University of Amsterdam

Romke van Dijk & Loek Sangers

Portable RFID Bumping Device

Research Project 1

Introduction

- Radio-frequency identification
- Lot of applications
  - Identification / tracking of goods
  - Public transportation
    - OV-chipkaart
  - Access control
    - Deloitte
    - UvA

Bumping vs Cloning

- Bumping
  - Short interaction with the tag
- Cloning
  - Gathering enough data to create a copy of the tag
- Bumping implies card / tag only attacks

MIFARE Classic

- Multiple size (1K, 2K and 4K)
- Memory split into sectors
  - Two keys: Key A and Key B
- Authentication + secure transmission
  - Proprietary stream cipher (Crypto1)
- Error codes
  - Parity correct or incorrect
- Weak pseudo random number generator
  - Same “random” number every second

MIFARE Classic EV1

- Fixed weaknesses
- Weakness in cipher

- ”Hard” nested authentication attack
  - Source: (Meijer et al., 2015)
- Requires offline calculation

Research questions

- Is it possible to clone a RFID tag within five minutes with a mobile device?
  - Maximal distance
  - Amount of cards
  - Attack vectors
  - Attack time

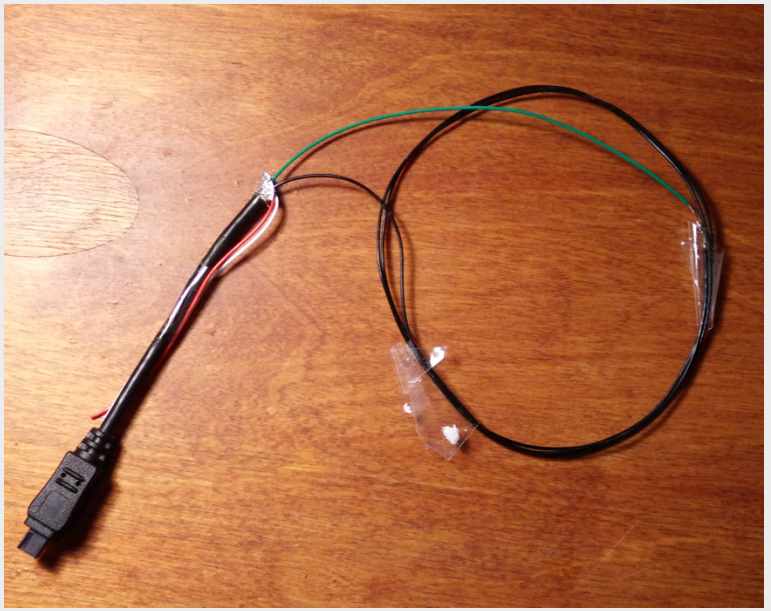
Proxmark3

- Costs: $299,-
- Programmable radio-frequency reader
- Eavesdrop
- OpenSource

Source: http://www.proxmark.org/

Antenna

- Costs: €5,-
- Simple USB Hirose cable
- Design by Proxmark community
- Range of 6-8



Maximal distance

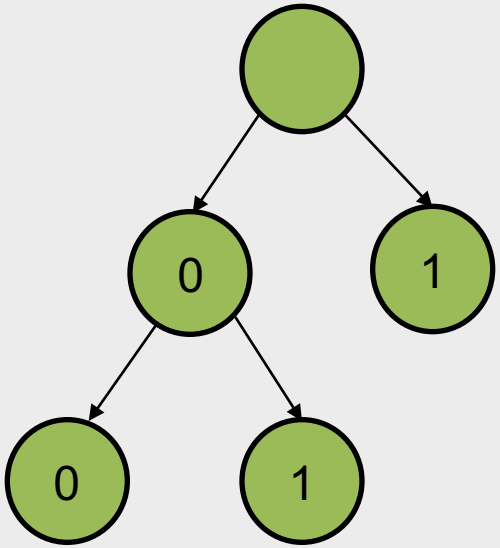
- According to specifications -> 10cm
- In practice -> 3-5 cm

