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

Anonymous Submission #129

Abstract

The Bluetooth standard specifies two incompatible wireless transports: Bluetooth Classic (BT) for high-throughput services and Bluetooth Low Energy (BLE) for very low-power services. Despite the similarity in name and use of similar security mechanisms, BT and BLE have different security architectures and threat models. In particular, pairing enables two devices to establish a long term key to secure the communication. Two devices have to pair over BT and BLE to use both transports securely. Since pairing the same devices twice is considered "user-unfriendly", Bluetooth v4.2 introduced Cross-Transport Key Derivation (CTKD). CTKD allows two devices to pair once, either over BT or BLE, and generate both BT and BLE long term keys. Despite CTKD allowing traversal of the security boundary between BT and BLE, the security implications of CTKD have not yet been investigated.

We present the first security analysis of CTKD and identify five cross-transport issues at the Bluetooth specification level. These issues enable, for the first time, exploitation of both BT and BLE by attacking either transport. Based on the identified issues, we demonstrate four novel cross-transport attacks resulting in device impersonation, traffic manipulation, and malicious session establishment. We refer to them as BLUR attacks, as they blur the security boundary between BT and BLE. The BLUR attacks are standard-compliant and therefore apply to all devices supporting CTKD, regardless of implementation. We successfully demonstrate the BLUR attacks on 13 devices with 10 unique Bluetooth chips, and discuss effective countermeasures. We disclosed our findings and countermeasures to the Bluetooth SIG in May 2020.

1 Introduction

Bluetooth is a pervasive wireless technology used by billions of devices including mobile phones, laptops, headphones, cars, speakers, medical, and industrial appliances [12]. Bluetooth is specified in an open standard maintained by the Bluetooth special interest group (SIG). The latest version of the standard is 5.2 [11]. The standard specifies two different, incompatible wireless transports, Bluetooth Classic (BT) and Bluetooth Low Energy (BLE). BT is best suited for high-throughput use cases, such as streaming audio and voice calls, while BLE is best suited for very low-power use cases such as localization and monitoring.

As BT and BLE were introduced at different points in time to address different use cases, the standard maintains *separate security architectures and threat models* for BT [11, p. 947] and BLE [11, p. 1617]. While these security architectures address different threat models, they use similar security mechanisms, including pairing and secure session establishment. Pairing enables devices to establish a shared long term key, and secure session establishment enables paired devices to establish a secure communication channel by negotiating a session key that is derived from the pairing long term key.

Devices that support both BT and BLE have to pair twice to use both transports securely. Bluetooth v4.2 (released in 2014) introduced *Cross-Transport Key Derivation (CTKD)* to mitigate the "user-unfriendly" requirement to pair the same devices twice. After pairing on one transport, CTKD allows the creation of a second long term key for the other transport [11, p. 1401]. For example, two devices can pair over BT, generate the BT long term key, and then run CTKD to derive the BLE long term key (without having to pair over BLE). All major Bluetooth software stacks (Apple, Linux, Android, and Windows) and hardware providers (Cypress, Intel, Qualcomm, Broadcom, Apple, Sony, and Bose) implement CTKD. Apple presented CTKD as a core "always on" Bluetooth feature to improve usability [42].

We present the first security analysis of CTKD, uncovering five standard-compliant security issues. Those issues are the first examples of cross-transport vulnerabilities for Bluetooth. Based on our findings, we demonstrate four cross-transport attacks, enabling device impersonation, traffic interception, and traffic manipulation, as well as unintended device sessions. Our attacks enable BT and BLE cross-transport exploitation, are standard-compliant and likely affect all devices supporting CTKD. We name our attacks BLUR attacks, as by exploiting

CTKD they blur the security boundary between BT and BLE.

In contrast to previously published attacks on BT and BLE [1, 3, 4, 10, 21, 22, 35, 37, 38, 41, 43], our attacks do not require the attacker to be present during pairing or secure session establishment. Therefore, our attacks have lower requirements for the attacker while still breaking BT and BLE security guarantees.

We implement the BLUR attacks using a widely available Bluetooth development board connected to a laptop running Linux and developing custom software based on open-source tools. This makes reproducing the BLUR attacks simple and affordable. Our evaluation demonstrates that all tested devices are vulnerable. We will release our tools to the public after the responsible disclosure process completes. We use our attack implementation to evaluate 13 devices, with 10 unique Bluetooth chips, from the major hardware and software vendors, e.g., Broadcom, Cambridge Silicon Radio (CSR), Cypress, Google, Intel, Linux, Qualcomm, and Windows and representing all Bluetooth versions that support CTKD (i.e., 4.2, 5.0, and 5.1) and even a device supporting Bluetooth version 4.1 to which CTKD has been backported.

We summarize our contributions as follows:

- We perform the first security analysis of CTKD (Section 3), and show that it enables crossing the security boundary between BT and BLE. We identify five novel and very serious issues, enabling cross-transport attacks between BT and BLE.

