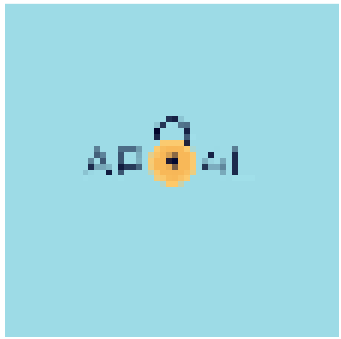
Coseners 2025



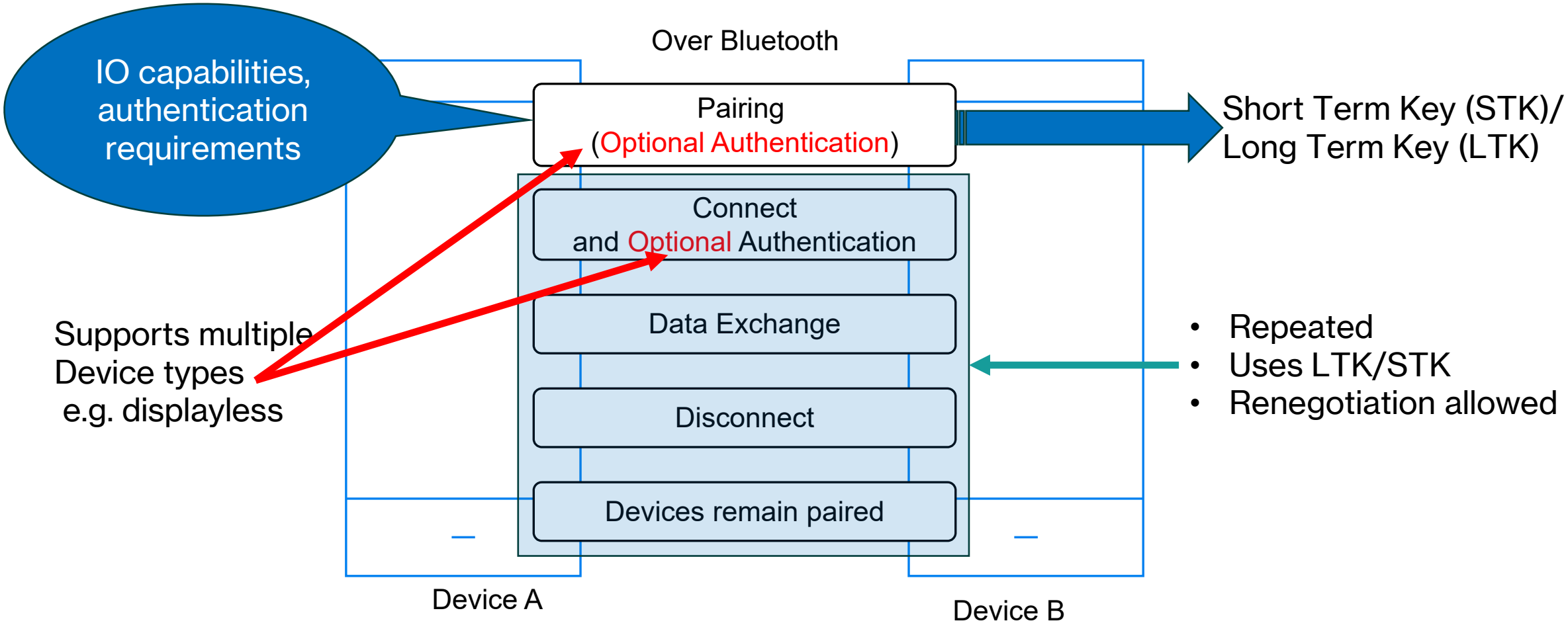
UNIVERSITY OF SURREY

End-point authentication method using gyroscope-based shared secret for inter-smartphone direct communication

