, local on a growing sphere
- adversary is also local (maybe several adversaries)
- adversary can impersonate and change the message destination
- honest people only see messages for which they are destinator
- all communication is subject to random noise with caveat:
 - adversary sees message with no noise (better equipment)
 - if time allows, honest participants see message with no noise (error correction)

Problem 1: Integrate Time in the Communication Model

- all communication are subject to a transmission speed limit!
- information is broadcast, local on a growing sphere
- adversary is also local (maybe several adversaries)
- adversary can impersonate and change the message destination
- honest people only see messages for which they are destinator
- all communication is subject to random noise with caveat:
 - adversary sees message with no noise (better equipment)
 - if time allows, honest participants see message with no noise (error correction)

Problem 1: Integrate Time in the Communication Model

- all communication are subject to a transmission speed limit!
- information is broadcast, local on a growing sphere
- adversary is also local (maybe several adversaries)
- adversary can impersonate and change the message destination
- honest people only see messages for which they are destinator
- all communication is subject to random noise with caveat:
 - adversary sees message with no noise (better equipment)
 - if time allows, honest participants see message with no noise (error correction)

Problem 2: Find a General Threat Model

- **distance fraud:**

- $P(x)$ far from all $V(x)$'s want to make one $V(x)$ accept (interaction with other $P(x')$ and $V(x')$ possible anywhere)
- → also captures distance hijacking

- **man-in-the-middle:**

- *learning phase:* \mathcal{A} interacts with many P 's and V 's

- **collusion fraud:**

- $P(x)$ far from all $V(x)$'s interacts with \mathcal{A} and makes one $V(x)$ accept, but $\text{View}(\mathcal{A})$ does not give any advantage to mount a man-in-the-middle attack

Problem 2: Find a General Threat Model

- **distance fraud:**

- $P(x)$ far from all $V(x)$'s want to make one $V(x)$ accept (interaction with other $P(x')$ and $V(x')$ possible anywhere)
- → also captures distance hijacking

- **man-in-the-middle:**

- *learning phase:* \mathcal{A} interacts with many P 's and V 's
- *attack phase:* $P(x)$'s far away from $V(x)$'s, \mathcal{A} interacts with them and possible $P(x')$'s and $V(x')$'s
- \mathcal{A} wants to make one $V(x)$ accept

- **collusion fraud:**

- $P(x)$ far from all $V(x)$'s interacts with \mathcal{A} and makes one $V(x)$ accept, but $\text{View}(\mathcal{A})$ does not give any advantage to mount a man-in-the-middle attack

Problem 2: Find a General Threat Model

- **distance fraud:**

- $P(x)$ far from all $V(x)$'s want to make one $V(x)$ accept (interaction with other $P(x')$ and $V(x')$ possible anywhere)
- → also captures distance hijacking

- **man-in-the-middle:**

- *learning phase*: \mathcal{A} interacts with many P 's and V 's
- *attack phase*: $P(x)$'s far away from $V(x)$'s, \mathcal{A} interacts with them and possible $P(x')$'s and $V(x')$'s
 \mathcal{A} wants to make one $V(x)$ accept
- → also captures impersonation

- **collusion fraud:**

- $P(x)$ far from all $V(x)$'s interacts with \mathcal{A} and makes one $V(x)$ accept, but $\text{View}(\mathcal{A})$ does not give any advantage to mount a man-in-the-middle attack

Problem 2: Find a General Threat Model

- **distance fraud:**

- $P(x)$ far from all $V(x)$'s want to make one $V(x)$ accept (interaction with other $P(x')$ and $V(x')$ possible anywhere)
- → also captures distance hijacking

- **man-in-the-middle:**

- *learning phase*: \mathcal{A} interacts with many P 's and V 's
- *attack phase*: $P(x)$'s far away from $V(x)$'s, \mathcal{A} interacts with them and possible $P(x')$'s and $V(x')$'s
 \mathcal{A} wants to make one $V(x)$ accept
- → also captures impersonation