- We propose four attacks to exploit the issues in CTKD (Section 4). Our attacks allow impersonation, interception, traffic manipulation, and unintended sessions. In Section 5, we present a low-cost implementation of the attacks based on a Linux laptop and a Bluetooth development board.

- We confirm that real-world BT and BLE devices are vulnerable to the BLUR attacks by evaluating our attacks on 13 unique devices (Section 6). We provide concrete countermeasures to fix the presented issues.

We disclosed our findings and countermeasures to the Bluetooth SIG in May 2020. The Bluetooth SIG acknowledged our findings and assigned CVE-2020-15802 to the BLUR attacks. In September 2020, the Bluetooth SIG released a security note about our report at https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/bluetooth-security/blurtooth/ (without contacting us).

2 Background

We now compare BT and BLE, and introduce CTKD.

2.1 A Comparison of BT and BLE

BT and BLE are two wireless transports specified in the Bluetooth standard. These transports are incompatible (i.e., while they use the same 2.4 GHz band the physical and link layers are different) and are designed to complement each other. BT is used for high-throughput and connection-oriented services, such as streaming audio and voice. BLE is used for very low-power and low-throughput services such as localization and monitoring. Typically, high-end devices, such as laptops, smartphones and tablets, provide BT and BLE (in a single radio chip), while low end devices such as mice, keyboards and wearables provide either BT or BLE.

BT and BLE have similar security mechanisms but different security architectures and threat models. Both transports provide a pairing mechanism, named Secure Simple Pairing (SSP), to let two devices establish a long term key. During pairing, BLE allows negotiating the entropy of the long term key while BT does not. Both transports provide a secure session establishment mechanism to derive a session key from the long term key and protect the communication. During session establishment, BT allows negotiating the entropy of the session key while BLE inherits the entropy of the session key from the entropy of the long term key.

BT and BLE support a "Secure Connections" mode that uses FIPS compliant security primitives such as AES-CCM for authenticated encryption, Elliptic-Curve Diffie-Hellman (ECDH) over P-256 for key agreement, mutual authentication procedures for the long term key, and AES-CMAC for keyed hashing. BT and BLE have similar association procedures that can be used to protect the pairing phase against man-in-the-middle attacks. Two examples of associations are "Just Works" that provides no protection and "Numeric Comparison" that provides protection against man-in-the-middle attacks by requiring user interaction (e.g., the user has to manually confirm that she sees the same numeric code on the pairing devices).

BT and BLE define master and slave roles in different ways. For BT, the master is the connection initiator, the slave is the connection responder, and roles can be switched. Both master or slave can request a role switch almost anytime after a radio link between the two is established. For BLE, master and slave roles are fixed and switching roles is not supported. The master acts as the connection initiator (BLE central) and the slave as the connection responder (BLE peripheral). High-end BLE devices, such as laptops and smartphones, implement both master and slave modes and are typically used as the master, while low-end devices, such as fitness trackers or smartwatches, typically implement only the slave mode.

2.2 Cross-Transport Key Derivation (CTKD)

Two devices that support BT and BLE have to pair over BT and over BLE to use both transports securely. Pairing the same two devices twice is considered "user-unfriendly" and the

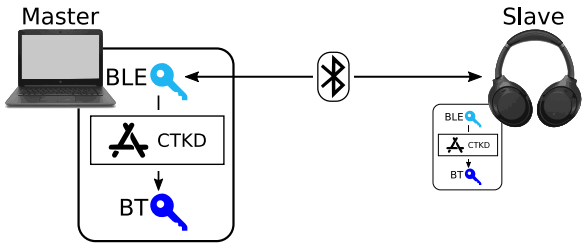

Figure 1: CTKD overview. CTKD is used by two devices who paired and share a long term key over BLE to derive a long term key for BT. CTKD can also be used to derive BLE pairing keys after two devices paired over BT.

Bluetooth standard version 4.2 (released in 2014) introduces CTKD to address this issue. As shown in Figure 1, CTKD enables two devices to pair once, either over BT or BLE, and then securely use both [11, p. 280]. For example, a user can pair a headset and a laptop over BLE, without putting the headset in BT discoverable mode, and then securely connect the headset and the laptop over BT (without having to pair over BT). It is also possible to do the initial pairing over BT, and use CTKD to generate the BLE pairing key.

Before explaining CTKD, it is important to review the differences between *pairable (bondable)* and *discoverable* states for BT and BLE. If a device is *pairable* then it will accept pairing requests from other devices. If if it is *discoverable* it will reveal its identity when other devices scan for nearby devices. Contrary to popular belief, a device is not required to be both discoverable and pairable for pairing but it only needs to be pairable. The device that initiates pairing only needs to know the identity (MAC address) of the pairable target device. For example, when pairing a laptop with headphones over BT, typically only the headphones are discoverable and pairable while the laptop is only pairable. Hence, it is possible to pair with a device even if it is not discoverable [40].