Vinod Khandkar, Nishanth Sastry, Ehsan Toreini, Kieron Ivy Turk

https://ap4l.github.io/

Bluetooth Communication



PASSKEY=Pairing with Authentication

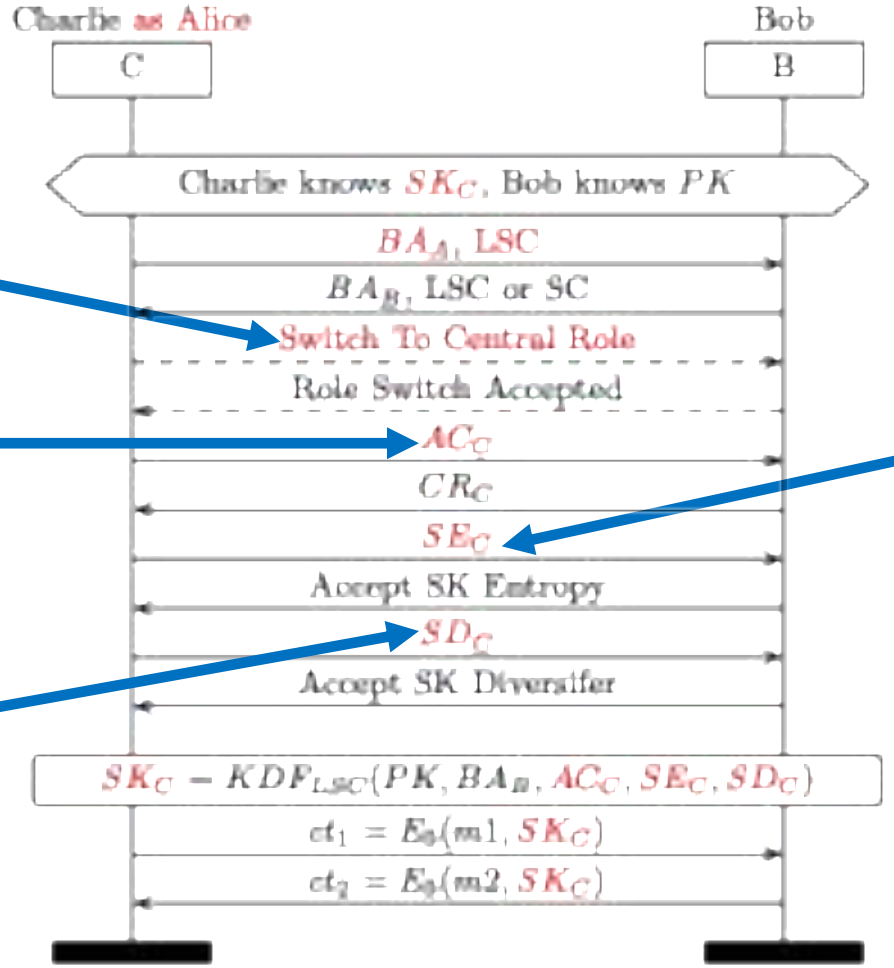
BT communication vulnerability

Disables existing encryption

Fixes the authentication challenge

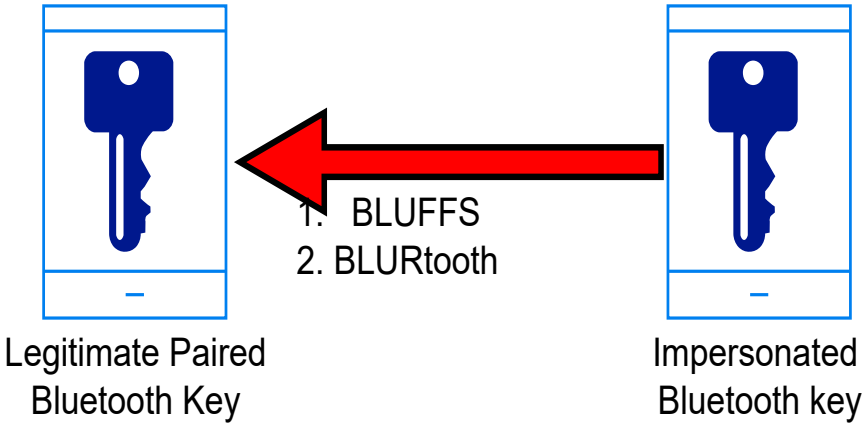
Fixes key derivation parameter

Sets session key entropy to lowest i.e. 1 byte



Courtesy: (2023) BLUFFS: Bluetooth Forward and Future Secrecy Attacks and Defenses DOI: https://doi.org/10.1145/3576915.3623066

