Cryptographic Analysis of the Bluetooth Secure Connection Protocol Suite

Marc Fischlin, **Olga Sanina**

Technische Universität Darmstadt, Germany

Asiacrypt 2021

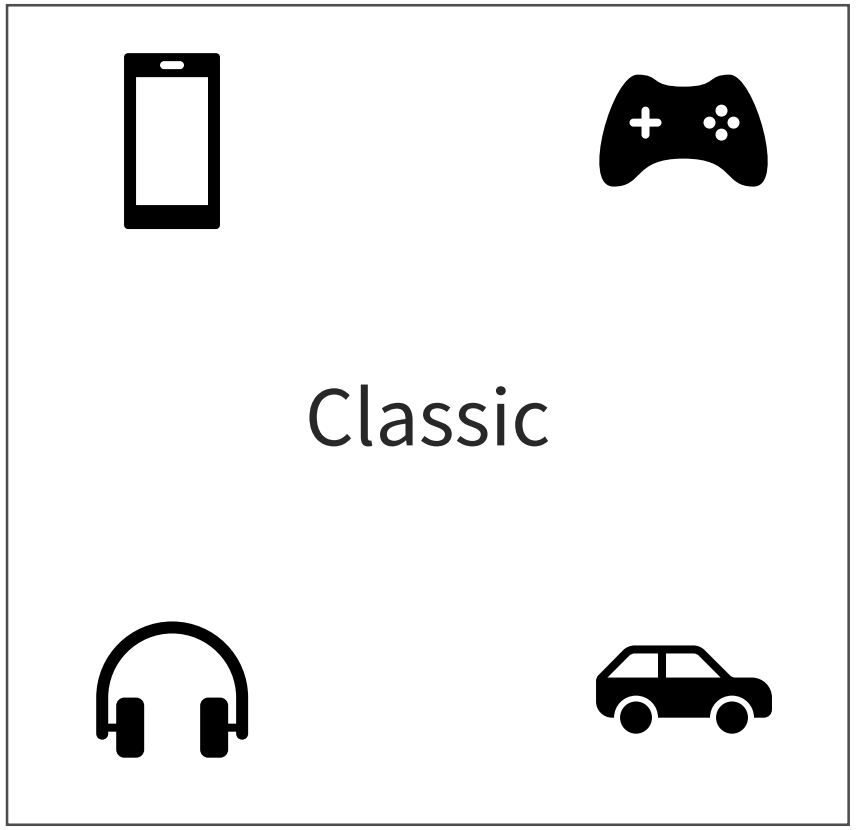
TECHNISCHE UNIVERSITÄT DARMSTADT

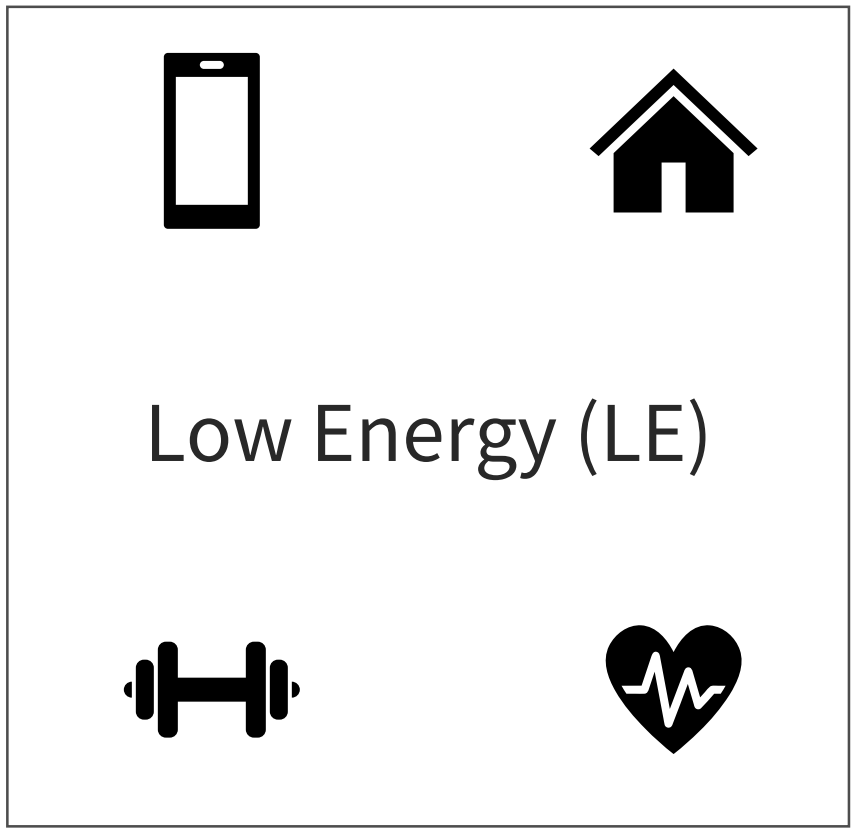
Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