The Bluetooth standard specifies the same CTKD function to derive BT and BLE long term keys. This function takes as inputs a 128-bit (16-byte) key and two 4-byte strings and derives a 128-bit (16-byte) key using AES-CMAC (see Section 5.3 for CTKD's internals). CTKD for BT derives a BLE long term key (K_{BLE}) from a BT long term key (K_{BT}) and the strings "`tmp2`" and "`brle`", while CTKD for BLE derives K_{BT} from K_{BLE} and the strings "`tmp1`" and "`lebr`". As the standard defines constant strings and no fresh nonces as inputs, the CTKD function derives the same output key when reusing the same input key.

CTKD is broadly supported by, e.g., Apple [42], Google [5], Cypress [14], Linux [13], Qualcomm [33], and Intel [23]. CTKD is combined with "Secure Connections", a security mode that was introduced to enhance the security primitives of BT and BLE without affecting their security mechanisms. For example, "Secure Connections" introduces AES-CCM authenticated-encryption for BT, and ECDH pairing for BLE.

3 Security Analysis of CTKD

To analyse the security of CTKD we introduce our system and attacker models and we describe how CTKD is used in a non adversarial setting. We then introduce the security issues that we discovered with CTKD. These security issues are then exploited by our attacks in Section 4 and addressed with concrete fixes in Section 7.2.

3.1 System Model

Our system model considers two victims, Alice and Bob, who want to securely communicate over BT and BLE. Alice and Bob support CTKD and during pairing and session establishment select the strongest security mechanisms: Secure Simple Pairing (SSP), "Secure Connections", and "Numeric Comparison". Those security procedures are expected to protect Alice and Bob against impersonation, eavesdropping, and man-in-the-middle attacks on BT and BLE [11, p. 269]. After completing pairing, Alice and Bob can run secure sessions over BT and/or BLE. Without loss of generality, we assume that Alice is the BT and BLE master and Bob is the BT and BLE slave. Note that we follow the Bluetooth specification of using the terms master/slave instead of more apt terms like leader/follower.

Regarding the notation, we indicate a BT pairing key with K_{BT}, a BT session key with SK_{BT}, a BLE pairing key with K_{BLE}, a BLE session key with SK_{BLE}. Moreover, we indicate a Bluetooth address with ADD, a public key with PK, a private key with SK, a shared Diffie-Hellman secret with DK, a nonce with N, and a message authentication code with MAC.

3.2 Attacker Model and Goals

Our attacker model considers Charlie, a remote attacker in Bluetooth range with Alice and Bob. The attacker aims to compromise the secure BT and BLE sessions between the victims without tampering with their devices. The attacker's knowledge is limited to what Alice and Bob advertise over the air, e.g., full or partial Bluetooth addresses, Bluetooth names, authentication requirements, IO capabilities, and device classes.

The attacker does not know any key shared between Alice and Bob and is not present while they pair or establish secure sessions. The attacker can scan and discover BT and BLE devices, jam the Bluetooth channel, pair with Alice and Bob CTKD, propose weak association mechanisms (e.g., "Just Works"), and dissect and craft unencrypted Bluetooth packets.

The attacker has four goals. The first goal is to impersonate Alice (to Bob) and take over Alice's secure sessions. The second intent is to impersonate Bob (to Alice) and take over Bob's secure sessions. Alice and Bob' impersonations are different goals as they require different attack techniques (i.e., Bluetooth master and slave impersonation attacks). The third

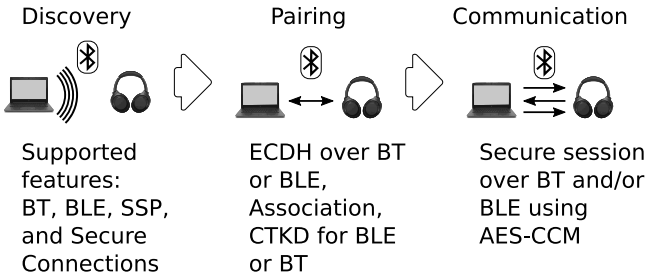

Figure 2: The three phases of the CTKD life cycle: Discovery (to exchange features), Pairing (to agree on a pairing key and, through CTKD, create a pairing key for the other transport), and Communication (to establish secure sessions on BT and/or BLE).

objective is to establish a man-in-the-middle position in a secure session between Alice and Bob and requires combining and synchronizing the impersonation attacks on Alice and Bob. The fourth goal is to pair and establish unintended and possibly stealthy sessions with Alice or Bob as an arbitrary device, without breaking existing pairings and secure sessions between Alice and Bob.

3.3 CTKD Life Cycle

We first demonstrate the CTKD life cycle in a non-adversarial setting to later highlight the CTKD issues (Section 3.4) and attacks (Section 4). The first phase of the CTKD life cycle is *Discovery*, see Figure 2. During Discovery, Alice and Bob find each other and exchange their capabilities (e.g., Alice scans while Bob is advertising his presence). During this phase Alice and Bob declare BT, BLE, SSP, and Secure Connections support. Note that the Bluetooth standard does not include CTKD support as a separate feature but it is implicitly activated by declaring BT, BLE, SSP, and Secure Connections.

