Attacking Ultra-Wideband

Security Analysis of UWB Applications in Smartphones

Alexander Heinrich & Jiska Classen
Secure Mobile Networking Lab - SEEMOO
Technical University of Darmstadt, Germany

SEEMOO TECHNISCHE UNIVERSITÄT DARMSTADT ATHENE National Research Center for Applied Cybersecurity emergenCITY


UWB Basics

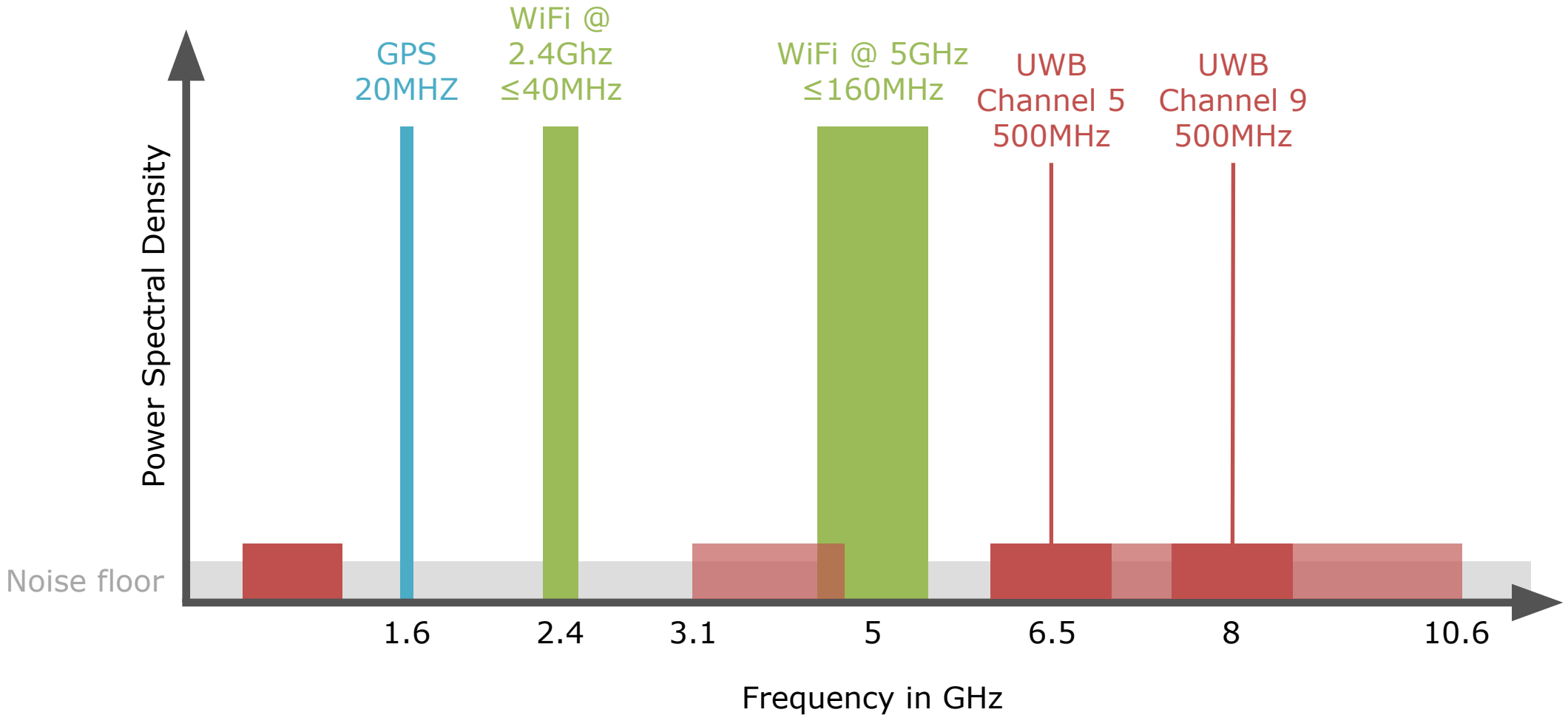
Ultra-Wideband (UWB)

Nobody knows what
it is or does

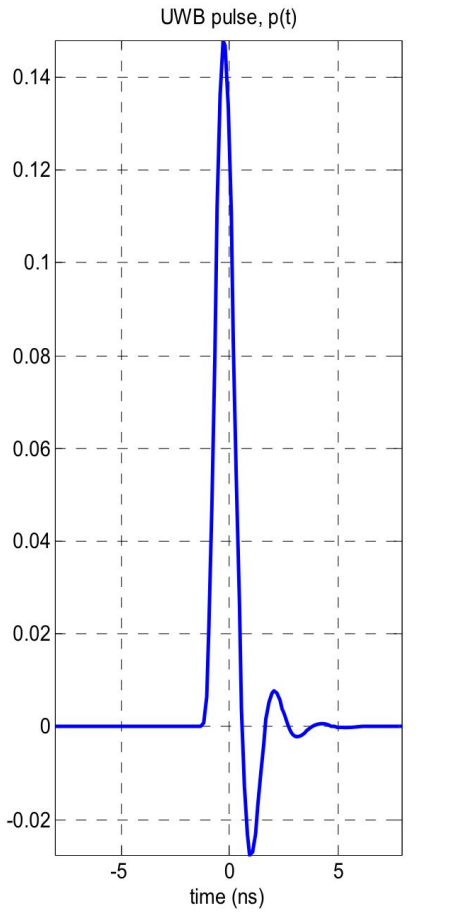
Non-interceptable with
cheap SDRs

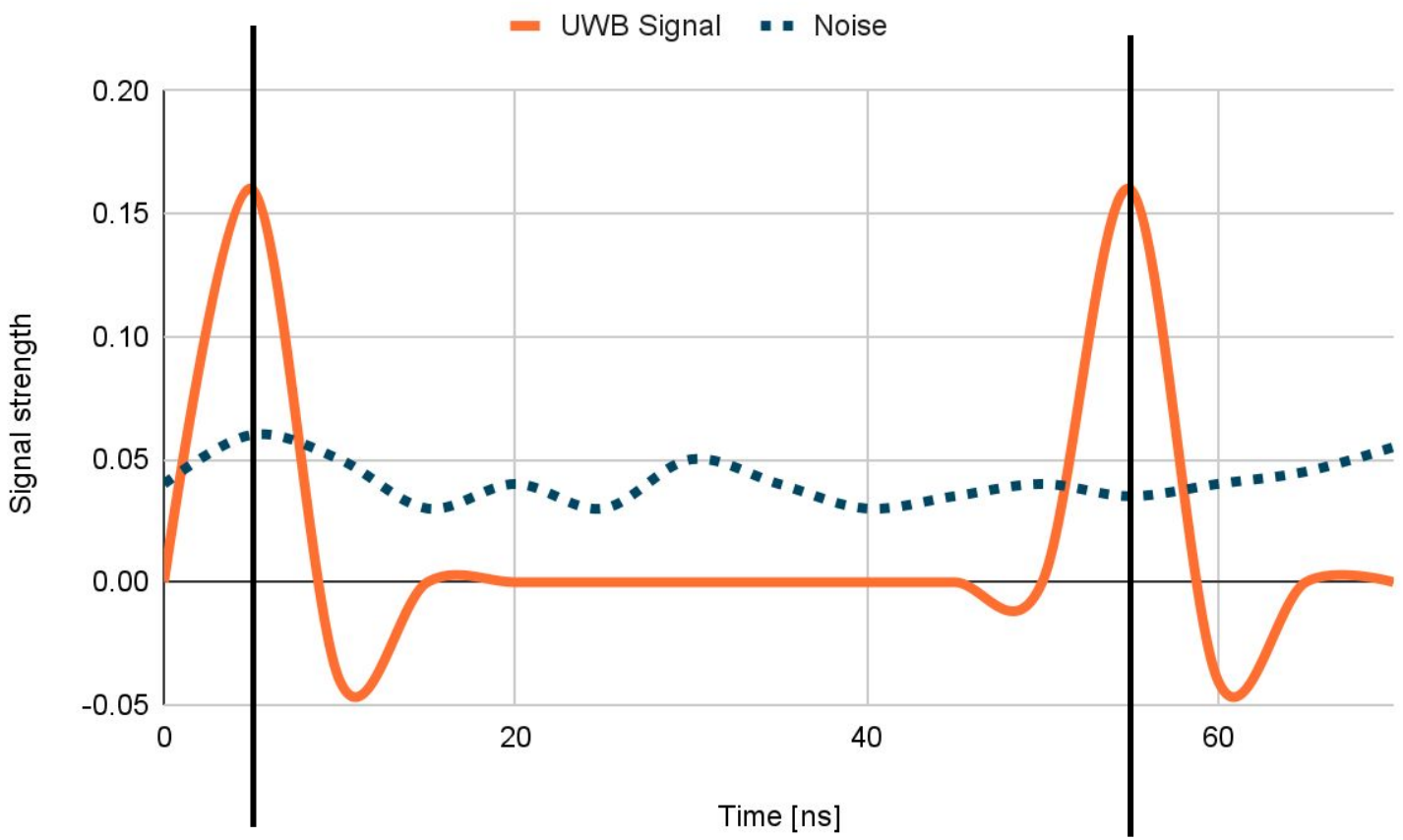
Only available in the latest
generation of devices

Must be
hacker-proof!

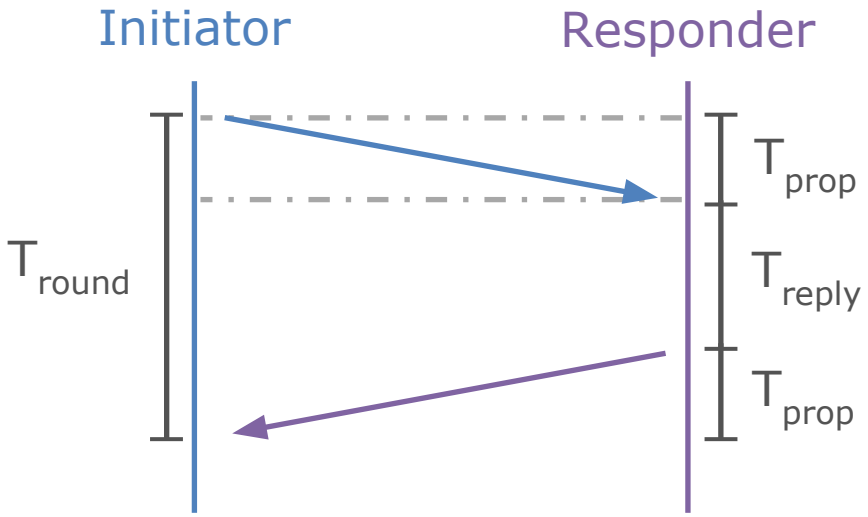

GPS
20MHZ
WiFi @
2.4Ghz
≤40MHz
WiFi @ 5GHz
≤160MHz
UWB
Channel 5
500MHz
UWB
Channel 9
500MHz
Power Spectral Density
Noise floor
1.6
2.4
3.1
5
6.5
8
10.6
Frequency in GHz

Impulse radio



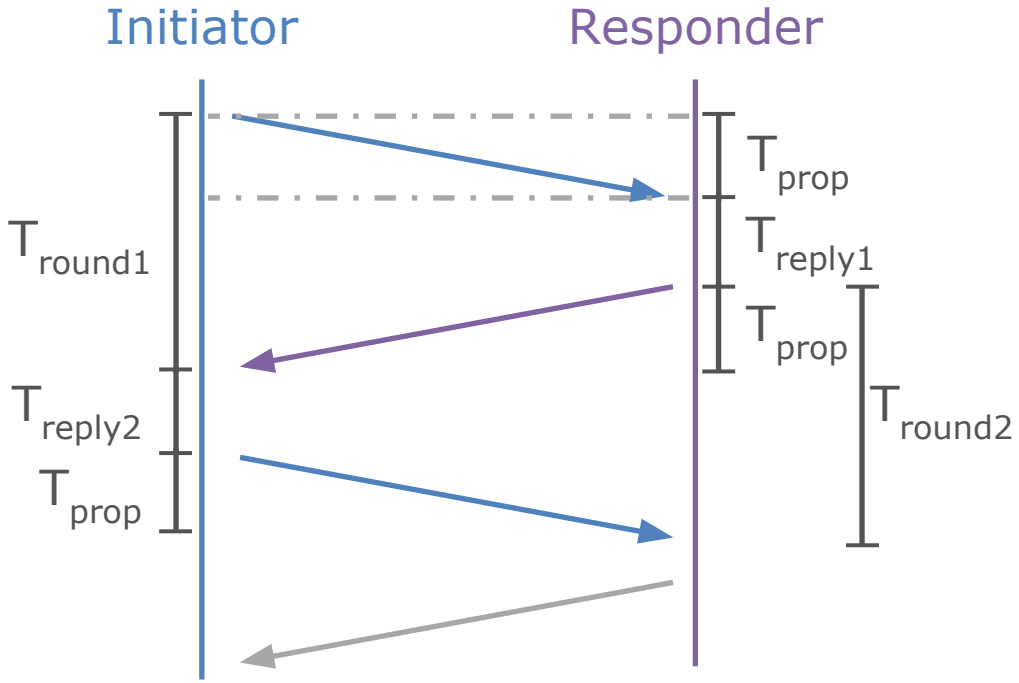


Single-sided two-way ranging (SS-TWR)

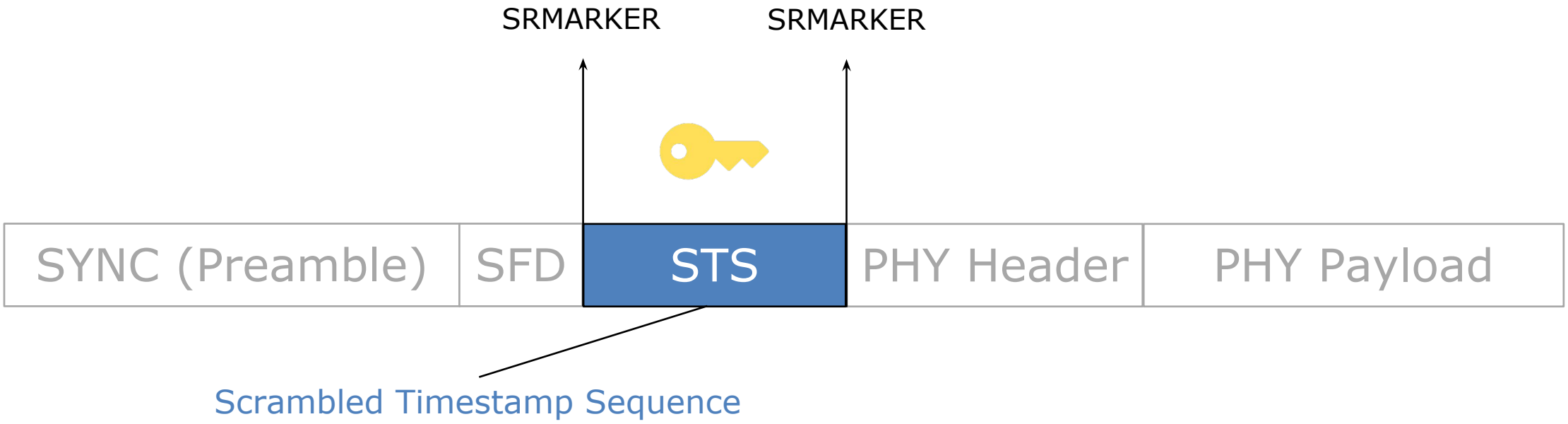


$$\frac{1}{2} \bullet (T_{round1} - T_{reply1})$$

Double-sided two-way ranging (DS-TWR)



- Signals travel with speed of light
- You cannot travel faster than speed of light



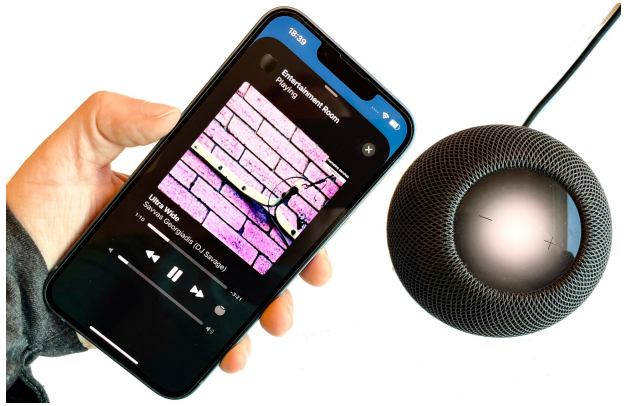
- Initiator and responder must trust each other
- They have a pre-shared secret

UWB Applications

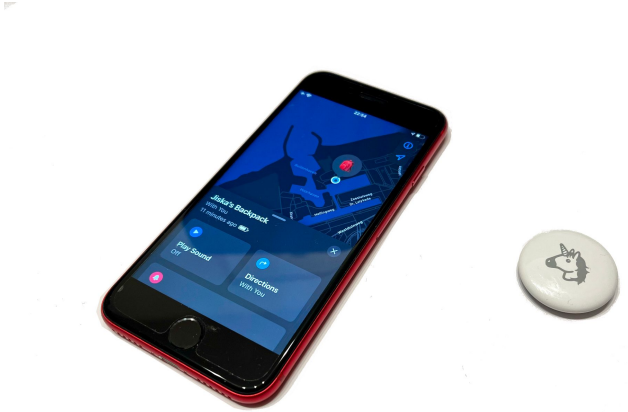
UWB in the Apple Ecosystem

AirDrop (iOS 13)
First prototype w/o frameworks. Firmware already hints towards future applications.