BT vulnerabilities in the wild

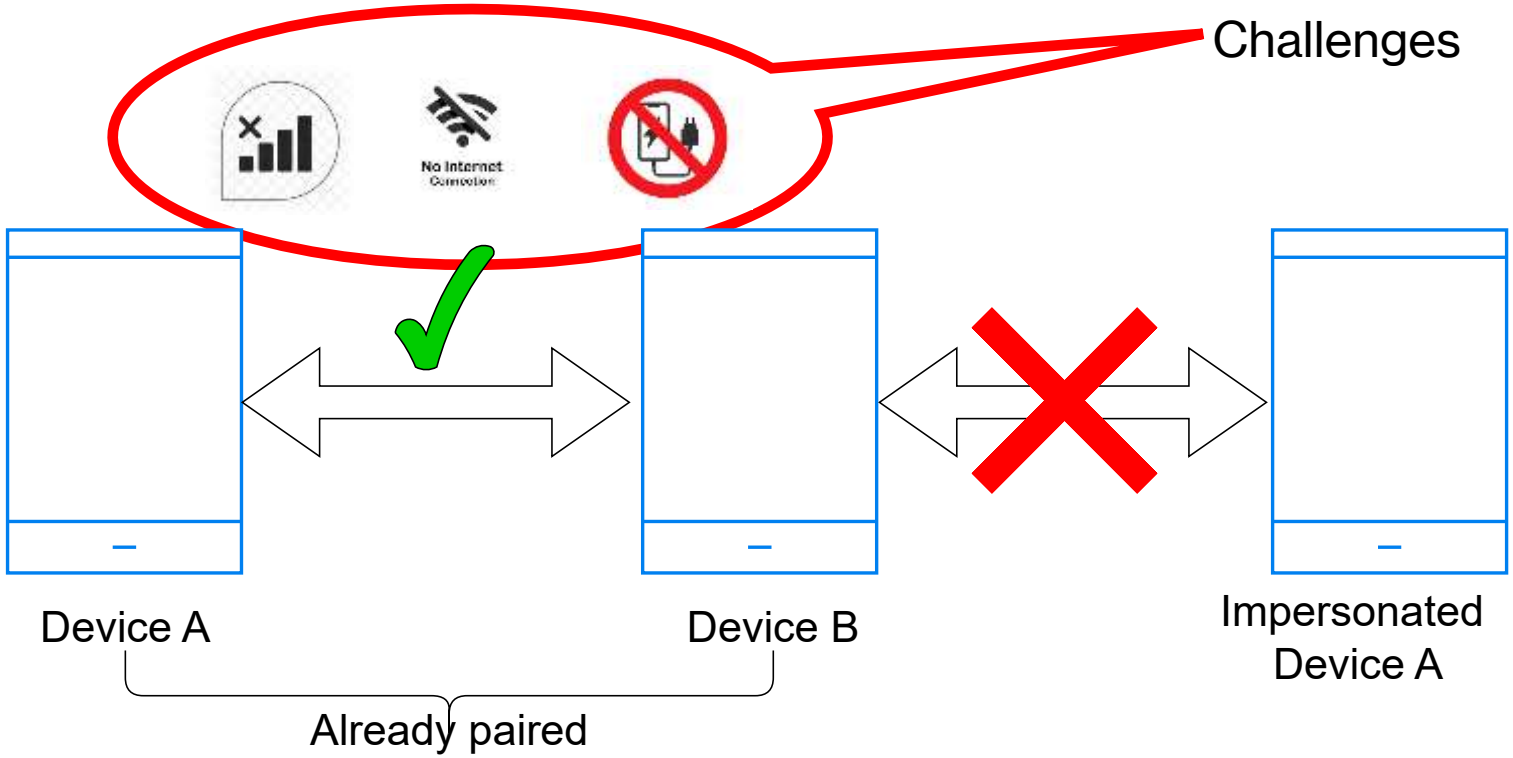


Attacked Chipset
- Infineon CYW20819
- Qualcomm Snapdragon 865
- Murata 339S00199