- **collusion fraud:**

- $P(x)$ far from all $V(x)$'s interacts with \mathcal{A} and makes one $V(x)$ accept, but $\text{View}(\mathcal{A})$ does not give any advantage to mount a man-in-the-middle attack

Problem 2: Find a General Threat Model

- **distance fraud:**

- $P(x)$ far from all $V(x)$'s want to make one $V(x)$ accept (interaction with other $P(x')$ and $V(x')$ possible anywhere)
- → also captures distance hijacking

- **man-in-the-middle:**

- *learning phase*: \mathcal{A} interacts with many P 's and V 's
- *attack phase*: $P(x)$'s far away from $V(x)$'s, \mathcal{A} interacts with them and possible $P(x')$'s and $V(x')$'s
 \mathcal{A} wants to make one $V(x)$ accept
- → also captures impersonation

- **collusion fraud:**

- $P(x)$ far from all $V(x)$'s interacts with \mathcal{A} and makes one $V(x)$ accept, but $\text{View}(\mathcal{A})$ does not give any advantage to mount a man-in-the-middle attack

Problem 2: Find a General Threat Model

- **distance fraud:**
 - $P(x)$ far from all $V(x)$'s want to make one $V(x)$ accept (interaction with other $P(x')$ and $V(x')$ possible anywhere)
 - → also captures distance hijacking
- **man-in-the-middle:**
 - *learning phase*: \mathcal{A} interacts with many P 's and V 's
 - *attack phase*: $P(x)$'s far away from $V(x)$'s, \mathcal{A} interacts with them and possible $P(x')$'s and $V(x')$'s
 \mathcal{A} wants to make one $V(x)$ accept
 - → also captures impersonation
- **collusion fraud:**
 - $P(x)$ far from all $V(x)$'s interacts with \mathcal{A} and makes one $V(x)$ accept, but $\text{View}(\mathcal{A})$ does not give any advantage to mount a man-in-the-middle attack

Problem 3: Crypto Assumptions to Make Proofs Correct

- **PRF masking:**

a bitstring a is chosen by the verifier and sent encrypted using the PRF

$$[M = a \oplus \text{PRF}_x(\dots)]$$

- **circular keying:**

if \mathcal{A} makes a query (y_i, a_i, b_i) , the oracle answers $(a_i \cdot x') + (b_i \cdot f_x(y_i))$

\mathcal{A} cannot distinguish if $x = x'$ or x and x' are independent

caveat: for all c_1, \dots, c_q s.t. $c_1 b_1 + \dots + c_q b_q = 0$, we must have $c_1 a_1 + \dots + c_q a_q = 0$

Problem 3: Crypto Assumptions to Make Proofs Correct

- **PRF masking:**

a bitstring a is chosen by the verifier and sent encrypted using the PRF

$$[M = a \oplus \text{PRF}_x(\dots)]$$

- **circular keying:**

if \mathcal{A} makes a query (y_i, a_i, b_i) , the oracle answers $(a_i \cdot x') + (b_i \cdot f_x(y_i))$

\mathcal{A} cannot distinguish if $x = x'$ or x and x' are independent

caveat: for all c_1, \dots, c_q s.t. $c_1 b_1 + \dots + c_q b_q = 0$, we must have $c_1 a_1 + \dots + c_q a_q = 0$

The SKI Protocol

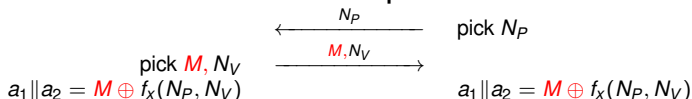
Verifier

secret: x

Prover

secret: x

initialization phase

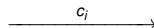


distance bounding phase

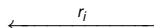
for $i = 1$ to n

pick $c_i \in \{1, 2, 3\}$

start clock



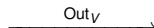
stop clock



$$r_i = \begin{cases} a_{1,i} & \text{if } c_i = 1 \\ a_{2,i} & \text{if } c_i = 2 \\ x_i \oplus a_{1,i} \oplus a_{2,i} & \text{if } c_i = 3 \end{cases}$$

check τ responses

check timers



f is a **circular-keying secure** PRF

SKI Security

Theorem

If f is a **circular-keying secure** PRF and V requires at least τ correct rounds,

