BLUFFS: Bluetooth Forward and Future Secrecy Attacks and Defenses

ACM CCS'23

Daniele Antonioli
(EURECOM, S3)

EURECOM
Sophia Antipolis

Bluetooth (BT)

- BT is a pervasive low-power wireless technology
  - Specified in bluetooth-core.pdf (v5.4) (layers, security, …)
  - BC: Bluetooth Classic
  - BLE: Bluetooth Low Energy
  - Used by smartphones, laptops, cars, wearables, sensors, …
- One BT spec vulnerability → Billions of exploitable devices
  - 2021: BLUR cross-transport overwrites on BC/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)

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 guarantees?
  - **Not** discussed in the BT spec and **no prior** evaluation
  - Despite **widespread** in the real-world (TLS1.3, Signal, …)

Contributions

- First study on BT FoS and FuS
- Uncover 2 FoS/FuS vulns in BC SK derivation
- Develop 6 BLUFFS attacks breaking BC sessions' FoS/FuS
- Exploit 18 popular devices (Intel, Broadcom, Apple, Google, Microsoft, CSR, Logitech, Infineon, Bose, Dell, Xiaomi, …)
- Fix the attacks with a compliant and practical protocol
- Report critical findings to BT SIG, get CVE-2023-24023
- Release BLUFFS toolkit to test the attacks and BC FoS/FuS

BLUFFS Threat model

- BC **should** provide FoS and FuS among sessions
  - Fresh SKs, PK not compromised
- Alice (Central) and Bob (Peripheral)
  - Paired and 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

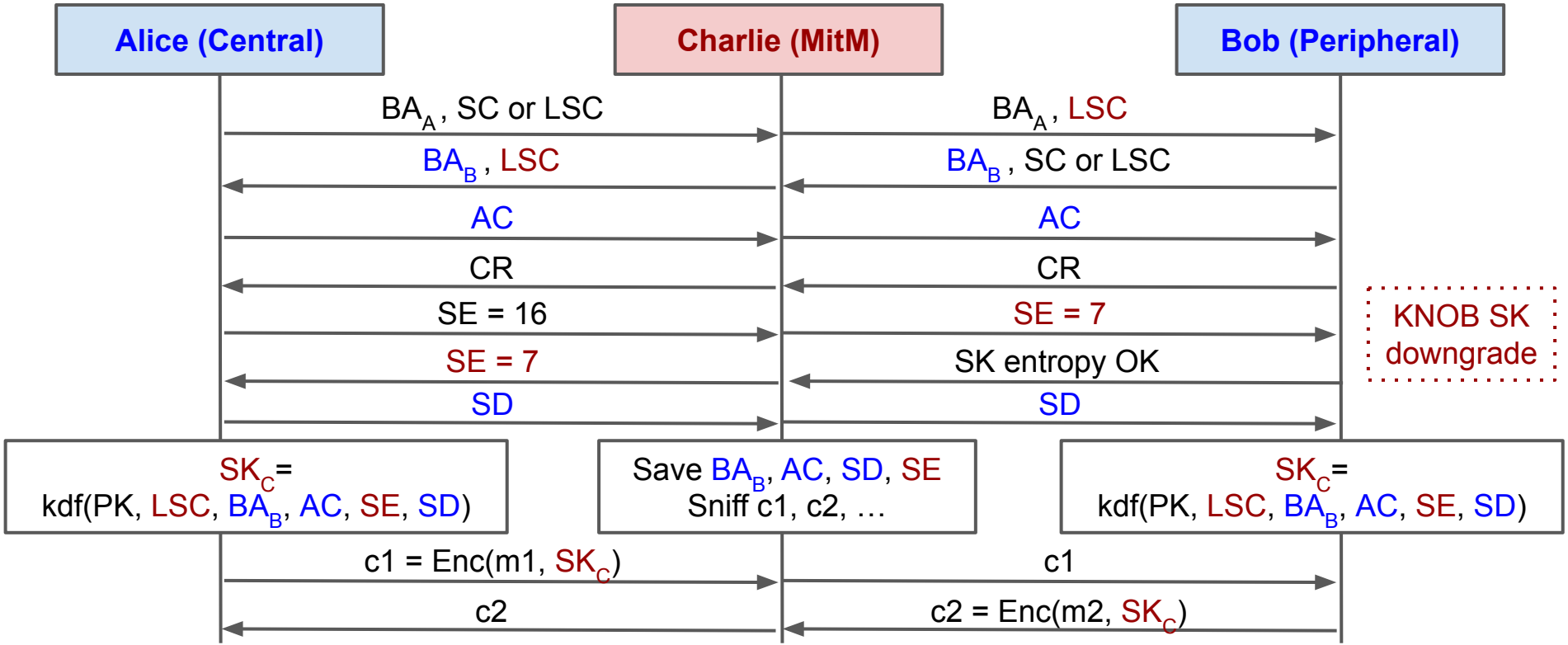
t_1: Charlie forces weak SK_c, saves SK_c kdf pars, sniffs s_{t1}, …