Nearby Interaction (iOS 14)
Framework to enable ranging between Apple devices & third parties.

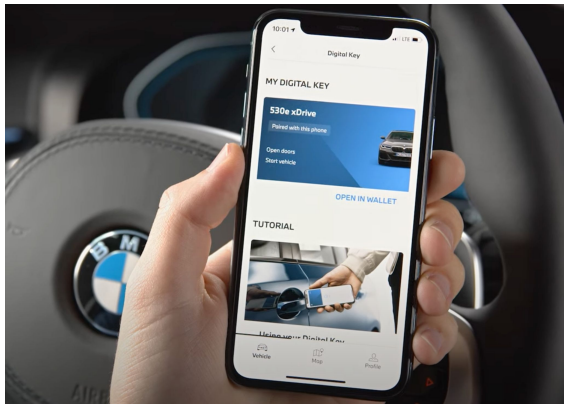


HomePod Handoff (iOS 14.4)
HomePod is permanently connected to power and beacons measurement packets continuously.



AirTag (iOS 14.5)
AirTag localization with distance and angle, battery-efficient implementation on AirTag.

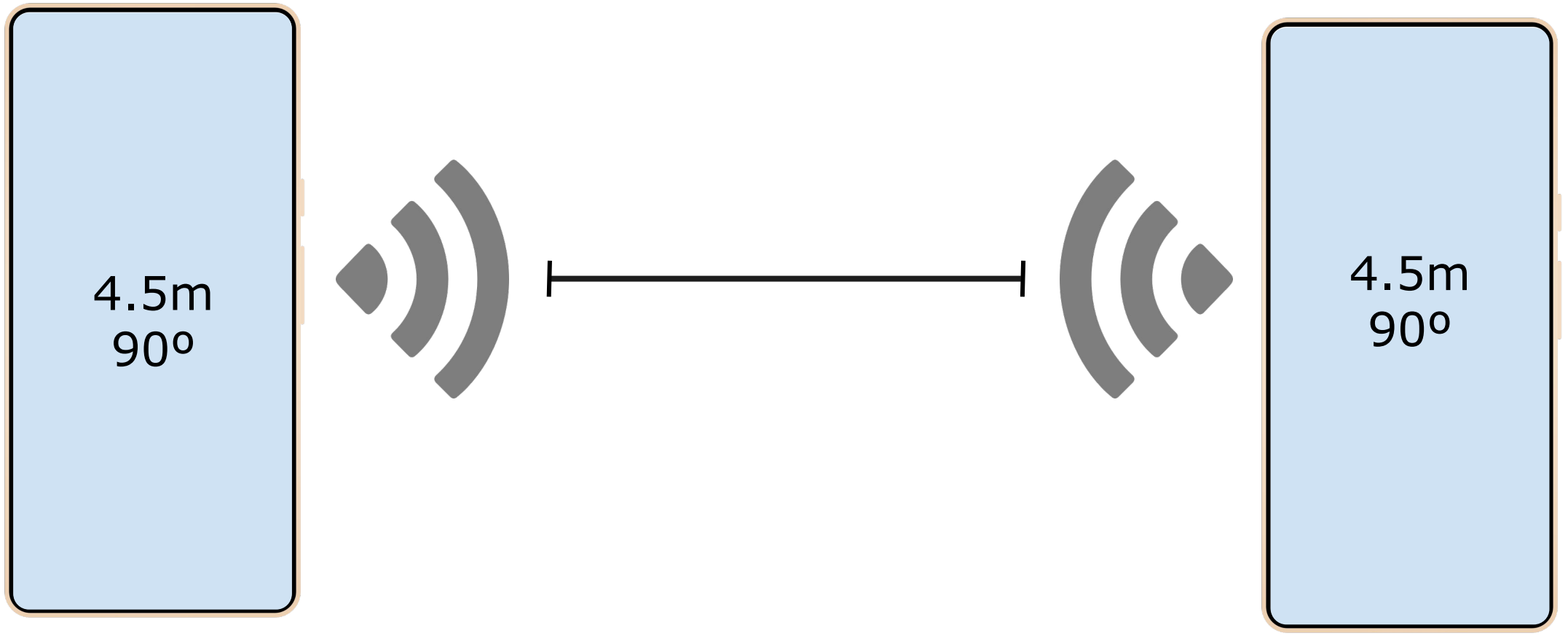
…to be continued



Digital Car Key (iOS 15)
Support for UWB-based digital keys as successor to NFC.

Nearby Share (Android)

