Bluetooth Security

NECS winter school, Jan 2024, Cortina

Daniele Antonioli (EURECOM)

Ciao! I am Daniele Antonioli

EURECOM
Sophia Antipolis

- Prof at EURECOM (S3)
  - French riviera, 🏖️, 🏔️
- Research in **applied system security and privacy**
  - Wireless (Bluetooth and Wi-Fi)
  - Embedded (cars, e-scooters, and fitness trackers)
  - Mobile (smartphones, Android)
  - Cyber-physical systems (MiniCPS, ICS)
- More at https://francozappa.github.io/
  - Search talk material on publications

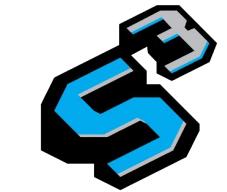
ORSHIN EU Grant (I am the technical lead)

ORSHIN: Open-source ReSilient Hardware and software for Internet of thiNgs

How to design embedded and connected devices taking advantage of open source hardware (and software)

ORSHIN

EURECOM S3 Group [site]



- Four faculties:
  - D. Balzarotti, A. Francillon, D. Antonioli, S. Aonzo
- Research topics (publications)
  - Malware, Binary, Vulnerability, Fuzzing, Web, Embedded, Wireless, Forensics, Protocols, …
- Hiring
  - Postdoc, PhD, RA, …
  - Interested? Reach out to me, or send me an email

Talk Outline

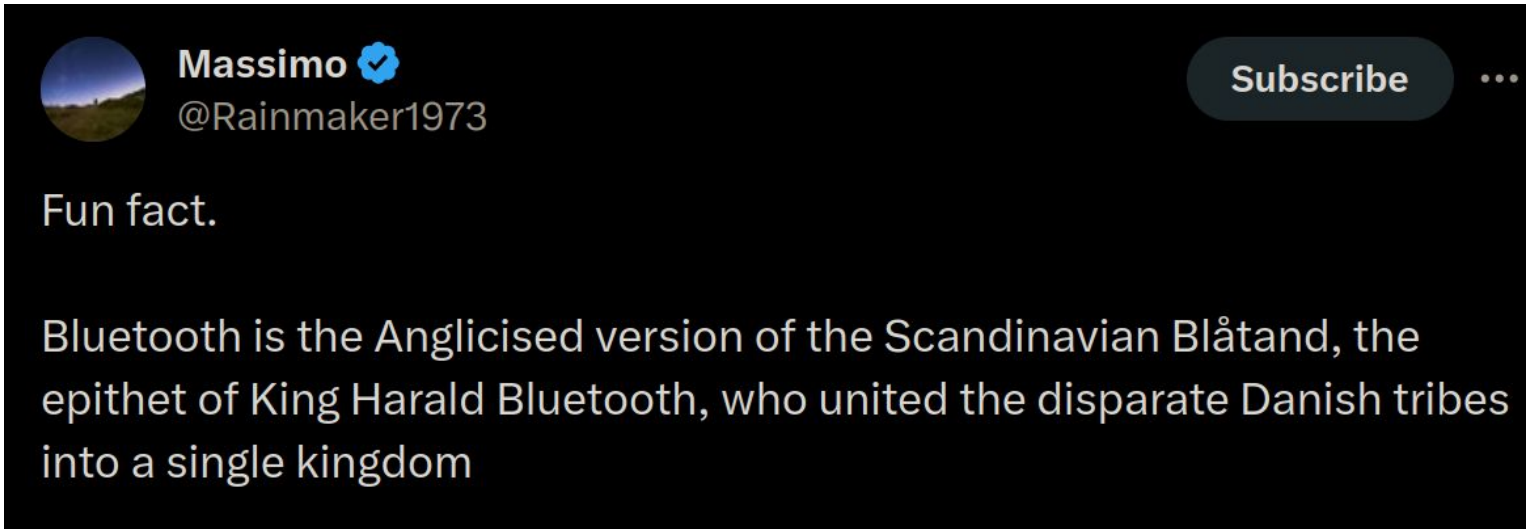
- **Introduction about Bluetooth Security**
- **Bluetooth standard protocols issues**
  - BLUR attacks [AsiaCCS'22]
  - BIAS and KNOB attacks on automotive [WOOT'22, ASRG'22,AutoISAC'22, Oakland'20, TOPS'20, SEC'19]
  - BLUFFS attacks [CCS'23, 37C3]
- **Proprietary protocols issues (still over Bluetooth)**
  - E-Spoofer attacks on Xiaomi e-scooters [WiSec'23]
  - BreakMi attacks on Xiaomi and Fitbit trackers [CHES'22,Hardwear.io'23]

Introduction about Bluetooth Security

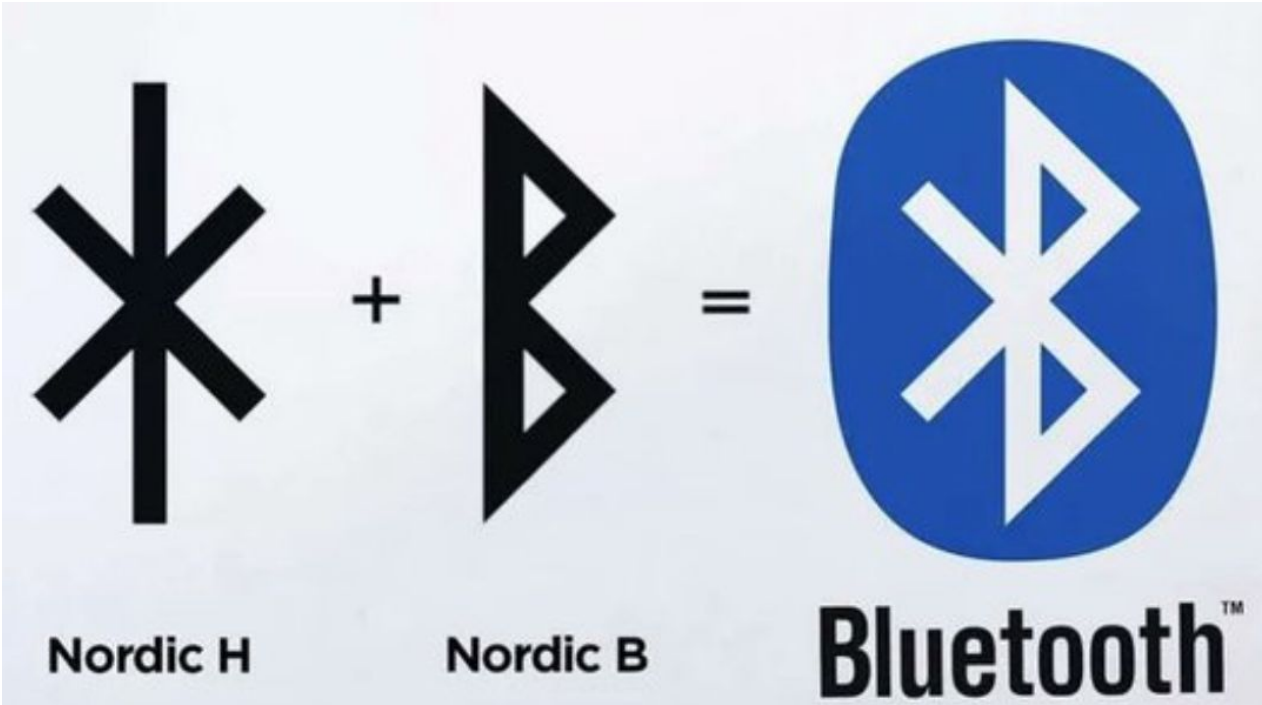
Bluetooth (BT)

- BT is a pervasive low-power wireless technology
  - Specified in bluetooth-core.pdf (v5.4)
  - BC: Bluetooth Classic (high throughput)
  - BLE: Bluetooth Low Energy (very low power)
  - Interoperable aka used by billions of heterogeneous devices, e.g., smartphones, laptops, cars, wearables, sensors, medical, …

BT Name (ref)


Massimo
@Rainmaker1973
Subscribe
Fun fact.
Bluetooth is the Anglicised version of the Scandinavian Blåtand, the epithet of King Harald Bluetooth, who united the disparate Danish tribes into a single kingdom

BT Logo (ref)



BT Specification (ref)

- BT specification
  - Defines technologies to create *interoperable* BT devices
  - Transports: BC, BLE, …
  - Components: Host, Controller, HCI, …
  - Security: Pairing, Session establishment, …
- One BT spec vulnerability → Billions of exploitable devices
  - 2021: BLUR cross-transport overwrites on BC and BLE
  - 2020: BIAS authentication bypasses on BC
  - 2019: KNOB key downgrades on BC and BLE

BT Security

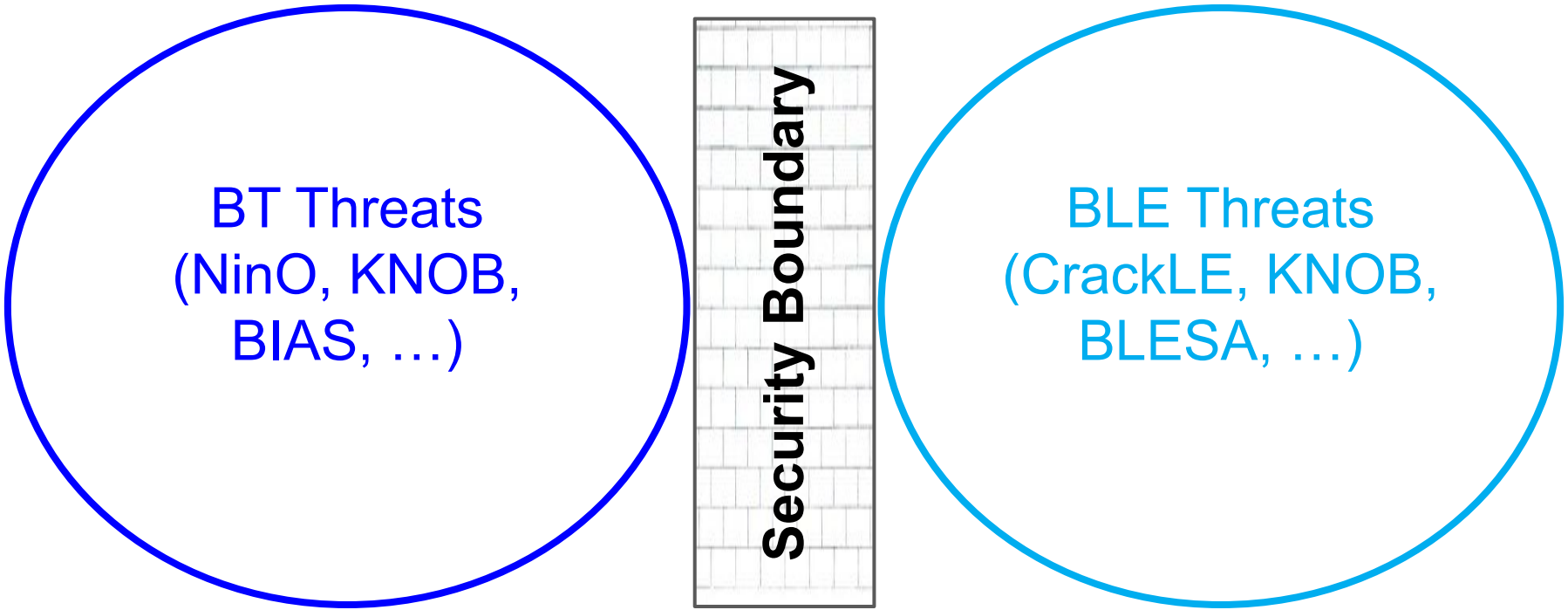
- Pairing
  - *Pairing key (PK)*, long term, BLE entropy negotiation
  - Optionally authenticated (numeric PIN, …)
- Session Establishment
  - *Session key (SK)*, fresh, BC entropy negotiation
  - `SK = kdf(PK, pars)`
- Negotiable security mode
  - Secure Connections (SC)
  - Legacy Secure Connections (LSC)