- Theoretical maximum -> 30 centimetres
  - Source: (NXP, 2008)
- Practical maximum -> 27 centimetres
  - Source: (Hancke et al., 2011)

Setup bumping device

Amount of cards

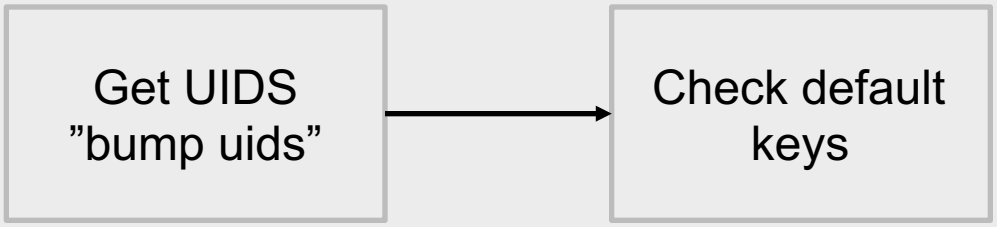
- Proxmark firmware: 1 Card
- Extended firmware: 3 Cards consistently
- Implemented Binary Tree Working Algorithm



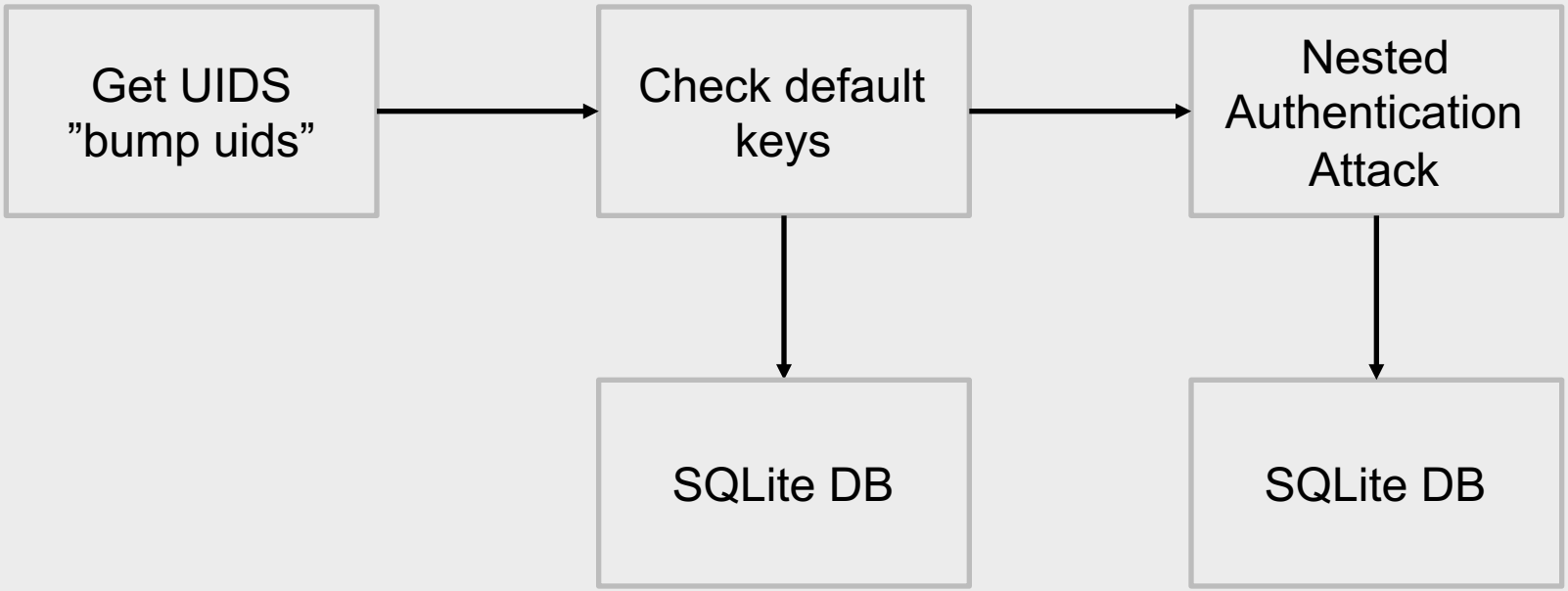
Attack framework

Get UIDS
”bump uids”

