On the Need for Provably Secure Distance Bounding

Serge Vaudenay

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

http://lasec.epfl.ch/

1. Introduction to Distance-Bounding
2. Some Insecurity Case Studies
3. On Incorrect Use of PRFs
4. Directions for Provable Security

1. Introduction to Distance-Bounding
2. Some Insecurity Case Studies
3. On Incorrect Use of PRFs
4. Directions for Provable Security

Motivation

for token-based authentication:
thwart man-in-the-middle

- wireless car locks
- creditcard payment (or contactless)
- corporate ID card for access control

solution: use a distance-bounding protocol

The Brands-Chaum Protocol

Distance-Bounding Protocols [Brands-Chaum EUROCRYPT 1993]

Verifier public key: y		**Prover** secret key: x
	initialization phase	
	$\xleftarrow{\text{Commit}(m)}$	pick m
	distance bounding phase for $i = 1$ to n	
pick c_i		
start clock	$\xrightarrow{c_i}$	
stop clock	$\xleftarrow{r_i}$	$r_i = m_i \oplus c_i$
check timers		
check responses		
	termination phase	
	$\xleftarrow{\text{open commitment}}$	
check signature	$\xleftarrow{\text{Sign}_x(c,r)}$	
	$\xrightarrow{\text{Out}_V}$	

Distance Fraud

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

a malicious prover P^* tries to prove that he is close to a verifier V

Mafia Fraud

Major Security Problems with the “Unforgeable” (Feige)-Fiat-Shamir Proofs of Identity and How to Overcome Them [Desmedt SECURICOM 1988]

$$\underbrace{P \longleftrightarrow \mathcal{A} \longleftrightarrow V}_{\text{far away}}$$

an adversary $\mathcal{A}$ tries to prove that a prover P is close to a verifier V

Terrorist Fraud

Major Security Problems with the “Unforgeable” (Feige)-Fiat-Shamir Proofs of Identity and How to Overcome Them [Desmedt SECURICOM 1988]

$$\underbrace{P^* \longleftrightarrow \mathcal{A} \longleftrightarrow V}_{\text{far away}}$$

a malicious prover P^* helps an adversary $\mathcal{A}$ to prove that P^* is close to a verifier V without giving $\mathcal{A}$ another advantage

Impersonation Fraud

A Formal Approach to Distance Bounding RFID Protocols

[Dürholz-Fischlin-Kasper-Onete ISC 2011]

$$\mathcal{A} \longleftrightarrow V$$

an adversary $\mathcal{A}$ tries to prove that a prover P is close to a verifier V

Distance Hijacking

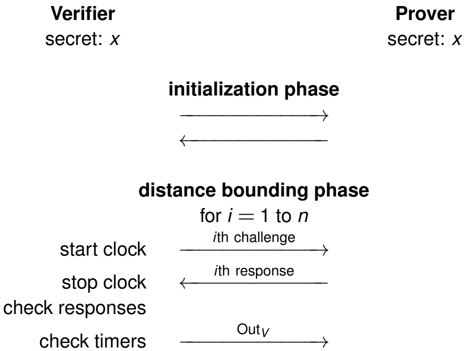
Distance Hijacking Attacks on Distance Bounding Protocols

[Cremers-Rasmussen-Čapkun IEEE S&P 2012]

$$\underbrace{P^* \longleftrightarrow P' \longleftrightarrow V}_{\text{far away}}$$

a malicious prover P^* tries to prove that he is close to a verifier V by taking advantage of other provers P'

Techniques



Verifier
secret: x

Prover
secret: x

initialization phase

distance bounding phase
for $i = 1$ to n

start clock
ith challenge

stop clock
ith response

check responses

check timers
Out_V

caveat: the rapid bit-exchange is subject to noise, so the verifier may require at least τ correct sessions to accept

2 Some Insecurity Case Studies

- The RC Protocol
- The Bussard-Bagga Protocol and Children

The RC Protocol

Location Privacy of Distance Bounding [Rassmussen-Čapkun ACM CCS 2008]

- integrate location-privacy
- based on the exchange of a continuous bitstream

The RC Protocol

$$
\begin{array}{rcl}
\textbf{Verifier} & & \textbf{Prover} \\
\text{secret: } K & & \text{secret: } K \\
 & \textbf{initialization phase} & \\
\text{receive } N_P & \xleftarrow{\text{secure}_K(N_P)} & \text{pick } N_P \\
\text{pick } M, N_V & \xrightarrow{\text{secure}_K(M, N_P)} & \text{receive } M\text{, check } N_P \\
 & \textbf{distance-bounding phase} & \\
\text{stream}_V = \text{Rand}_V^1 \| M \| N_V \| \text{Rand}_V^2 & \xrightarrow{\text{stream}_V} & \text{parse until } M \\
\text{parse until } N_V \oplus N_P & \xleftarrow{\text{stream}_P} & \text{stream}_P = \text{Rand}_P^1 \| N_V \oplus N_P \| \text{Rand}_P^2 \\
\text{check time between } N_V \text{ and } N_V \oplus N_P & \xrightarrow{\text{Out}_V} &
\end{array}
$$