ATHENE
National Research Center for Applied Cybersecurity

Privacy and Trust for Mobile Users

Bluetooth

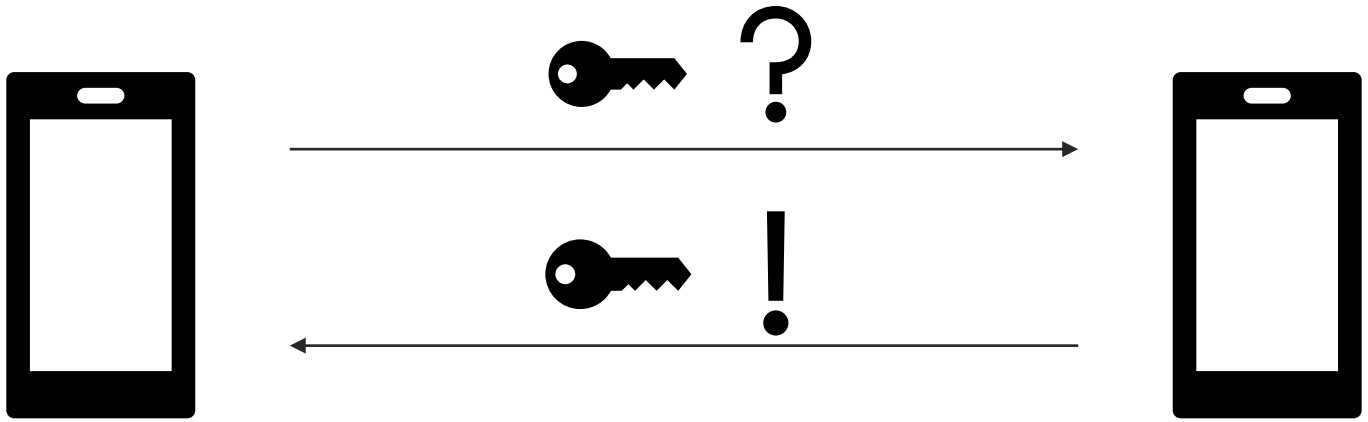




Bluetooth Key Exchange (KE)

Suite of protocols

Strongest protocol:
Secure Connection



Why do we need yet another analysis?

Previous analyses

[Lin09], [SS19], [TH21]