After Discovery, Alice and Bob initiate *Pairing* that can be performed either over BT or BLE. As a result of pairing Alice and Bob establish a secret pairing key (e.g., K_{BLE} or K_{BT}) using SSP with Secure Connections. In particular, this pairing mode uses ECDH to generate a shared secret and a key derivation function that generates the pairing key using as inputs the shared secret, Alice and Bob' ADD, and two nonces. Once Alice and Bob share a pairing key, then they complete a Bluetooth association phase. There are different association mechanism and in our threat model we assume that Alice and Bob use a strong mechanism (e.g., Alice and Bob generate the same numeric sequence and the user confirms those).

After association is completed, Alice and Bob run the CTKD key derivation function to compute a second pairing key for the transport that was not used while pairing (e.g., derive K_{BT} from K_{BLE}or vice versa). The Bluetooth standard provides a CTKD function that is deterministic, as it uses a pairing key and constant strings (e.g., `"brle"` or `"lebr"`) as inputs [11, p. 1401]. Moreover, the Bluetooth standard does not require to exchange any packet over the air to signal when CTKD is used and the outcome of its usage.

As soon as Alice and Bob complete Pairing they start the *Communication* phase. During this phase Alice and Bob establish secure sessions over BT and/or BLE. Each session derives a fresh session key from the correspondent pairing key and session nonces (e.g., SK_{BT} from K_{BT}, and SK_{BLE} from K_{BLE}), and uses the session key to encrypt and integrity-protect the link layer traffic with AES-CCM.

CTI	Name	Phase	Summary
1	Roles	Discovery	Role asymmetries
2	Sec. Conn.	Discovery	No Secure Connections
3	Association	Pairing	No uniform association
4	Key Overw.	Pairing	Overwrite pairing keys
5	States	Comm.	Pairable over BT and BLE

Table 1: Cross-transport issues (CTIs) with CTKD. The issues are at the Bluetooth specification level. SC abbreviates Secure Connections and KO abbreviates Key Overwrite.

3.4 Cross-Transport Issues with CTKD

CTKD is an interesting attack surface for several reasons. CTKD crosses the security boundary between BT and BLE. Therefore, a CTKD vulnerability is exploitable for both BT and BLE. As CTKD bridges BT and BLE, an attacker can exploit known vulnerabilities on BT to exploit BLE and vice versa. As CTKD is an optional feature and is transparent to the user, an attack exploiting CTKD is hard to detect. As CTKD requires Secure Connections support, an attacker can break the most secure BT and BLE modes by targeting CTKD.

Despite the listed reasons, the Bluetooth standard does not provide a security analysis of CTKD and does not include CTKD in the BT and BLE threat models [11, p. 1401]. As a result, CTKD remains an unexplored attack surface and in this work, we address this concern by performing the first security analysis of CTKD. Our analysis uncovers five cross-transport issues (summarized in Table 1). We now describe each issue in detail by using the CTKD life cycle phases presented in Section 3.3.

CTI 1: Roles (Discovery) During Discovery, Alice and Bob can discover each other and trigger Pairing both over BT and BLE. This is a consequence of CTKD as it enables more ways to pair devices with less user interaction. Alice, as master, is expected to send pairing requests over BT or BLE to Bob, and the user expects to pair Alice and Bob by discovering Bob on Alice's screen and sending a pairing request to Bob. However, BT master and slave roles are not fixed

(unlike BLE) and Alice can receive pairing requests over BT. The attacker can take advantage of this role asymmetry to impersonate a slave device that is already trusted by Alice and send a ***pairing request*** to Alice over BT even if Alice is expecting to receive only BT and BLE ***pairing responses***.

CTI 2: Secure Connections (Discovery) During Discovery, Alice and Bob exchange their capabilities before starting the pairing process. To use CTKD they declare "Secure Connections" support for the transport used for pairing. However, the specification does not specify if CTKD support requires "Secure Connections" support only for the pairing transport or for both transports. From our experiments, we find that CTKD is used when "Secure Connections" is only supported by the pairing transport. This issue considerably increases the CTKD attack surface, as an attacker is not limited to target only devices which support BLE ***and*** BT "Secure Connections" but can also target devices that support BLE ***or*** BT "Secure Connections".

CTI 3: Association (Pairing) During Pairing, Alice and Bob can pair either over BT or BLE. While BT and BLE pairings use different protocols they both include an association phase. The issue is that CTKD does not *enforce the chosen association mechanism across BT and BLE*. This issue can be exploited by the attacker to pair with a weak association mechanism, such as "Just Works", on one transport while the other transport expects a strong association mechanism, such as "Numeric Comparison". This is especially dangerous in case of impersonation attacks because the user is not going to notice an attacker that is re-pairing using "Just Works" pretending to be a trusted device.