Attack Principles

Mafia Fraud Attack against the RC Distance-Bounding Protocol [Mitrokotsa-Vaudenay IEEE RFID-TA 2012]

- the adversary intercepts a complete session between P and V
- the adversary guesses the position of N_V in stream_V
- assume the adversary knows the locations of P and V
  he can deduce the position of $N_V \oplus N_P$, thus the value of N_P
- the adversary can now impersonate P by replaying $\text{secure}_K(N_P)$
- he replies by $\text{stream}_V \oplus (\text{offset} \| N_P \| \cdots \| N_P)$
- if the offset length modulo $|N_V|$ is correct, the verifier accepts

- **success probability:** $\frac{1}{|\text{stream}_V|} \times \frac{1}{|N_V|}$

2 Some Insecurity Case Studies

- The RC Protocol
- The Bussard-Bagga Protocol and Children

The BB Protocol

Distance-Bounding Proof of Knowledge Protocols to Avoid Real-Time Attacks [Bussard-Bagga IFIP SEC 2005]

- protection against terrorist fraud
- based on public-key cryptography
- generic: several DBPK possible instantiations

The Generic DBPK Protocol

Verifier
public key: y

Prover
secret key: x

initialization phase

pick $k, v, v', e = \mathrm{Enc}_k(x)$
$z_{k,i} = \mathrm{commit}(k_i, v_i)$
$\xleftarrow{\quad z_k, z_e \quad}$ $z_{e,i} = \mathrm{commit}(e_i, v'_i)$

distance bounding phase
for $i = 1$ to n

pick c_i
start clock $\xrightarrow{\quad c_i \quad}$
stop clock $\xleftarrow{\quad r_i \quad}$ $r_i = \begin{cases} k_i & \text{if } c_i = 0 \\ e_i & \text{if } c_i = 1 \end{cases}$

termination phase

check openable commitments $\xleftarrow{\quad \gamma \quad}$ $\gamma_i = \begin{cases} v_i & \text{if } c_i = 0 \\ v'_i & \text{if } c_i = 1 \end{cases}$
check timers
$\xleftrightarrow{\quad \mathrm{PoK}(x)\ldots \quad}$
$\xrightarrow{\quad \mathrm{Out}_V \quad}$

Proposed Instances

- **one-time pad DBPK**: $\mathsf{Enc}_k(x) = x \oplus k$
- **addition modulo q DBPK-Log**: $\mathsf{Enc}_k(x) = x - k \bmod q$
- **modular addition with random factor DBPK-Log**: $\mathsf{Enc}_k(x; u) = (u, ux - k \bmod q)$

The Reid et al. Protocol

Detecting Relay Attacks with Timing-based Protocols

[Reid-Nieto-Tang-Senadji ASIACCS 2007]

Verifier secret: x		**Prover** secret: x
	initialization phase	
pick N_V	$\xrightarrow{V,N_V}$	pick N_P
$k = f_x(P \Vert V \Vert N_V \Vert N_P)$ $e = \mathrm{Enc}_k(x)$	$\xleftarrow{P,N_P}$	$k = f_x(P \Vert V \Vert N_V \Vert N_P)$ $e = \mathrm{Enc}_k(x)$
	distance bounding phase for $i = 1$ to n	
pick c_i		
start clock	$\xrightarrow{c_i}$	
stop clock	$\xleftarrow{r_i}$	$r_i = \begin{cases} k_i & \text{if } c_i = 0 \\ e_i & \text{if } c_i = 1 \end{cases}$
check responses		
check timers	$\xrightarrow{\mathrm{Out}_V}$	

Attack Principles for the Reid et al. Protocol

The Swiss-Knife RFID Distance Bounding Protocol

[Kim-Avoine-Koeune-Standaert-Pereira ICISC 2008]

- select i
- let a protocol run between P and V except replace c_i by $1 - c_i$ and r_i by bit $\in_U \{0, 1\}$
- observation 1: the response to $1 - c_i$ is r_i (given by P)
- observation 2: the response to c_i is bit $\oplus\, 1_{V \text{ does not accept}}$
- the adversary deduces k_i and e_i, thus $x_i = k_i \oplus e_i$
- iterate with another i and reconstruct the secret x
- the adversary can impersonate P to V!