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)!

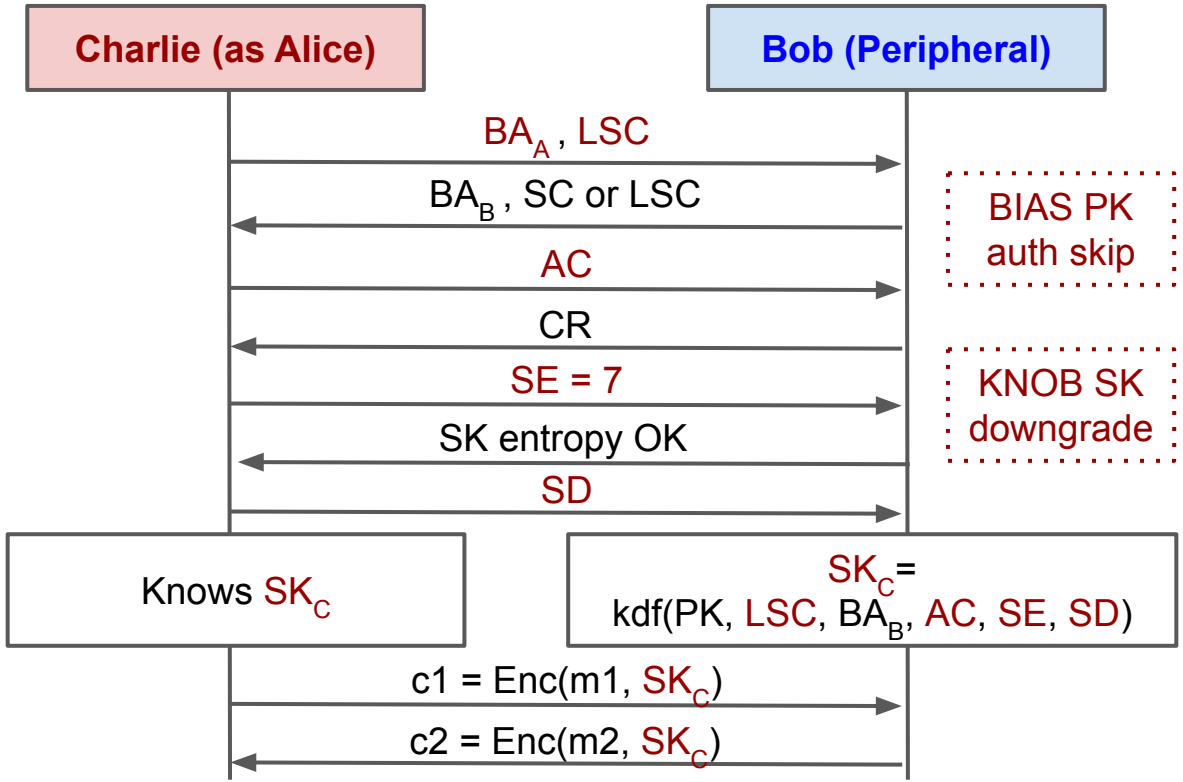
t1: Force weak SK_C, save SK_C kdf pars, sniff [A3, A6]