- Always considered a stand-alone protocol from the family

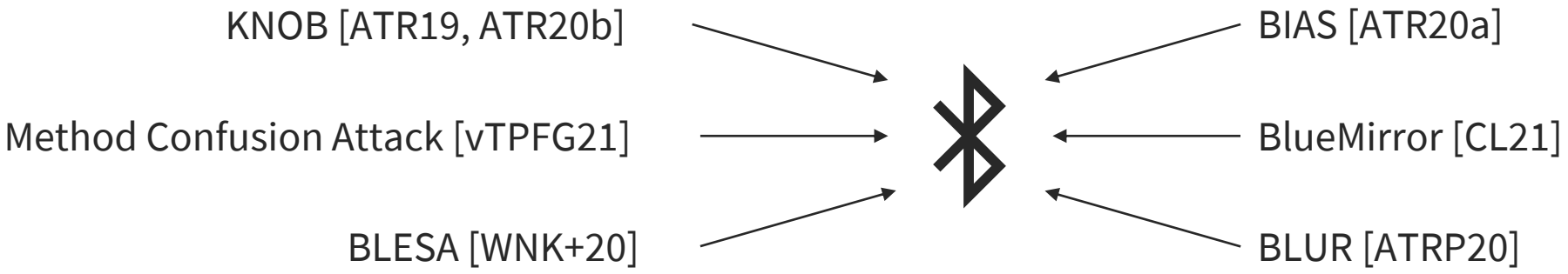
- Not close to the Standard:
  - Assumed on fresh Diffie-Hellman (DH) share
    but devices can use in up to 8 connections
    → No correctness property in [Lin09]
  - [Lin09] and [SS19] considered full point
    but only *x*-coordinate is used

[Lin09] Lindell. Comparison-based key exchange and the security of the numeric comparison mode in Bluetooth v2.1, *CT-RSA 2009*
[SS19] Sun and Sun. On secure simple pairing in bluetooth standard v5.0-part i: Authenticated link key security and its home automation and entertainment applications, *Sensors 2019*
[TH21] Troncoso and Hale. The bluetooth cyborg: Analysis of the full human-machine passkey entry ake protocol, *NDSS 2021*

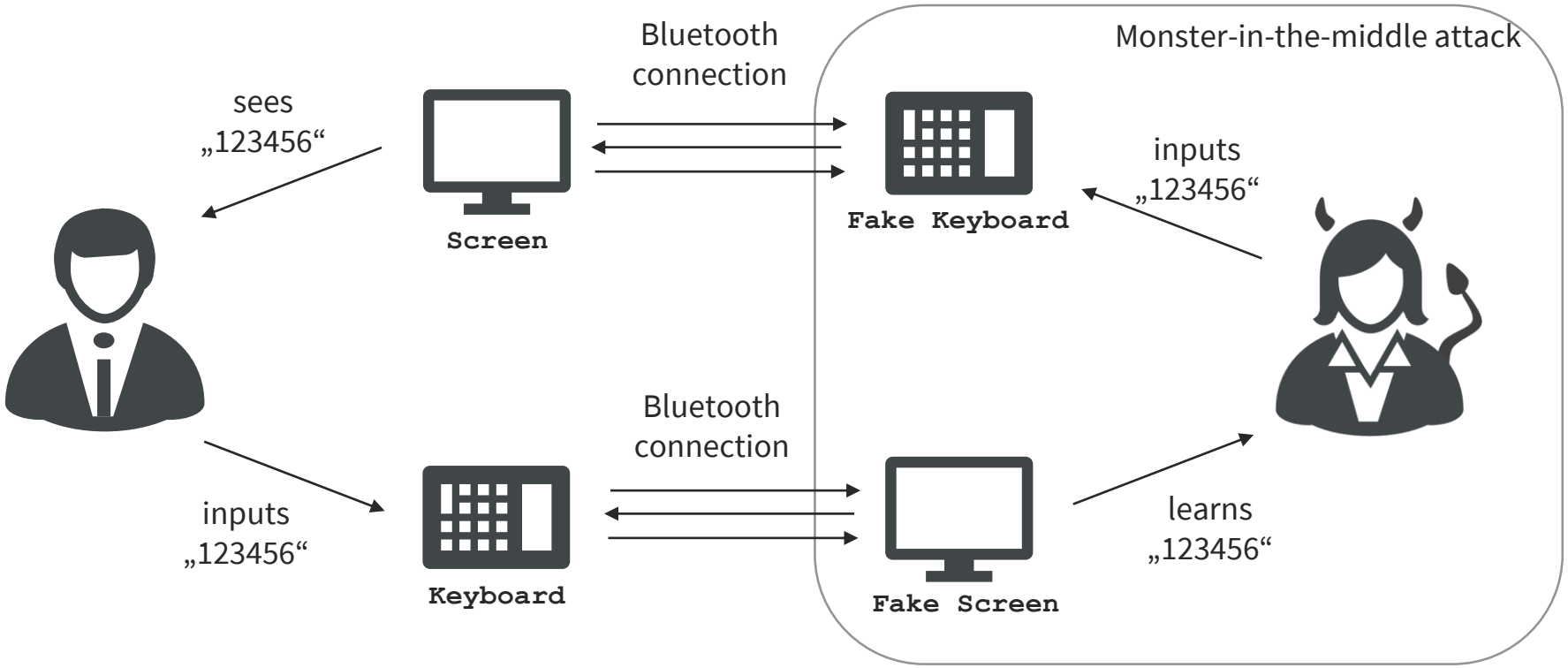
Why is it important to analyze the protocol suite?