Attack Principles for One-Time Pad DBPK

The Bussard-Bagga and Other Distance-Bounding Protocols under Man-in-the-Middle Attacks [Bay-Boureanu-Mitrokotsa-Spulber-Vaudenay Inscrypt 2012]

- select i
- let a protocol run between P and V except
  replace c_i by $1 - c_i$ and r_i by $r_i^* \in_U \{0,1\}$
  !! tricky things with PoK and commitments (requires to guess c_i)
- observation 1: the response to $1 - c_i$ is r_i (given by P)
- observation 2: the response to c_i is $r_i^* \oplus 1_{V \text{ does not accept}}$
- the adversary deduces k_i and e_i, thus $x_i = k_i \oplus e_i$
- iterate with another i and reconstruct the secret x
- the adversary can impersonate P to V!

Attack Principles for Other Instances

The Bussard-Bagga and Other Distance-Bounding Protocols under Man-in-the-Middle Attacks [Bay-Boureanu-Mitrokotsa-Spulber-Vaudenay Inscrypt 2012]

for **addition modulo q DBPK-Log**:

- guess the most significant bit x_n of x
- set $c_n = 0$, get r_n from P and deduce k_n
- if $x_n = k_n$, start again until $x_n \neq k_n$
- since $e = x - k + k_n q$, we deduce some relations B

$$x_i = B_i(e_i \oplus k_i, e \bmod 2^{i-1}, k \bmod 2^{i-1})$$

- apply the previous attack with $i = 1, 2, \ldots$

for **addition with random factor DBPK-Log**:

- more complicated (involves lattice reduction techniques)

Terrorist Fraud Attacks for Stronger Encryption

Distance-Bounding for RFID: Effectiveness of 'Terrorist Fraud' in the Presence of Bit Errors [Hancke IEEE RFID-TA 2012]

- P^* helps $\mathcal{A}$ for the initialization phase
- P^* provides $\mathcal{A}$ with all (k_i, e_i) pairs with $n - \tau$ of them flipped
- $\mathcal{A}$ answers to challenges using these pairs
- P^* helps $\mathcal{A}$ for the termination phase
- since there are τ correct responses, V accepts
- $\mathcal{A}$ cannot reconstruct x based on the noisy (k_i, e_i) pairs
- caveat: previous argument does not apply to "simple" encryptions such as one-time-pad and other variants

1. Introduction to Distance-Bounding
2. Some Insecurity Case Studies
3. **On Incorrect Use of PRFs**
4. Directions for Provable Security

Security Proofs Based on PRF

- if the adversary can break the scheme with a PRF, then he can break an idealized scheme with the PRF replaced by a truly random function
- this argument is valid when both these conditions are met:
  1. the adversary does not have access to the PRF key
  2. the PRF key is only used by the PRF
- as far as distance fraud is concerned, condition 1 is not met!
- for most of terrorist fraud protections, condition 2 is not met!

The TDB Protocol

How Secret-Sharing can Defeat Terrorist Fraud

[Avoine-Lauradoux-Martin ACM WiSec 2011]

Verifier		**Prover**
secret: x		secret: x
	initialization phase	
	$\xleftarrow{N_P}$	pick N_P
pick N_V	$\xrightarrow{N_V}$	
$a_1 \Vert a_2 = f_x(N_P, N_V)$		$a_1 \Vert a_2 = f_x(N_P, N_V)$
	distance bounding phase	
	for $i = 1$ to n	
pick $c_i \in \{1, 2, 3\}$		
start clock	$\xrightarrow{c_i}$	
stop clock	$\xleftarrow{r_i}$	$r_i = \begin{cases} a_{1,i} & \text{if } c_i = 1 \\ a_{2,i} & \text{if } c_i = 2 \\ x_i \oplus a_{1,i} \oplus a_{2,i} & \text{if } c_i = 3 \end{cases}$
check responses		
check timers	$\xrightarrow{\text{Out}_V}$	

Distance Fraud with a Programmed PRF

On the Pseudorandom Function Assumption in (Secure) Distance-Bounding Protocols [Boureanu-Mitrokotsa-Vaudenay Latincrypt 2012]

- given a PRF g, let

$$f_x(N_P, N_V) = \begin{cases} x \| x & \text{if } N_P = x \\ g_x(N_P, N_V) & \text{otherwise} \end{cases}$$

  f is a PRF!

- a malicious prover selects $N_P = x$ to make $a_1 = a_2 = x$
- whatever c_i, we have $r_i = x_i$
- the malicious prover can send r_i before receiving c_i!