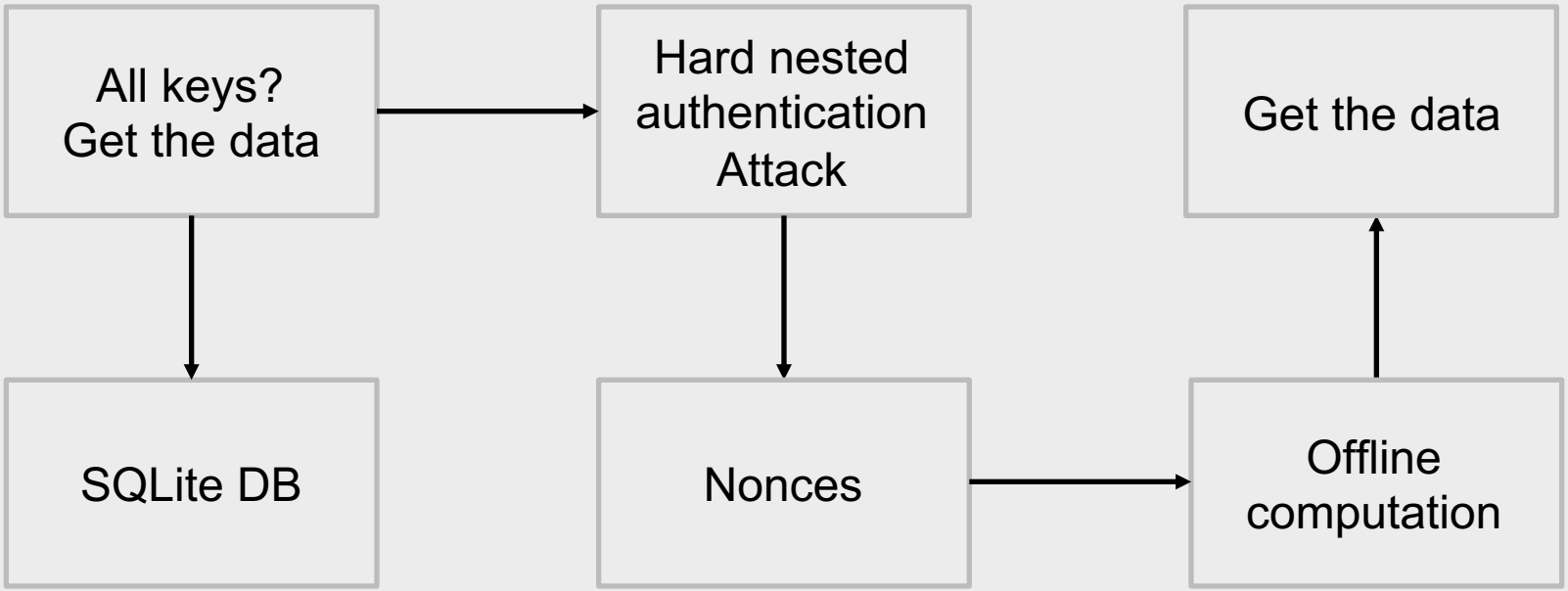
Attack framework



Attack framework



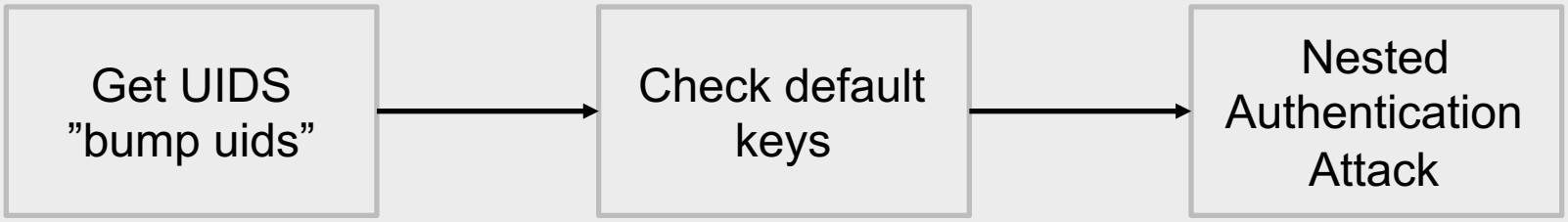
Attack framework



Attack vectors