CTI 4: Key Overwrite (Pairing) During Pairing, Alice and Bob use CTKD to derive a second pairing term key for the transport not used for pairing. If Alice and Bob already shared a long term key for such transport *CTKD will overwrite the existing pairing key*. This is an issue because an attacker who is impersonating either Alice or Bob can use CTKD to overwrite long term keys. For example, if Alice and Bob are running a secure session over BT then the attacker can pair with Bob over BLE while impersonating Alice and overwrite the BT key that is shared by Alice and Bob.

CTI 5: States (Communication) During Communication, Alice and Bob establish secure sessions over BT and/or BLE. In our experiments, we observed that Alice and Bob *remain pairable over BT and BLE*. Bob also *remains discoverable over BLE*. This is not the case without CTKD where a device is pairable and optionally discoverable only on one transport. This issue gives the attacker more options to discover and pair with victim devices. For example, the attacker can pair on the transport that is not currently in use by Alice and Bob. Furthermore, in some CTKD use cases one transport is supposed to be used only for pairing and deriving keys for the other. Hence, that transport is always in a pairable state but never used after pairing. This enables the attacker to establish unintended malicious sessions on both transports by pairing on the unused one and forcing CTKD.

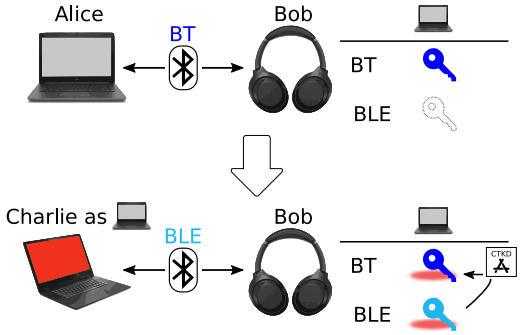

Figure 3: BLUR impersonation attack strategy. Charlie pairs with Bob over one transport (e.g., BLE) and (over)writes the pairing keys for both transports, including Alice's BT pairing key.

4 BLUR Attacks on CTKD

We now design four novel CTKD cross-transport attacks based on the five cross-transport issues that we discuss in Section 3.4. We provide the first attacks that exploit CTKD, blurring the security boundary between BT and BLE. Our attacks are standard-compliant and enable impersonation, interception, and manipulation of traffic between victims, as well as unintended sessions with a victim device. We call our attacks *BLUR attacks*.

4.1 Master and Slave Impersonation

Figure 3 presents the BLUR impersonation attack strategy Before the attack takes place Alice and Bob (the victims) are running a secure BT session and they share a BT long term key (K_{BT}). As a side effect of CTKD, Alice and Bob are pairable on BLE. Charlie (the attacker), targets BLE (which is not used by the victims) and pairs with Bob over BLE as Alice and triggers CTKD, while the real Alice is communicating with Bob over BT. Because of CTKD, Charlie forces Bob to overwrite the BT pairing key that he established with Alice with his own. As a result, Charlie takes over Alice's BT session from BLE. The real Alice can no longer connect to Bob as she does not possess the correct K_{BT} and can attempt to re-pair with Bob only when Charlie terminates his BT session with Bob. Charlie uses the described attack strategy to perform master and slave impersonation attacks as follows:

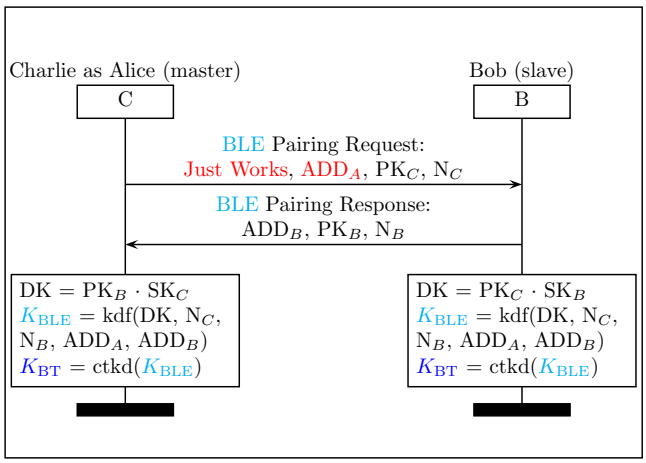

Figure 4: Master impersonation attack and takeover. Charlie (acting as master) pairs with Bob over BLE, overwriting Alice's key.

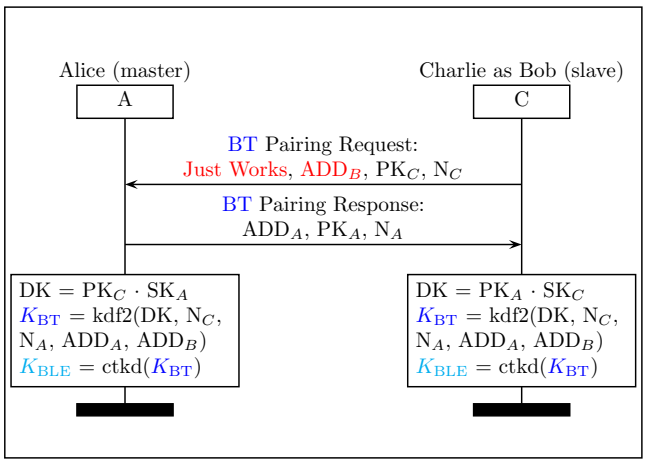

Figure 5: Slave impersonation attack and takeover. Charlie (acting as slave) sends a BT pairing request to Alice (master) as Bob, overwriting Bob's key.

