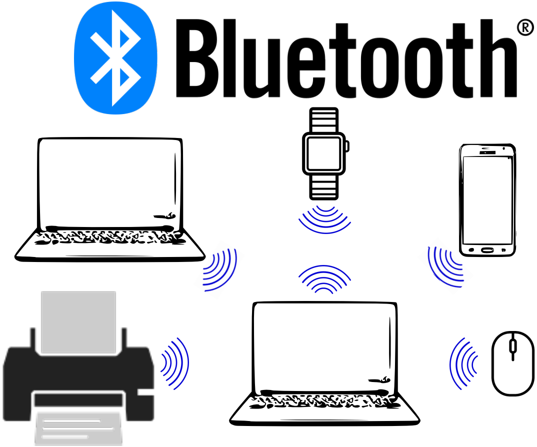
IEEE S&P 2020

# BIAS: Bluetooth Impersonation AttackS

Daniele Antonioli (EPFL), Nils Tippenhauer (CISPA), Kasper Rasmussen (Oxford Univ.)

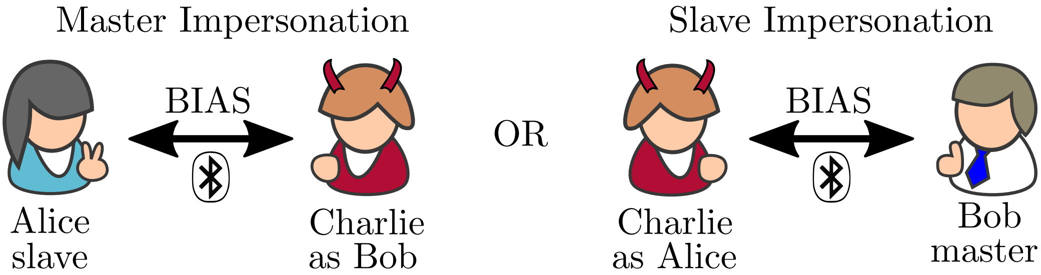
# Bluetooth standard

- Bluetooth standard
  - Specifies **Bluetooth Classic (BT)** and Bluetooth Low Energy (BLE)
  - 1 vulnerability in the standard = billions of exploitable devices



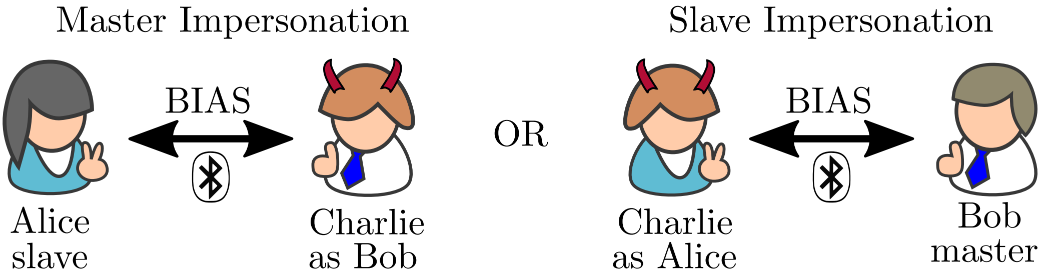
# Contribution: Bluetooth Impersonation AttackS (BIAS)

- **Bluetooth Impersonation AttackS (BIAS)**
  - Exploiting standard-compliant vulnerabilities in Bluetooth authentication
  - To impersonate any Bluetooth device without having to authenticate



# Contribution: Bluetooth Impersonation AttackS (BIAS)

- **Bluetooth Impersonation AttackS (BIAS)**
  - ▸ Exploiting standard-compliant vulnerabilities in Bluetooth authentication
  - ▸ To impersonate any Bluetooth device without having to authenticate