Talk Threat model

- BC and BLE **should** provide
  - Confidentiality, integrity, authenticity
  - Via pairing and session establishment
- Alice (Central) and Bob (Peripheral)
  - Share PK
  - Use SC or LSC
- Charlie (attacker)
  - Model: proximity-based, cannot compromise PK or all SKs
  - Goals: break pairing and session establishment
  - Impact: impersonate and MitM devices

BLUR Attacks [AsiaCCS'22]

BT and BLE Security Are Considered Separately



We Blur the Security Boundary abusing CTKD

BT Threats
(NinO, KNOB,
BIAS, …)

BLE Threats
(CrackLE, KNOB,
BLESA, …)

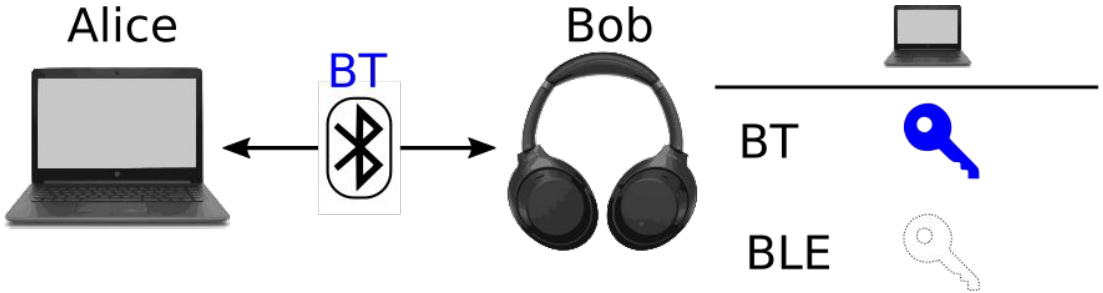
We perform Cross-Transport Attacks on BT and BLE

BT Threats
(NinO, KNOB
BIAS, …)

NEW: BT-BLE
Cross-Transport
Threats (BLUR)

E Threats
LE, KNOB,
ESA, …)

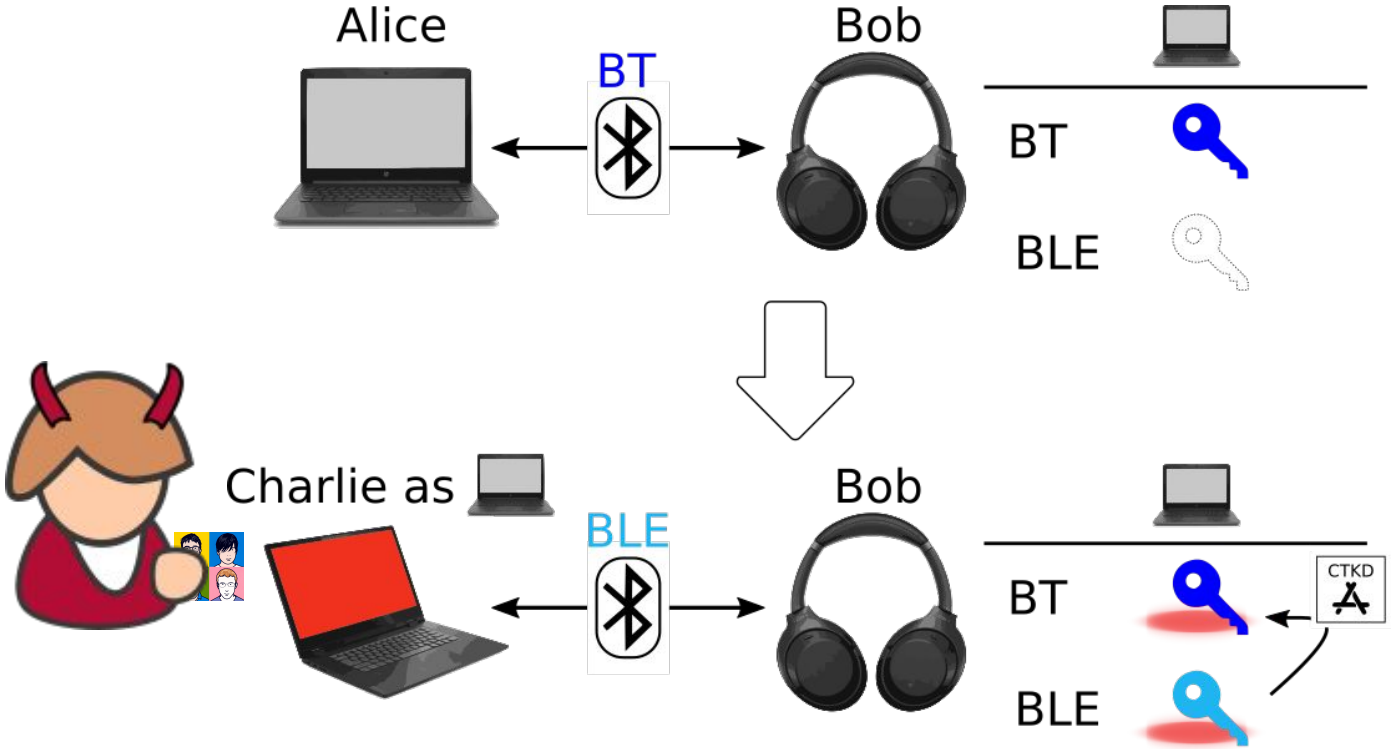
BLUR Attacks: Cross-Transport Central Impersonation



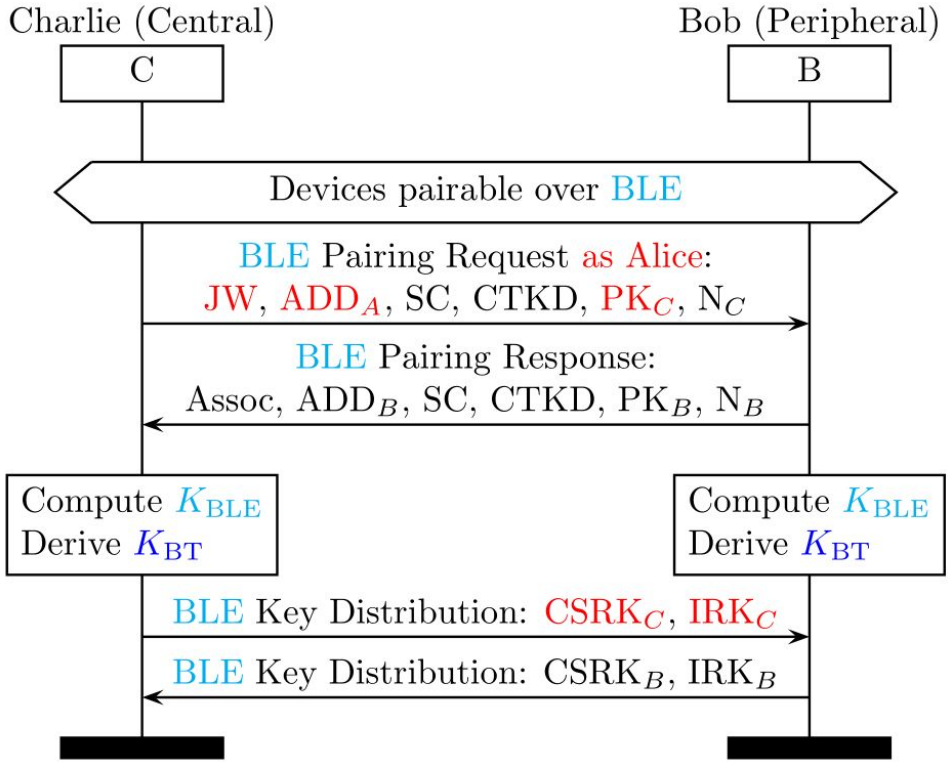
What happens if Charlie tries to pair over BLE with Bob while impersonating Alice?

NEW: Cross-transport Central Impersonation

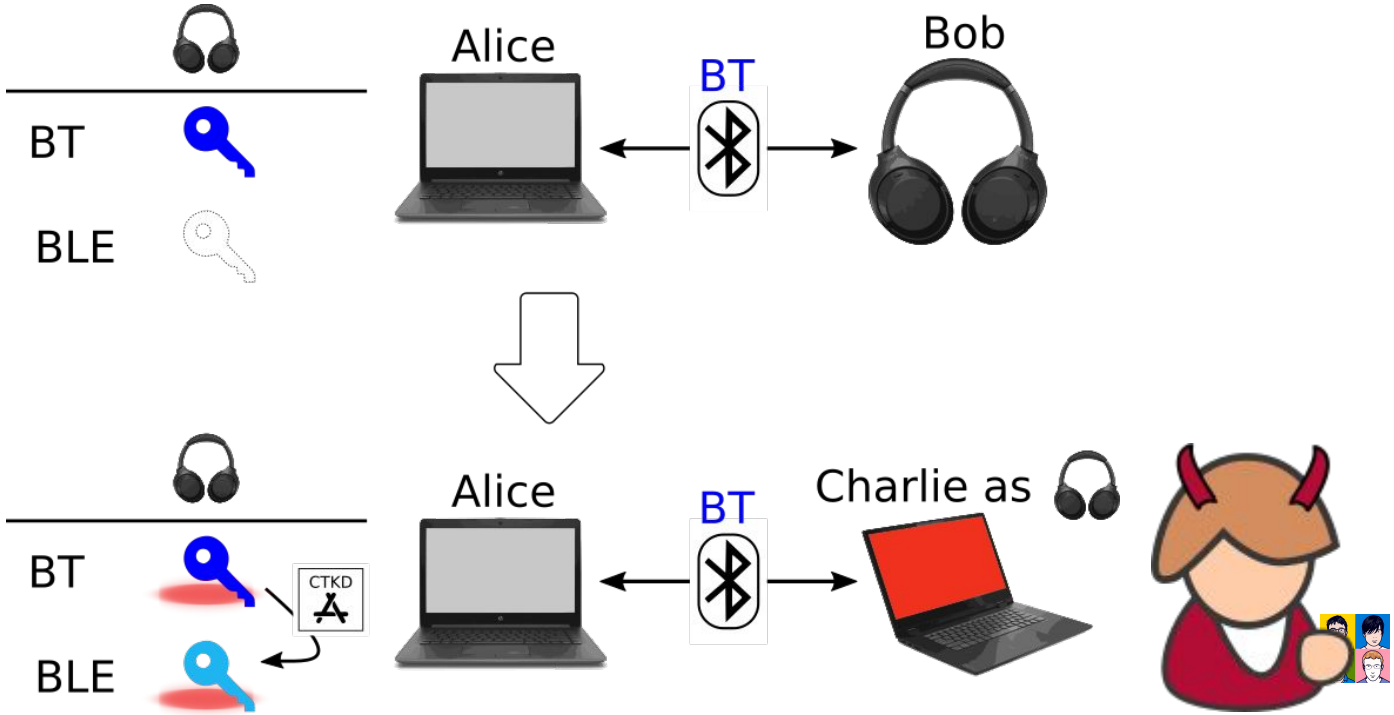
BLUR Attacks: Cross-Transport Central Impersonation