1. BLUFFS: https://doi.org/10.1145/3576915.3623066
2. BLURTOOTH: https://doi.org/10.1145/3488932.3523258

Another scenario:
- Tourist group visiting remote locations

Research Problem



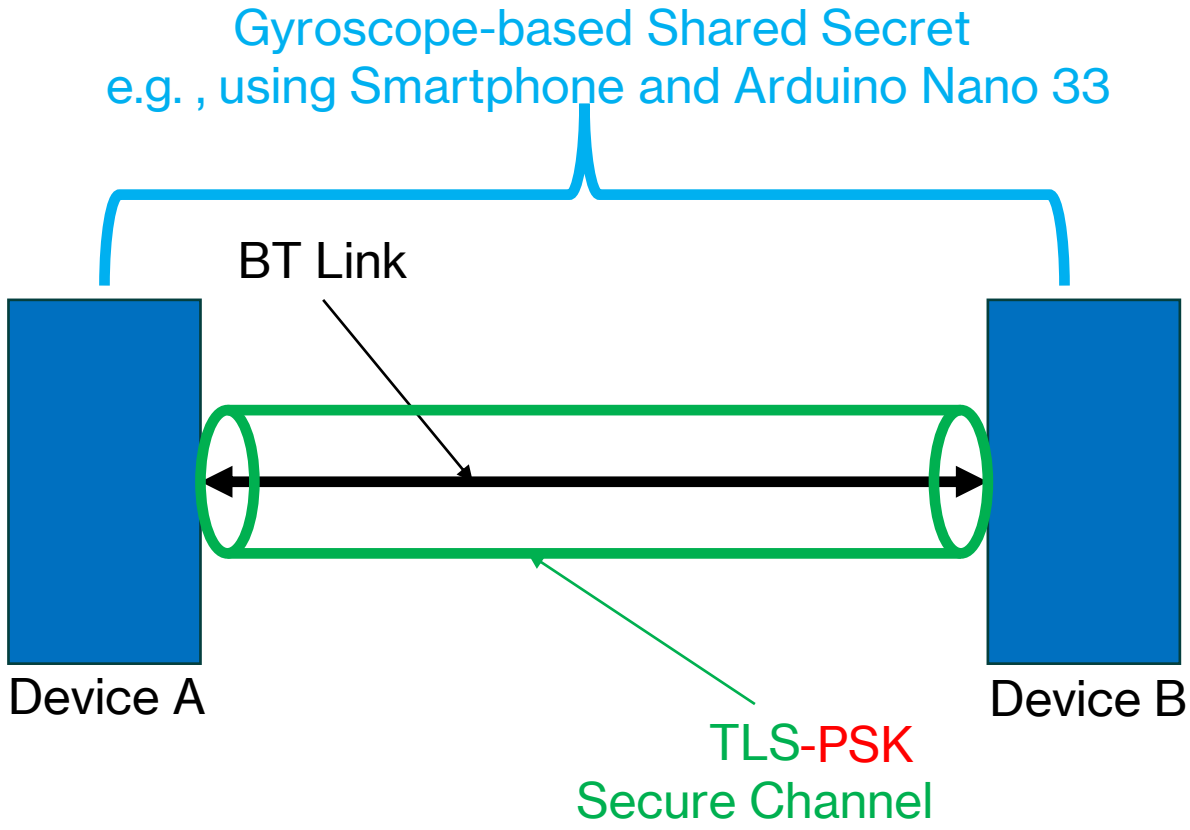
Existing solutions:

- Third-party infrastructure-based certificates/QR-codes
- High overhead customized application layer

Proposed System Design

Challenges

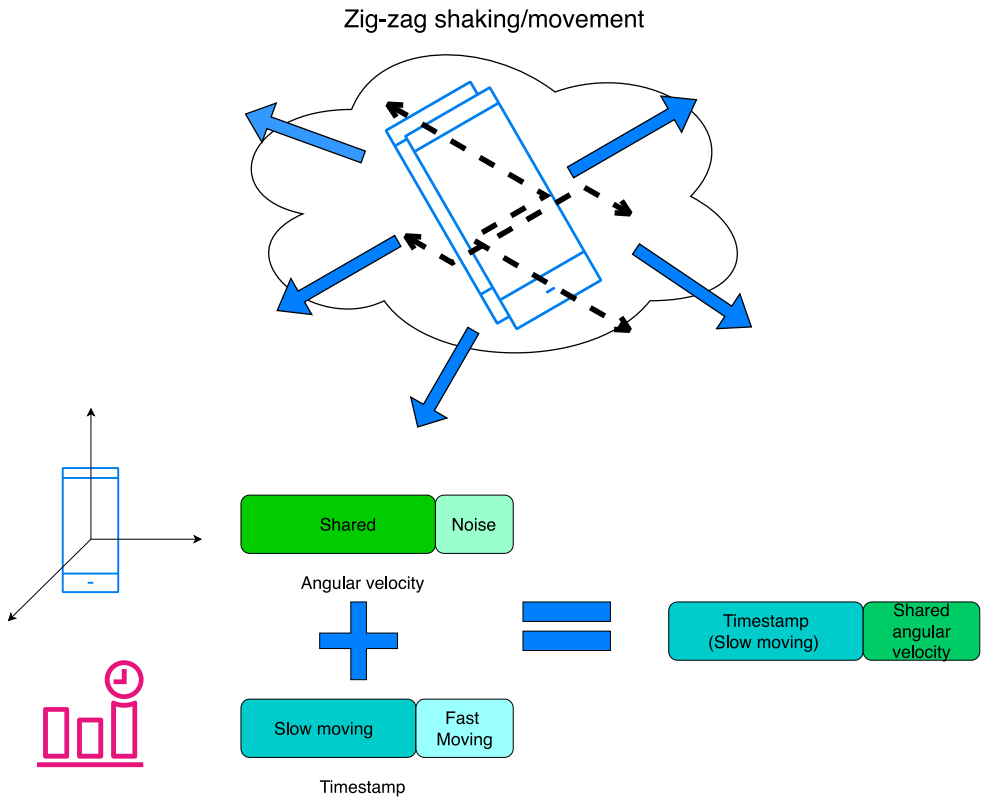
- Without a certificate or QR code operation
- Remote device authentication by initiating the device
- Low power operation
- Low data overhead operation