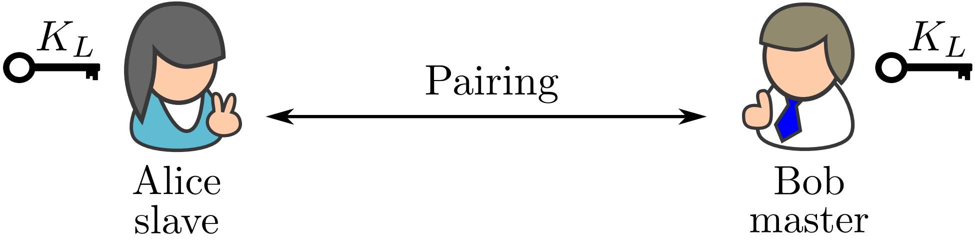


# Bluetooth Threat Model

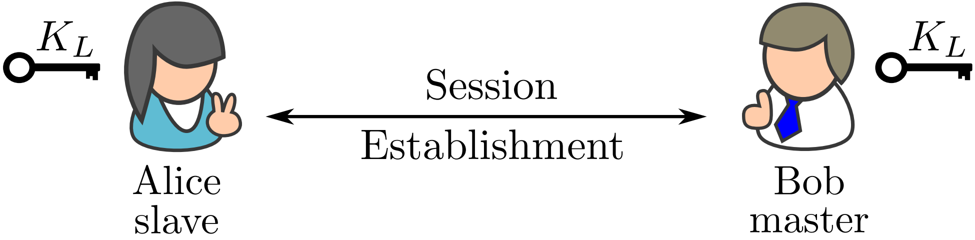
Alice
slave

Bob
master

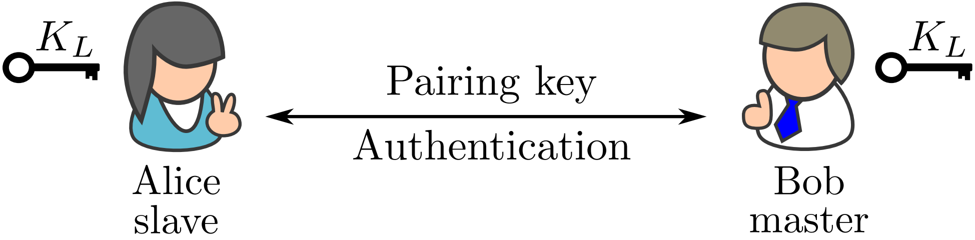
# Bluetooth Threat Model



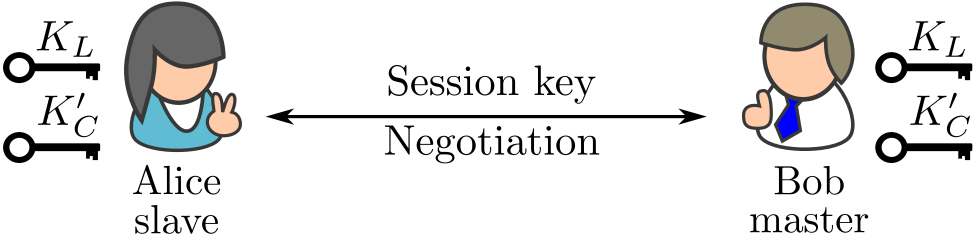
# Bluetooth Threat Model



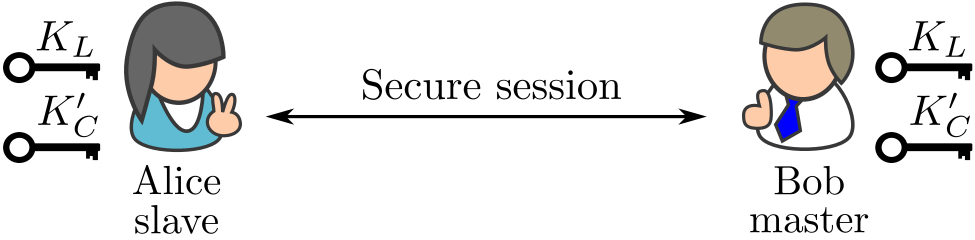
# Bluetooth Threat Model



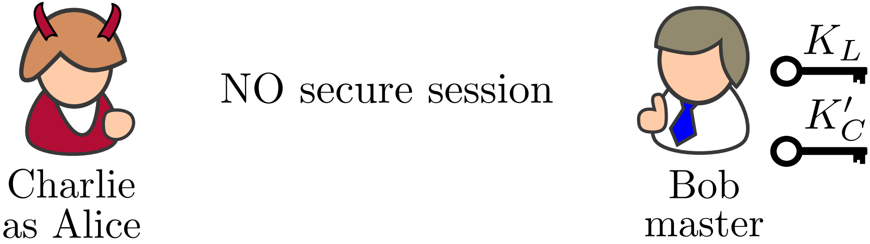
# Bluetooth Threat Model



# Bluetooth Threat Model



# Bluetooth Threat Model



Charlie as Alice

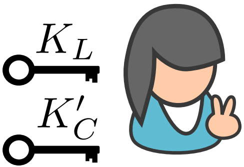
NO secure session

Bob master

$K_L$

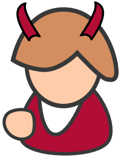
$K'_C$

# Bluetooth Threat Model



Alice
slave

NO secure session

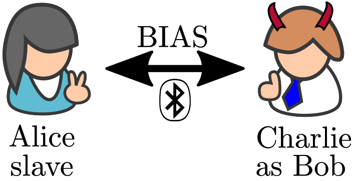
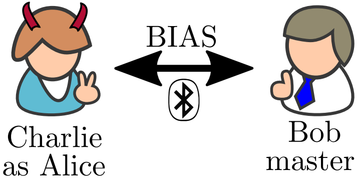


Charlie
as Bob

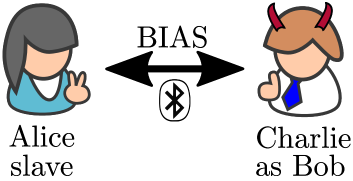
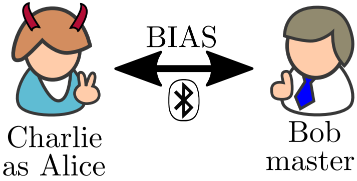
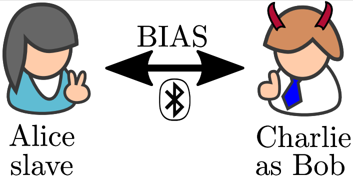
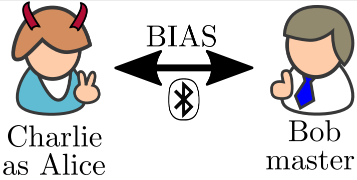
# BIAS Attacks on Bluetooth Session Establishment

| BIAS Attacks | Master Impersonation | Slave Impersonation |
|---|---|---|
| Legacy Secure Connections | | |
| Secure Connections | | |