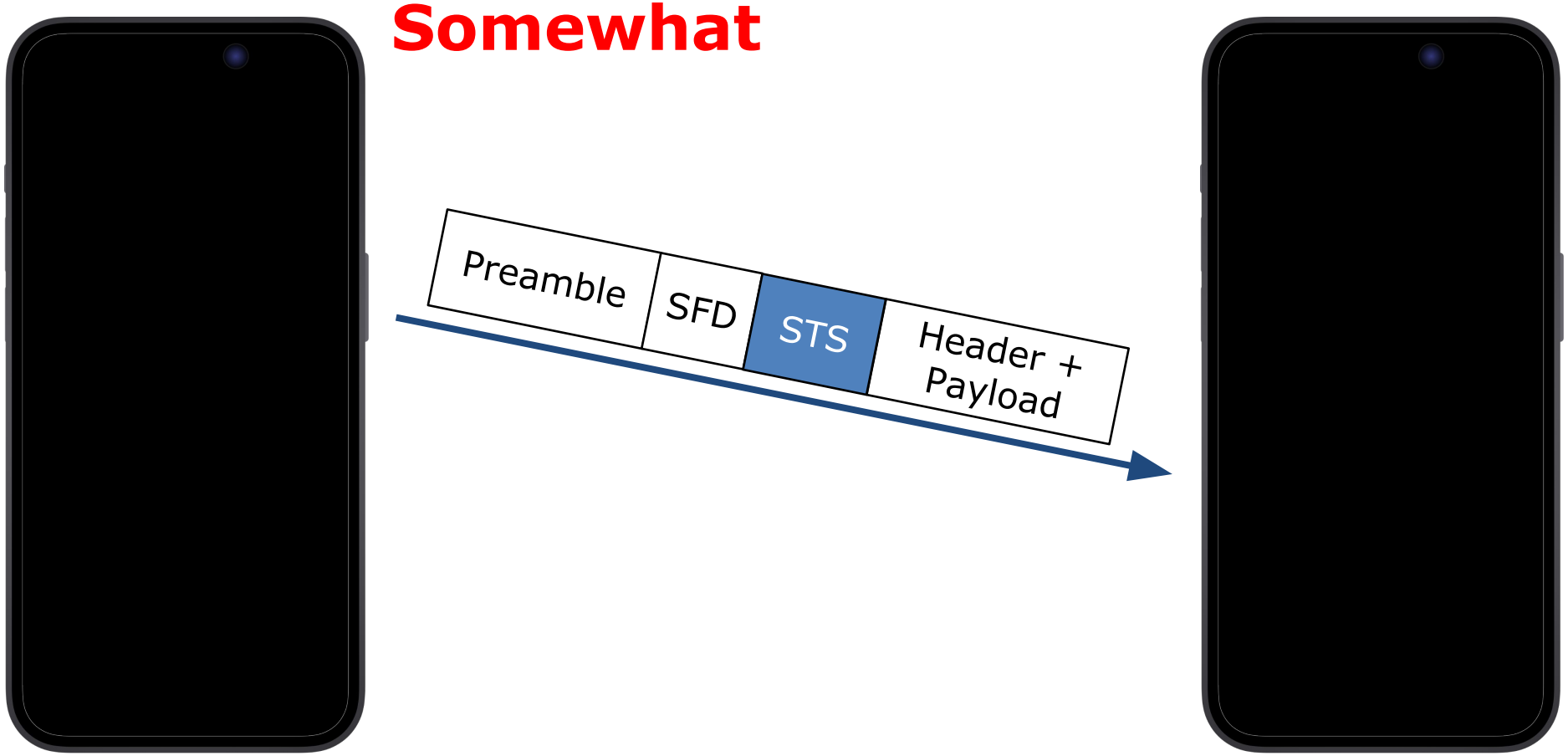
Android UWB SDK



UWB Internals

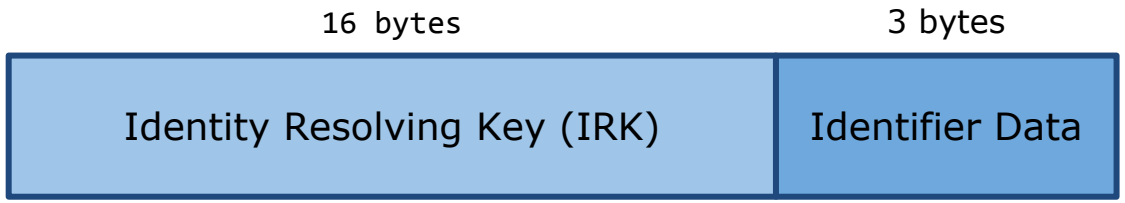
UWB Secure Ranging

Somewhat



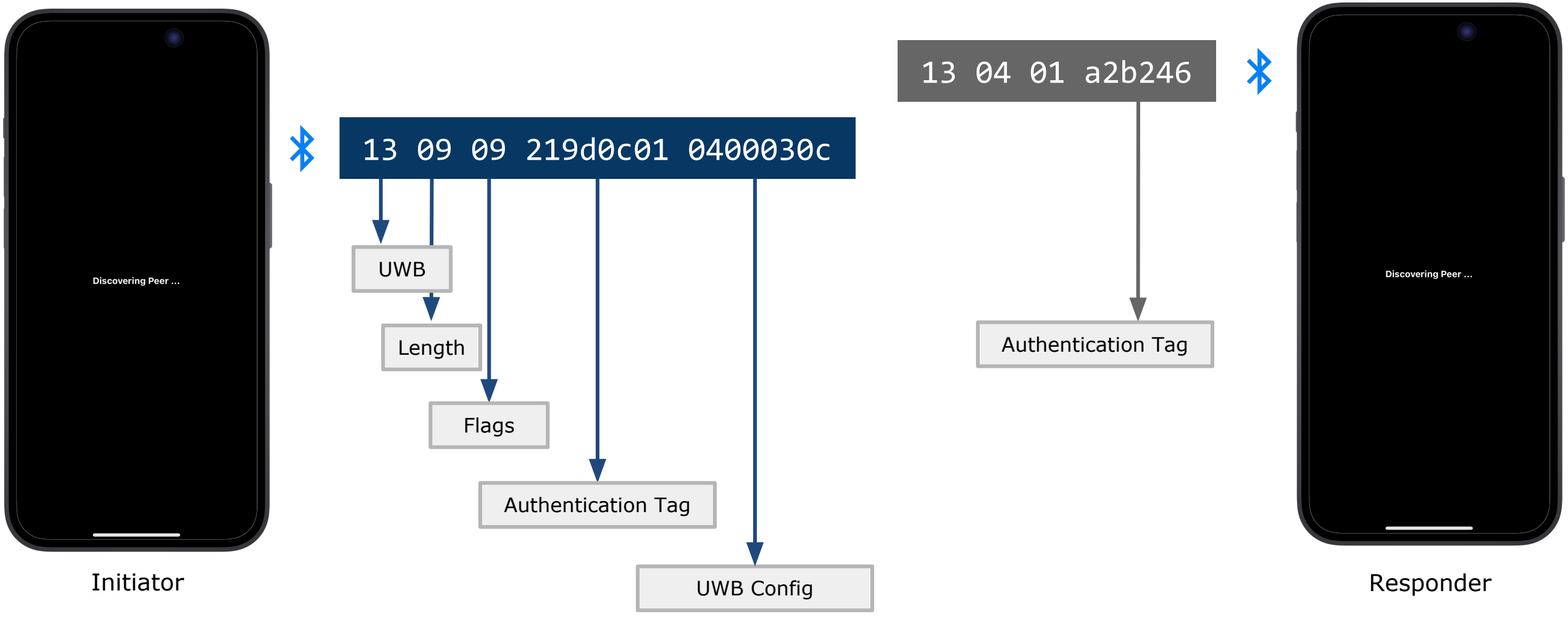
Security aspects on iOS

NIDiscoveryToken



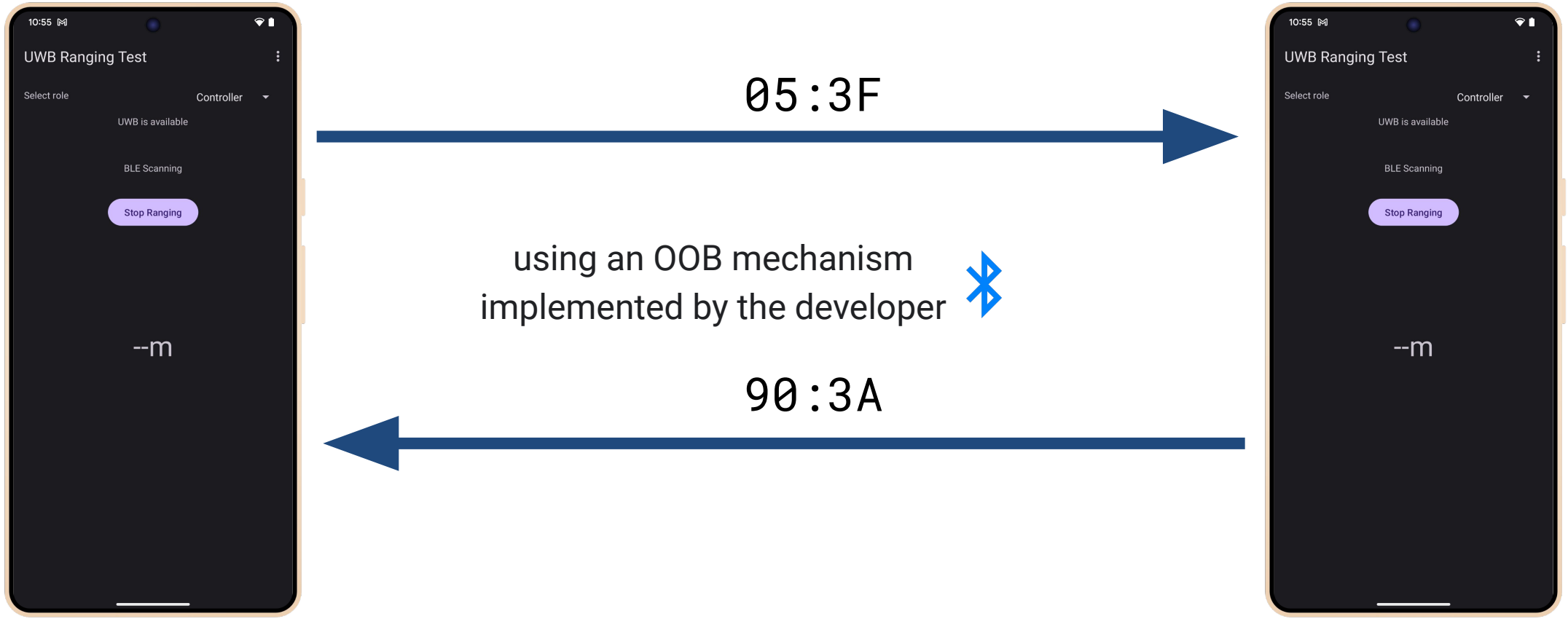
SipHash(MAC address , IRK) = Auth Tag

iOS Discovery




Initiator Token [7:15]
+
Responder Token [7:15]
=
STS

Device discovery on Android



Controller

Controllee

Security aspects of Android Ranging

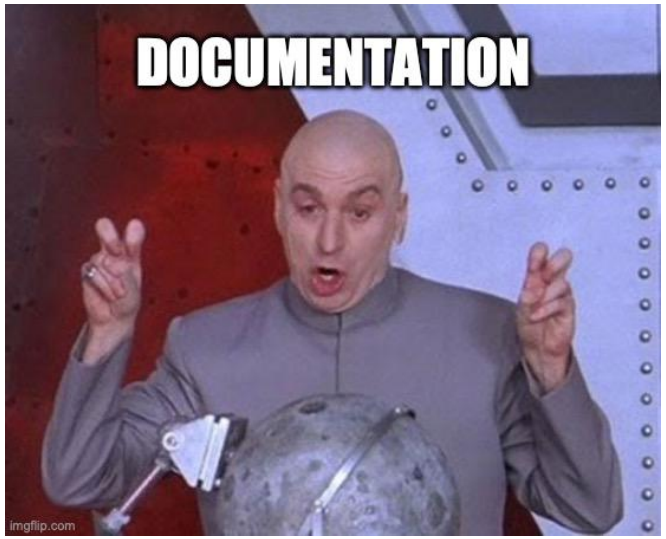
Controller

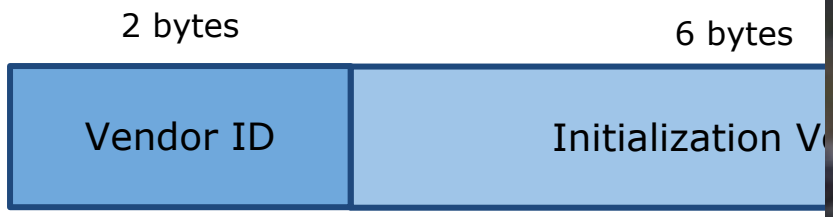
Controllee

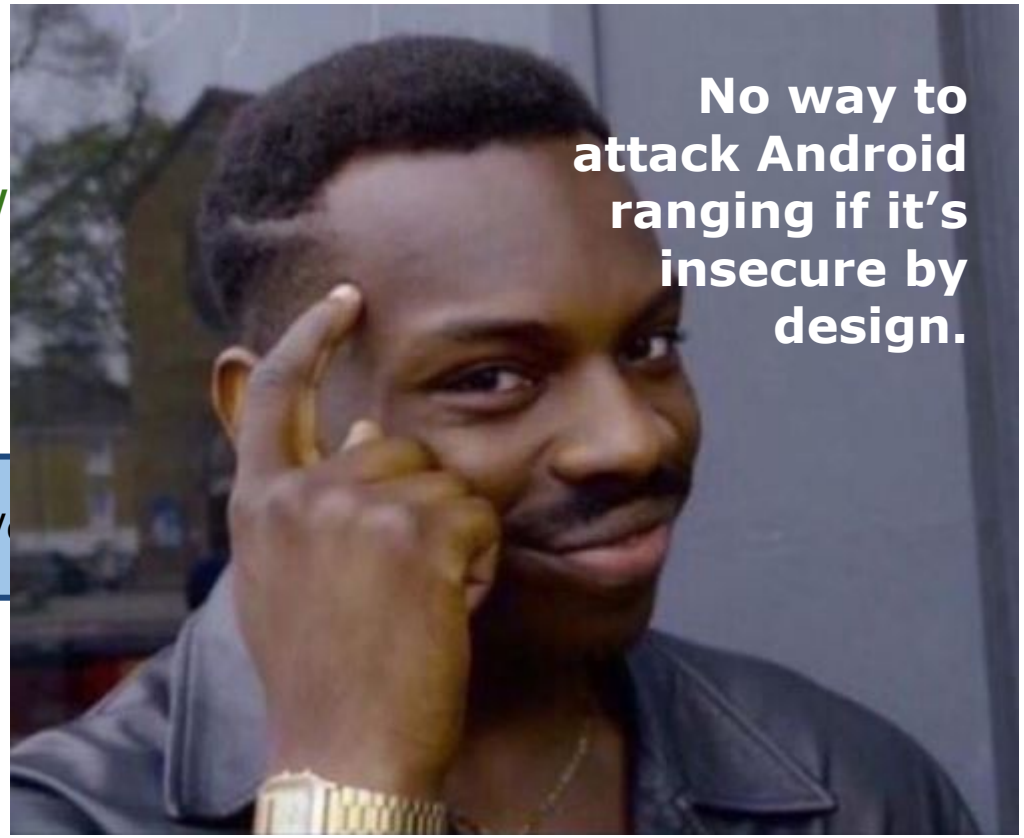
SessionKeyInfo

```
// SessionKeyInfo is used to encrypt the ranging session.

// If the profile uses STATIC STS, this byte array is 8-byte
   two bytes as Vendor_ID and next six bytes as STATIC_STS_IV
```

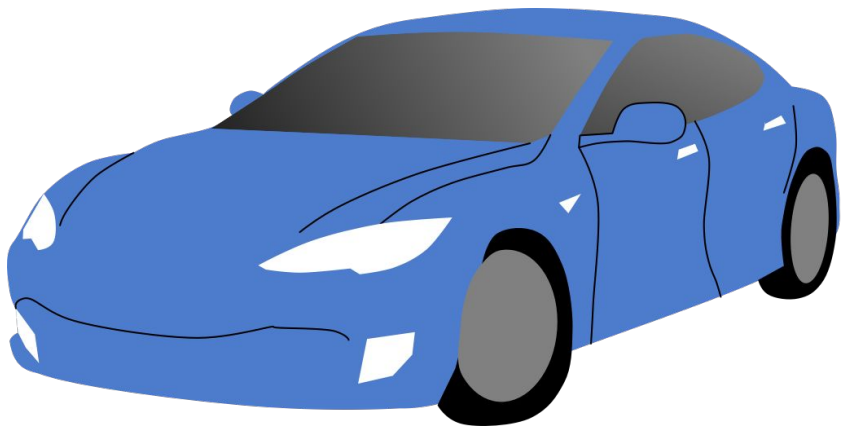






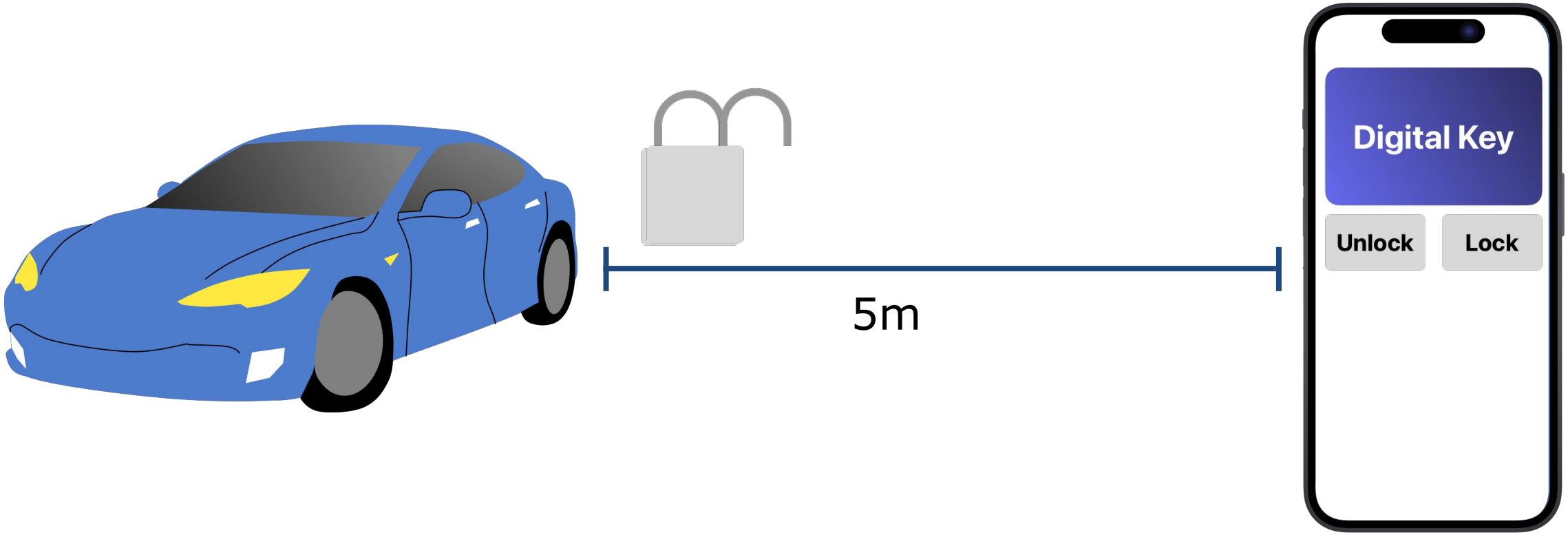
All publicly available UWB profiles use `STATIC_STS`.