BT: Bluetooth
TLS: Transport Layer Security
PSK: Pre Shared Key

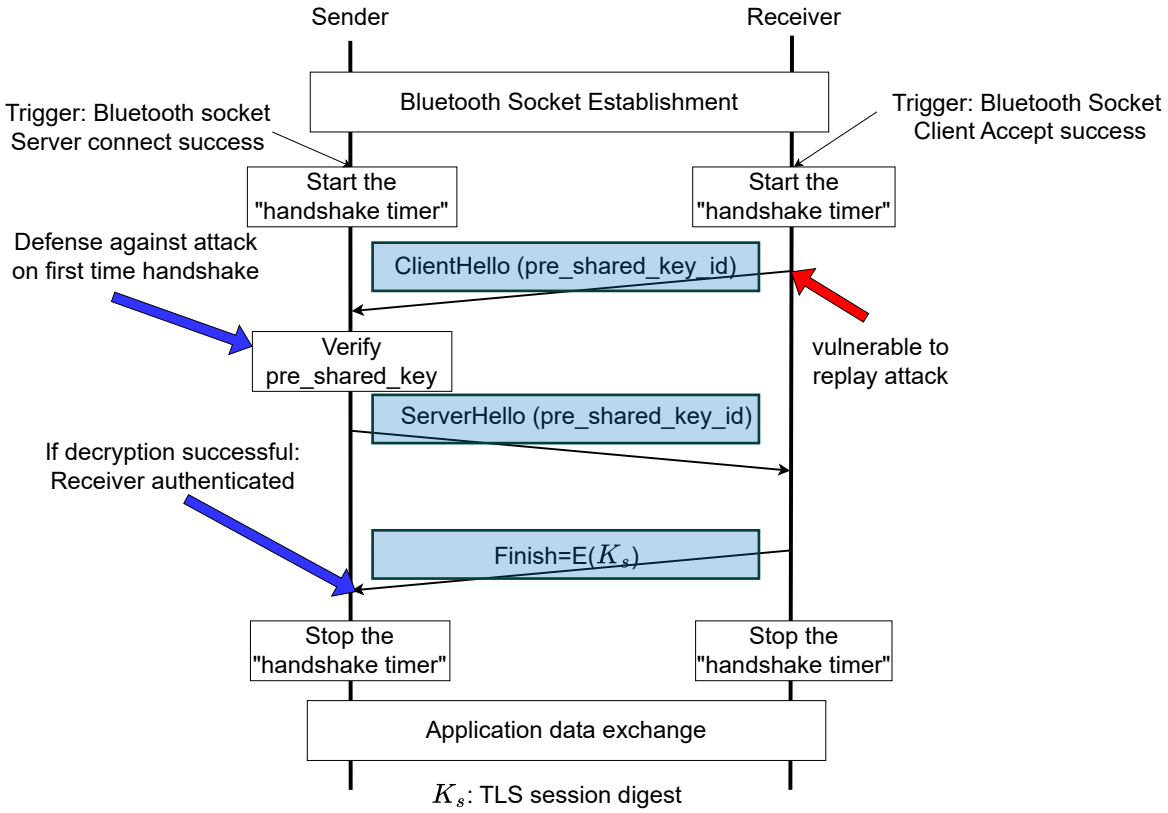
Methods

Shared secret generation



Secret length > 256 bits
Success rate: Above 80%
Entropy: 6.7 bits/8 bits

End-point authentication