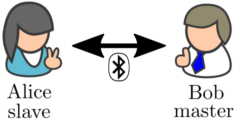
# BIAS Attacks on Bluetooth Session Establishment

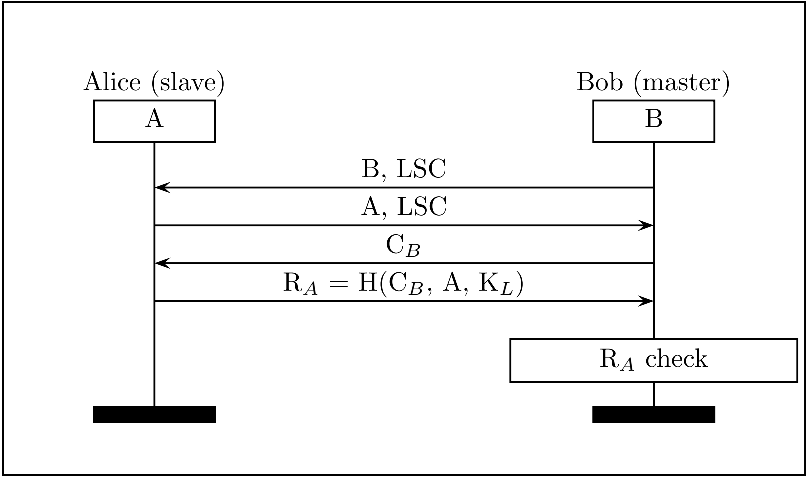
| BIAS Attacks | Master Impersonation | Slave Impersonation |
|---|---|---|
| Legacy Secure Connections | <br>Alice slave<br>BIAS<br>Charlie as Bob | <br>Charlie as Alice<br>BIAS<br>Bob master |
| Secure Connections | | |

# BIAS Attacks on Bluetooth Session Establishment

| BIAS Attacks | Master Impersonation | Slave Impersonation |
|---|---|---|
| Legacy Secure Connections | <br>BIAS<br>Alice slave<br>Charlie as Bob | <br>BIAS<br>Charlie as Alice<br>Bob master |
| Secure Connections | <br>BIAS<br>Alice slave<br>Charlie as Bob | <br>BIAS<br>Charlie as Alice<br>Bob master |

# Legacy Secure Connection (LSC) Authentication





Alice (slave)

Bob (master)

A

B

B, LSC

A, LSC

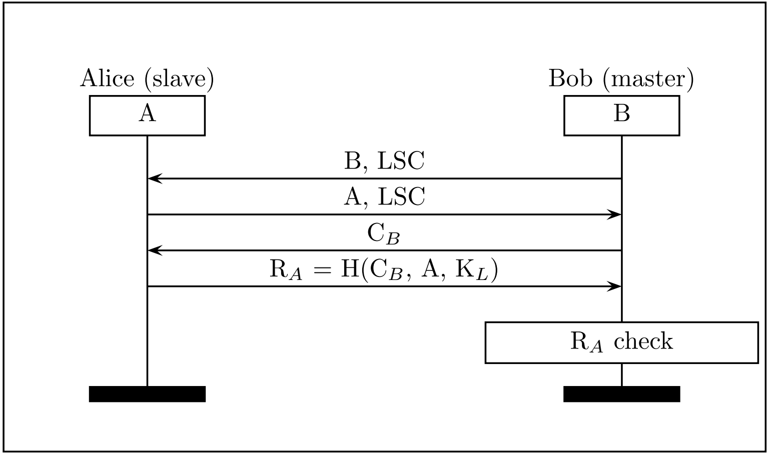
$C_B$

$R_A = H(C_B, A, K_L)$

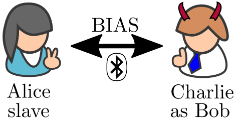
$R_A$ check

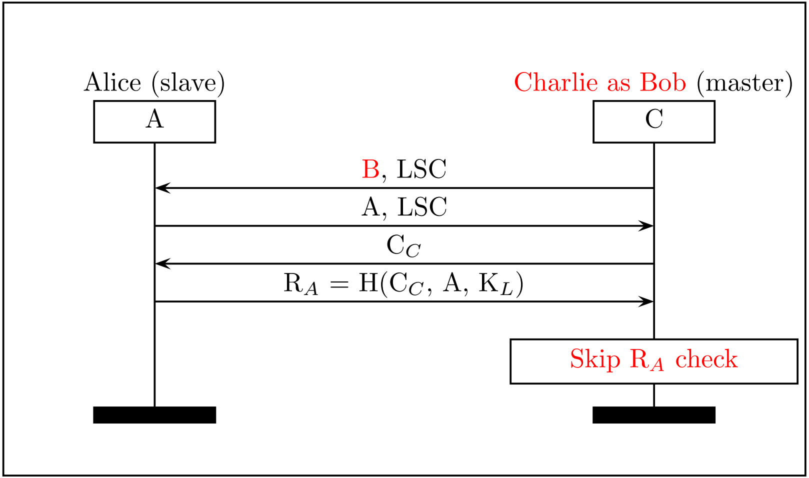
# Standard-Compliant Vulnerabilities in LSC Authentication