Accuracy & Reliability

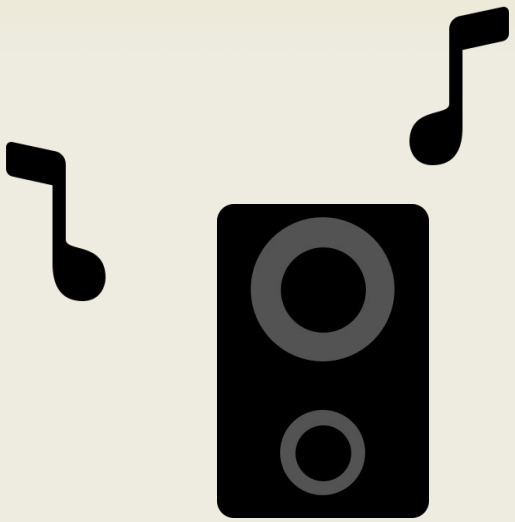


1m ±50cm

Accurate to 50cm



Accurate to 50cm

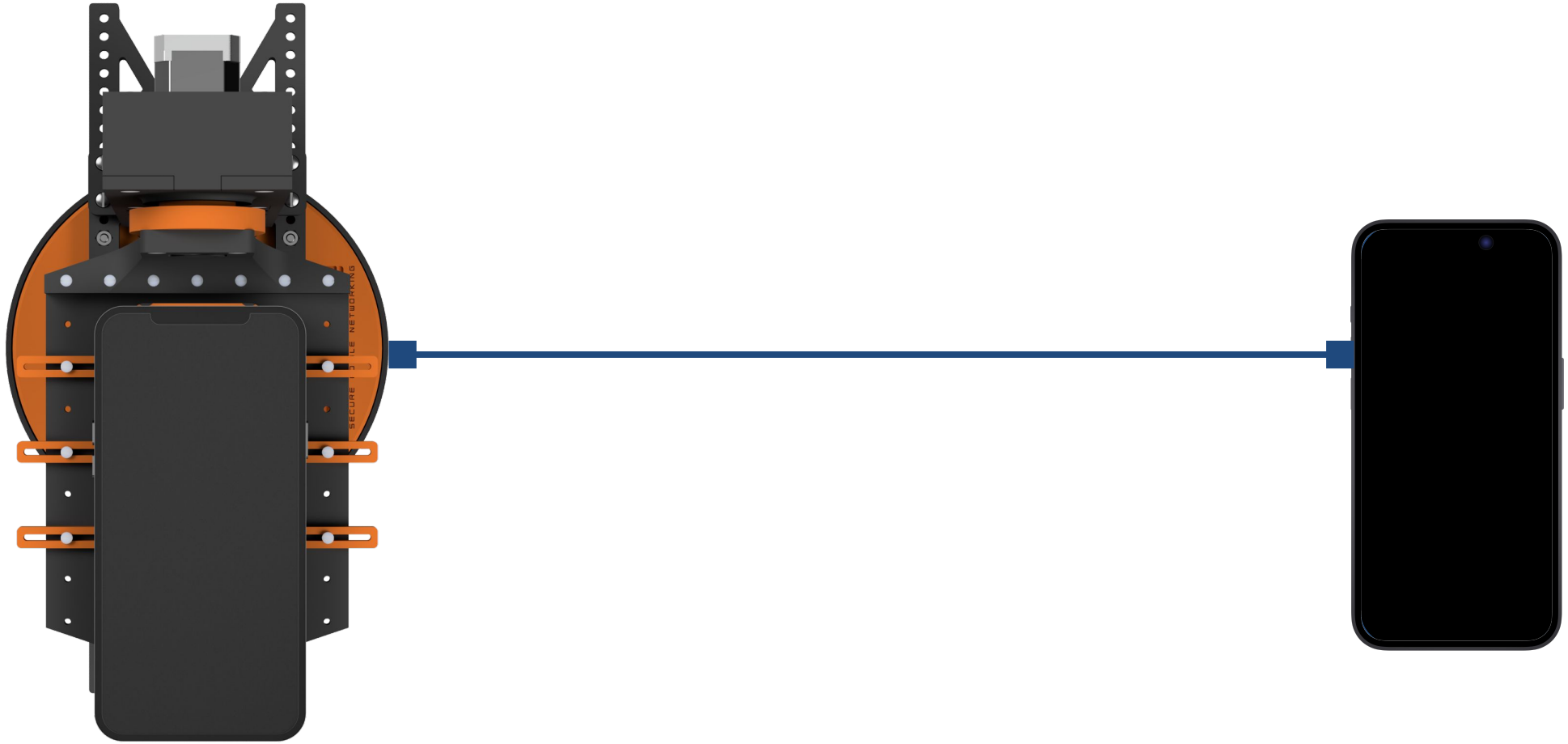


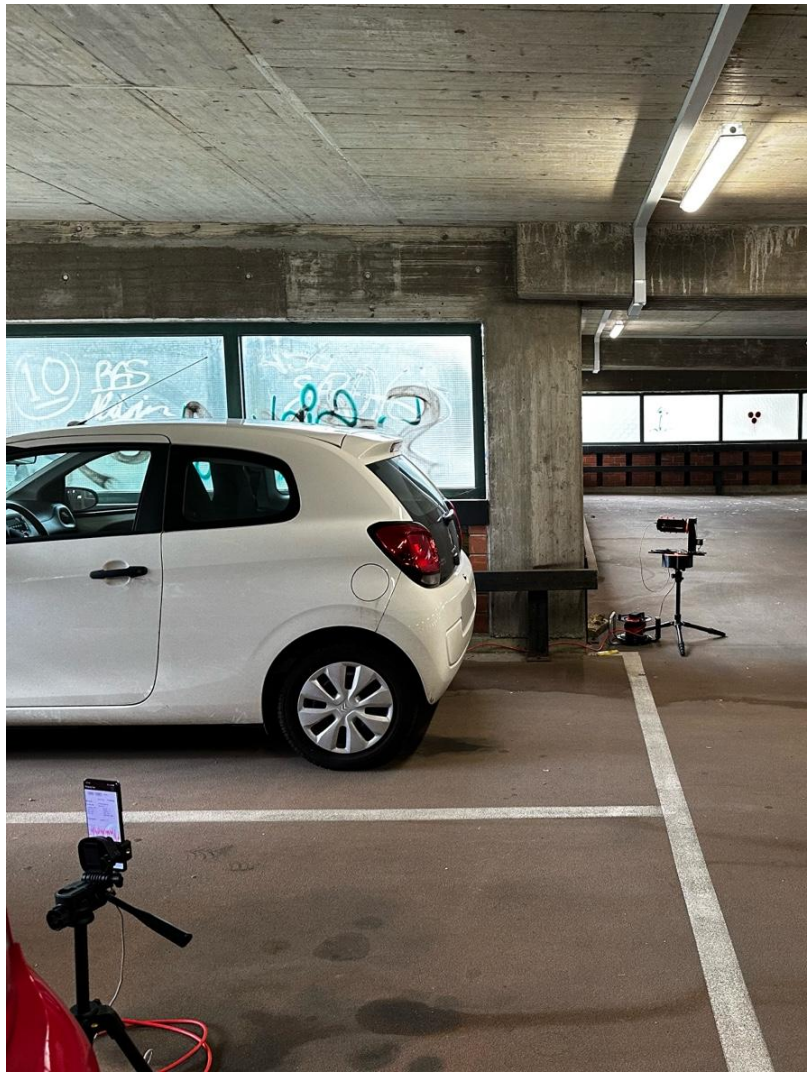
Meow

Reliable

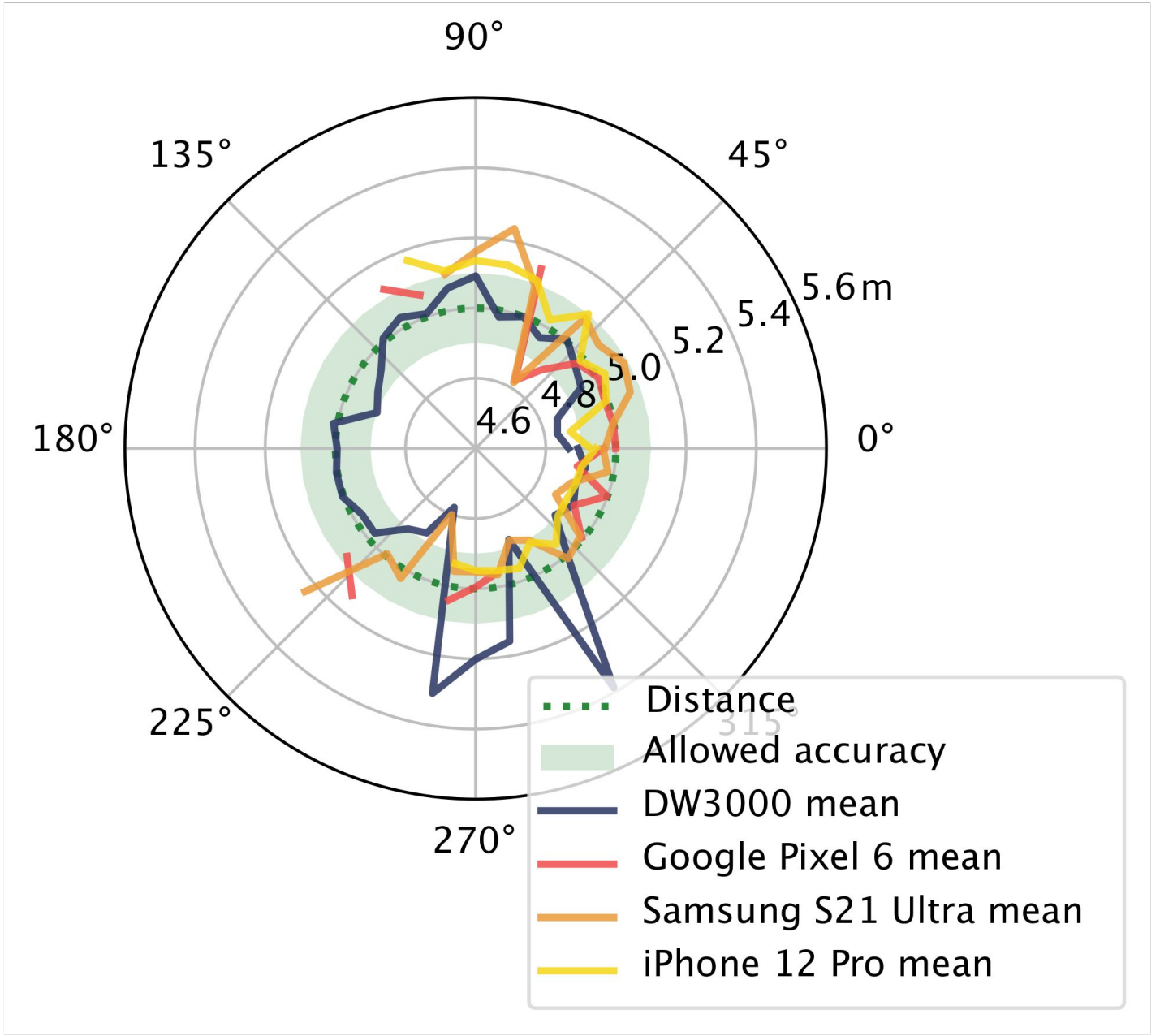
GWEn: Gimbal-based platform for Wireless Evaluation

Measurement Setup

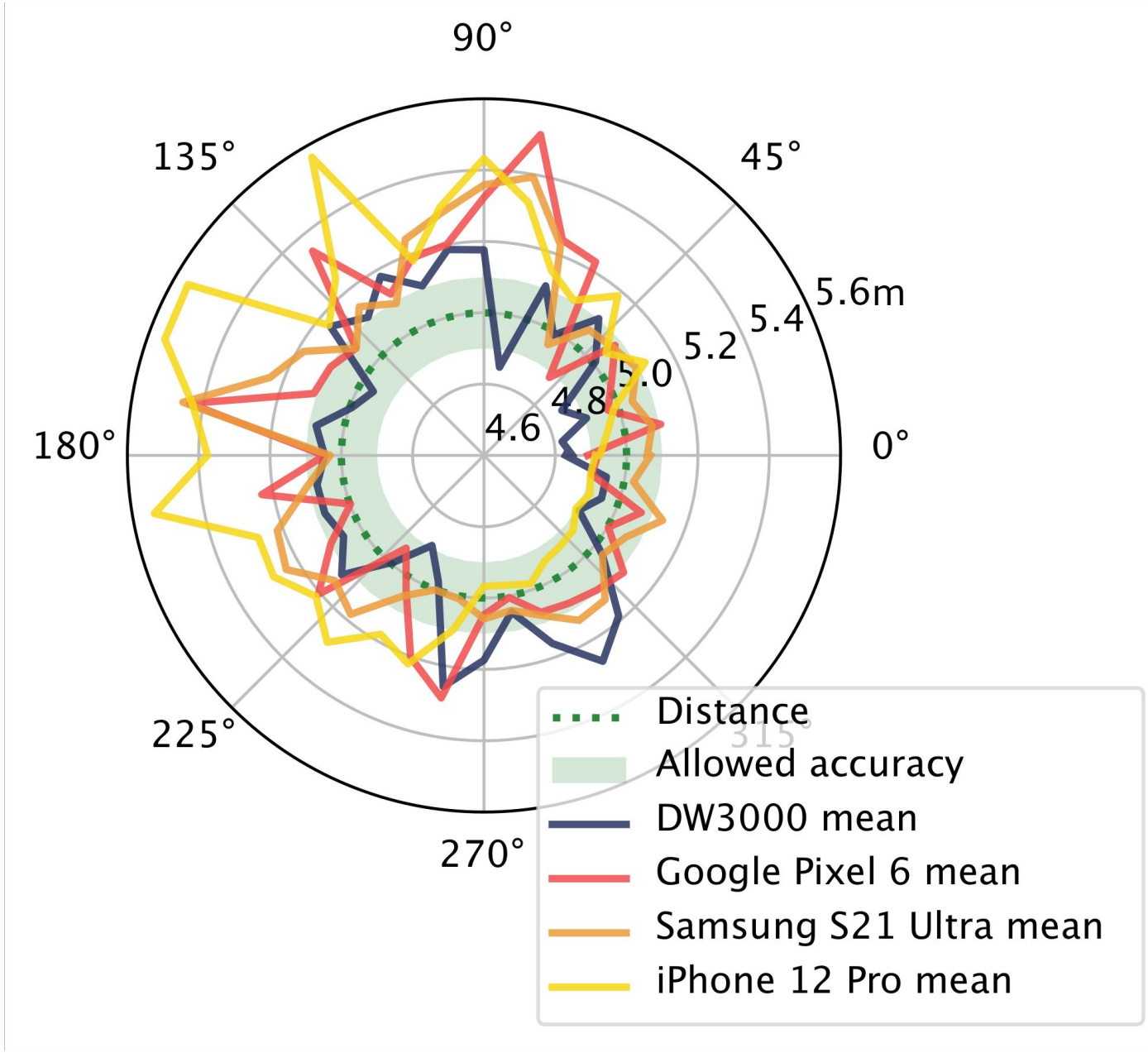




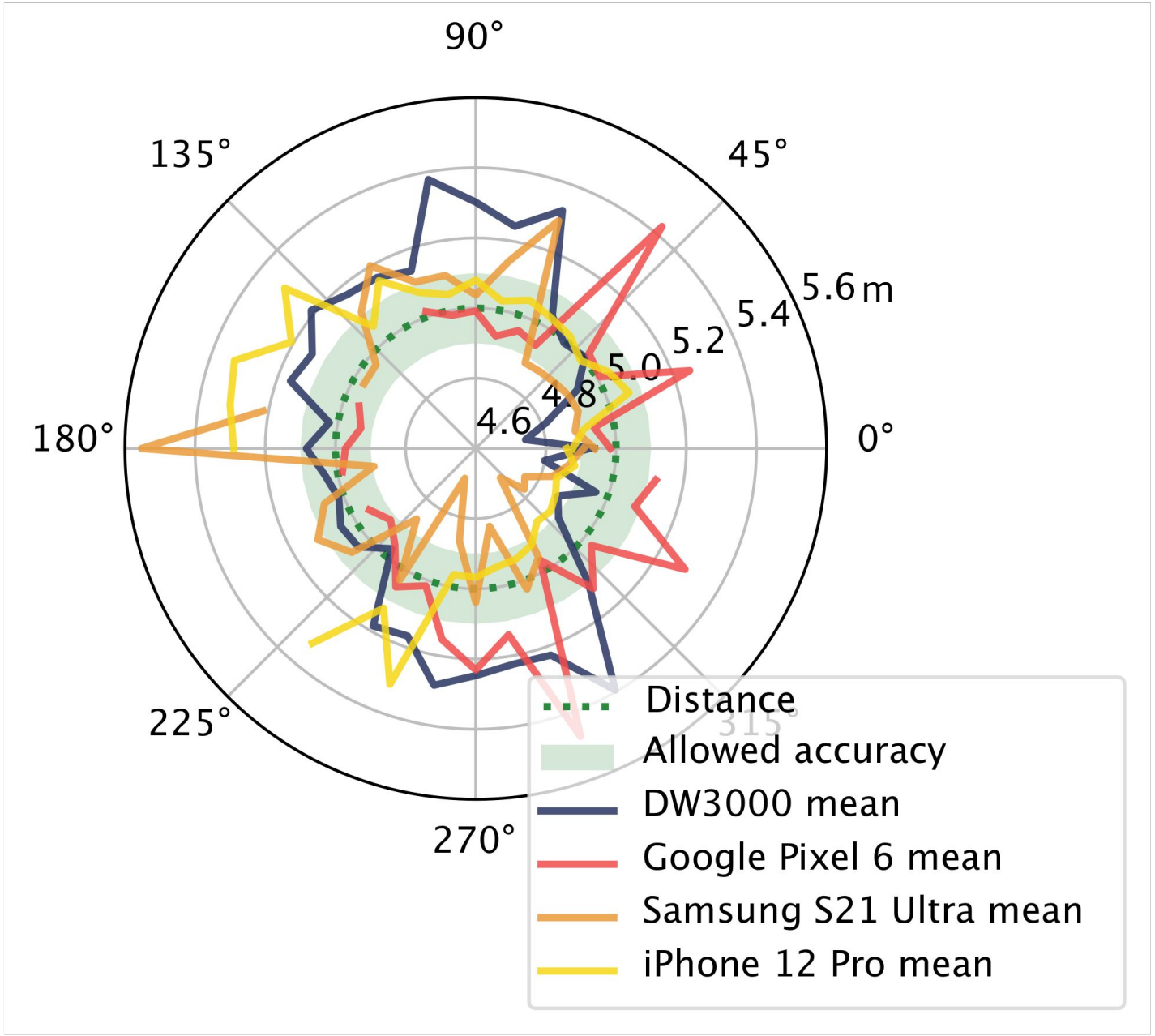
Outside


90°
135°
45°
180°
0°
225°
270°
4.6
4.8
5.0
5.2
5.4
5.6m
Distance
Allowed accuracy
DW3000 mean
Google Pixel 6 mean
Samsung S21 Ultra mean
iPhone 12 Pro mean