Man-in-the-Middle Attack with a Programmed PRF

On the Pseudorandom Function Assumption in (Secure) Distance-Bounding Protocols [Boureanu-Mitrokotsa-Vaudenay Latincrypt 2012]

- given a PRF g: $\text{trapdoor}_x(\bar{\alpha}\|t) \Longleftrightarrow t = g_x(\bar{\alpha}) \oplus \text{right\_half}(x)$,

  $$f_x(N_P,N_V) = \begin{cases} (a_1 = \alpha\|\beta\ ,\ a_2 = \gamma\|\beta \oplus g_x(\alpha)) & \text{if } \neg\text{trapdoor}_x(N_V) \\ & \text{where } (\alpha,\beta,\gamma) = g_x(N_P,N_V) \\ a_1 = a_2 = x & \text{otherwise} \end{cases}$$

  f is a PRF!
- the adversary plays with P and sends $c = (1,\ldots,1,3,\ldots,3)$ to obtain from the responses $\text{left\_half}(a_1) = \bar{\alpha}$ and $\text{right\_half}(x \oplus a_1 \oplus a_2) = g_x(\bar{\alpha}) \oplus \text{right\_half}(x) = t$
- so, he can form $N_V = \bar{\alpha}\|t$ satisfying $\text{trapdoor}_x(N_V)$
- the adversary plays with P again with the lastly constructed N_V and gets $r = x$
- the adversary can now impersonate P to V!

Other Results based on Programmed PRFs

On the Pseudorandom Function Assumption in (Secure) Distance-Bounding Protocols [Boureanu-Mitrokotsa-Vaudenay Latincrypt 2012]

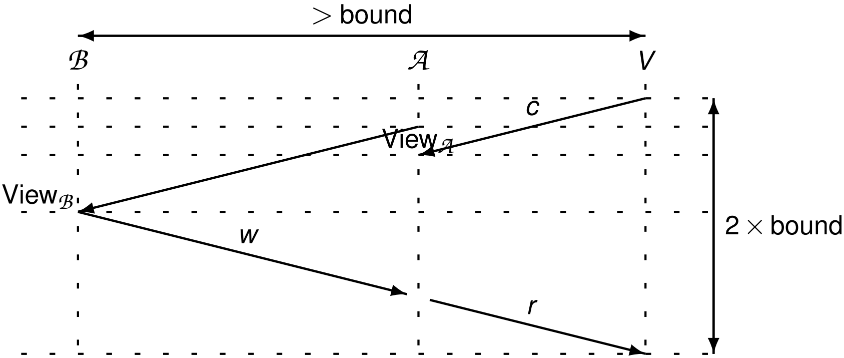
protocol	distance fraud	man-in-the-middle attack
TDB Avoine-Lauradoux-Martin [ACM WiSec 2011]	√	√
Dürholz-Fischlin-Kasper-Onete [ISC 2011]	√	–
Hancke-Kuhn [Securecomm 2005]	√	–
Avoine-Tchamkerten [ISC 2009]	√	–
Reid-Nieto-Tang-Senadji [ASIACCS 2007]	√	√
Swiss-Knife Kim-Avoine-Koeune-Standaert-Pereira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

1. Introduction to Distance-Bounding
2. Some Insecurity Case Studies
3. On Incorrect Use of PRFs
4. **Directions for Provable Security**

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)

Lemma



If the $\mathcal{B}$-V distance is larger than bound but the response r to c is received within at most 2.bound time, then r is a function of View$_{\mathcal{A}}$, c, and w, where w is a function from View$_{\mathcal{B}}$, independent from c.

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 string is chosen by the verifier and sent encrypted using the PRF
  $$a = M \oplus \mathrm{PRF}_x(\cdots)$$
- **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 $c_1, \ldots, c_q$ s.t. $c_1 b_1 + \cdots + c_q b_q = 0$, we must have $c_1 a_1 + \cdots + c_q a_q = 0$

The SKI Protocol

[Serge-Katerina-Ioana]

Verifier secret: x — **Prover** secret: x

initialization phase

$\xleftarrow{N_P}$ pick N_P

pick M, N_V $\xrightarrow{M, N_V}$

$a_1 \| a_2 = M \oplus f_x(N_P, N_V)$ — $a_1 \| a_2 = M \oplus f_x(N_P, N_V)$

distance bounding phase

for $i = 1$ to n

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

start clock $\xrightarrow{c_i}$

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

check τ responses

check timers $\xrightarrow{\mathrm{Out}_V}$

f is a circular-keying secure PRF

many variants possible

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

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

Conclusion

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