1. LSC authentication is **not used mutually** for session establishment
2. A device can **switch authentication role**



# BIAS Attack on LSC: Master Impersonation





Alice (slave)

Charlie as Bob (master)

A

C

B, LSC

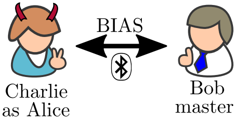
A, LSC

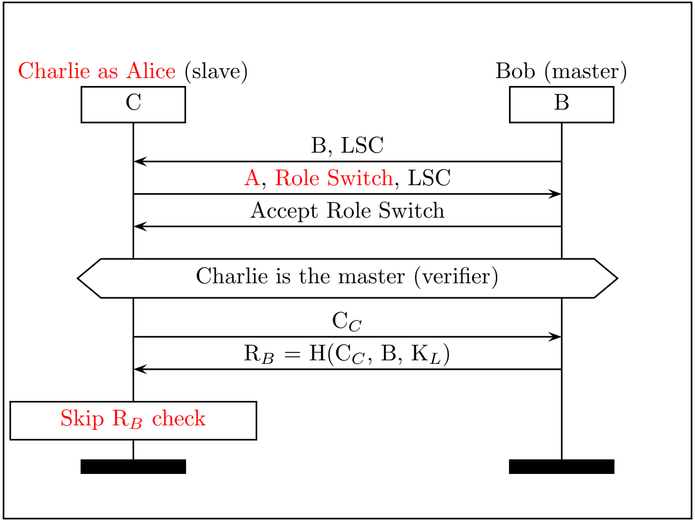
$C_C$

$R_A = H(C_C, A, K_L)$

Skip $R_A$ check

# BIAS Attack on LSC: Slave Impersonation





Charlie as Alice (slave) — C

Bob (master) — B

B, LSC

A, Role Switch, LSC

Accept Role Switch

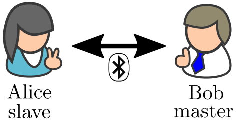
Charlie is the master (verifier)

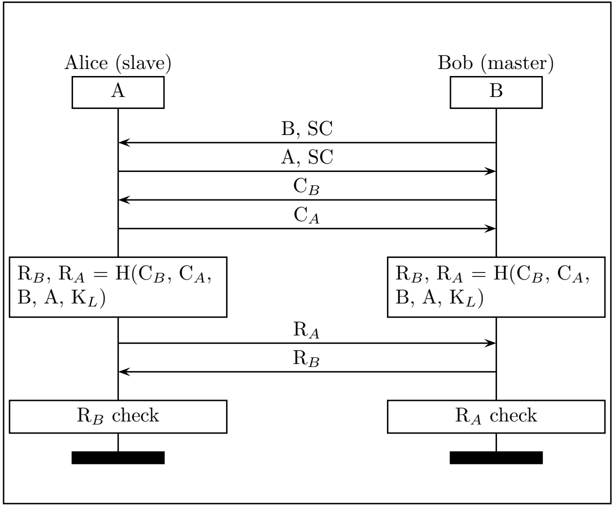
$C_C$

$R_B = H(C_C, B, K_L)$

Skip $R_B$ check

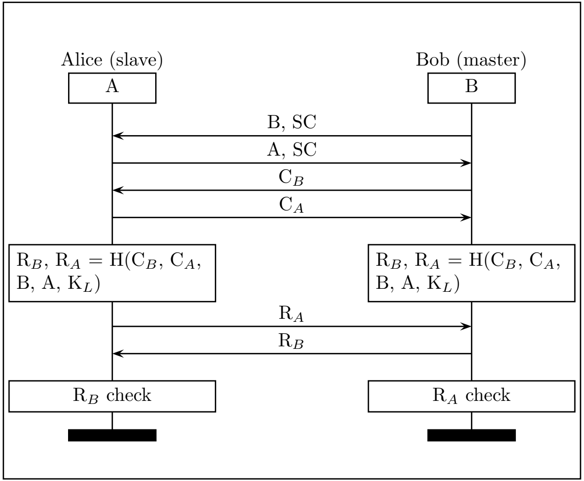
# Secure Connections (SC) Authentication



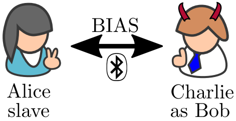

Alice (slave)
Bob (master)
A
B
B, SC
A, SC
$C_B$
$C_A$
$R_B$, $R_A$ = H($C_B$, $C_A$, B, A, $K_L$)
$R_B$, $R_A$ = H($C_B$, $C_A$, B, A, $K_L$)
$R_A$
$R_B$
$R_B$ check
$R_A$ check

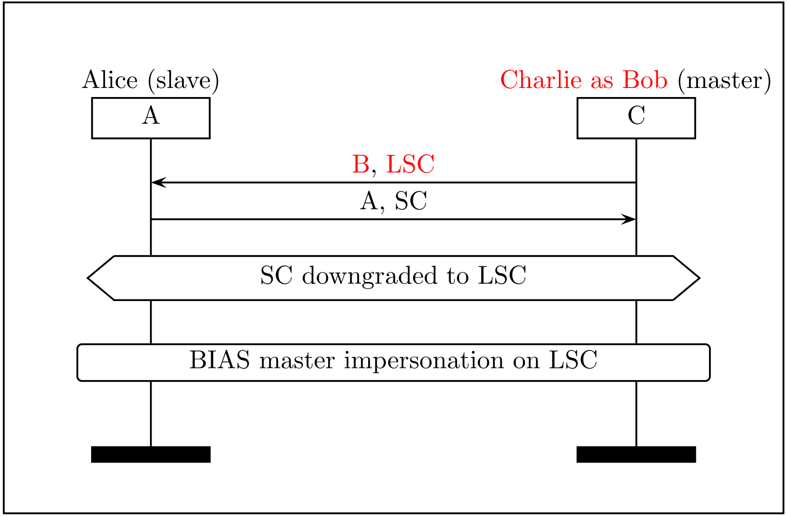
# Standard-Compliant Issues with SC Authentication