Motivation

- Protocols depend on device features → **all protocols are in use**
- Various MITM attacks on protocols



Breaking Passkey Entry [ZWD+20]



[ZWD+20] Zhang, Weng, Dey, Jin, Lin, and Fu. Breaking secure pairing of bluetooth low energy using downgrade attacks, *USENIX Security 2020*

Our Contribution

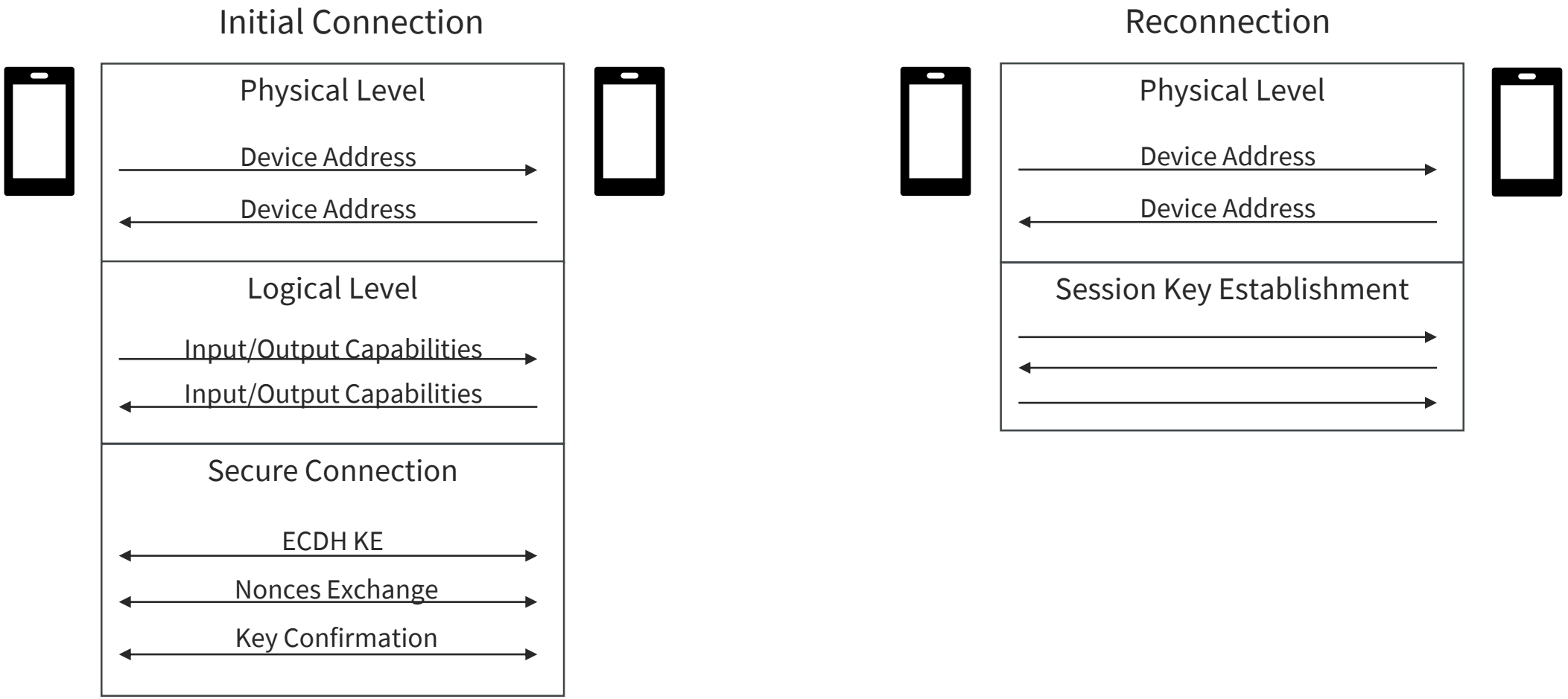
Our Contribution