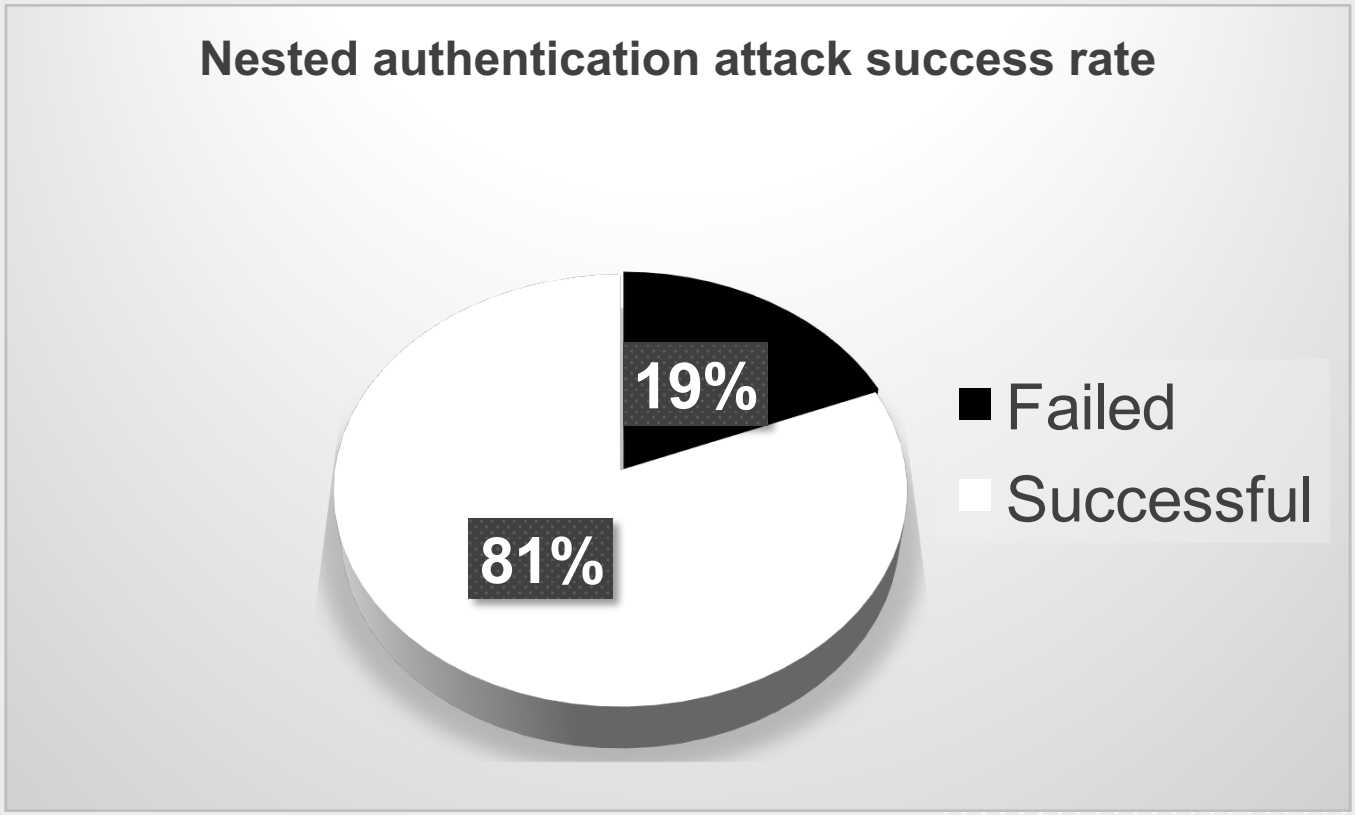
- Experiment
- Random key A to sector n
  - Repeated 100 times
  - Amount of keys is increased
- Calculate the time per step