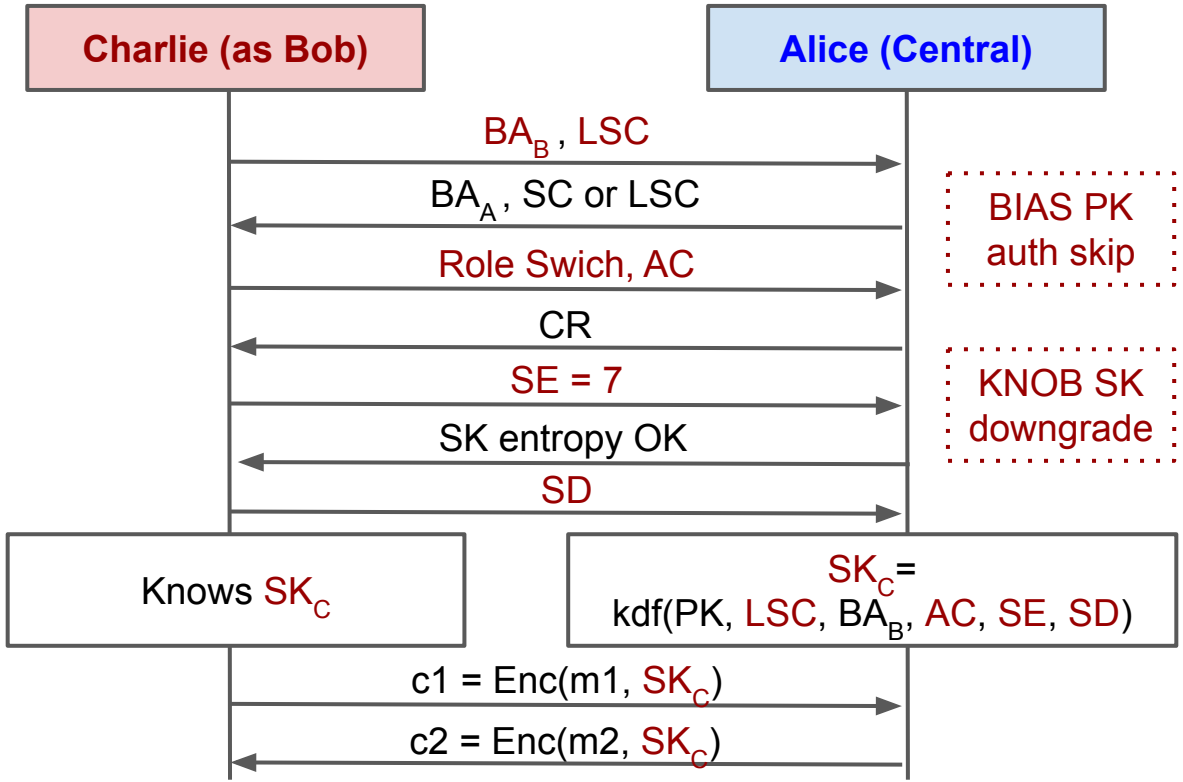
t2: Brute force SK_c and break s_{t1}, …, s_{t2} (break FoS)

- 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)