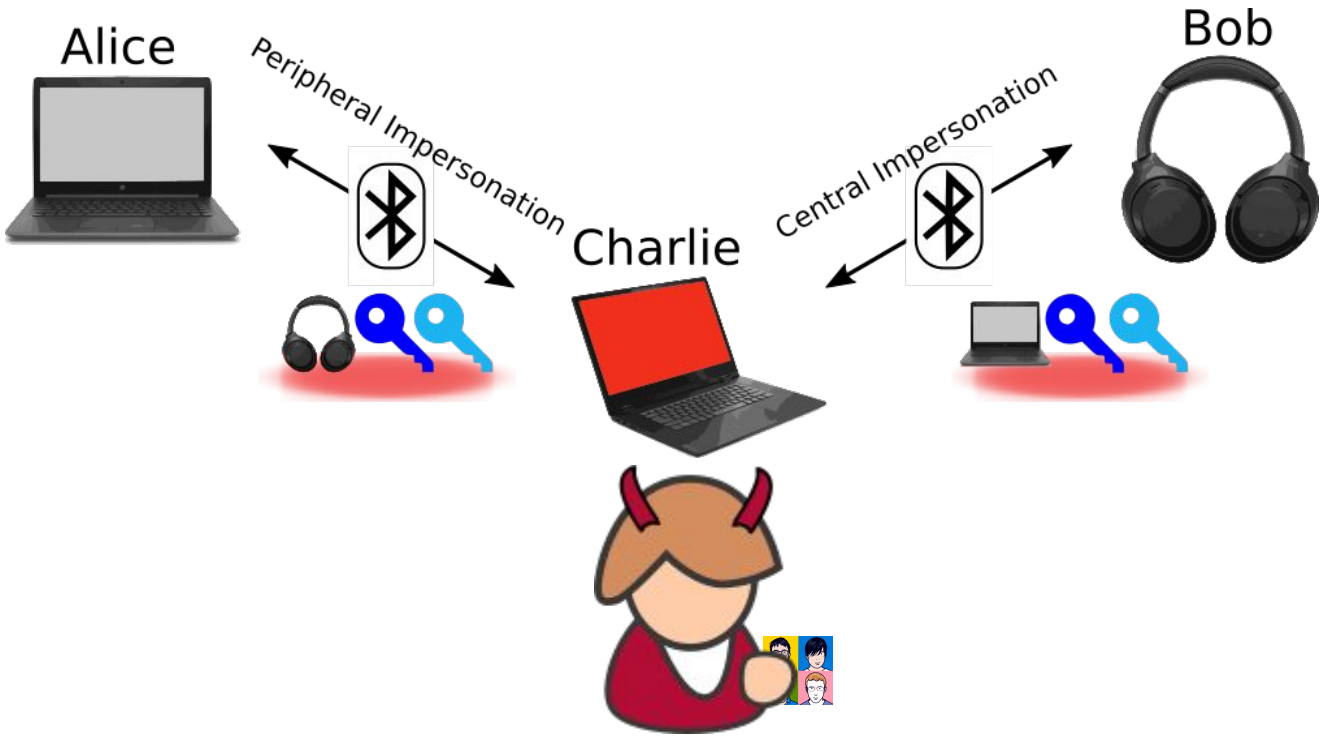
BLUR Attacks: Cross-Transport Central Impersonation (2)



BLUR Attacks: Cross-Transport Peripheral Impersonation



BLUR Attacks: Cross-Transport MitM



Evaluation: Exploiting 16 devices (14 unique chips)

Device			Chip		Bluetooth	BLUR Attack			
Producer	Model	OS	Producer	Model	Version	Role	MI/SI	MitM	US
Cypress	CYW920819EVB-02	Proprietary	Cypress	CYW20819	5.0	Peripheral	✓	✓	✓
Dell	Latitude 7390	Win 10 PRO	Intel	8265	4.2	Peripheral	✓	✓	✓
Google	Pixel 2	Android	Qualcomm	SDM835	5.0	Peripheral	✓	✓	✓
Google	Pixel 4	Android	Qualcomm	702	5.0	Peripheral	✓	✓	✓
Lenovo	X1 (3rd gen)	Linux	Intel	7265	4.2	Peripheral	✓	✓	✓
Lenovo	X1 (7th gen)	Linux	Intel	9560	5.1	Peripheral	✓	✓	✓
Samsung	Galaxy A40	Android	Samsung	Exynos 7904	5.0	Peripheral	✓	✓	✓
Samsung	Galaxy A51	Android	Samsung	Exynos 9611	5.0	Peripheral	✓	✓	✓
Samsung	Galaxy A90	Android	Qualcomm	SDM855	5.0	Peripheral	✓	✓	✓
Samsung	Galaxy S10	Android	Broadcom	BCM4375	5.0	Peripheral	✓	✓	✓
Samsung	Galaxy S10e	Android	Broadcom	BCM4375	5.0	Peripheral	✓	✓	✓
Samsung	Galaxy S20	Android	Broadcom	BCM4375	5.0	Peripheral	✓	✓	✓
Xiaomi	Mi 10T Lite	Android	Qualcomm	9312	5.1	Peripheral	✓	✓	✓
Xiaomi	Mi 11	Android	Qualcomm	10765	5.2	Peripheral	✓	✓	✓
Sony	WH-1000XM3	Proprietary	CSR	12414	4.2	Central	✓	✓	✓
Sony	WH-CH700N	Proprietary	CSR	12942	4.1†	Central	✓	✓	✓

KNOB and BIAS attacks on automotive IVI [WOOT'22, ASRG'22, AutoISAC'22, Oakland'20, TOPS'20, SEC'19]

Bluetooth In-Vehicle Infotainment (IVI) Unit

Common Bluetooth Services provided by IVIs

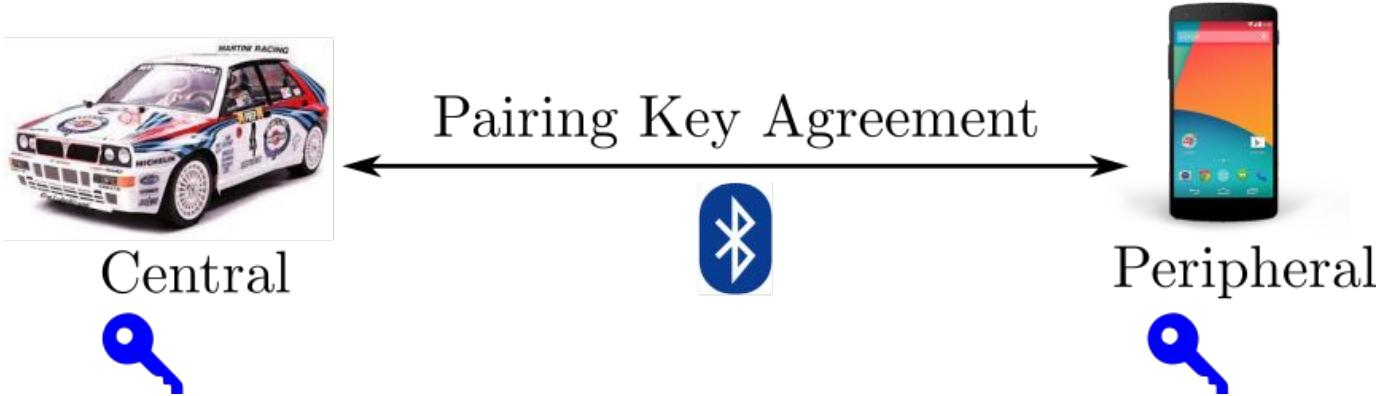
Bluetooth profile	Acronym	Vehicle action
Advanced audio distribution	A2DP	Stream music from a source
Audio/Video remote control	AVRCP	Control music/video player
Hands-free	HFP	Manage calls
Message access	MAP	Read SMS
OBject EXchange	OBEX	Send/receive data
PAN Network Encapsulation	BNEP	Join Internet connection
Phone book access	PBA	Read contacts
Serial Port	SPP	Emulate a serial port
SIM access	SAP	Access a SIM card

Bluetooth Threats for Vehicles

- Implementation Level Bluetooth Threats (ILBT)
  - Mature research area (buffer overflows, use after free, …)
  - E.g. Salinas IVI RAT exploiting D-Bus, Bluetooth and SMS
- **Protocol Level Bluetooth Threats (PLBT)**
  - **Unexplored** and **impactful** (portable attacks)
  - E.g., BIAS impersonation [Oakland'21]
  - E.g., KNOB key downgrade [SEC'20, TOPS'20]

Attack Scenario: Bluetooth Pairing

1. Pair the IVI (car) with a phone
2. Devices generate a long-term pairing key
3. Accept all permissions and synch data



Attack Scenario: Bluetooth Session Establishment

1. Authenticate the pairing key
2. Negotiate a session key
3. Encrypt the traffic
4. Use Bluetooth services (audio, calls, Internet, …)

