Mechanised Models and Proofs for Distance-Bounding

Ioana Boureanu, Catalin Dragan, François Dupressoir, David Gerault, Pascal Lafourcade
Questions:
• What if $A$ knows more than one key?
• Can we model physicalities (time, distance) in a computational framework?
Distance Bounding Protocols

\[ P(x) \]

\[ V(x) \]

Agree on \( r^0, r^1 = F(NP, NV, x) \)

For \( i \) from 1 to \( n \):

\[ C_i \]

\[ R_i = r^{ci}_i \]
Classical Threats

DF/DH

A (x) → V (x, y) → P (y)

MF

P (x) ↔ A_p ↔ V (x)

(TF)

A (x) ↔ A_v ↔ A_2 ↔ V (x)
FlexiDB: A Motivating Example

\[ A^{x_1, x_2...x_t(x_0)} \]
FlexiDB: Party Corruption

- Outsider
  - Knows
  - 0 Keys

- 1-weak-Insider
  - Knows
  - 1 Key

- 1-strong-Insider
  - Chooses

- n-weak-Insider
  - Knows
  - n Keys

- n-strong-Insider
  - Chooses
FlexiDB: Network Corruption

• Dummy
  • Send/receive within range

• Amplifier
  • Send/receive from afar

• Injector
  • Send/receive/block/overwrite within range

• Full
  • All of the above
FlexiDB: An Overview

- All parties have a position in the metric space
  - Parties = provers, verifiers, 2 adversarial entities
- Adversary = \{A_P, A_V\}
  - Depending on the threat
  - Parametrised by channel/party corruption abilities
- A Challenger provides Oracles to A:
  - Join
  - Move
  - Replace
  - Start session
FlexiDB Threats: GMF

- Learning phase: \((\text{Loc}(A_p, A_v), dP, dV) \leftarrow A\)
- A wins if V accepts an authentication on x
- No new attacks
  - (Except for toy protocols)
FlexiDB Threats: GDF

• Learning phase: (Loc(A_p), dP, dV) <- A
• A wins if V accepts an authentication on x
• New attacks
  • Motivating example (n-weak Insider, full)
  • PRF programming attacks (1-weak Insider, full)
  • TF-resistant protocols (1-strong Insider, amplifier)
  • EMV-RRP-V2 (1-weak Insider, full)
Easycrypt Mechanisation

• Easycrypt modules: Environment, P/V, $O_{PV}$
• Environment with physicalities
  • Time
    • Global clock, real
    • Get_time, Add_time
  • Locations
    • Real (1d)
    • Get_locations, Set_locations
    • Distance $|x-x'|$
• Models a form of Outsider, full type GMF
  • Adv can only interact w/ the prover once during attack phase
  • Single prover/verifier
• Tested on EMV-RRP
Conclusion

• New model with more granularity
  • On party corruption
  • On network corruption

• New attacks
  • Maybe too strong, but interesting for future applications

• Mechanisation in EC
  • As an proof-of-concept on modeling physicalities in EC
  • Working model for EMV-RRP
Thank you!