- there is no DF with $\Pr[\text{success}] \geq B(n, \tau, \frac{3}{4})$
- there is no MiM with $\Pr[\text{success}] \geq B(n, \tau, \frac{2}{3})$
- for all CF such that $\Pr[\text{CF succeeds}] \geq p$ there is an associated MiM such that

$$\Pr[\text{MiM}(\text{View}_{\mathcal{A}}) \text{ succeeds} | \text{CF succeeds}] \geq \frac{p}{(1 + \sqrt{1-p})^2}$$

$$B(n, \tau, \rho) = \sum_{i=\tau}^n \binom{n}{i} \rho^i (1 - \rho)^{n-i}$$

SKI Security

Theorem

If f is a **circular-keying secure** PRF and V requires at least τ correct rounds,

- there is no DF with $\Pr[\text{success}] \geq B(n, \tau, \frac{3}{4})$
- there is no MiM with $\Pr[\text{success}] \geq B(n, \tau, \frac{2}{3})$
- for all CF such that $\Pr[\text{CF succeeds}] \geq p$ there is an associated MiM such that

$$\Pr[\text{MiM}(\text{View}_{\mathcal{A}}) \text{ succeeds} | \text{CF succeeds}] \geq \frac{p}{(1 + \sqrt{1-p})^2}$$

$$B(n, \tau, \rho) = \sum_{i=\tau}^n \binom{n}{i} \rho^i (1-\rho)^{n-i}$$

SKI Security

Theorem

If f is a *circular-keying secure* PRF and V requires at least τ correct rounds,

- there is no DF with $\Pr[\text{success}] \geq B(n, \tau, \frac{3}{4})$
- there is no MiM with $\Pr[\text{success}] \geq B(n, \tau, \frac{2}{3})$
- for all CF such that $\Pr[\text{CF succeeds}] \geq p$ there is an associated MiM such that

$$\Pr[\text{MiM}(\text{View}_{\mathcal{A}}) \text{ succeeds} | \text{CF succeeds}] \geq \frac{p}{(1 + \sqrt{1-p})^2}$$

$$B(n, \tau, \rho) = \sum_{i=\tau}^n \binom{n}{i} \rho^i (1 - \rho)^{n-i}$$

Conclusion

- several proposed protocols from the literature are insecure
- several security proofs from the literature are incorrect
- SKI offers provable security

Conclusion

- several proposed protocols from the literature are insecure
- several security proofs from the literature are incorrect
- SKI offers provable security

Conclusion

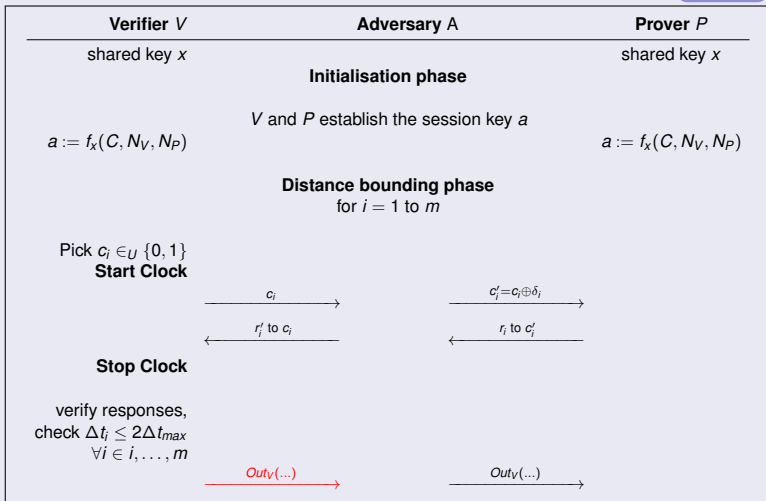
- several proposed protocols from the literature are insecure
- several security proofs from the literature are incorrect
- SKI offers provable security

Thank you!