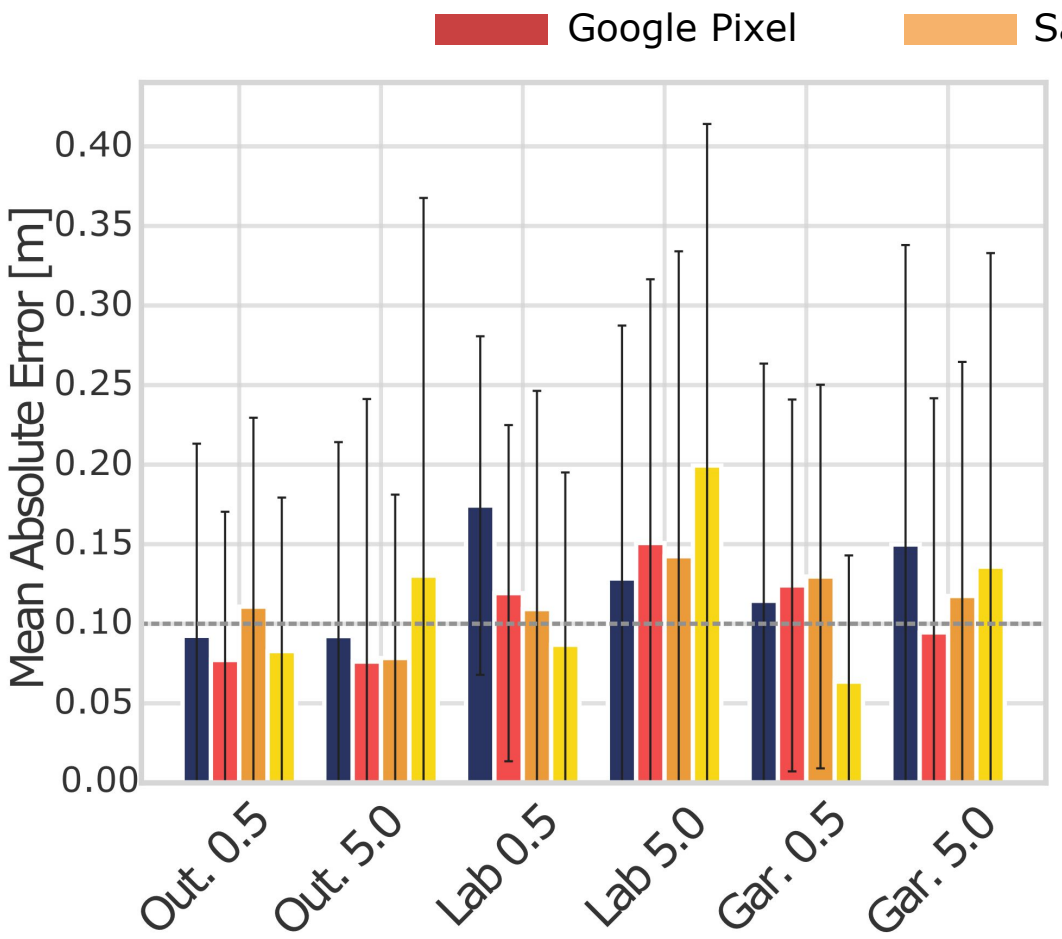
Lab

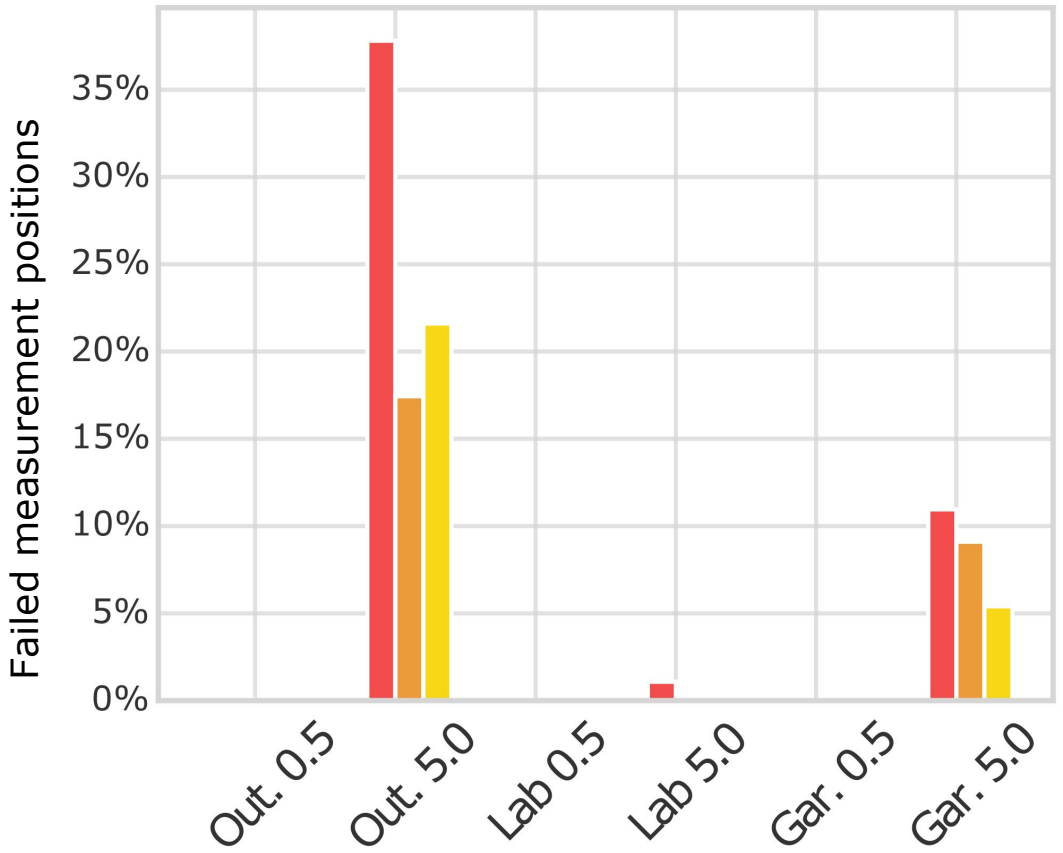

90°
135°
45°
180°
0°
225°
270°
4.6
4.8
5.0
5.2
5.4
5.6m
Distance
Allowed accuracy
DW3000 mean
Google Pixel 6 mean
Samsung S21 Ultra mean
iPhone 12 Pro mean

Garage


90°
135°
45°
180°
0°
225°
270°
315°
4.6
4.8
5.0
5.2
5.4
5.6 m
Distance
Allowed accuracy
DW3000 mean
Google Pixel 6 mean
Samsung S21 Ultra mean
iPhone 12 Pro mean

Results


Google Pixel
Samsung Galaxy
Apple iPhone
Mean Absolute Error [m]
0.00
0.05
0.10
0.15
0.20
0.25
0.30
0.35
0.40
Out. 0.5
Out. 5.0
Lab 0.5
Lab 5.0
Gar. 0.5
Gar. 5.0


Failed measurement positions
0%
5%
10%
15%
20%
25%
30%
35%
Out. 0.5
Out. 5.0
Lab 0.5
Lab 5.0
Gar. 0.5
Gar. 5.0

Attacks against Keyless Entry

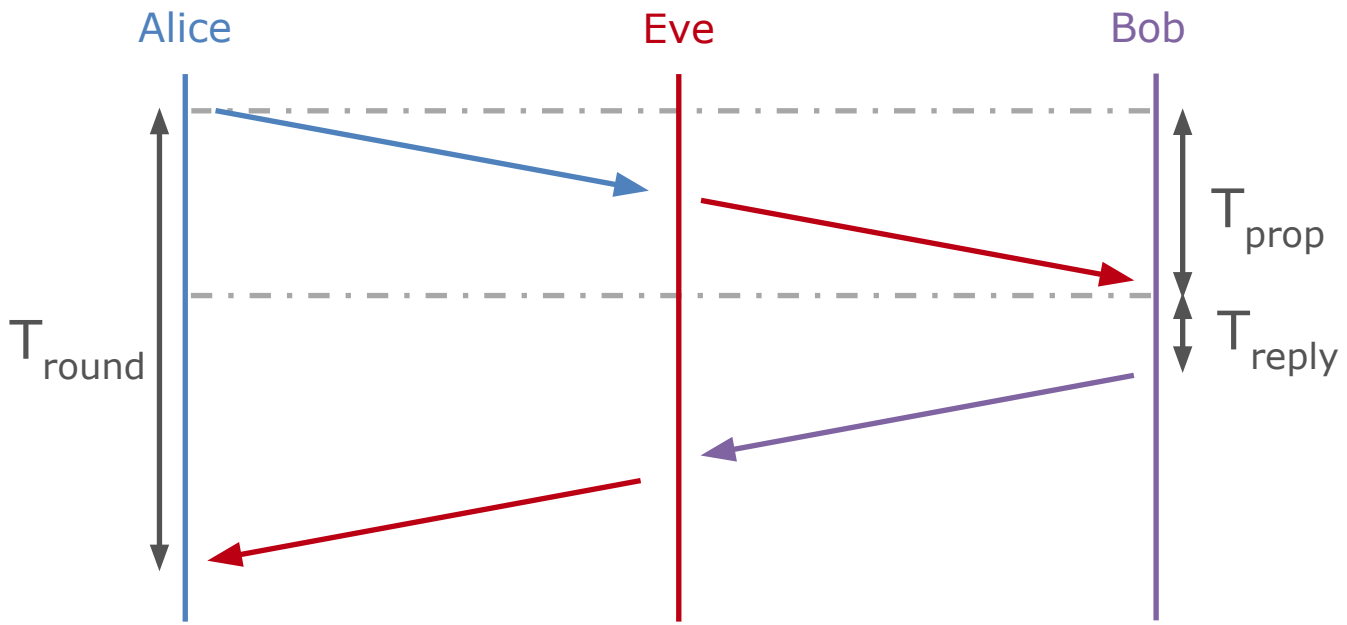

Daily
Mail

Legacy Car Key Relay Attack

Stronger Signal = Lower Distance

While upper time limits can be enforced, the signal's modulation scheme doesn't allow for fully preventing relay attacks.

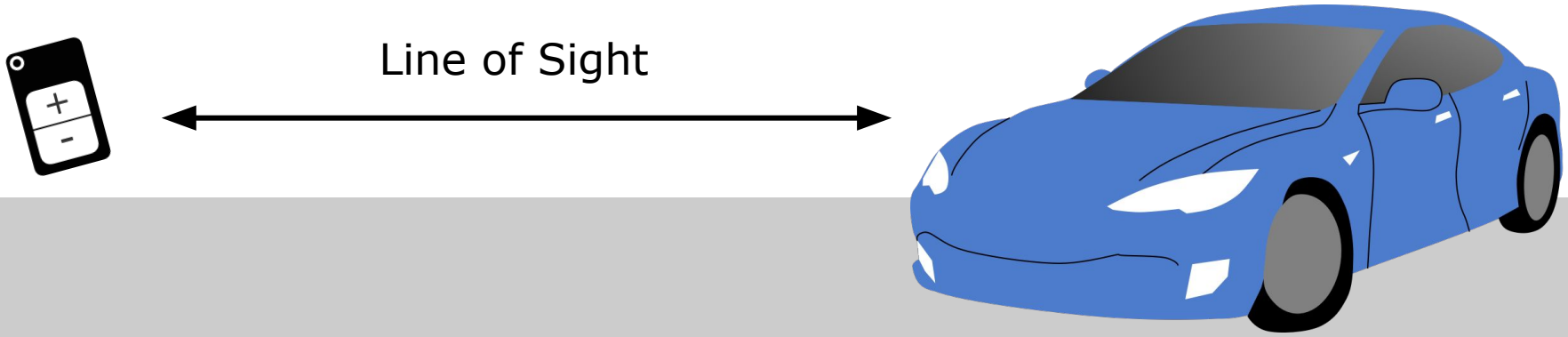
UWB Relay Attack



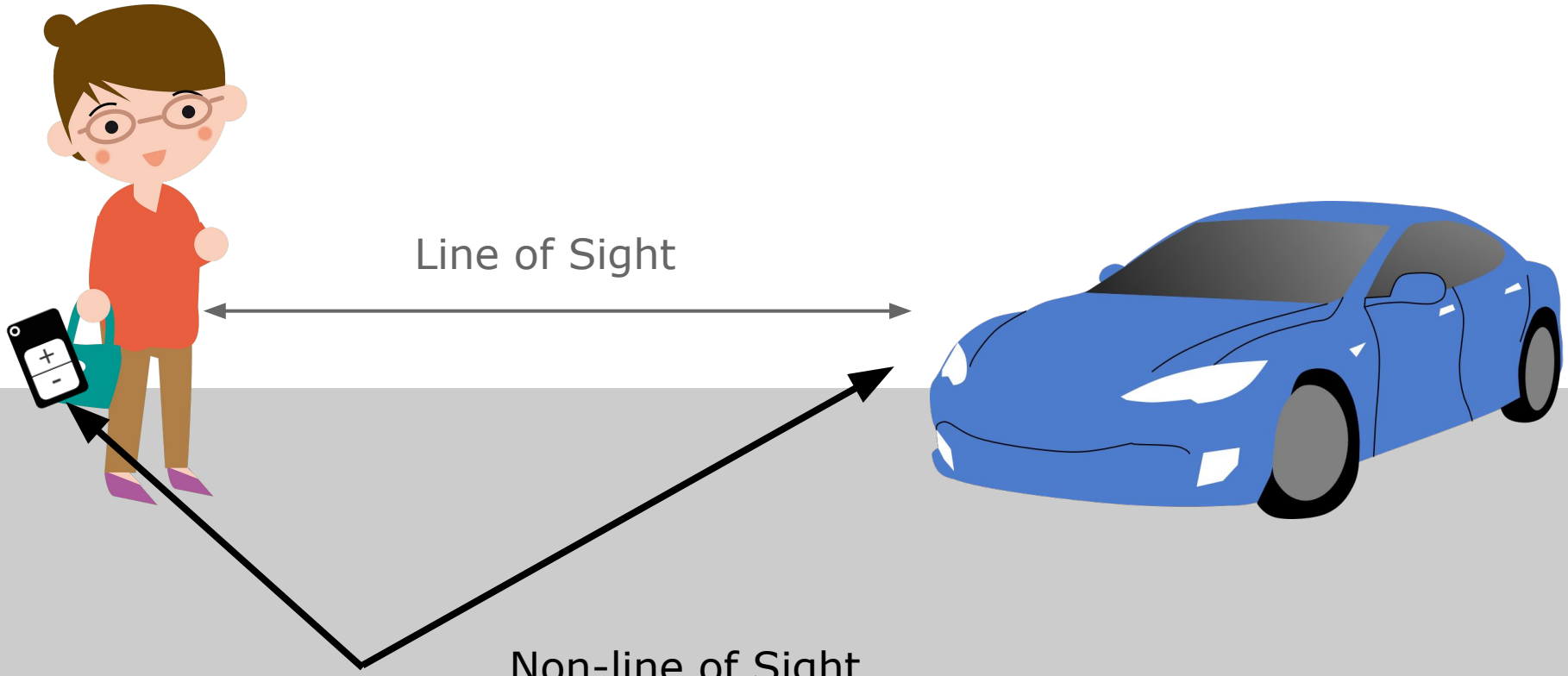
- Eve increases the time of flight (propagation delay).
- The distance will be **enlarged, not shortened** 😟