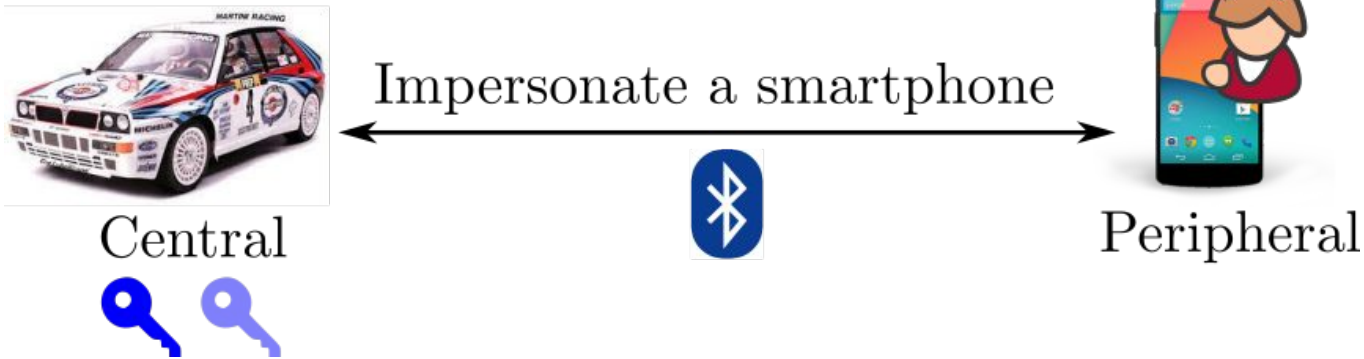
Central

Session Establishment

Peripheral

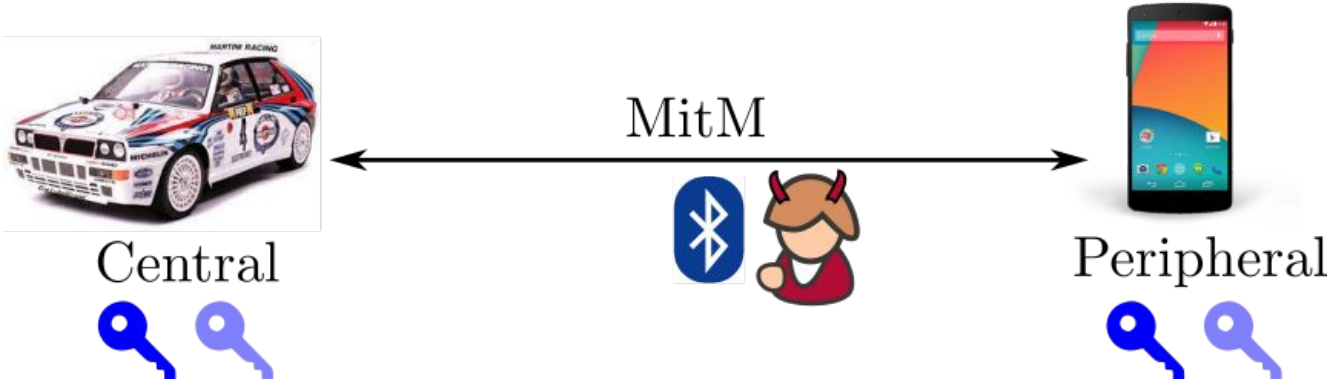
Attack Scenarios: BIAS+KNOB Impersonation Attack

1. Start a session with IVI spoofing the trusted phone
2. Skip pairing key authentication (**BIAS attack**)
3. Negotiate a low entropy session key and brute force it (**KNOB attack**)



Attack Scenarios: BIAS+KNOB MitM Attack

1. Impersonate trusted smartphone to car IVI
2. Impersonate trusted car IVI to smartphone
3. Machine-in-the-middle their connection



Testing PLBTs on IVIs (ala Car Hacking: For Poories)

- **Lab** experiments
  - Buy popular IVIs second-hand
  - Power them up in the lab
  - Evaluate them against PLBTs
- **On-the-road** experiments
  - Drive our cars to a safe environment
  - Evaluate them against PLBTs
- Testing equipment
  - power supply, cables, laptop, devboards, …

Eval: All tested IVIs are **vulnerable to BIAS+KNOB**

Lab

OtR

	KIA 96560-B2211CA	Toyota PT546-00170	Suzuki IGNIS	Skoda Fabia	Skoda Octavia
	Car unit	Car unit	Car	Car	Car
Session issues					
Entropy downgrade	1 byte	1 byte	1 byte	1 byte	1 byte
Role switch auth bypass	Yes	Yes	Yes	Yes	Yes
Vulnerable to KNOB & BIAS	Yes	Yes	Yes	Yes	Yes
Pairing issues					
Always Discoverable	No	No	No	Yes	Yes
Always Pairable	Yes	No	No	Yes	Yes
Just Works Downgrade	Yes	Yes	No	Yes	Yes

Eval: IVIs pairing caps are OK, **session caps are NOT**

Lab

OtR

	KIA 96560-B2211CA	Toyota PT546-00170	Suzuki IGNIS	Skoda Fabia	Skoda Octavia
	Car unit	Car unit	Car	Car	Car
Pairing capabilities					
Secure Simple Pairing (SSP)	Yes	Yes	Yes	Yes	Yes
Input Output	Display	Display	Display	Display	Display
Authentication Requirement	AitM	None	AitM	AitM	AitM
Association	Num Comp	Num Comp	Num Comp	Num Comp	Num Comp
Session capabilities					
Secure Connections (SC)	No	No	No	No	No
Unilateral authentication	Yes	Yes	Yes	Yes	Yes
E_0 cipher (weak)	Yes	Yes	Yes	Yes	Yes

BLUFFS Attacks [CCS'23, 37c3]

Forward and Future Secrecy (FoS, FuS)

- Forward Secrecy (FoS)
  - Protects past sessions against key compromise
  - Eg: `key = HKDF(const, key_past)`
- Future Secrecy (FuS)
  - Protects future sessions against key compromise
  - Eg: `key_future = HKDF(dhss, key)`

BT FoS and FuS?

- **Not** discussed in the BT specification
- **No prior** evaluations (academia, industry, …)
- Despite **widespread** real-world usage (TLS1.3, Signal, …)
- **BLUFFS research** fills this relevant gap!

BLUFFS Threat model

- BC **should** provide FoS and FuS among sessions
  - long term PK is not compromised
  - fresh SK derivation is not vulnerable
- Alice (Central) and Bob (Peripheral)
  - Share PK
  - Use SC or LSC
- Charlie (attacker)
  - Model: proximity-based, cannot compromise PK or all SKs
  - Goals: break sessions' FoS and FuS
  - Impact: impersonate and MitM devices across sessions

BLUFFS Attacks

t_0: Alice and Bob establish PK

t_1: Charlie forces weak SK_c, saves SK_c kdf pars, sniffs s_{t1}, …

t_2: Charlie brute forces SK_c and breaks s_{t1}, …, s_{t2} (breaks FoS)

t_3: Charlie re-forces SK_c and breaks s_{t3}, s_{t4}, … (breaks FuS)

BLUFFS Attacks

t_0: Alice and Bob establish PK

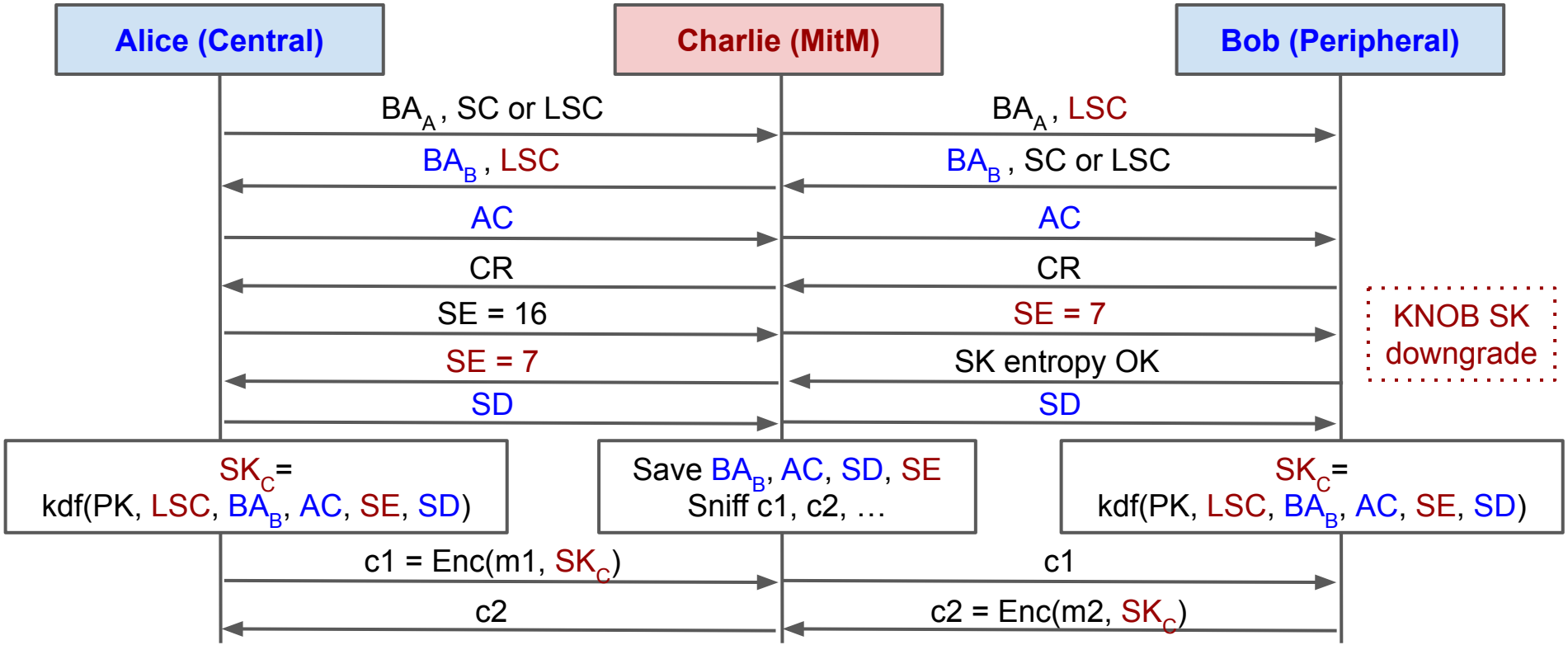
t_1: Charlie forces weak SK_c, saves SK_c kdf pars, sniffs s_{t1}, …

t_2: Charlie brute forces SK_c and breaks s_{t1}, …, s_{t2} (breaks FoS)

t_3: Charlie re-forces SK_c and breaks s_{t3}, s_{t4}, … (breaks FuS)

t_∞: Charlie celebrates (One More Time)!