Master impersonation Charlie impersonates Alice (master) and takes over her BT secure session with Bob as in Figure 4. Charlie discovers Bob as he is pairable over BLE and sends a BLE pairing request using Alice's Bluetooth address (ADD$_A$), Secure Connections support (to trigger CTKD), and "Just Works" association to avoid user interaction. Charlie's BLE pairing request does not collide with the BT traffic exchanged by Alice and Bob as BT and BLE use different physical layers and link layers.

Bob sends Charlie a BLE pairing response believing that Alice wants to pair (or re-pair) over BLE using CTKD. Charlie and Bob use the exchanged public keys to compute DK. Then they use DK and the exchanged nonces (N*C*, N*B*) to compute K$_{BLE}$. Then, they locally compute K$_{BT}$ from K$_{BLE}$ using the CTKD's key derivation function (ctkd). As a result of the master impersonation attack, Charlie forces Bob to overwrite the BT pairing key that he established with Alice with his BT pairing key, establishes a BLE pairing key with Bob, and takes over Alice's BT session.

Slave impersonation Charlie impersonates Bob (slave) and takes over his BT secure session with Alice as in Figure 5. In this case Charlie has to wait until the secure BT session between Alice and Bob is interrupted (e.g., by running a master impersonation attack against Bob). Then Charlie can exploit role asymmetries between BT and BLE by sending a BT pairing request to Alice who is typically expecting pairing responses either over BT or BLE. Charlie's pairing request include Secure Connections support (to trigger CTKD), Bob's Bluetooth address (ADD$_B$) and "Just Works" association to avoid user interaction.

Alice, who is pairable over BT, sends a BT pairing response believing that Bob wants to re-pair over BT using CTKD. Charlie and Alice use the exchanged public keys to compute DK. Then they use DK and the exchanged nonces to derive K$_{BT}$(kdf2). Then they locally derive K$_{BLE}$ from K$_{BT}$ using CTKD's key derivation functions (ctkd). As a result of the slave impersonation attack, Charlie forces Alice to overwrite the BT pairing key that she established with Bob with his BT key, shares a BLE key with Alice, and takes over Bob's BT session. Bob cannot re-establish secure sessions with Alice as he no longer possesses the correct pairing keys.

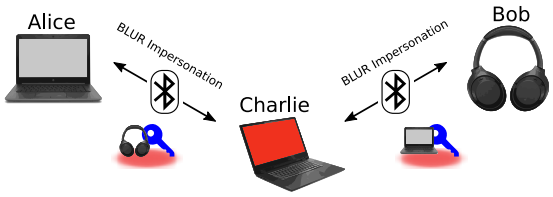

Figure 6: BLUR man-in-the-middle attack. The attacker uses the BLUR Impersonation attack against two devices that were previously paired. The two devices do not detect a change but Charlie now has access to all traffic.

As summarized in Table 2, the master impersonation attack takes advantage of all the cross-transport issues that we present in Section 3.4 except CTI 1. In particular, the attacker takes advantage of non-consistent "Secure Connections" support (CTI 2), lack of consistency between BT and BLE association methods (CTI 3), more opportunities to pair (CTI 5), and key overwriting (CTI 4). The slave impersonation attack takes advantage of all CTIs except CTI 5, including the role asymmetries between BT and BLE (CTI 1).

4.2 Man-in-the-Middle

Figure 6 presents the high-level description of our BLUR man-in-the-middle attack. As in the previous section, Alice and Bob are paired over BT and they run a secure session over BT.

	CTI 1 Roles	CTI 2 Sec. Conn.	CTI 3 Assoc.	CTI 4 Key Overw.	CTI 5 States
Master Imp.	x	✓	✓	✓	✓
Slave Imp.	✓	✓	✓	✓	x
MitM	✓	✓	✓	✓	✓
Unin. Sess.	x	✓	x	x	✓

Table 2: Mapping the requirements of our four BLUR attacks to the discovered cross-transport issues (CTI).