1. SC negotiation **is not integrity-protected**
2. SC support is **not enforced** for pairing and session establishment

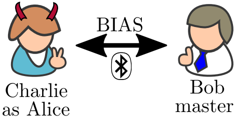

Alice (slave)
A
Bob (master)
B
B, SC
A, SC
$C_B$
$C_A$
$R_B$, $R_A$ = H($C_B$, $C_A$, B, A, $K_L$)
$R_B$, $R_A$ = H($C_B$, $C_A$, B, A, $K_L$)
$R_A$
$R_B$
$R_B$ check
$R_A$ check

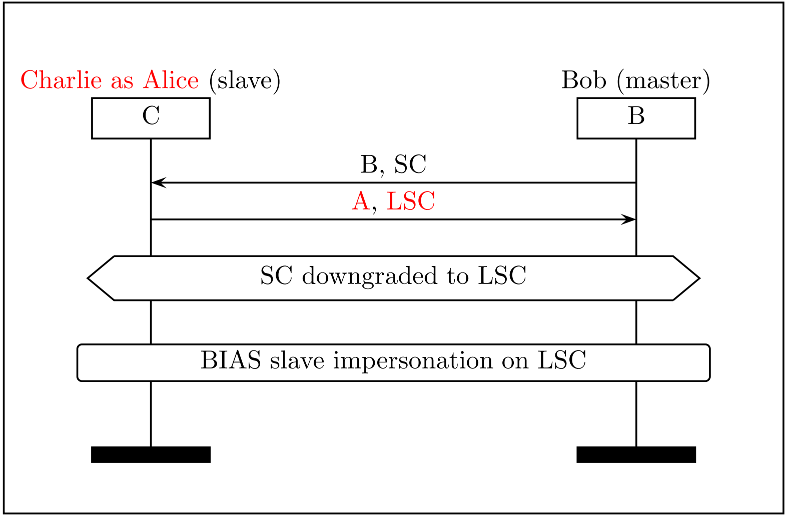
# BIAS Attack on SC: Master Impersonation





# BIAS Attack on SC: Slave Impersonation





Charlie as Alice (slave)

Bob (master)

C

B

B, SC

A, LSC

SC downgraded to LSC

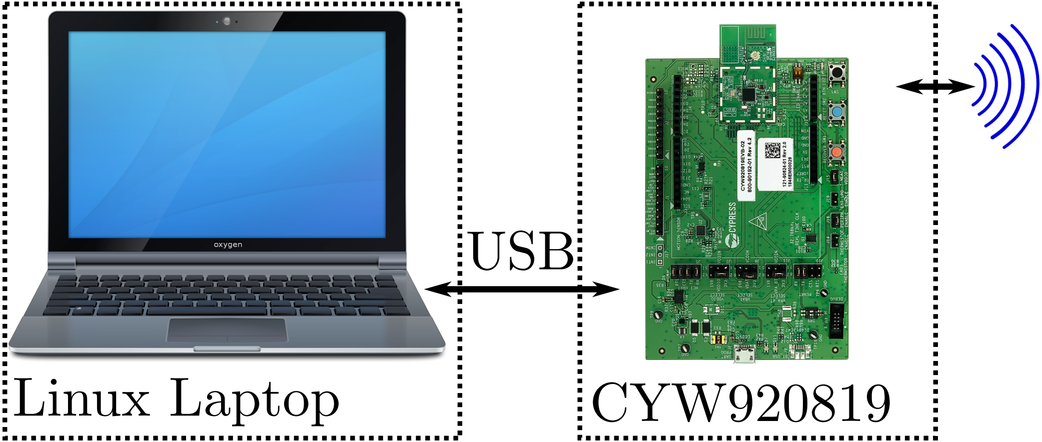
BIAS slave impersonation on LSC

# Very Secure Connections (VSC) ?!

- Let’s define Very Secure Connections (fictional security mode)
    - Use SC authentication (mutual)
    - Not vulnerable to SC downgrade

- Are we safe against impersonation attacks on VSC?
    - No, VSC is vulnerable to master and slave **reflection attacks**
    - See the paper for the details