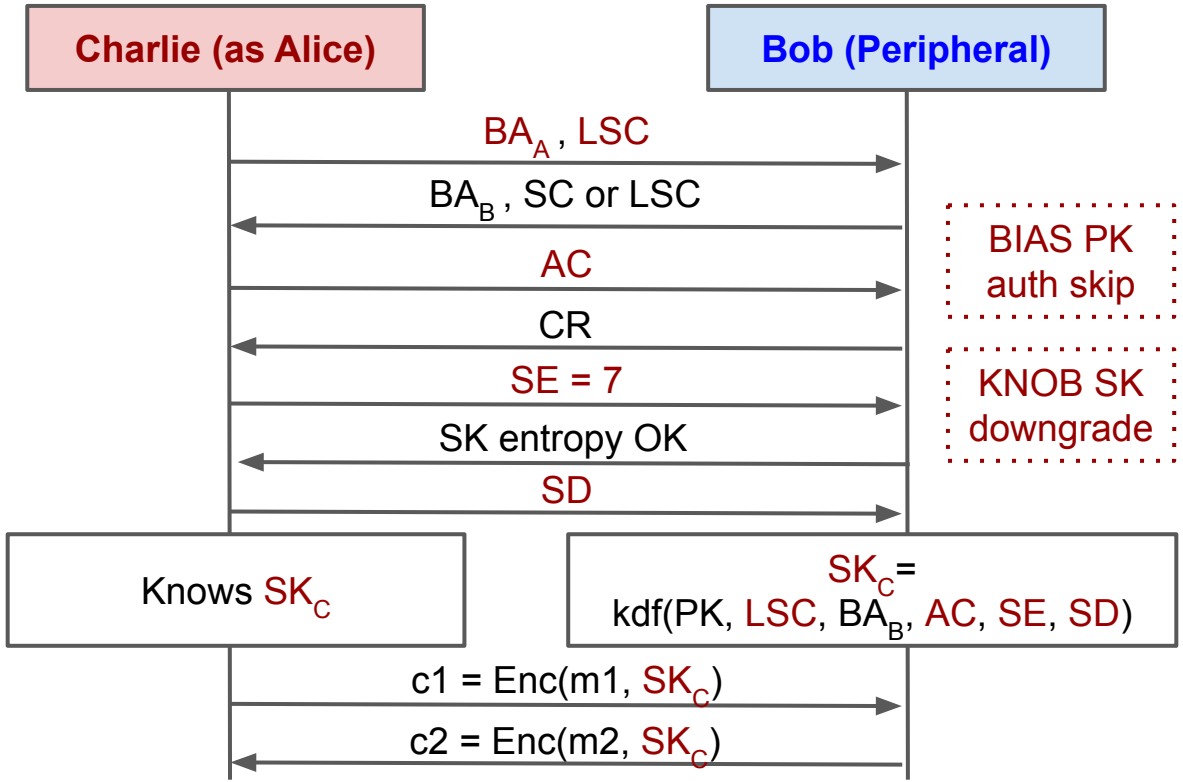
t_1: Force weak SK_C, save SK_C kdf pars, sniff



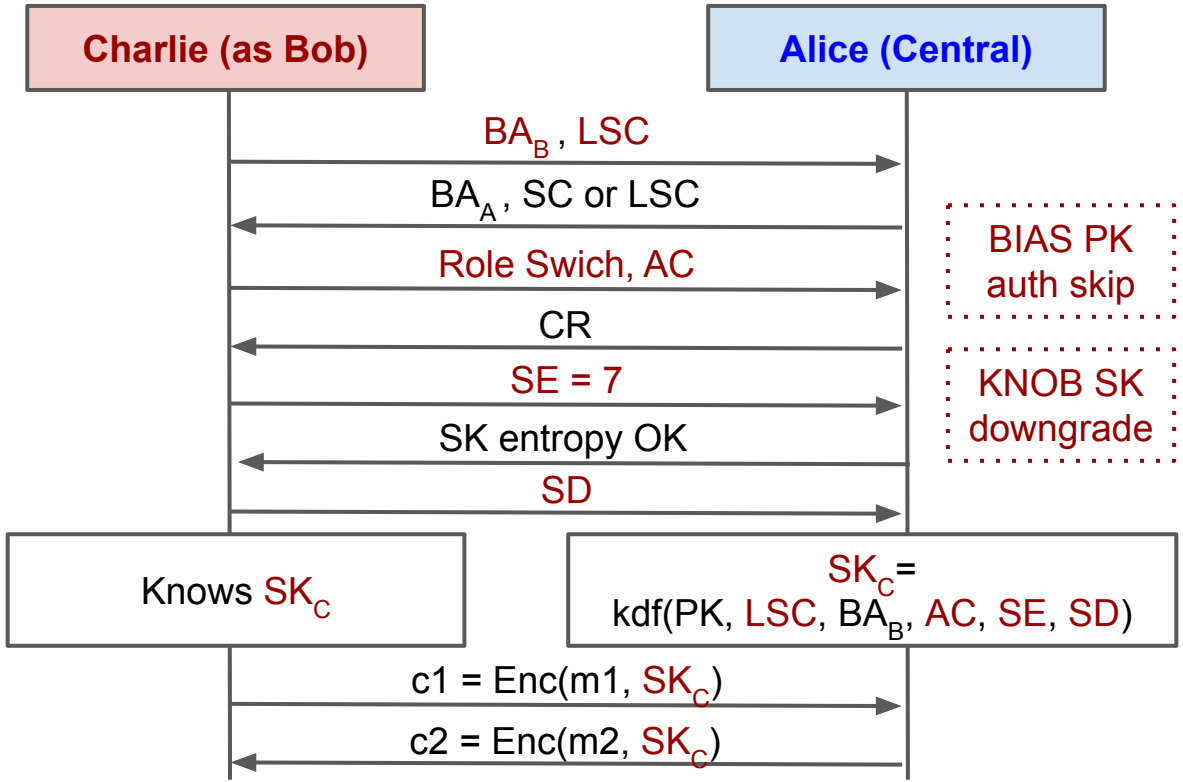
t_2: Brute force SK_c and break s_{t1}, …, s_{t2} (break FoS)

- SK_c has 56 bits of entropy (SE = 7)
  - 2^{55} trials on average (other than 2^{55} x sessions)
  - 56 bit sym keys broken since DES (Deep Crack, COPACOBANA)
  - keylenght.com sets a min of 84 bits (56 bits in 1982)
  - Doable in weeks with a low-cost setup
- SK_c has 8 bits of entropy (SE = 1)
  - Doable in real time (even with pen and paper)

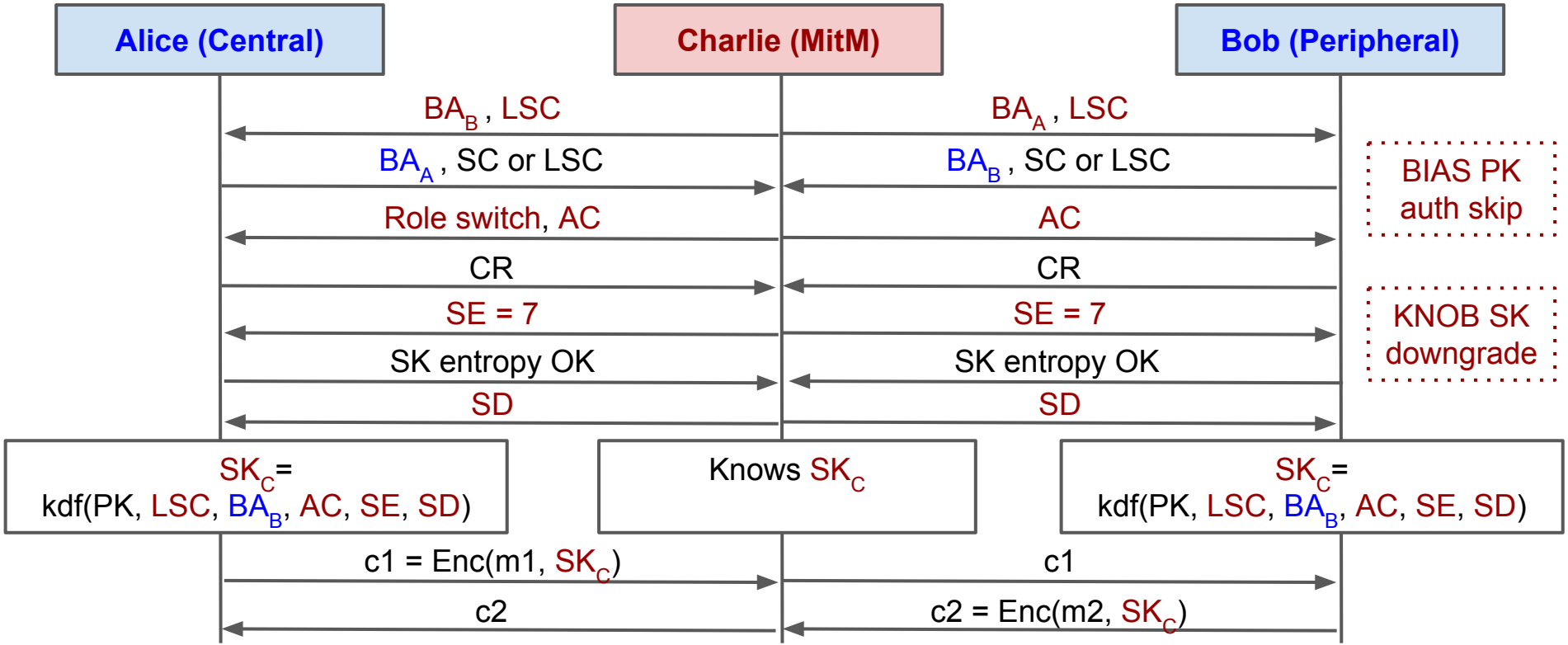
t_3: Re-force SK_C and break s_{t3}, s_{t4}, … (break FuS)



t_3: Re-force SK_C and break s_{t3}, s_{t4}, … (break FuS)



t_3: Re-force SK_C and break s_{t3}, s_{t4}, … (break FuS)



Six BLUFFS Attacks Labels

A1: Spoofing a LSC Central (t_3)

A2: Spoofing a LSC Peripheral (t_3)

A3: MitM LSC victims (t_1, t_3)

A4: Spoofing a SC Central (t_3)

A5: Spoofing a SC Peripheral (t_3)

A6: MitM SC victims (t_1, t_3)

BLUFFS Attacks Exploiting 18 devices (17 chips)

Chip	Device(s)	BTv	A1	A2	A3	A4	A5	A6
LSC Victims								
Bestechnic BES2300	Pixel Buds A-Series[3]	5.2	✓	✓	✓	✓	✓	✓
Apple H1	AirPods Pro	5.0	✓	✓	✓	✓	✓	✓
Cypress CYW20721	Jaybird Vista	5.0	✓	✓	✓	✓	✓	✓
CSR/Qualcomm BC57H687C-GITM-E4	Bose SoundLink[1,2]	4.2	✓	✓	✓	✓	✓	✓
Intel Wireless 7265 (rev 59)	Thinkpad X1 3rd gen	4.2	✓	✓	✓	✓	✓	✓
CSR n/a	Logitech BOOM 3[1]	4.2	✓	×	✓	✓	×	✓
SC Victims								
Infineon CYW20819	CYW920819EVB-02	5.0	✓	✓	✓	✓	✓	✓
Cypress CYW40707	Logitech MEGABLAST	4.2	✓	✓	✓	✓	✓	✓
Qualcomm Snapdragon 865	Mi 10T[4]	5.2	✓	✓	✓	×	×	×
Apple/USI 339S00761	iPhones 12[4], 13[4]	5.2	✓	✓	✓	×	×	×
Intel AX201	Portege X30-C[4]	5.2	✓	✓	✓	×	×	×
Broadcom BCM4389	Pixel 6[4]	5.2	✓	✓	✓	×	×	×
Intel 9460/9560	Latitude 5400[4]	5.0	✓	✓	✓	×	×	×
Qualcomm Snapdragon 835	Pixel 2[4]	5.0	✓	✓	✓	×	×	×
Murata 339S00199	iPhone 7[4]	4.2	✓	✓	✓	×	×	×
Qualcomm Snapdragon 821	Pixel XL[4]	4.2	✓	✓	✓	×	×	×
Qualcomm Snapdragon 410	Galaxy J5[4]	4.1	✓	✓	✓	×	×	×

BLUFFS Attacks Exploiting 18 devices (17 chips)