1. First analysis of the full Secure Connection protocol suite
2. Analysis of Secure Connection as trust-on-first-use (TOFU) KE
3. Investigation of privacy mechanism in Bluetooth LE

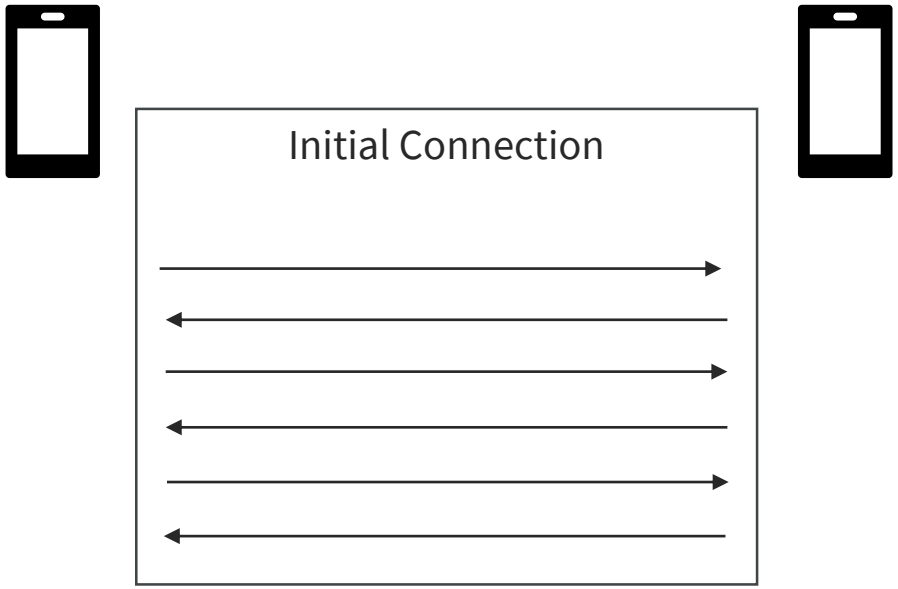
> *This submission may be the most precise and exhaustive I've read when it comes to explaining BR/EDR and BLE Pairing.*
>
> - Anonymous reviewer