# Implementation of the BIAS Attacks



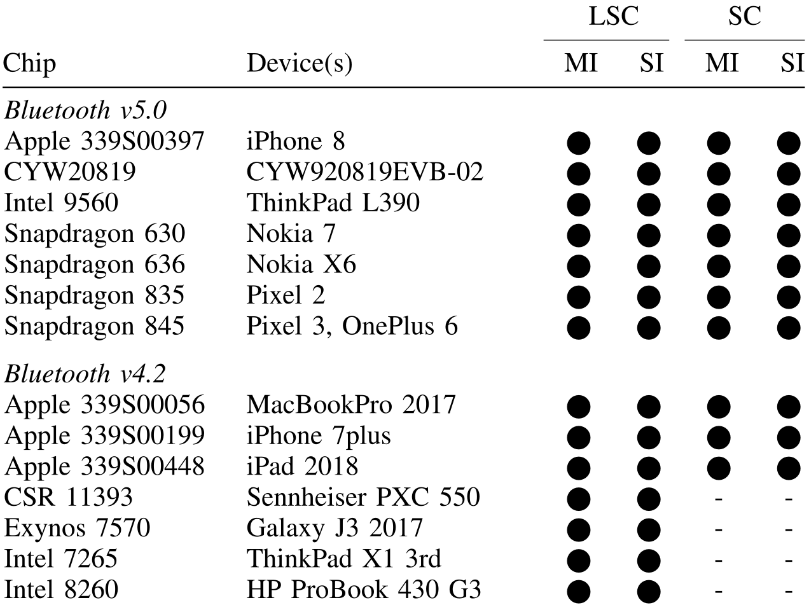
Linux Laptop

USB

CYW920819

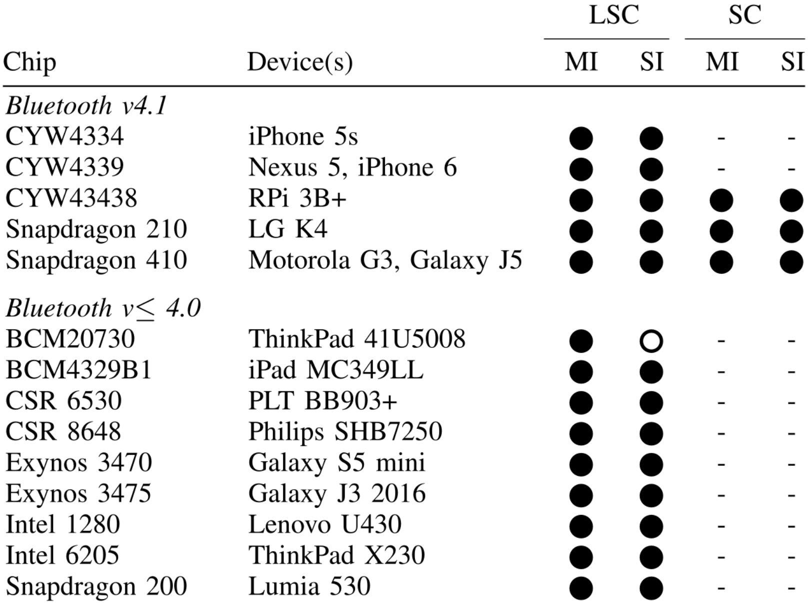
https://github.com/francozappa/bias

# Evaluation: BIAS Attacks on 31 Devices (28 BT Chips)



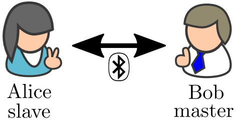
| Chip | Device(s) | LSC | | SC | |
|---|---|---|---|---|---|
| | | MI | SI | MI | SI |
| *Bluetooth v5.0* | | | | | |
| Apple 339S00397 | iPhone 8 | ● | ● | ● | ● |
| CYW20819 | CYW920819EVB-02 | ● | ● | ● | ● |
| Intel 9560 | ThinkPad L390 | ● | ● | ● | ● |
| Snapdragon 630 | Nokia 7 | ● | ● | ● | ● |
| Snapdragon 636 | Nokia X6 | ● | ● | ● | ● |
| Snapdragon 835 | Pixel 2 | ● | ● | ● | ● |
| Snapdragon 845 | Pixel 3, OnePlus 6 | ● | ● | ● | ● |
| *Bluetooth v4.2* | | | | | |
| Apple 339S00056 | MacBookPro 2017 | ● | ● | ● | ● |
| Apple 339S00199 | iPhone 7plus | ● | ● | ● | ● |
| Apple 339S00448 | iPad 2018 | ● | ● | ● | ● |
| CSR 11393 | Sennheiser PXC 550 | ● | ● | - | - |
| Exynos 7570 | Galaxy J3 2017 | ● | ● | - | - |
| Intel 7265 | ThinkPad X1 3rd | ● | ● | - | - |
| Intel 8260 | HP ProBook 430 G3 | ● | ● | - | - |

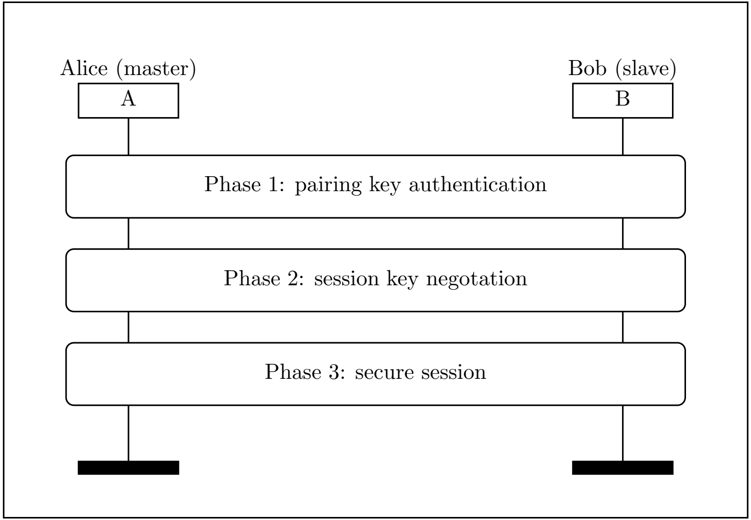
# Evaluation: BIAS Attacks on 31 Devices (28 BT Chips)