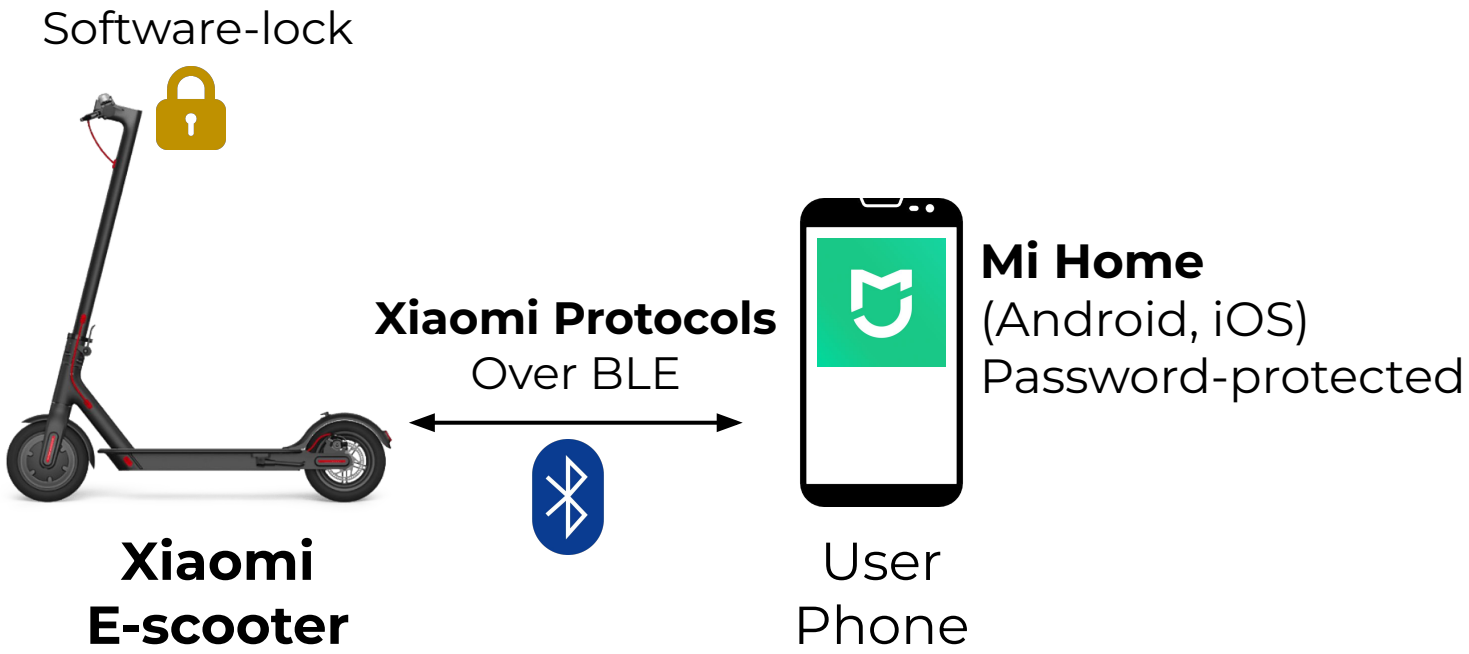
- *LSC Victims*
  - All vulnerable
  - Except Logitech BOOM 3 against A2, A5 (require Central auth)
  - Google Pixel Buds A-Series accept SE = 1 (no KNOB patch)
- *SC Victims*
  - All vulnerable if other victim supports LSC
  - Eighth devices are not vulnerable to A4, A5, A6 (enforce SC btw pairing and session establishment)

BLUFFS Impact Billions of BT Devices

- *Devices*: laptops, smartphones, tablets, headsets, cars, …
- *OSes*: iOS, Android, Linux, Windows, …
- *Software*: BlueZ, Gabeldorsche, Bluedroid, proprietary, …
- *Hardware*: Intel, Broadcom, Logitech, Infineon, Qualcomm, Apple, Microsoft, CSR, …
- *BT versions*: 5.2, 5.1, 5.0, 4.2, 4.1, …
- One BT spec vulnerability → Billions of exploitable devices

E-Spoofer attacks on Xiaomi E-Scooters [WiSec'23]

System Model



Attacker Models

Proximity Attacker

Xiaomi Protocols
Over BLE

Xiaomi
E-scooter

Xiaomi Protocols
Over BLE

Remote Attacker (Android app)

User
Phone

Xiaomi E-Scooter Protocols Introduction

- **P1, P2, P3, P4 (since 2016)**
  - *Application-layer* Pairing and Session phases
  - *No BLE link-layer* security
- **Pairing** phase
  - Devices agree on a **Pairing Key** (**PK**)
- **Session** phase
  - Devices compute a **Session Key** (**SK**) from PK
  - Devices use SK to establish a secure channel

P4: Pairing (ECDH, AES-CCM)

PAIRING

chal, **PUB_e**

PUB_a

SS = ECDH(**PUB_e**,**PRV_a** or **PUB_a**,**PRV_e**)
PK||**OTK** = HKDF(key=**SS**,inp=**const**)

resp = AES-CCM(key=**OTK**,inp=**chal**)

ECDH to generate **PK** from **SS**.

App auth using **OTK**.

P4: Proximity/Remote Attacks

MALICIOUS PAIRING

chal, **PUB_e**

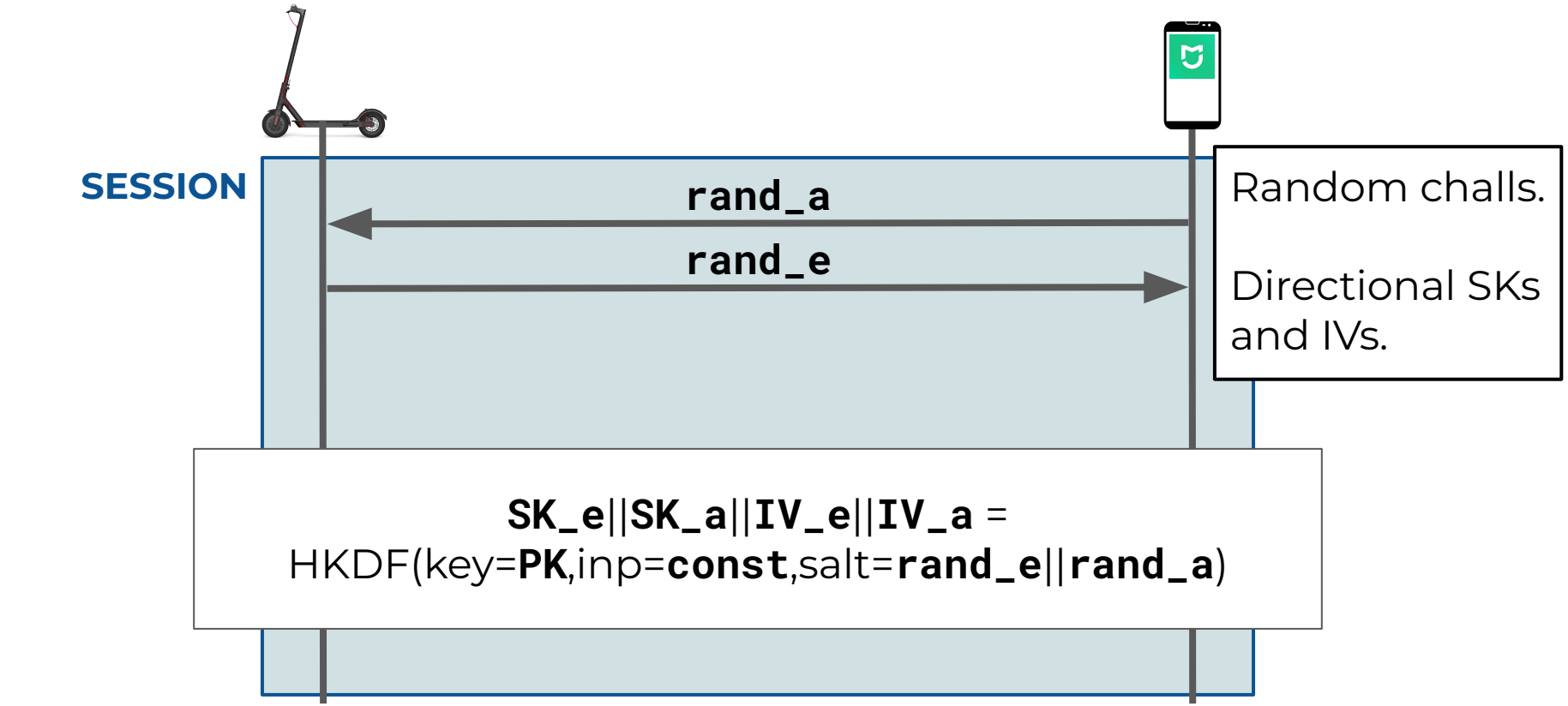
PUB_a

Unauthorized and **non authenticated** pairing.

SS = ECDH(**PUB_e**,**PRV_a** or **PUB_a**,**PRV_e**)
PK||OTK = HKDF(key=**SS**,inp=**const**)

resp = AES-CCM(key=**OTK**,inp=**chal**)

P4: Session (HKDF, AES-CCM) (1)



P4: Session (HKDF, AES-CCM) (2)

SESSION

resp_a = HKDF(key=**SK_a**,inp=**rand_a**||**rand_e**)

resp_e = HKDF(key=**SK_e**,inp=**rand_e**||**rand_a**)

AES-CCM(key=**SK_a**,IV=**IV_a**||**cnt**, inp=**Read/Write Req**)

AES-CCM(key=**SK_e**,IV=**IV_e**||**cnt**, inp=**Read/Write Resp**)

Mutual session auth.

Encrypted and integrity protected comms.

P4: Proximity/Remote Attacks

SESSION DOWNGRADE

p4_session_downgrade_cmd

esc_name

Session **downgraded to P3** (more insecure).