Attack #1: GhostPeak

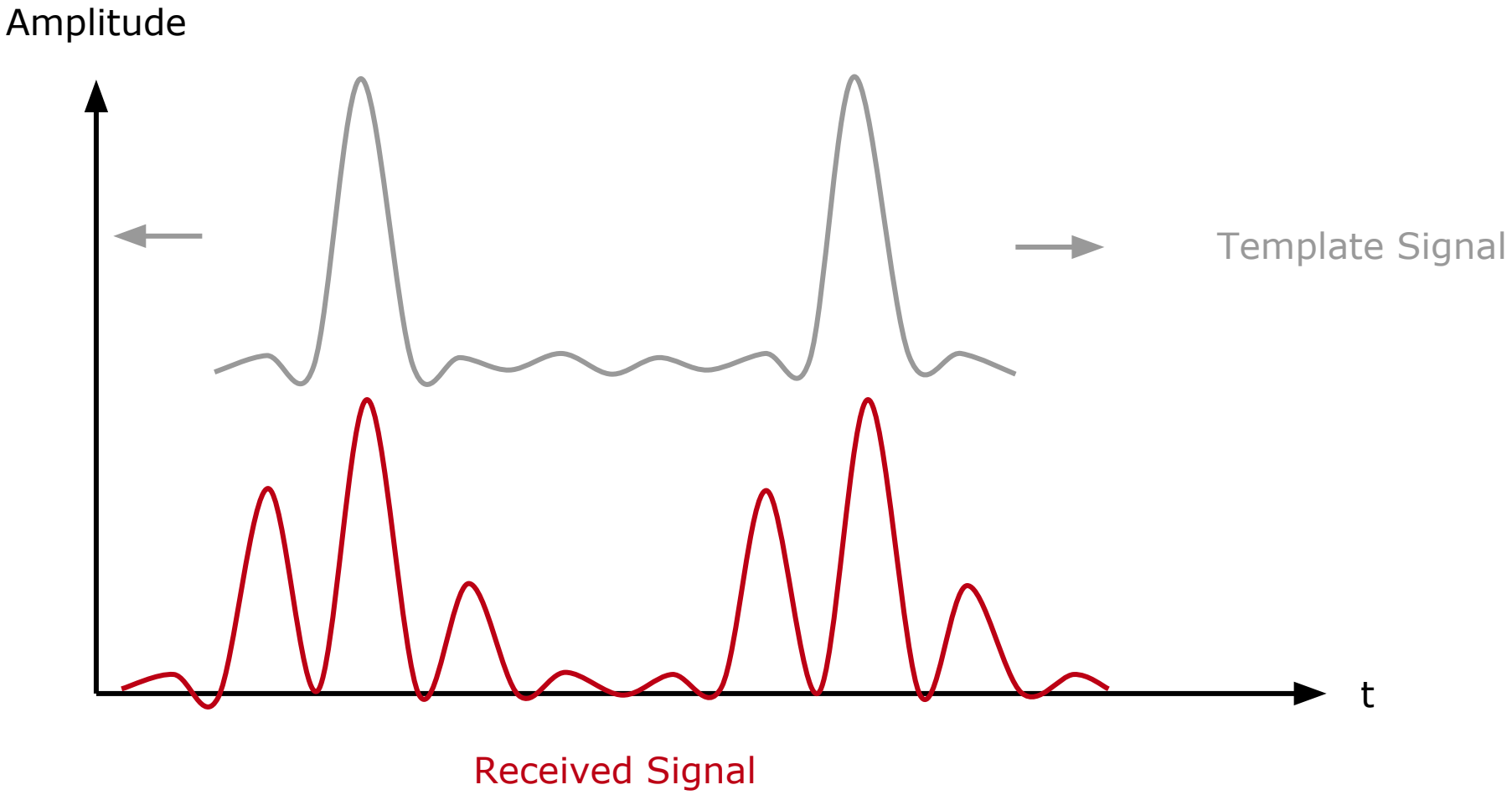
by P.Leu, G. Camurati, A. Heinrich, M. Roeschlin, C. Anliker, M. Hollick, J. Classen from ETH Zurich and TU Darmstadt


Line of Sight

Due to reflections and blocking objects, the non-line of sight path might be stronger than the actual (line of sight) distance!

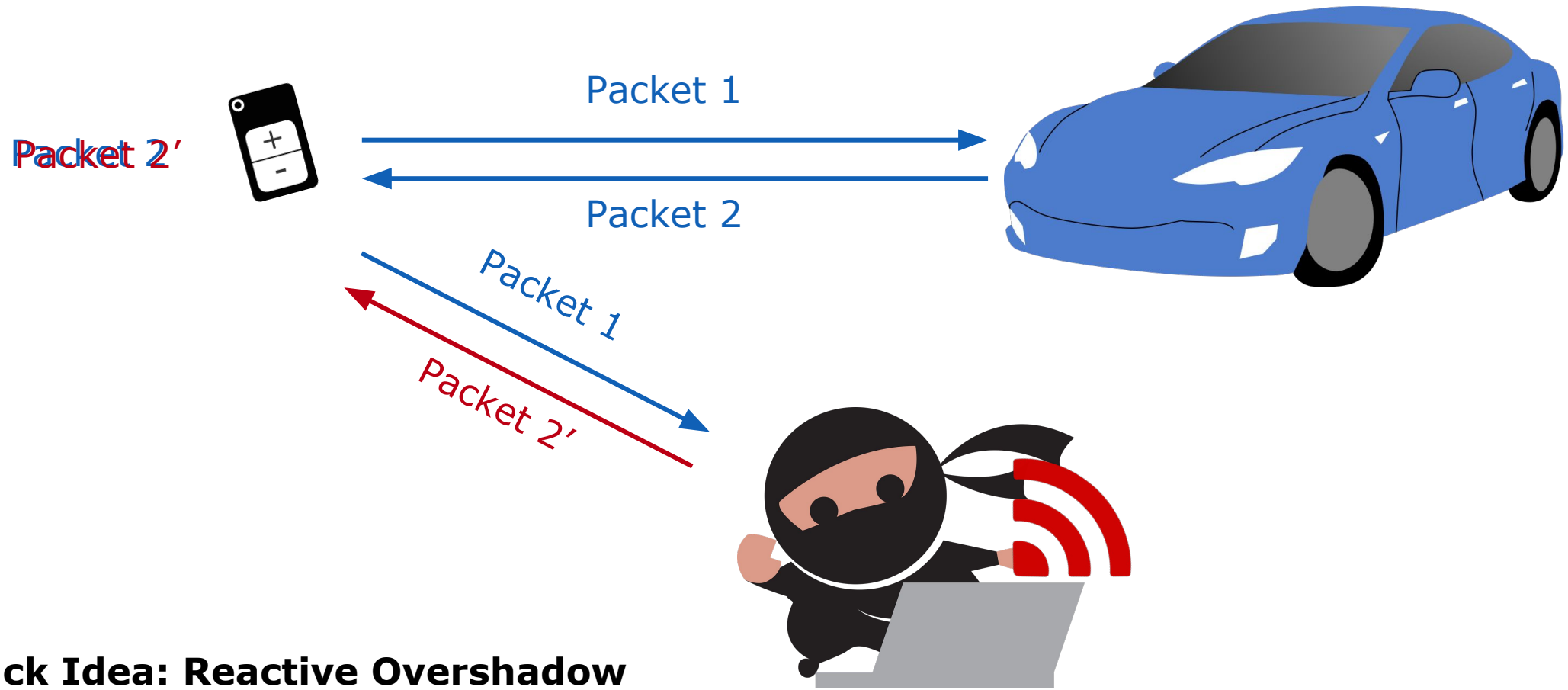


User expectation: Car should still open at 50cm distance, even when the key is in a pocket.

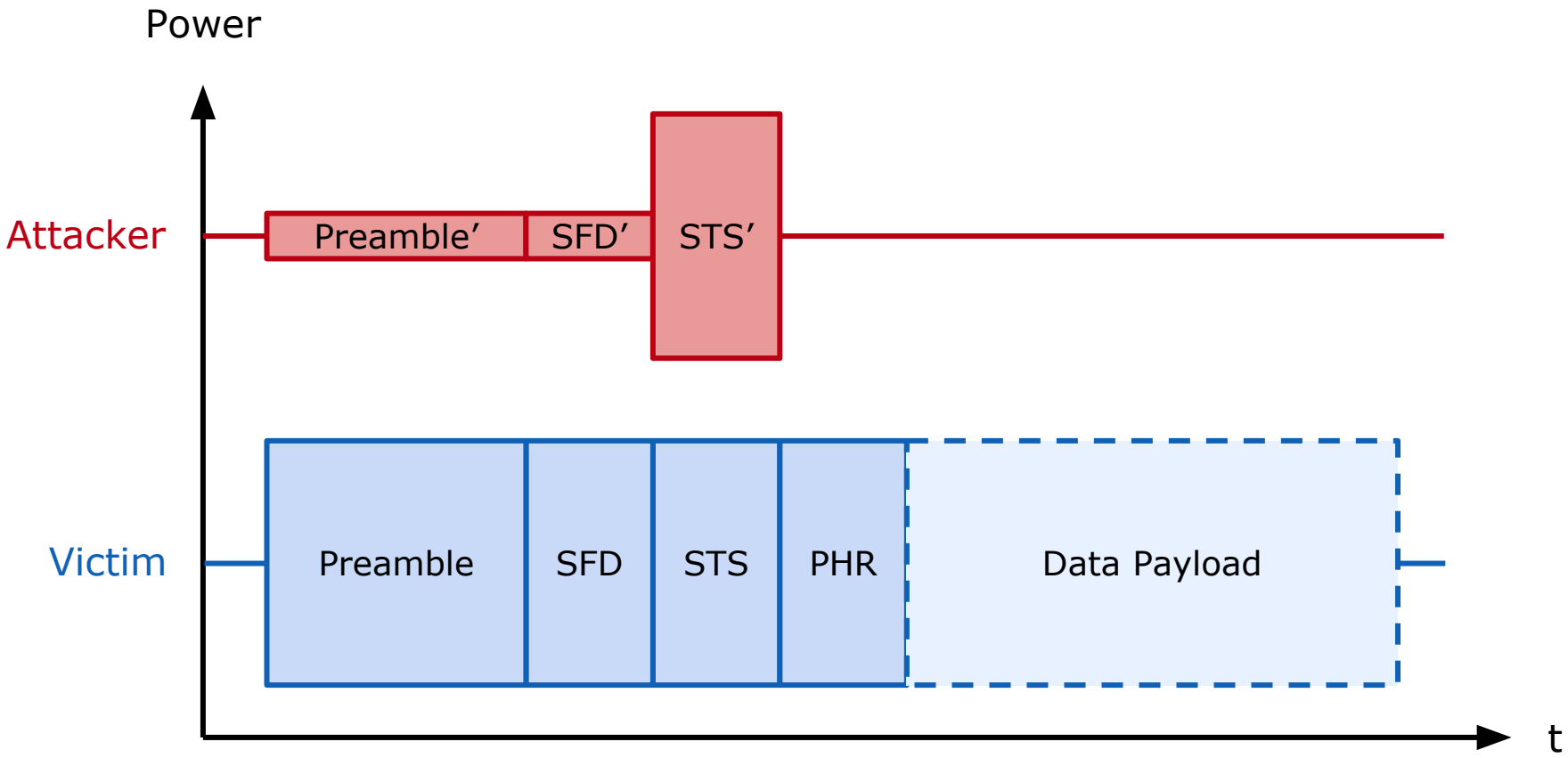


Solution: Find the first (shortest) path by correlating the received signal with a template signal.

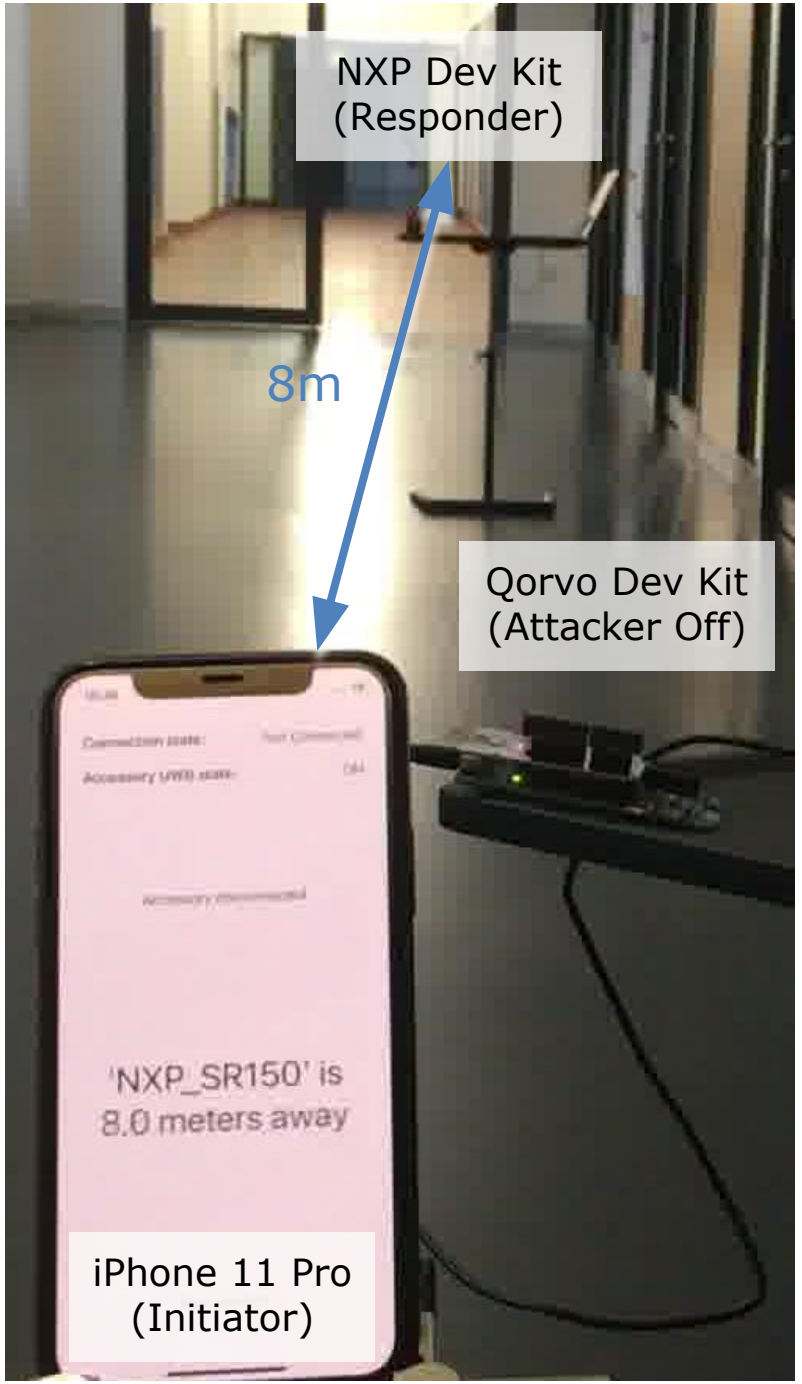
We take a path that has meets a minimum power threshold & is within the search window.



Attack Idea: Reactive Overshadow
Use the first packet as trigger for the attack.
Confuse the correlation algorithm in the following packets with “ghost peaks”.



Implementation with UWB Development Kit
Attack costs reduce to 50€ with a dev kit.
Restriction: We have to send a valid preamble and SFD, but can reduce their power.
Effectively we only overshadow the STS!


NXP Dev Kit
(Responder)
8m
Qorvo Dev Kit
(Attacker Off)
'NXP_SR150' is
8.0 meters away
iPhone 11 Pro
(Initiator)


NXP Dev Kit
(Responder)
0m
Qorvo Dev Kit
(Attacker On)
Connection state:
Not Connected
Accessory UWB state:
ON
Accessory disconnected
'NXP_SR150' is
0.0 meters away
iPhone 11 Pro
(Initiator)

Affected devices

Device Type	Affected	Success rate
Apple U1 chip	✔ (max. 12m)	4%
Samsung Galaxy phones	not reliable	not measurable
Qorvo DW3000 UWB chip	not reliable	not measurable
NXP Trimension chips	not reliable	not measurable

If one of the involved chips is vulnerable, the attack works, e.g., distance reduction U1–NXP is possible.

Countermeasures

- Attack success is random, as not all overlay signals lead to distance reduction.
  - Monitor jumps in distance measurements.
  - Combine 10–15 measurements to mean results.