| | | LSC | | SC | |
|---|---|---|---|---|---|
| Chip | Device(s) | MI | SI | MI | SI |
| *Bluetooth v4.1* | | | | | |
| CYW4334 | iPhone 5s | ● | ● | - | - |
| CYW4339 | Nexus 5, iPhone 6 | ● | ● | - | - |
| CYW43438 | RPi 3B+ | ● | ● | ● | ● |
| Snapdragon 210 | LG K4 | ● | ● | ● | ● |
| Snapdragon 410 | Motorola G3, Galaxy J5 | ● | ● | ● | ● |
| *Bluetooth v≤ 4.0* | | | | | |
| BCM20730 | ThinkPad 41U5008 | ● | ○ | - | - |
| BCM4329B1 | iPad MC349LL | ● | ● | - | - |
| CSR 6530 | PLT BB903+ | ● | ● | - | - |
| CSR 8648 | Philips SHB7250 | ● | ● | - | - |
| Exynos 3470 | Galaxy S5 mini | ● | ● | - | - |
| Exynos 3475 | Galaxy J3 2016 | ● | ● | - | - |
| Intel 1280 | Lenovo U430 | ● | ● | - | - |
| Intel 6205 | ThinkPad X230 | ● | ● | - | - |
| Snapdragon 200 | Lumia 530 | ● | ● | - | - |

# BIAS + KNOB: Break Bluetooth Session Establishment





Alice (master)

A

Bob (slave)

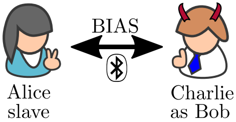
B

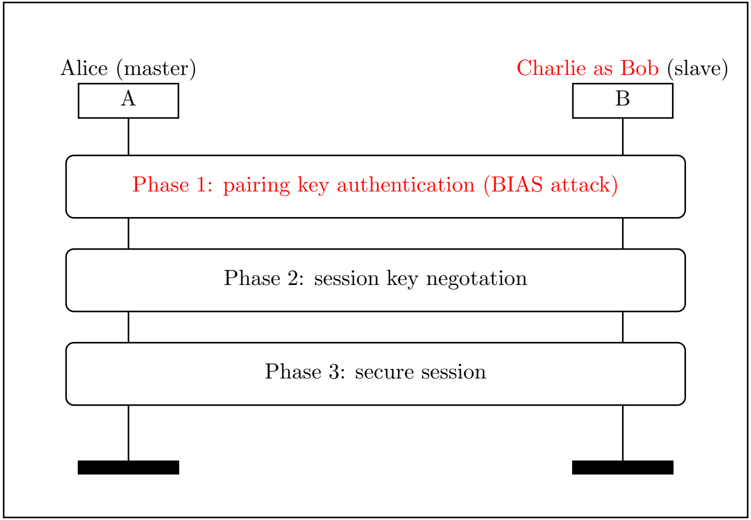
Phase 1: pairing key authentication

Phase 2: session key negotation

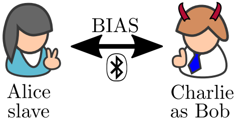
Phase 3: secure session

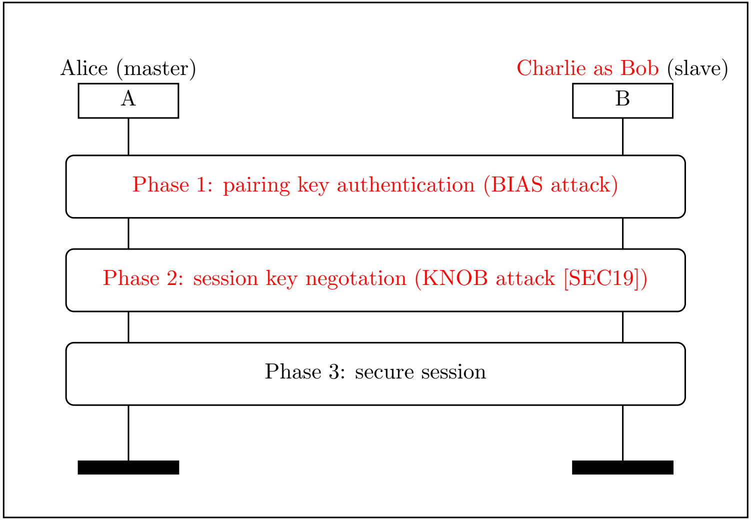
# BIAS + KNOB: Break Bluetooth Session Establishment




Alice (master)
Charlie as Bob (slave)
A
B
Phase 1: pairing key authentication (BIAS attack)
Phase 2: session key negotation
Phase 3: secure session

# BIAS + KNOB: Break Bluetooth Session Establishment





Alice (master)

Charlie as Bob (slave)