PK = AES-ECB(key=**const**,inp=**esc_name**)

Arbitrary Read/Write Req XOR **PK**

Read/Write Resp XOR **PK**

Evaluation Setup

M365

Essential

Mi 3

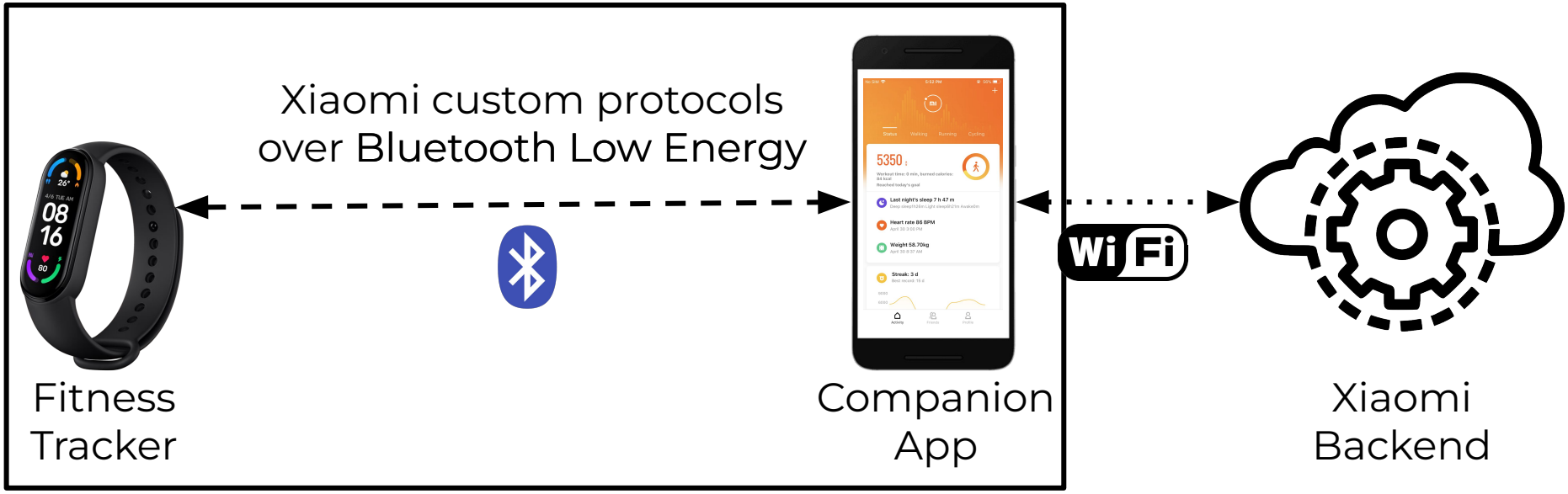
- 5 BLE boards (M365, Pro 1, Pro 2, Essential, Mi 3)
- 8 BLE firmware (P1, P2, P3, P4)

Evaluation Results

E-scooter	BLE Board	BLE Fw	Protocol	Strategy	Prox/Rem Adv.	
					Spoof Mi Home	*Arb R/W*
M365	M365	072	P1	RE	✓	✓
M365	M365	081	P2	RE, MP, SD	✓	✓
M365	Pro 1	090	P3	RE	✓	✓
M365	M365	122	P4v1	RE, MP, SD	✓	✓
M365	Pro 2	129	P4v1	RE, MP, SD	✓	✓
Essential	Essential	152	P4v1	RE, MP, SD	✓	✓
Mi 3	Mi 3	153	P4v1	RE, MP, SD	✓	✓
Mi 3	Mi 3	157	P4v2	RE, MP	✓	✓

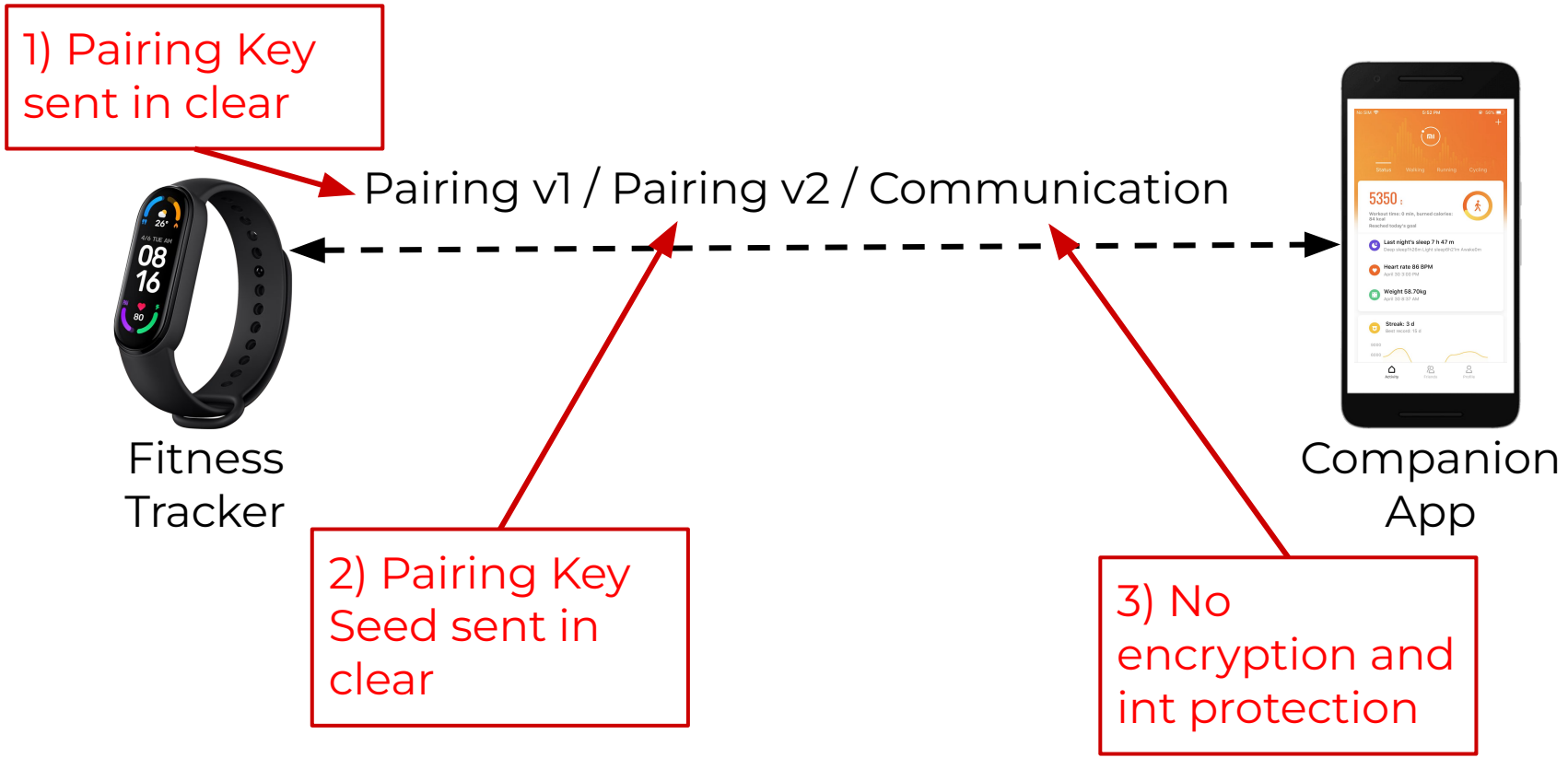
BreakMi attacks on-
Xiaomi and Fitbit Fitness Trackers
[CHES’22, HWIO’23]

System Model (Xiaomi)