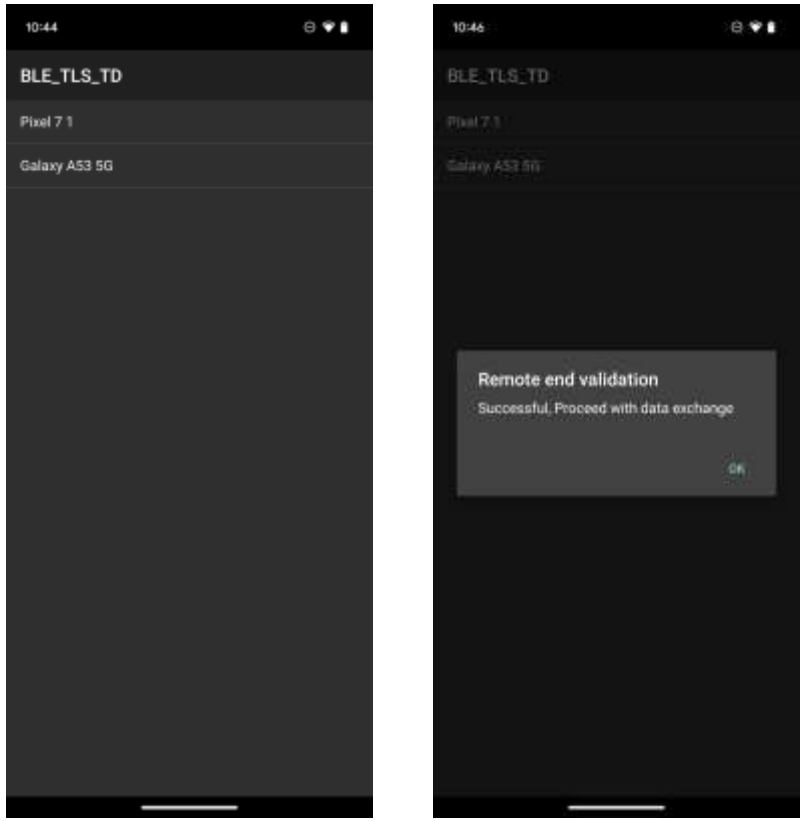


Overhead:

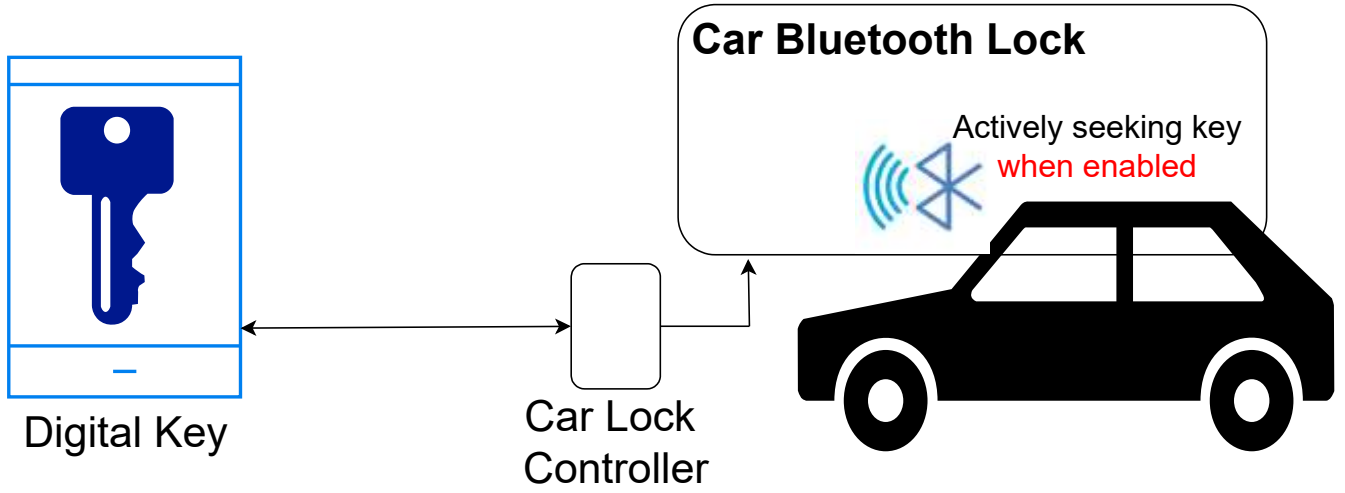
- ≈ 2ms
- 400-500 bytes

Real-world application

Step-1: Receiver Validation



Step 2: Digital Car-lock Controller
(To be developed)



Contact: v.khandkar@surrey.ac.uk

Attack resilience