Attack framework



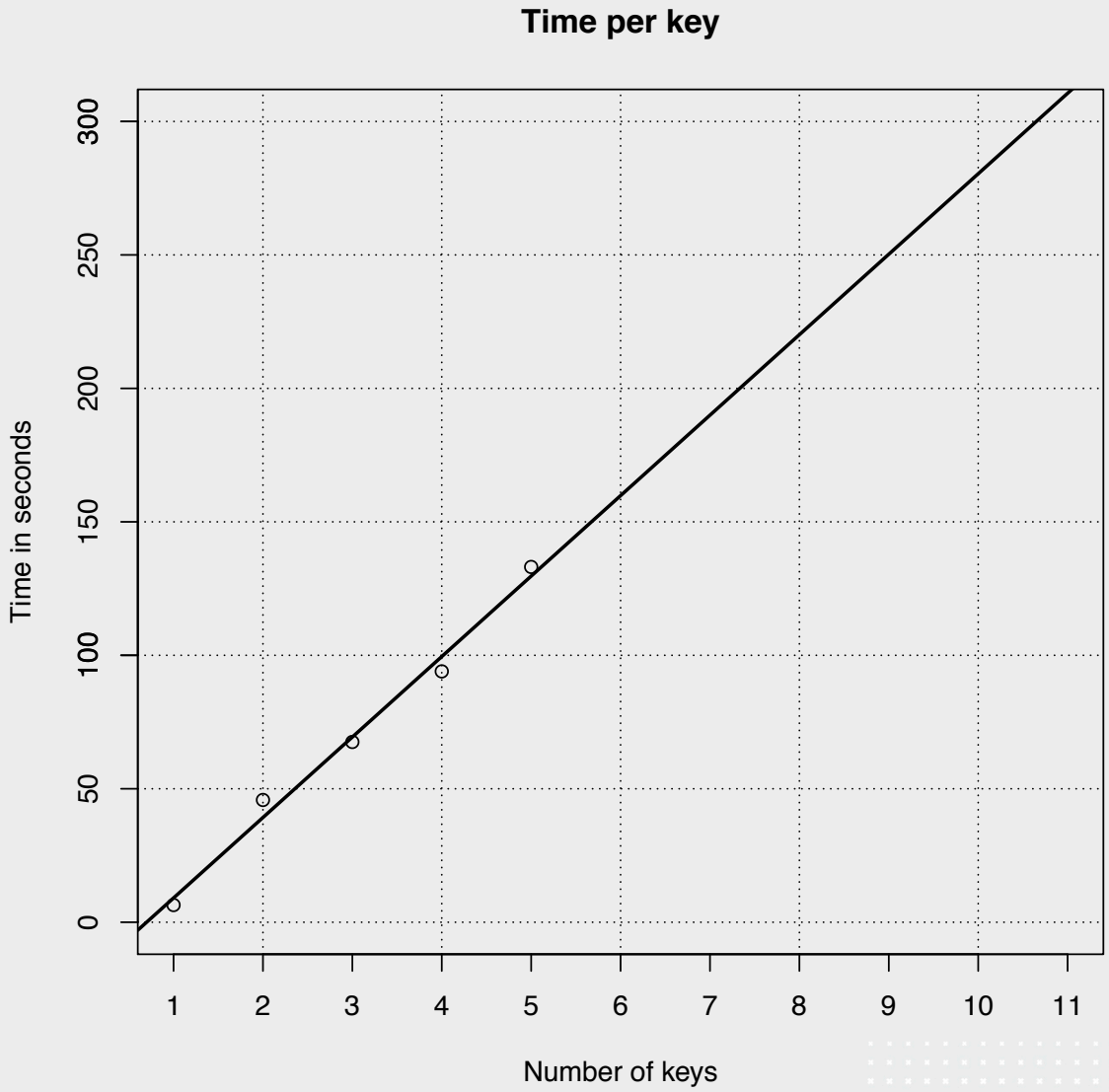
2-3 seconds

Attack framework



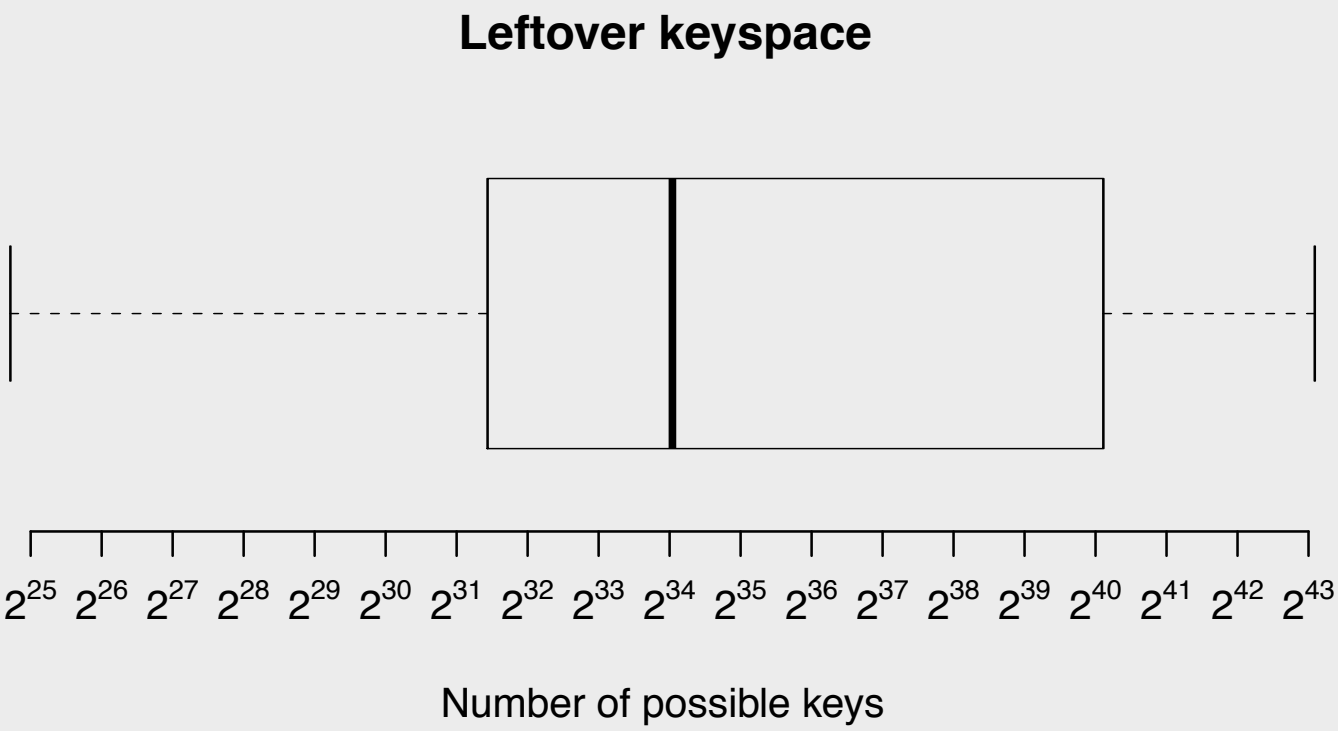
Attack vectors

- Nested authentication
  - Total of 2006 random keys
  - 1628 successfully recovered (81%)
  - Timing issues


Time per key
Time in seconds
0
50
100
150
200
250
300
1
2
3
4
5
6
7
8
9
10
11
Number of keys