A Generic MiM Attack [7, 6]

Non-Narrow DB Attacker

◀ *flaws* |



A Generic MiM Attack [7, 6]

Non-Narrow DB Attacker



- this non-narrow attacker \mathcal{A} can find the j th bit of the key x , i.e., :

$$x_j = r'_j \oplus r_j \oplus \overline{Out_V}$$

- depending on the protocol, this \mathcal{A} can be more or less successful

A Generic MiM Attack [7, 6]

Reid *et al.* Encryption Failure

◀ (DBPK enc) | ▶ (Reid's.)

- consider $\mathcal{E}_k(x) = x - k \bmod n$ in Reid *et al.*, with $x \in \mathbf{Z}_n$, $k \in_U \mathbf{Z}_n$, n fixed with m bits (i.e., $e = x - k \bmod n$)



$$e = x - k + cn, \quad (1)$$

where $c = 1_{k > x}$

- For $e_0 = \text{lsb}(e)$, we have

$$e_0 = \begin{cases} x_0 \oplus k_0, & \text{if } x \geq k, \\ x_0 \oplus k_0 \oplus n_0, & \text{if } x < k. \end{cases}$$

or,

$$e_0 = x_0 \oplus k_0 \oplus c \times n_0.$$

A Generic MiM Attack [7, 6]

Ex.: n odd, $lsb(x)$

◀ (MiM attack) |

- $n_0 = 1 \stackrel{(2)}{\Rightarrow} e_0 = x_0 \oplus k_0 \oplus c$ where $c = 1_{k > x}$

-

$$p = \Pr[c = 1] = \Pr[k > x] = 1 - \frac{(x + 1)}{n}.$$

- $x > n/2 \Rightarrow$ most of c 's are 0 $\Rightarrow x_0$ is the majority of the obtained $e_0 \oplus k_0 \Rightarrow$
- \mathcal{A} tries N sessions, i.e.,:

$$\text{Bit}_i = e_0 \oplus k_0 = x_0 \oplus c_i, \forall i \in \{1, \dots, N\},$$

- \mathcal{A} uses a majority function to find x_0 such as

$$\text{Majority}(\text{Bit}_1, \dots, \text{Bit}_N) \approx \begin{cases} x_0, & \text{if } x > \frac{n}{2}, \\ x_0 \oplus 1 & \text{if } x < \frac{n}{2} \end{cases}$$

A Generic MiM Attack [7, 6]

Ex.: n odd, $lsb(x)$



◀ (MiM attack) |

- so, $\Pr[\text{Bit}_i = x_0 \oplus 1_{x < n/2}] = 1/2 + |p - 1/2|$.
- so, by the **Chernoff bound** bound,

$$\Pr [\text{Maj}(\text{Bit}_1, \dots, \text{Bit}_N) = x_0 \oplus 1_{x < n/2}] \geq 1 - e^{-2N(p-1/2)^2}.$$

- take $N \approx (1/2 - (x + 1)/n)^{-2}$ to deduce x_0 by the guess $1_{x < n/2}$.

A Generic MiM Attack [7, 6]

MiM Attacks on DB Cont'd

◀ (MiM attack)|

- the other cases for the attack for other encryption functions are similar
- ! other protocols can be attacked in this fashion
- !! ● secure encryption functions may not be enough for the security of the DB protocols against MiM!

The Reid et al. Protocol

◀ (MiM attack) |

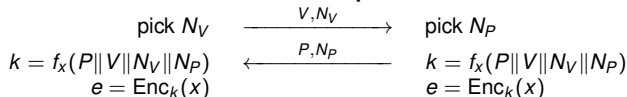
Verifier

secret: x

Prover

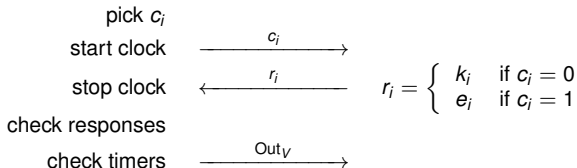
secret: x

initialization phase



distance bounding phase

for $i = 1$ to n



PRFs

$\mathcal{D}^{\mathcal{O}}$: Black-Box Oracle Queries to Distinguish

Let \mathcal{F} be a family of functions from D^R , b be a bit.