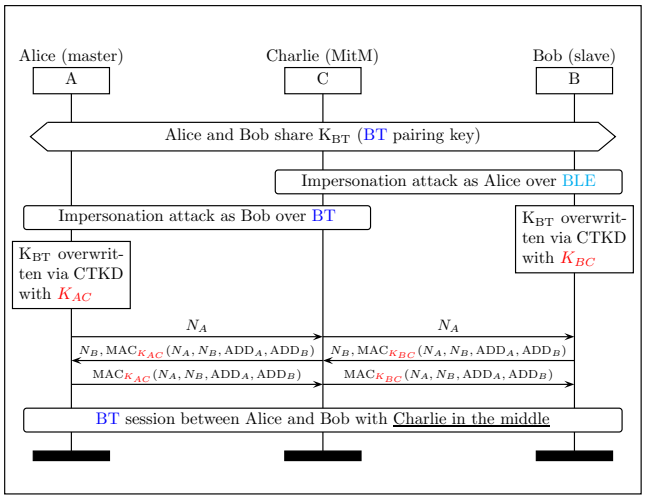

Figure 7: MitM attack and takeover. Charlie impersonates Alice as in Figure 4, impersonates Bob as in Figure 5, let the victims mutually authenticate and then gets access to their traffic.

During this attack, Charlie sequentially performs the master and slave impersonation attacks described in Section 4.1. As a result, the attacker overwrites Alice and Bob's BT pairing keys with known keys, establishes BLE long term keys with Alice and Bob, and positions himself in the middle to access all traffic between the victims and to inject valid traffic both on BT and BLE.

Figure 7 shows the details of the MitM attack. Firstly, Charlie impersonates Alice to Bob over BLE (as in Figure 4), overwrites Bob's BT key with his key (K_{BC}). Secondly, Charlie impersonates Bob to Alice over BT as in Figure 5 and overwrites Alice's BT key with his key (K_{AC}). Then, Alice and Bob exchange two nonces (N_A, N_B) to authenticate the BT pairing key. Charlie mutually authenticates with Bob and Alice by using a message authentication code (MAC) function keyed with the appropriate key and input parameters. Finally, Alice and Bob establish a secure BT session with Charlie in the middle, and Charlie gets access to all traffic exchanged by Alice and Bob and can modify and inject arbitrary valid traffic between Alice and Bob.

As summarized in Table 2, the BLUR man-in-the-middle attack is a composition of the master and slave impersonation BLUR attacks and takes advantage of all the CTI that we present in Section 3.4.

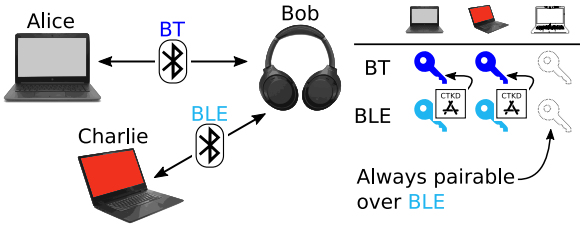

Figure 8: BLUR unintended sessions attack. Charlie sends a BLE pairing request to Bob (who remains pairable over BLE due to CTKD) as an unknown device with arbitrary capabilities. After CTKD completes, Charlie can establish secure but unintended BT and BLE sessions with Bob without breaking Bob's existing pairings and sessions.

4.3 Unintended Sessions

Figure 8 presents a BLUR unintended session attack targeting Bob. In this scenario, Alice and Bob are running a secure session over BT but they are still pairable over BLE in order to accept pairing requests with other devices and run CTKD. Charlie targets Bob (slave) by sending him a pairing request over BLE as an unknown device. Charlie can pretend to be any device having arbitrary capabilities, e.g., Bluetooth address, Bluetooth name, device class, "Secure Connections" support, and weak association. Bob, accepts to pair with Charlie while continuing his session with Alice. Then, Charlie and Bob negotiate K_{BLE}, and derive K_{BT} using CTKD. Now, Charlie can establish secure but unintended BT and BLE sessions with Bob without breaking his existing pairings or sessions with other devices (e.g., with Alice).

Charlie can also establish unintended sessions with Alice (master). In particular, he can impersonate a BLE slave and start advertising his presence. Once Alice discovers Charlie, she can establish a BLE connection with him, and Charlie can explicitly request to pair using a SMP Security Request packet [11, p. 1401]. Then, Alice and Charlie compute K_{BLE}, and derive K_{BT} using CTKD. Now, Charlie can establish secure but unintended BT and BLE sessions with Alice without breaking her existing pairings or sessions with other devices (e.g., with Bob). Charlie can take advantage of the unintended sessions with Alice and Bob in many ways. For example, he can use the session to drop known exploits such as BlueBorne [6], BLEEDINGBIT [7], or SweynTooth [19], new exploits, and to enumerate and tamper with BT and BLE services and characteristics (including the protected ones).

Those attacks are particularly effective when the victims are using one transport only to pair and derive keys with CTKD. For example, a Bluetooth speaker only streams music over BT but is also pairable over BLE to enable users to

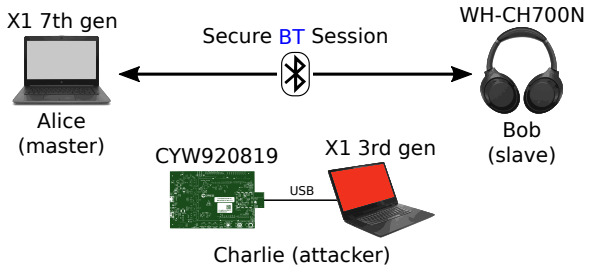

Figure 9: Example BLUR Attack Scenario. Alice (master) is a ThinkPad X1 7th gen, Bob (slave) is a pair of Sony WH-CH700N headphones and Charlie (attacker) is a CYW920819 board connected via USB to a ThinkPad X1 3rd gen. Alice and Bob have paired in absence of Charlie, and are running a secure BT session.

discover it without having to put it into BT pairing mode. As summarized in Table 2 the unintended session BLUR attack takes advantage of CTI 2 and CTI 4.