A

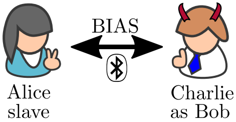
B

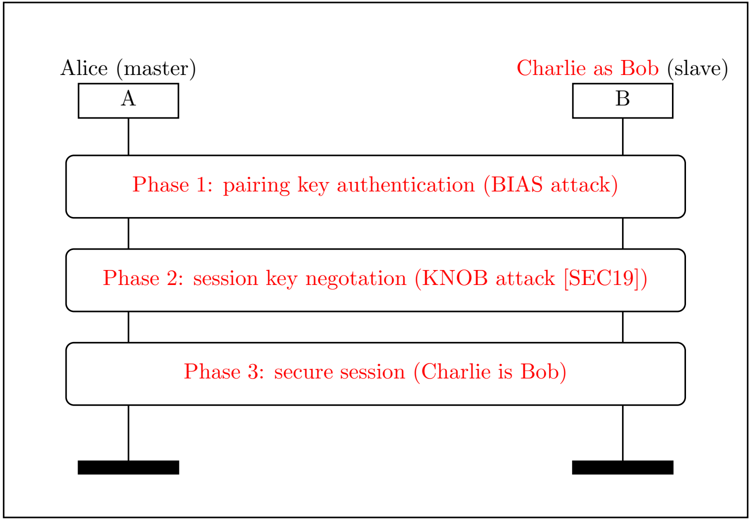
Phase 1: pairing key authentication (BIAS attack)

Phase 2: session key negotiation (KNOB attack [SEC19])

Phase 3: secure session

# BIAS + KNOB: Break Bluetooth Session Establishment





Alice (master)

Charlie as Bob (slave)

A

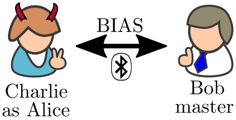
B

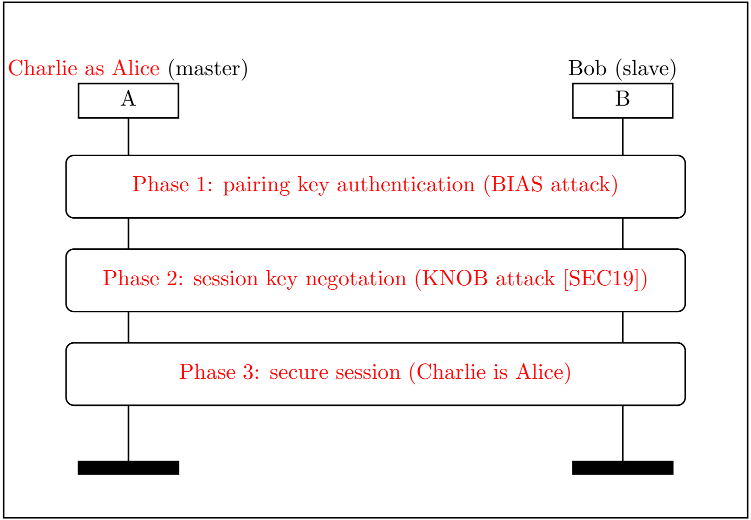
Phase 1: pairing key authentication (BIAS attack)

Phase 2: session key negotation (KNOB attack [SEC19])

Phase 3: secure session (Charlie is Bob)

# BIAS + KNOB: Break Bluetooth Session Establishment





Charlie as Alice (master)

Bob (slave)

A

B

Phase 1: pairing key authentication (BIAS attack)

Phase 2: session key negotiation (KNOB attack [SEC19])

Phase 3: secure session (Charlie is Alice)

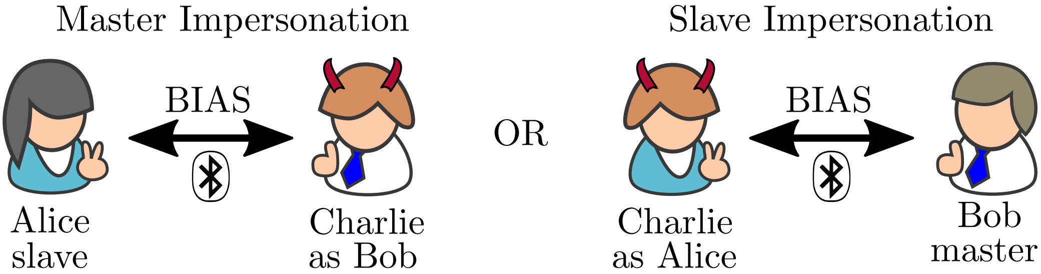
# BIAS Attacks Countermeasures and Disclosure

- We propose a set of countermeasures
  - Use LSC authentication **mutually** during session establishment
  - **Integrity-protect** session establishment with the pairing key
  - **Enforce SC support** across pairing and session establishment

- We disclosed the BIAS attacks, and the Bluetooth standard has been updated
  - However, most of the devices are still vulnerable
  - E.g., no user or device updates, no device recalls

# Conclusion: Bluetooth Impersonation AttackS (BIAS)

- **Bluetooth Impersonation AttackS (BIAS)**
  - Exploiting standard-compliant vulnerabilities in Bluetooth authentication
  - To impersonate any Bluetooth device without having to authenticate
  - Website: `https://francozappa.github.io/about-bias/`
  - Code: `https://github.com/francozappa/bias`



Master Impersonation

Alice
slave

BIAS

Charlie
as Bob

OR

Slave Impersonation

Charlie
as Alice

BIAS

Bob
master