- Attack exploits back-search window in correlation.
  - Reduce back-search window to <12m

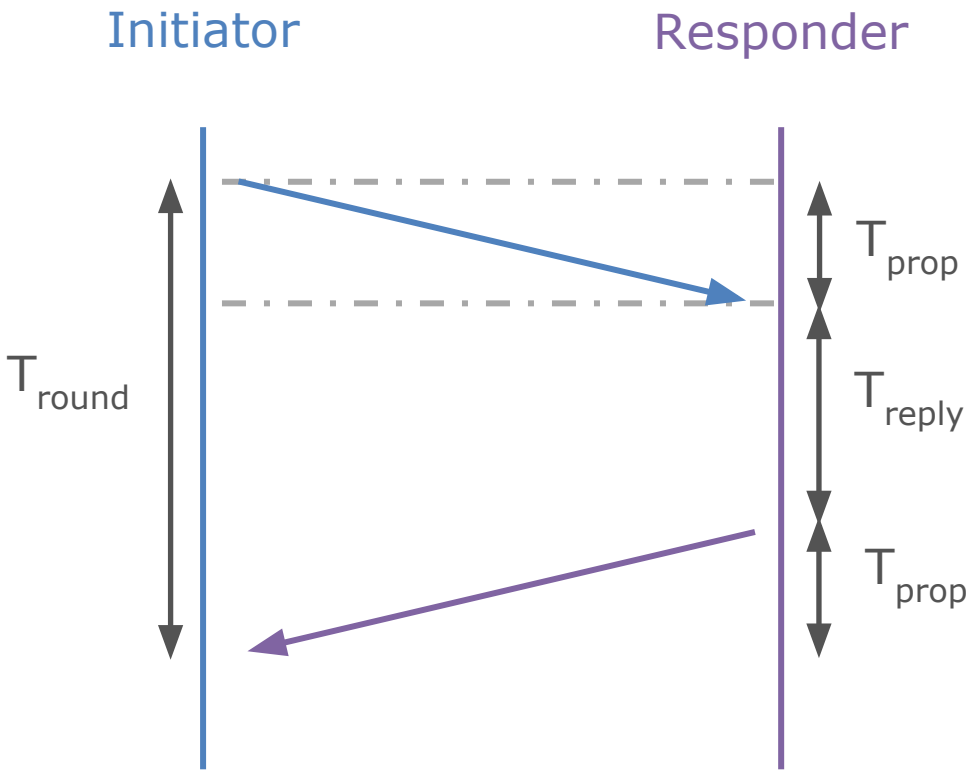
    (but reduces usability in non-line of sight!)

- Overshadowing the STS might corrupt bits.
  - Monitor for bitflips in STS, only allow a low threshold.

Attack #2: Time for Change

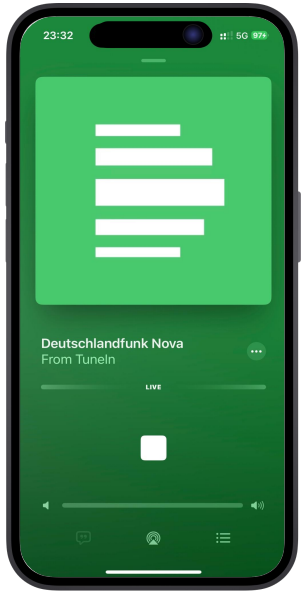
by C. Anliker, G. Camurati, S. Čapkun from ETH Zurich

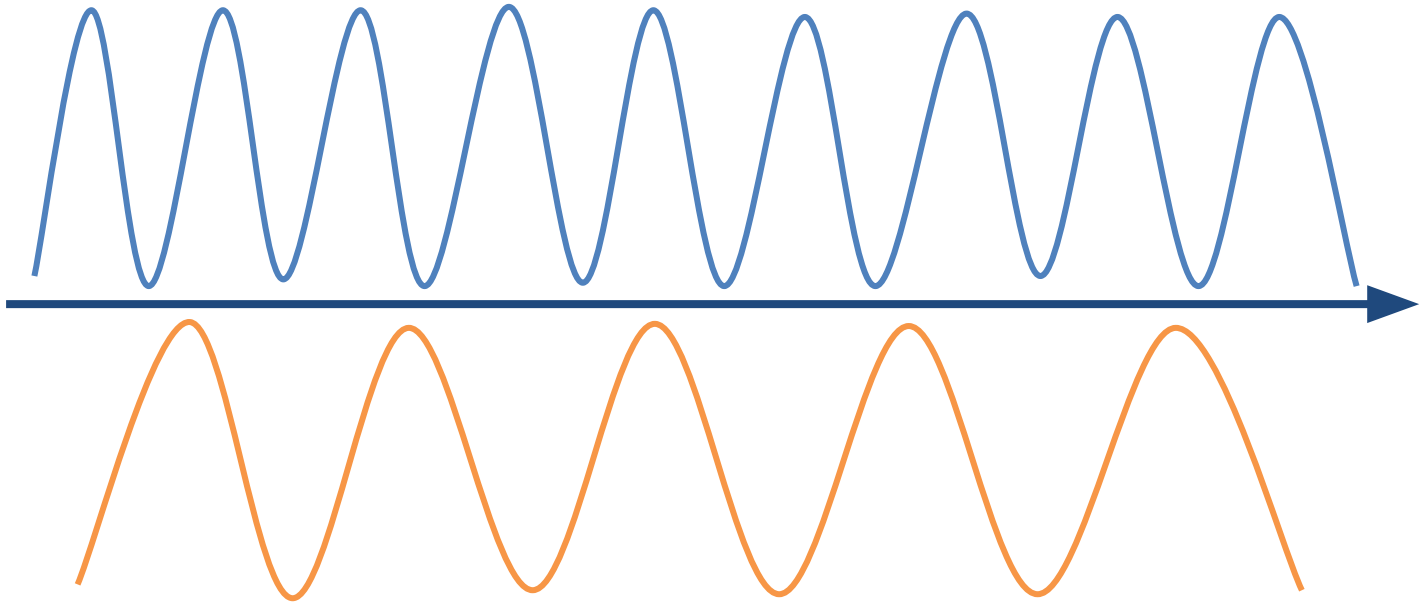
Clock Drifts in Single-Sided ranging

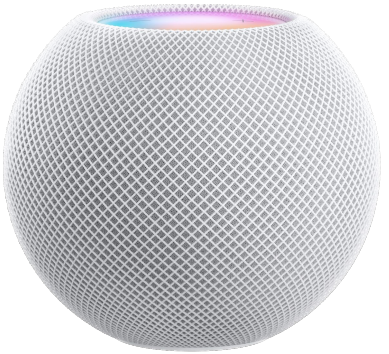


$$T_{ToF} = ½ \bullet (T_{round1} - T_{reply1}(1 - \textbf{clockDrift}))$$

Clock Drift Measurement





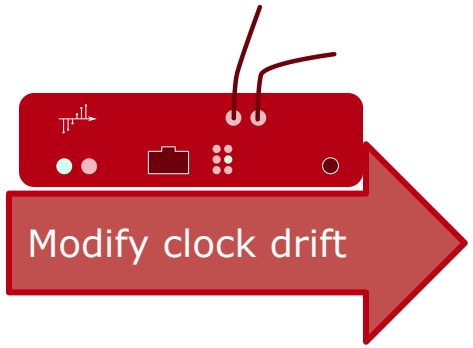


= Clock drift

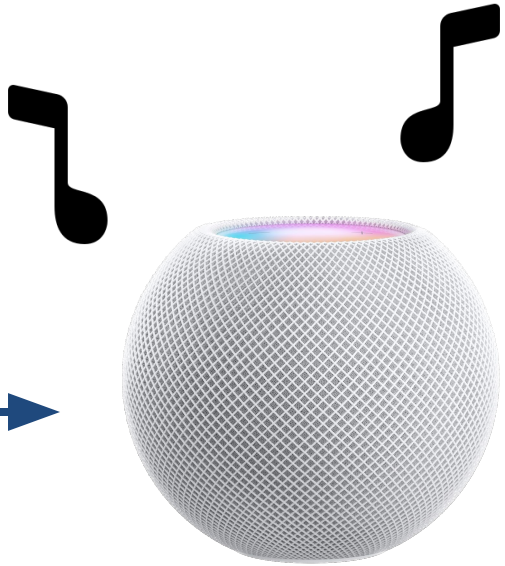
Attack Principle

0

0

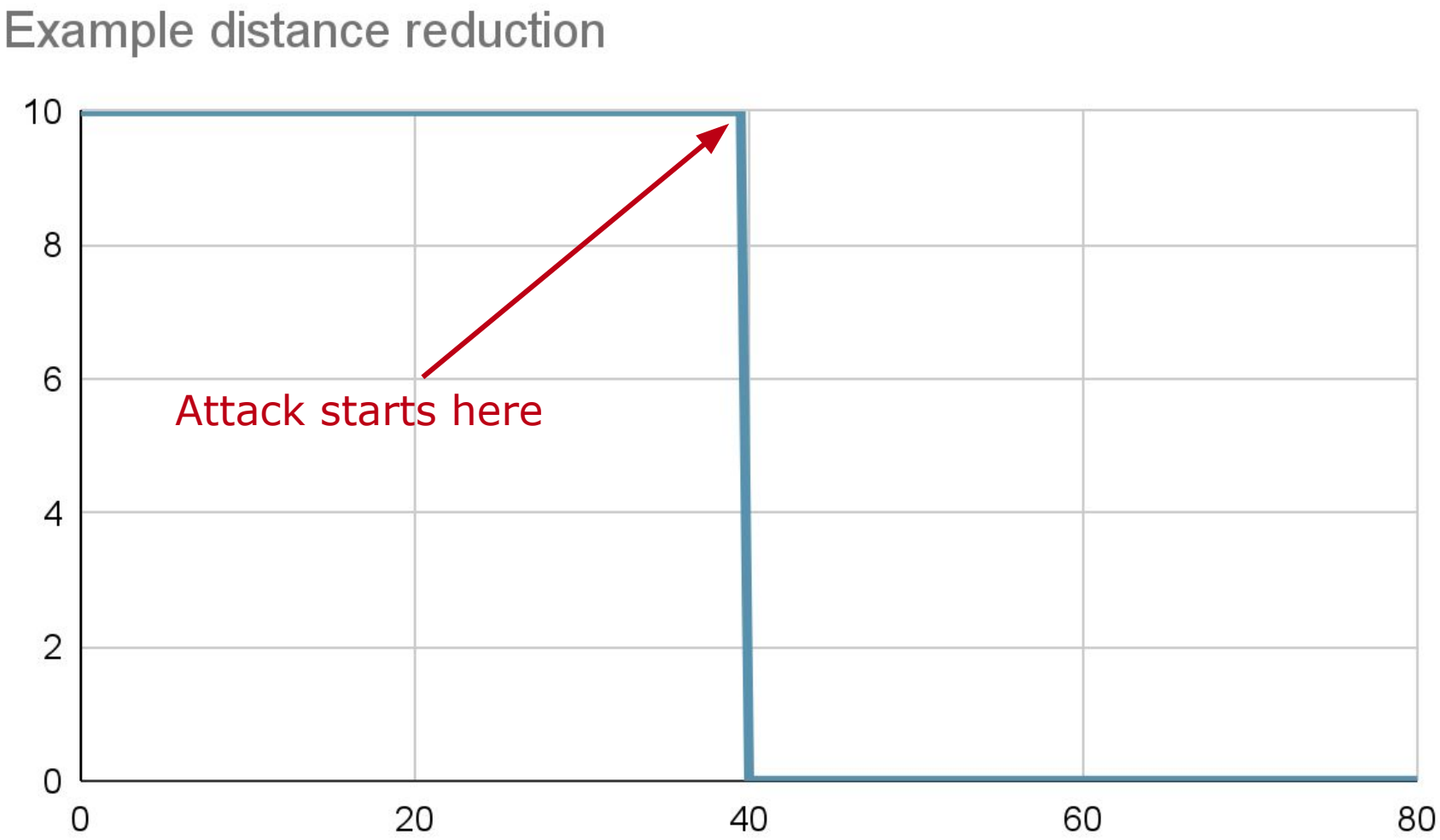


-40



-12m distance reduction

Attack Results



Affected devices

Device Type	Affected	Reason
Apple devices	✗	Use on DS-TWR
Android phones	✗	Use on DS-TWR
Qorvo DW3000 UWB chip	✔	If configured to SS-TWR
NXP Trimension chips	**?**	not tested

Countermeasures

- Attack results controllable and succeed 100%
  - Detect changes in the clock drift
  - Monitor duplicate signals

- No secure way to verify the clock-drift
  - Based on carrier-frequency
  - Reducing tolerances can help

Conclusion

- Physical layer attacks are hard to prevent
  - Demodulation is complex
  - The real-world can never be simulated

- Enhancing the standards
  - Proper sample implementations can prevent certain attacks
  - Good limits

- Many things to explore
  - Different manufacturers
  - OS-level integration

Attack the secure ranging session keys.

Create a universal attack that works on the signal level.

Q&A

https://github.com/seemoo-lab

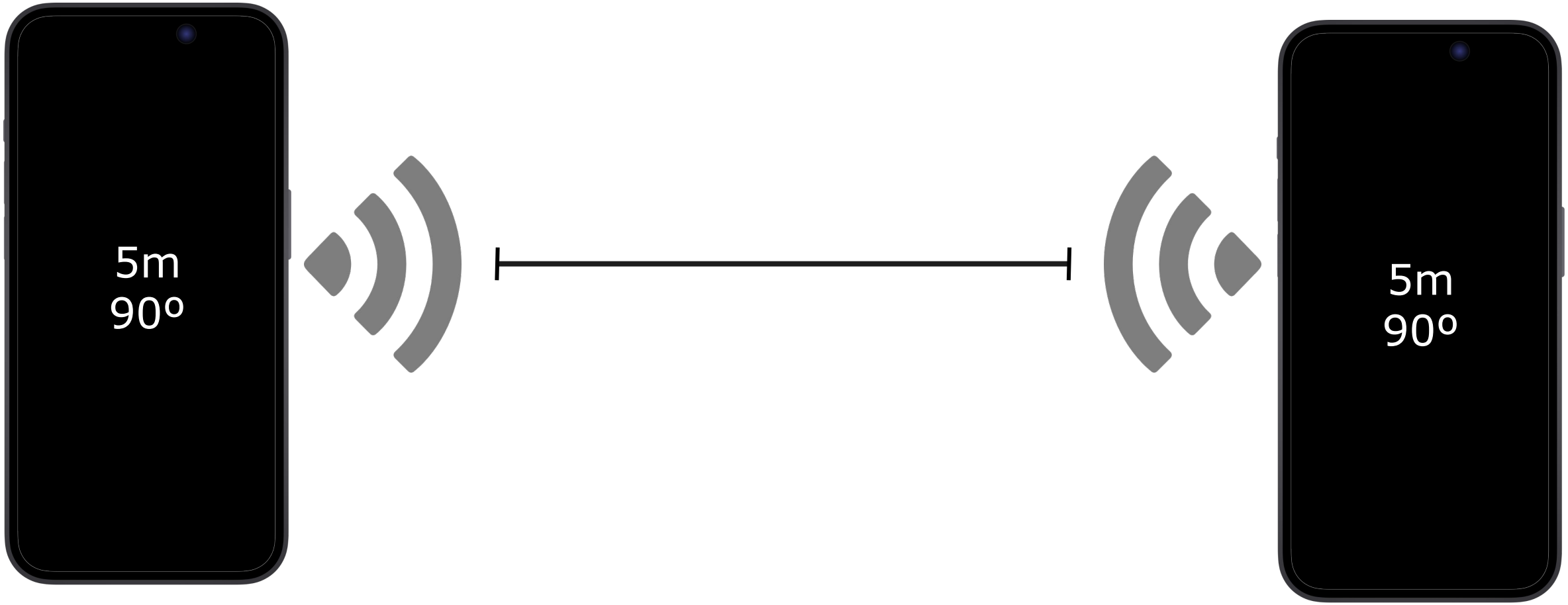
Twitter: @naehrdine, @Sn0wfreeze

[jclassen|aheinrich]@seemoo.de

AirDrop

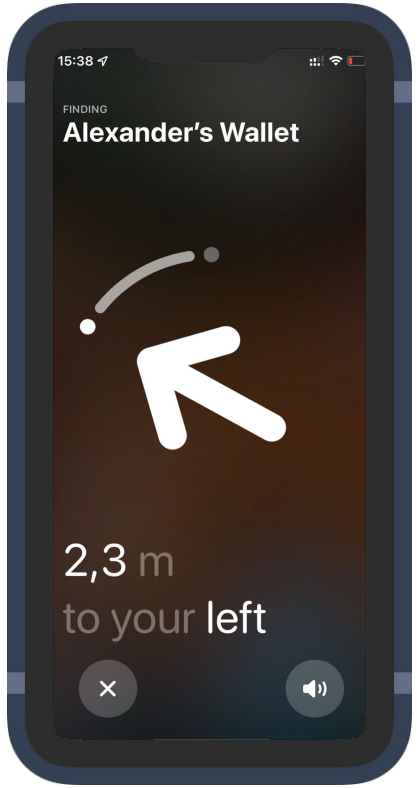

14:14
AirDrop
Done
A
Alexander
Tap to Share
People
A
Alexander
11:41
Etterbeek
21°
Mostly Cloudy
H:24° L:13°
Weather
TUESDAY
27
No events today
Calendar
AirDrop
Alex would like to share a photo.
Decline
Accept
Health
Wallet
Settings
Search