Security analysis

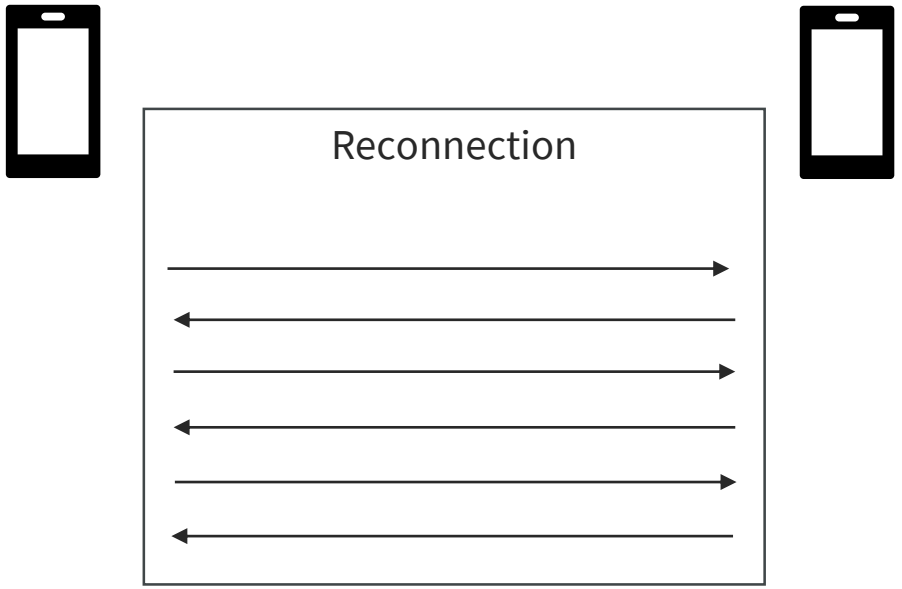
High-Level Protocol Description



TOFU (**T**rust-**O**n-**F**irst-**U**se) Model



Passive:
eavesdrop the communication



Active:
drop, modify messages, reveal the session key…

Security Model

[BR93]

- **Key Secrecy**
  - Session key remains secret
    → Adversary cannot distinguish between the real key and a random string

- **Match Security**
  - Partnered sessions derive the same session key
  - At most two sessions are partnered

- **Adversarial oracles**
  - Test, Reveal, Send, InitSession, Reconnect, NextPK

[BR93] Bellare and Rogaway. Entity authentication and key distribution, *CRYPTO'93*

Security Results

- **Assumptions**
  - PRF-ODH [BFGJ17]; AES is PRF
  - TOFU (passive during initial connection, active during reconnection)

The Secure Connection protocol suite achieves security

[BFGJ17] Brendel, Fischlin, Günther, and Janson. PRF-ODH: Relations, instantiations, and impossibility results, *CRYPTO 2017*

Privacy analysis

Motivation

- Mostly privacy as linkability of physical characteristics
- Linkability of cryptographic transcript [SSY19]
  - Pointed out reusing of the DH share can link the device
  - No analysis of address randomization mechanism

[SSY19] Sun, Sun, and Yang. On secure simple pairing in bluetooth standard v5.0-part II: privacy analysis and enhancement for low energy, *Sensors 2019*

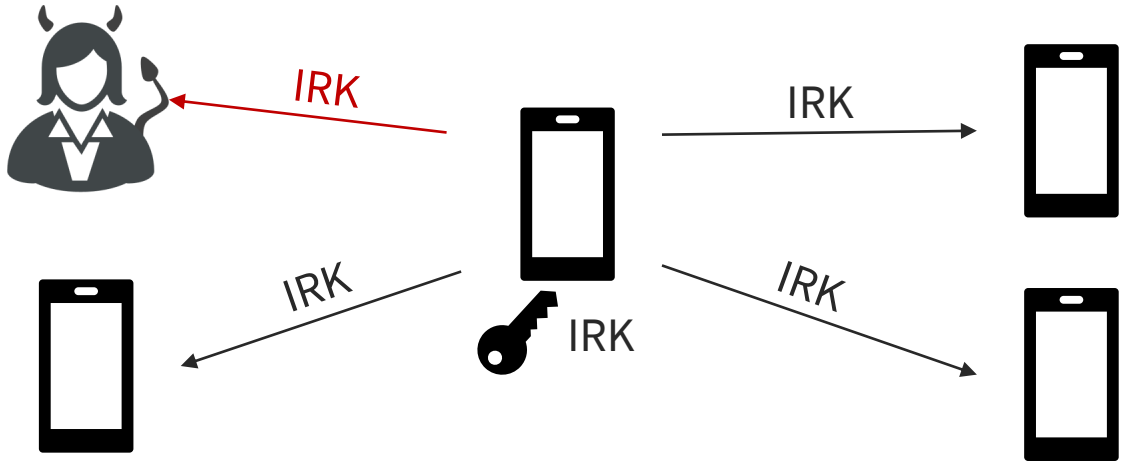
Privacy Mechanism

Non-resolvable random addresses

- Random value
- Initial connection

Resolvable random addresses

- Random value *prand* + encrypted with **I**dentity **R**esolving **K**ey (IRK)
- Reconnections