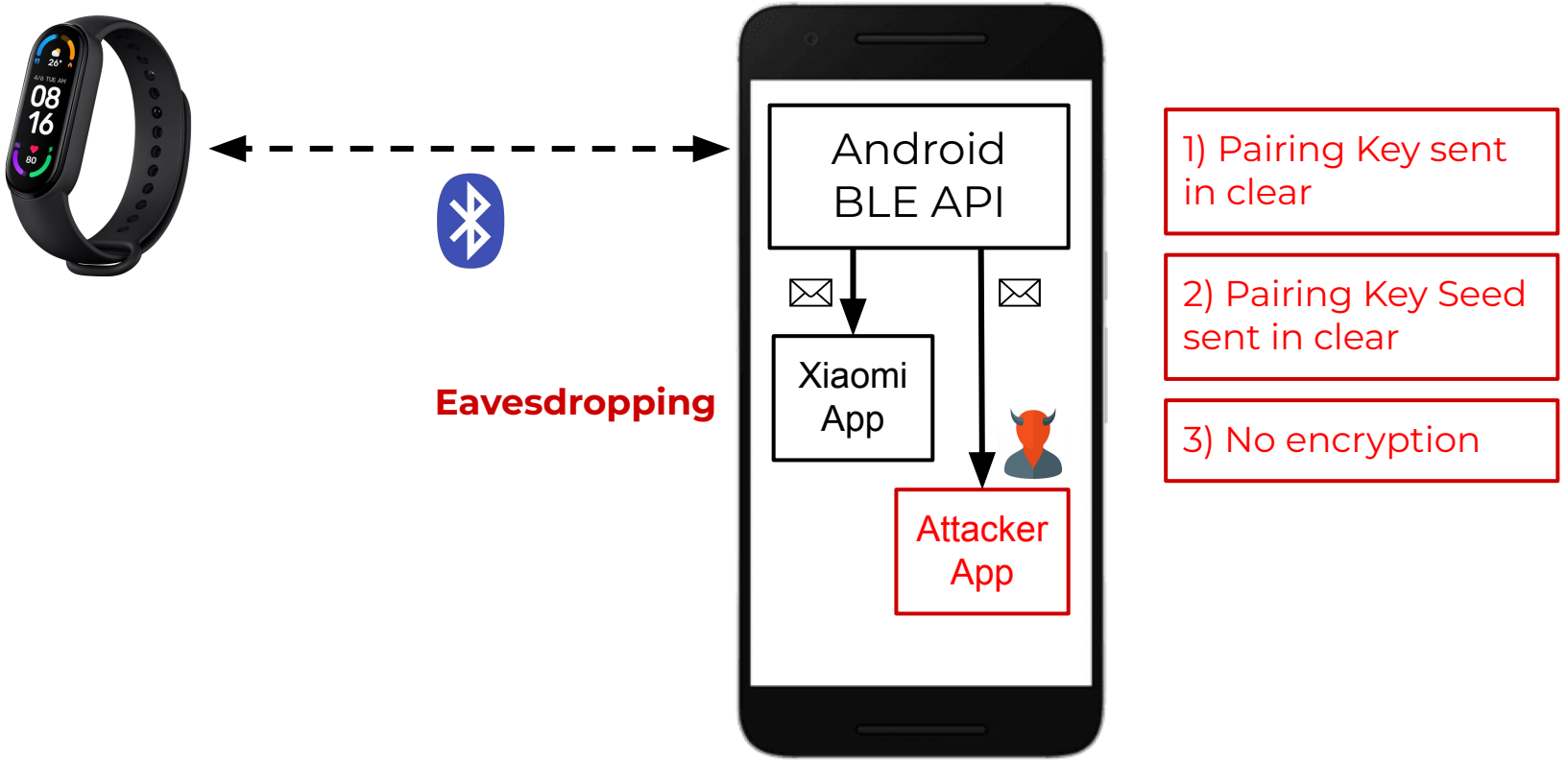


Our focus

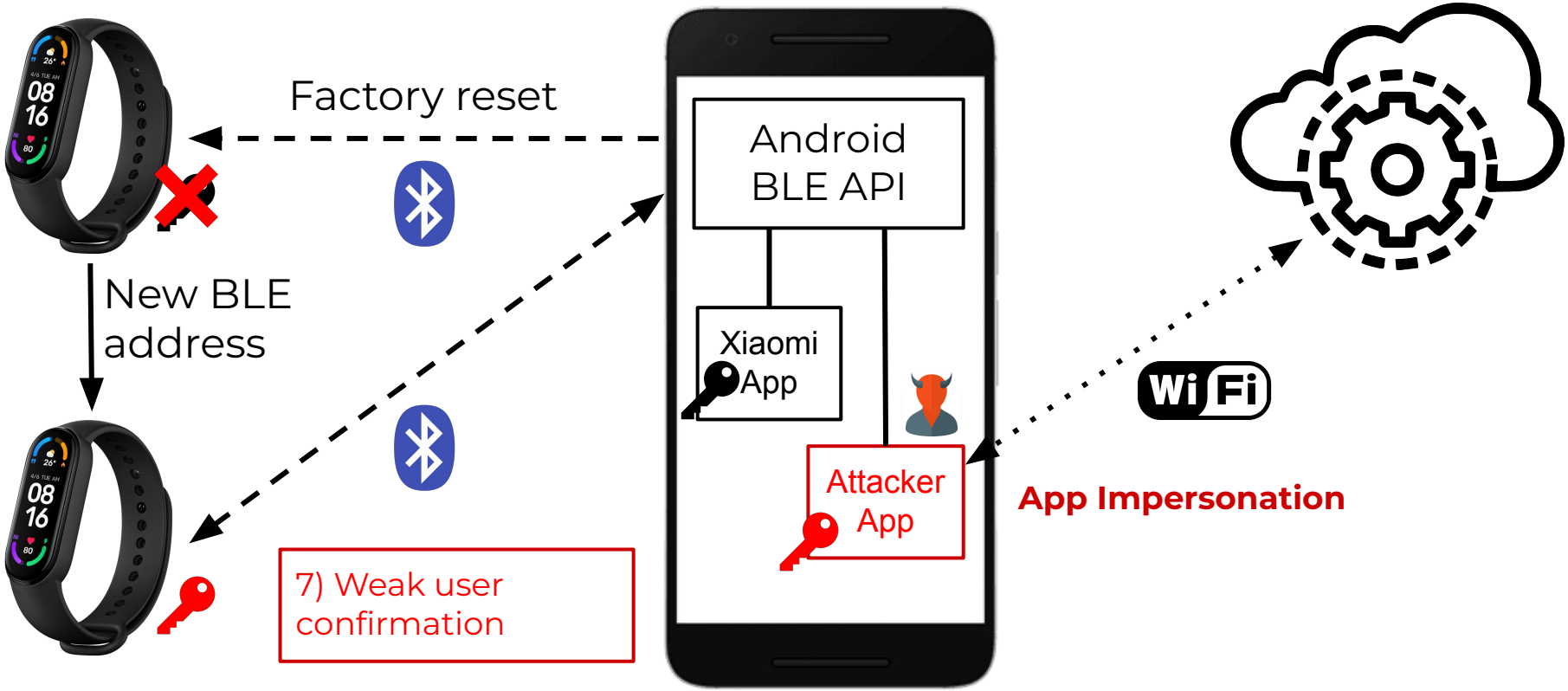
Some Xiaomi Security Protocols Vulns



Remote Eavesdropping



Remote App Impersonation



Evaluation Results

	Proximity Attacks				Remote Attacks	
	Trac Imp.	App Imp.	MitM	Eavesdr.	App Imp.	Eavesdr.
Zepp Life	n/a	✔	✔	✔	✔	n/a
Zepp	n/a	✔	✔	✔	✔	n/a
Mi Band 2	✔	n/a	✔	✔	n/a	✔
Mi Band 3	✔	n/a	✔	✔	n/a	✔
Amazfit Cor 2	✔	n/a	✔	✔	n/a	✔
Mi Band 4	✔	n/a	✔	✔	n/a	✔
Mi Band 5	✔	n/a	✔	✔	n/a	✔
Mi Band 6	✔	n/a	✔	✔	n/a	✔

Videos

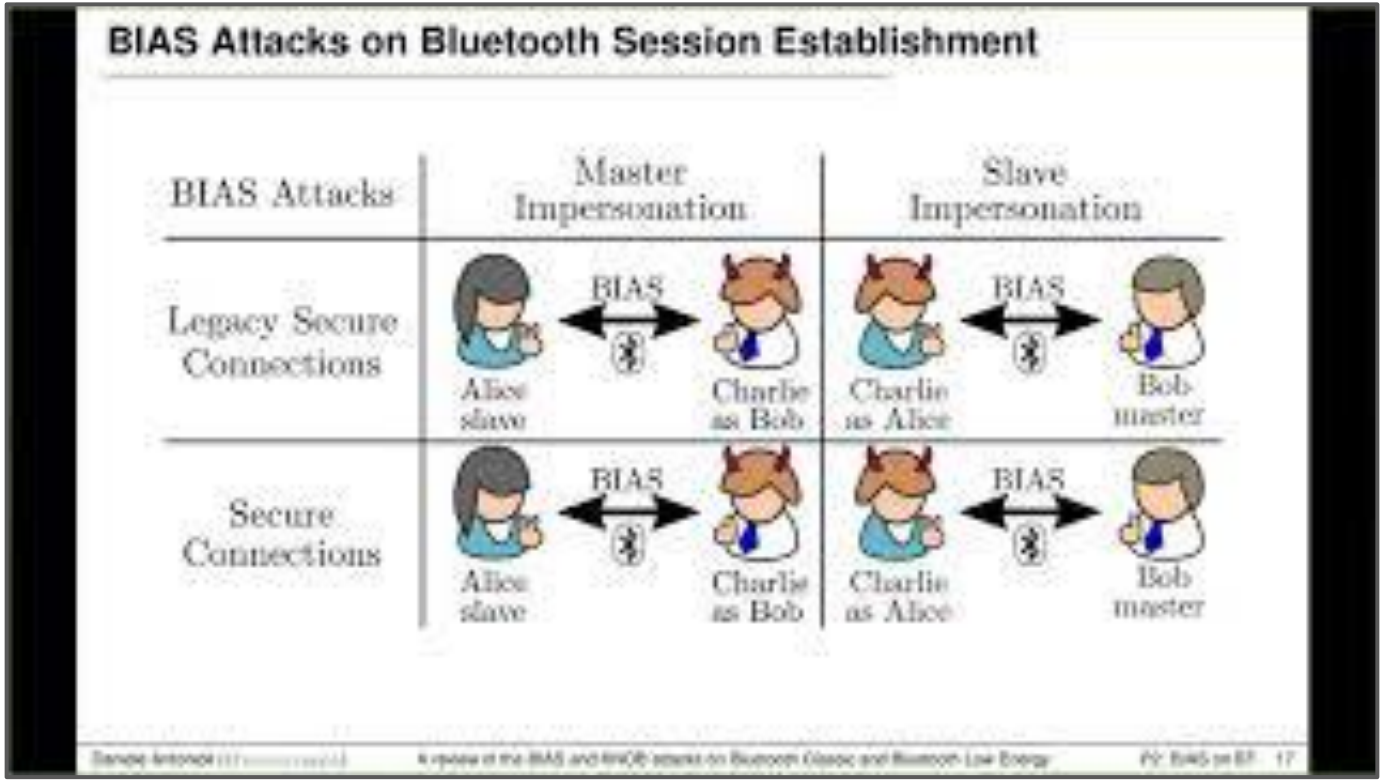
BLUR talk at AsiaCCS'23

BLURtooth: Exploiting Cross-Transport Key Derivation in Bluetooth Classic and Bluetooth Low Energy

ACM AsiaCCS'22

Daniele Antonioli (EURECOM and EPFL)
Nils Ole Tippenhauer (CISPA)
Kasper Rasmussen (University of Oxford)
Mathias Payer (EPFL)

KNOB and BIAS Attacks at IACR'20



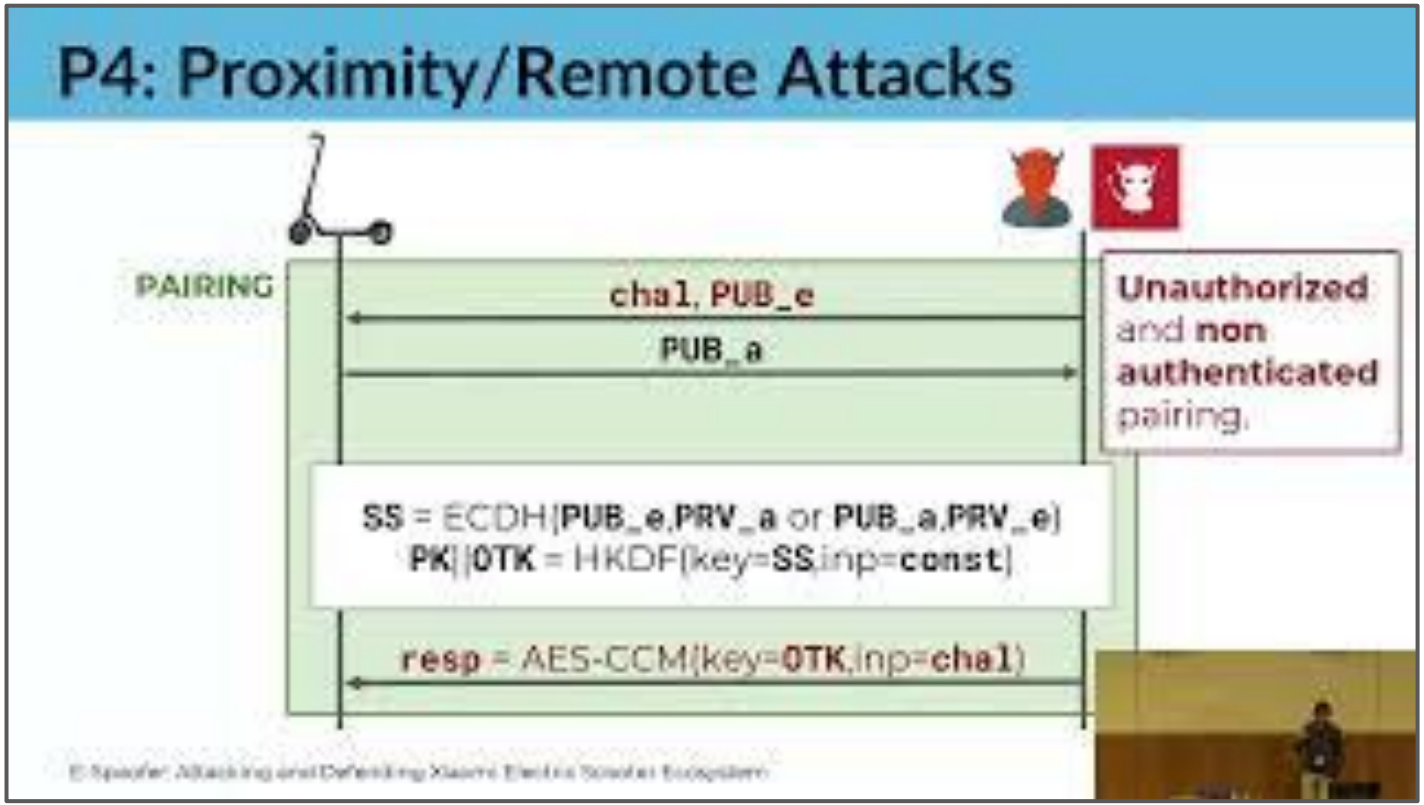
KNOB and BIAS automotive security talk at ASRG'22

BLUFFS talk at 37c3

https://media.ccc.de/v/37c3-12342-bluffs_bluetooth_forward_and_future_secrecy_attacks_and_defenses

BreakMi talk at HWIO’23 (Marco Casagrande)

E-Spoofer talk at WiSec'23 (Marco Casagrande)



ORSHIN summary (Prof. Aurelien Francillon)

https://vimeo.com/880421366