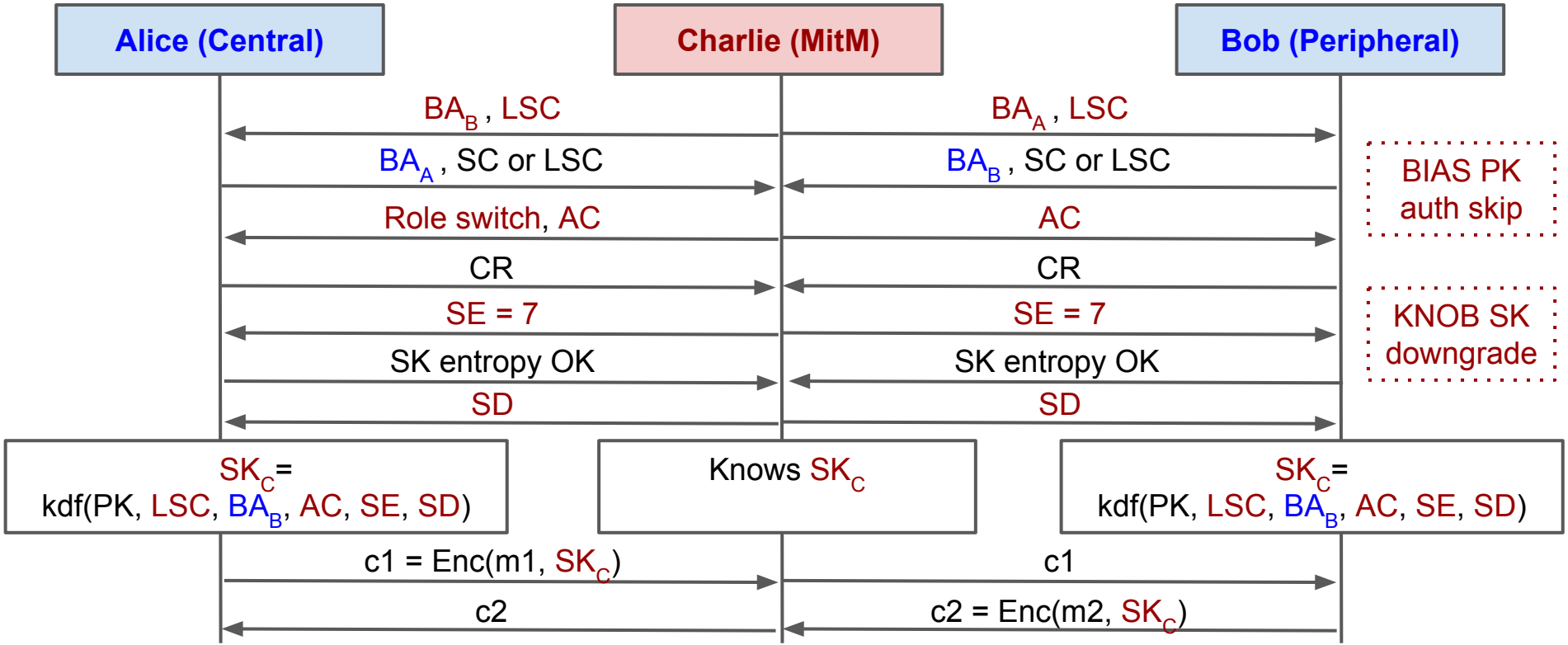
t3: Re-force SK_C and break s_{t3}, s_{t4}, … (break FuS) [A1, A4]



t3: Re-force SK_C and break s_{t3}, s_{t4}, … (break FuS) [A2, A5]



t3: Re-force SK_C and break s_{t3}, s_{t4}, … (break FuS) [A3, A6]



BLUFFS Attacks Summary and Root Causes (Vulns)

BLUFFS attack	RC1	RC2	RC3	RC4
A1: Spoofing a LSC Central	✓	✓	✓	×
A2: Spoofing a LSC Peripheral	✓	✓	✓	×
A3: MitM LSC victims	✓	✓	✓	×
A4: Spoofing a SC Central	✓	✓	✓	✓
A5: Spoofing a SC Peripheral	✓	✓	✓	✓
A6: MitM SC victims	✓	✓	✓	✓

RC1: LSC SK diversification is unilateral

RC2: LSC SK diversification does not use nonces

RC3: LSC SK diversifiers are not integrity protected

RC4: Downgrading SC to LSC does not require authentication

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	✓	✓	✓	×	×	×

Conclusion and Q&A

- First study on BT FoS and FuS (paper, slides)
- Uncover 2 FoS/FuS vulns in BC SK derivation
- Develop 6 BLUFFS attacks breaking BC sessions' FoS/FuS
- Exploit 18 popular devices (Intel, Broadcom, Apple, Google, Microsoft, CSR, Logitech, Infineon, Bose, Dell, Xiaomi, …)
- Fix the attacks with a compliant and practical protocol
- Report critical findings to BT SIG, get CVE-2023-24023
- Release BLUFFS toolkit to test the attacks and BC FoS/FuS