Nearby Interaction

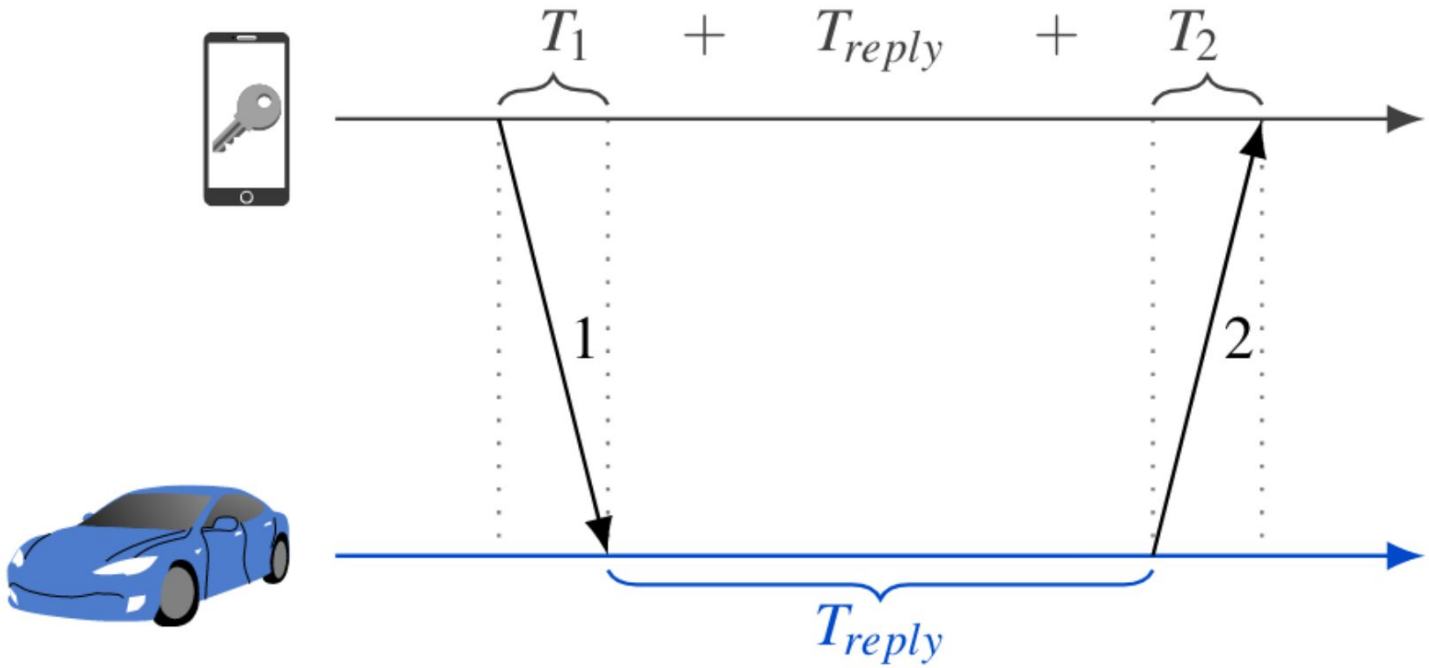


Find My


AirTag
Assembled in China
Designed by Apple in California


15:38
FINDING
Alexander's Wallet
2,3 m
to your left

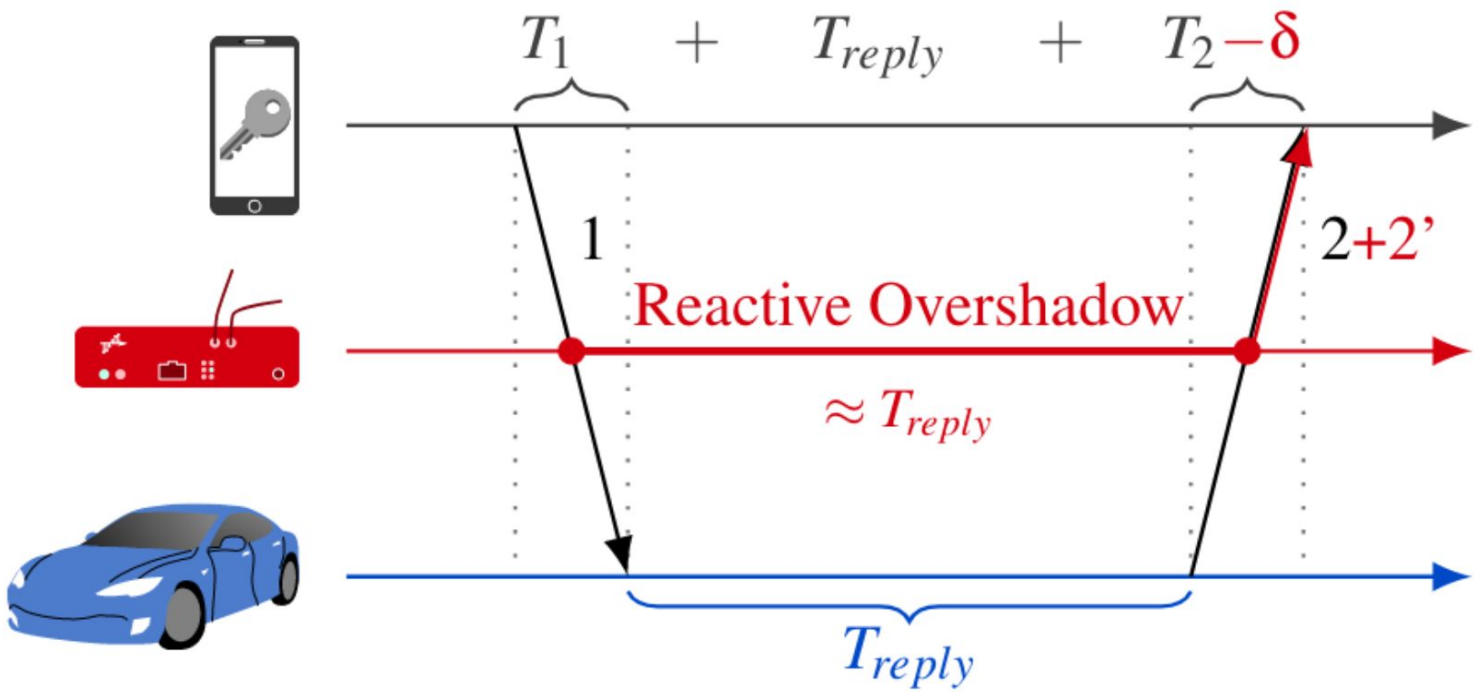
Normal Digital Key behavior



$d = 10\,\text{m}$

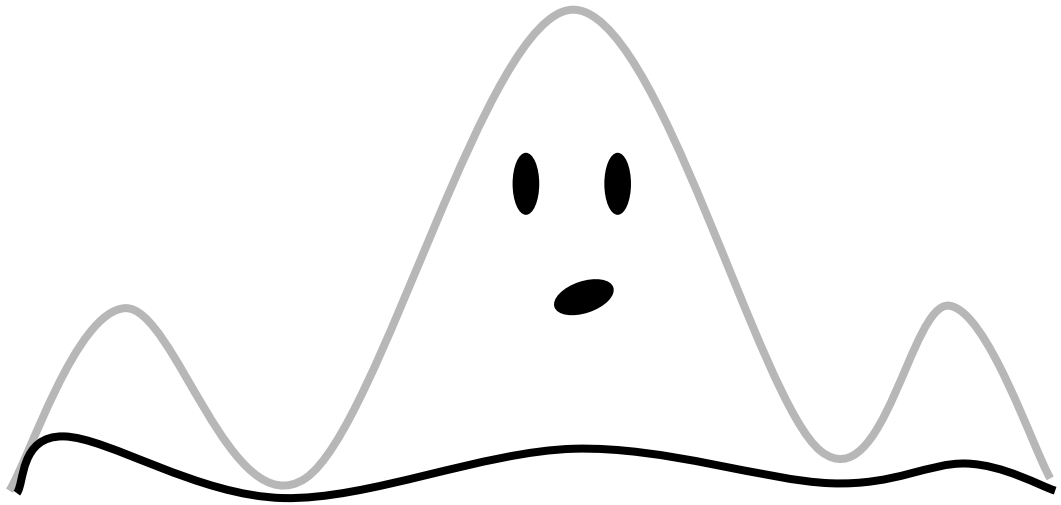
Car does not unlock.

Reactive overshadow

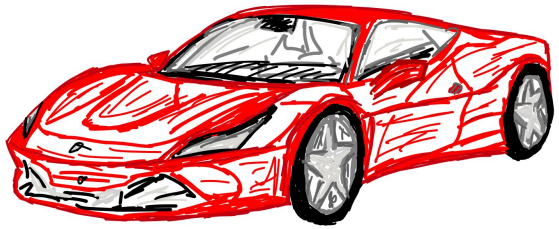


$d = 1$ m

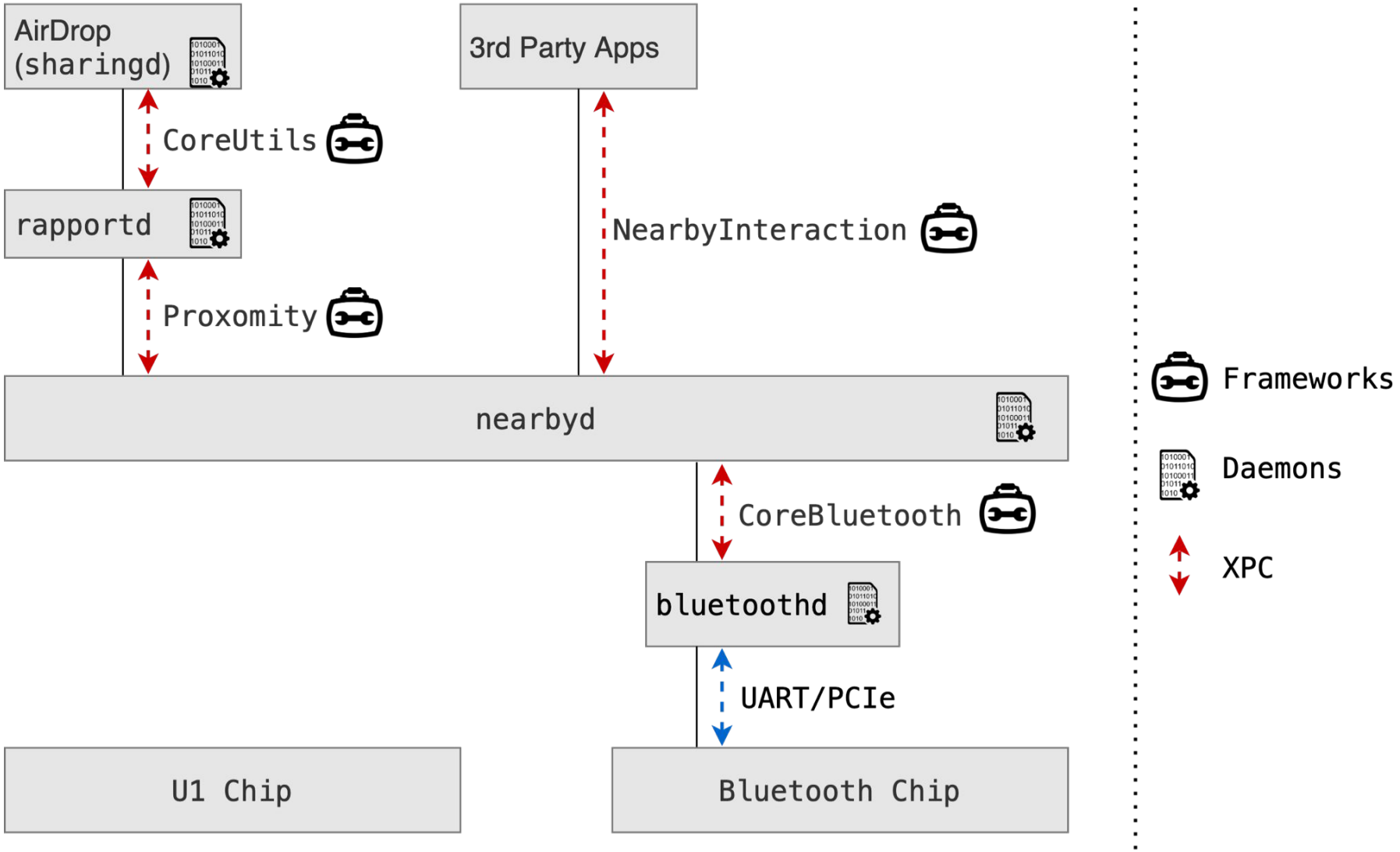
Car unlocks.



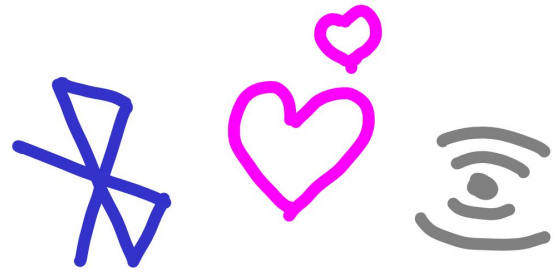
UWB to X



UWB System Architecture



Lessons Learned



- Bluetooth and Ultra Wideband are tightly coupled on iOS.
- Apple’s own RTKit-based wireless chips have an interesting architecture with many security features like secure boot and ASLR.
- Many features in the chip can be instrumented from user space.

Content

Introduction to UWB

- Applications
  - Now the Car Key is included
- UWB Internals on iOS
  - UWB Frameworks and System Components
  - Which iOS Version supports what (-> Jiska double-checks)
- UWB internals on Android
  - What processes and Frameworks are involved ? -> Alex checks
  - Which protocols supports what? -> Samsung, Nearby Share, Android UWB
- Accuracy and reliability of Smartphones
  - Introduction to GWEn
  - Our measurement setup
  - Results
- Attacks against UWB
  - What does not work
    - Relay and Amplification attacks
  - GhostPeak
  - Time for Change

Attacking the packet timestamps