- 1: **Parameters:** sec. param. s ; *poly*; a ppt. alg. \mathcal{D} ;
 $\ell := \ell(s)$, $L := L(s)$, $\ell, L > 1$; $D = \{0, 1\}^\ell$, $R = \{0, 1\}^L$;
- 2: $view_{\mathcal{D}} := \emptyset$
- 3: while (no special end-query)
- 4: $x \leftarrow \mathcal{D}(view_{\mathcal{D}}; r_{\mathcal{D}})$; $x \in D$
- 5: $y \leftarrow \mathcal{O}(x)$; $y \in R$
- 6: $view_{\mathcal{D}} := view_{\mathcal{D}} \cup \{y\}$
- 7: end while

PRFs

The PRF Game $PRF_{\mathcal{F}, \mathcal{D}}^b$

- 1: **Parameters:** sec. param. s ; $\ell := \ell(s)$, $L := L(s)$, $\ell, L > 1$;
 $D = \{0, 1\}^\ell$, $R = \{0, 1\}^L$; a family $\mathcal{F} := \mathcal{F}(s)$ of fct. in D^R ;
 a ppt. alg. \mathcal{D} , a bit b .
- 2: $f^0 \leftarrow_{\mathcal{U}} [D \Rightarrow R]$ // pick a random function from D to R
- 3: $f^1 \leftarrow_{\mathcal{U}} \mathcal{F}$ // sample a function from the family
- 4: $\bar{b} \leftarrow \mathcal{D}^{O_{f^b}}$
- 5: return \bar{b}

◀ (trapdoor PRFs)

PRFs

The PRF assumption

Consider the parameters before.

We say that the family \mathcal{F} is a *PRF* or that the family \mathcal{F} respects the *PRF assumption* if for any ppt. algorithm \mathcal{D} ,

$$\left| \Pr[\text{Out}(\text{PRF}_{\mathcal{F},\mathcal{D}}^0) = 1] - \Pr[\text{Out}(\text{PRF}_{\mathcal{F},\mathcal{D}}^1) = 1] \right| < \text{negl}(s),$$

where *negl* is a function over natural numbers eventually lower than the inverse of any polynomial and the probability is taken over the random coins of \mathcal{D} .

◀ (trapdoor PRFs) |



G. Avoine, C. Lauradoux, and B. Martin.

How Secret-sharing can Defeat Terrorist Fraud.

In Proceedings of the 4th ACM Conference on Wireless Network Security – WiSec'11, Hamburg, Germany, June 2011. ACM, ACM Press.



S. Brands and D. Chaum.

Distance-Bounding Protocols (Extended Abstract).

In Proceedings of EUROCRYPT'93, pages 344–359, Lofthus, Norway, May 1993.



S. Drimer and S. J. Murdoch.

Keep your enemies close: distance bounding against smartcard relay attacks.

In Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium, pages 7:1–7:16, Berkeley, CA, USA, 2007. USENIX Association.



U. Dürholz, M. Fischlin, M. Kasper, and C. Onete.

A Formal Approach to Distance Bounding RFID Protocols.
In Proceedings of the 14th Information Security Conference ISC 2011, LNCS, pages 47–62. SPRINGER, 2011.



Ford.

Safe and Secure *SecuriCode*TM Keyless Entry.
<http://www.ford.com/technology/>, 2011.



J. Reid, J. M. Gonzalez Nieto, T. Tang, and B. Senadji.
Detecting Relay Attacks with Timing-based Protocols.
In Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security, ASIACCS '07, pages 204–213. ACM, 2007.



Y.-J. Tu and S. Piramuthu.

RFID Distance Bounding Protocols.
In Proceedings of the First International EURASIP Workshop on RFID Technology, 2007.