Attack vectors

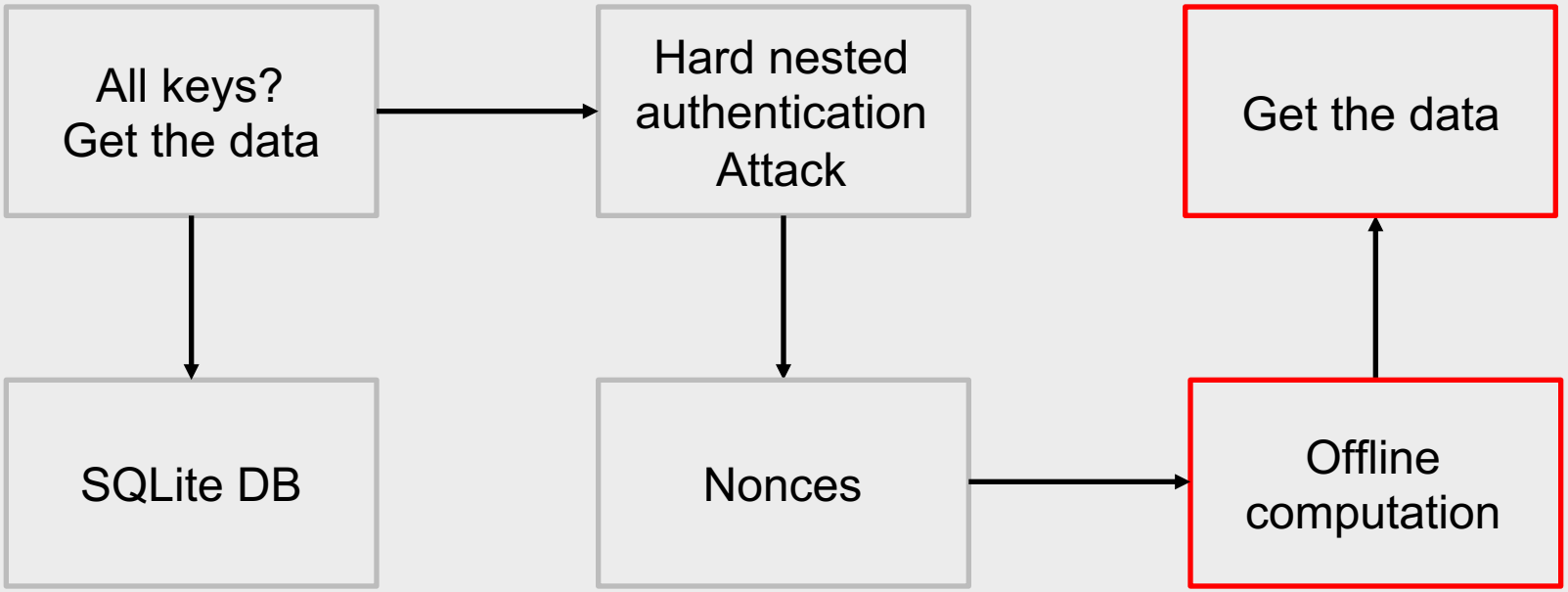
- Hard nested authentication
  - Limit ”sum property” or 10.000 encrypted nonces
  - Minimum: 49 seconds
  - Maximum: ~3 minutes


Leftover keyspace
2^{25} 2^{26} 2^{27} 2^{28} 2^{29} 2^{30} 2^{31} 2^{32} 2^{33} 2^{34} 2^{35} 2^{36} 2^{37} 2^{38} 2^{39} 2^{40} 2^{41} 2^{42} 2^{43}
Number of possible keys

Attack vectors

- 2^{36} -> within one hour (CPU)
  - Blapost's solver
- 2^{48} (full space) with 5 nonces
  - 14 hours (GPU).
  - Estimated 36 minutes (Dedicated hardware (budget 20,000)) Source: (Ming-Yang Chih et al., 2010)

Attack framework



Demo

- Live

Conclusion

- Able to clone MIFARE Classic 1K
  - Mobile device
  - Multiple cards
  - With a range of 6-8 centimetres
  - Small budget
  - Within 5 minutes (<= 10 non default keys)

Conclusion

- Able to clone MIFARE Classic 1K EV1
  - Within ~5 minutes (<=2 non default keys)
  - Second interaction required

Any questions?

- About?
  - Maximal distance
  - Amount of cards
  - Attack framework
  - Attack time