Model

- **Outsider privacy**
  - The target device cannot be linked
    → Adversary cannot distinguish the target device from some other
  - The **I**dentity **R**esolving **K**ey (IRK) of the target remains secret

- **Adversarial oracle**
  - Test

Privacy Results

- **Assumptions**
  - Adversary is passive and does not learn the IRK
  - DH shares are fresh in each session
  - Device-specific information (e.g. Input/Output capabilities) is the same
  - AES is PRF

Address randomization mechanism achieves a decent level of privacy

Overall advantage of the adversary is close to $q_s^2 \cdot 2^{-|prand|+2}$,

where q_s^2 - number of Test queries, $|prand| = 24$.

NOTE: the result does not rule out linkability of the device via physical means!

Summary

Summary

- The Secure Connection protocol suite is secure in TOFU model
- Bluetooth LE achieves outsider privacy when ruling out physical traceability
- Bluetooth Standard is hard to navigate due to the size and lack of clarity

Thank You!

Olga Sanina

olga.sanina [at] cryptoplexity [dot] de

References

[ATR19] Antonioli, Tippenhauer, and Rasmussen. The KNOB is broken: Exploiting low entropy in the encryption key negotiation of bluetooth BR/EDR, *USENIX Security 2019*

[ATR20a] Antonioli, Tippenhauer, and Rasmussen. BIAS: Bluetooth impersonation AttackS, *IEEE S&P 2020*

[ATR20b] Antonioli, Tippenhauer, and Rasmussen. Key negotiation downgrade attacks on bluetooth and bluetooth low energy, *ACM TOPS 2020*

[ATRP20] Antonioli, Tippenhauer, Rasmussen, and Payer. BLURtooth: Exploiting Cross-Transport Key Derivation in Bluetooth Classic and Bluetooth Low Energy, *arXiv 2020*

[BFGJ17] Brendel, Fischlin, Günther, and Janson. PRF-ODH: Relations, instantiations, and impossibility results, *CRYPTO 2017*

[BR93] Bellare and Rogaway. Entity authentication and key distribution, *CRYPTO 1993*

[CL21] Claverie and Lopes-Esteves. Bluemirror: Reflections on bluetooth pairing and provisioning protocols, *IEEE SPW (WOOT) 2021*

[Lin09] Lindell. Comparison-based key exchange and the security of the numeric comparison mode in Bluetooth v2.1, *CT-RSA 2009*

References

[SS19] Sun and Sun. On secure simple pairing in bluetooth standard v5.0-part i: Authenticated link key security and its home automation and entertainment applications, *Sensors 2019*

[SSY19] Sun, Sun, and Yang. On secure simple pairing in bluetooth standard v5.0-part II: privacy analysis and enhancement for low energy, *Sensors 2019*

[TH21] Troncoso and Hale. The bluetooth cyborg: Analysis of the full human-machine passkey entry ake protocol, *NDSS 2021*

[vTPFG21] von Tschirschnitz, Peuckert, Franzen, and Grossklags. Method confusion attack on bluetooth pairing, *IEEE S&P 2021*

[WNK+20] Wu, Nan, Kumar, Tian, Bianchi, Payer, and Xu. BLESA: Spoofing attacks against reconnections in Bluetooth low energy, *IEEE SPW (WOOT) 2020*

[ZWD+20] Zhang, Weng, Dey, Jin, Lin, and Fu. Breaking secure pairing of bluetooth low energy using downgrade attacks, *USENIX Security 2020*