5 Implementation

In this section we describe our attack scenario, our implementation of a custom attack device to perform the BLUR attacks and our re-implementation of CTKD's key derivation function. The tools that we developed will be open-sourced.

5.1 Attack Scenario

Our attack scenario follows the example in Figure 9 and includes two victims, Alice (master) and Bob (slave). In Figure 9 Alice is represented by a 7th generation ThinkPad X1 laptop and Bob by a pair of Sony WH-CH700N headphones. The attacker (Charlie) uses a CYW920819 development board [15] and a 3rd generation ThinkPad X1 laptop as an attack device. The implementation of the attack device is presented in Section 5.2. In our evaluation, we use the same attack scenario with different victim devices.

To understand the capabilities of the victims and the attacker we summarize their most important Bluetooth features in Table 3. We note that Bob is capable of using CTKD over BLE even if he does not support "Secure Connections" over BT and does not support Bluetooth version 4.2. This confirms the "Secure Connections" cross-transport issue (CTI 2) that we discuss. Furthermore to conduct the attacks we had to develop an attack device that enabled us to change all the features in Table 3. Some of those features, such as the version and subversion numbers, are particularly challenging to modify as they require patching a Bluetooth firmware that is typically proprietary and closed-source.

	Alice	Bob	Charlie
Device(s)	X1 7th gen	WH-CH700N	X1 3rd gen / CYW920819
Radio Chip	Intel	CSR	Intel / Cypress
Subversion	256	12942	256 / 8716
Version	5.1	4.1	5.0
Name	x7	WH-CH700N	x1
ADD	Redacted	Redacted	Redacted
Class	0x1c010c	0x0	0x0
BT SC	True	Only Controller	True
BT AuthReq	0x03	0x02	0x03
BLE SC	True	True	True
BLE AuthReq	0x2d	0x09	0x2d
CTKD	True	True	True
h7	True	False	True
Role	Master	Slave	Master
IO	Display	No IO	Display
Association	"Numeric C."	"Just Works"	"Numeric C."
Pairable	True	True	True

Table 3: Relevant Bluetooth features for Alice, Bob, and Charlie in our example attack scenario. Alice and Bob support CTKD even if Bob's Host does not support BT SC (BT "Secure Connections"). We redact the devices' Bluetooth addresses for privacy reasons.

5.2 Custom Attack Device

To implement the BLUR attack we had to develop a custom attack device. As we can see from its block diagram in Figure 10, the attack device consists of a Linux laptop implementing the Bluetooth host component using BlueZ (i.e., user-space) and the Linux kernel. The laptop is connected via USB to a CYW920819 development board. The board implements the Bluetooth controller using a firmware and a baseband. The laptop and the board support BT, BLE, SSP, Secure Connections, and CTKD and they communicate using the Host Controller Interface (HCI) protocol over USB.

For the host, we used standard Linux tools to configure an interface (e.g., `hciconfig`), and to discover and pair with a device (e.g., `bluetoothctl`, `hcitool` and `btmgmt`). In particular, `btmgmt` was very useful as, unlike other tools, it enables to decide the type of pairing request and declared association mechanism. Furthermore, we wanted to access the traffic exchanged over the air by our attack device. This is not available on a standard Bluetooth device. To achieve this goal we sent a proprietary HCI command from the host to enable diagnostic mode on the controller. This mode tells the board to copy all the BT and BLE link-layer packets and send them over HCI to the host. Then, we added extra C code to the Linux kernel

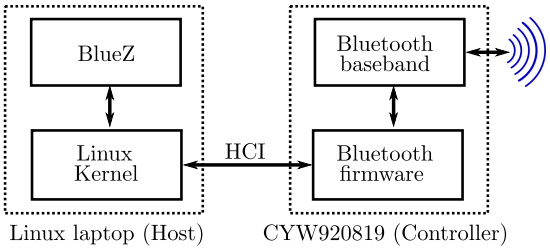

Figure 10: Attack Device Block Diagram. The attack device is composed of Linux laptop (Host) and a CYW920819 (Controller) connected via USB and communicating using the Host Controller Interface (HCI) protocol.

to parse those HCI packets. With this setup, we can monitor both HCI and link-layer traffic directly from the host without requiring over-the-air BT and BLE sniffers.

Modifying the controller required us to interact directly with the development board's Bluetooth firmware. To extract the firmware we used a proprietary HCI command from Cypress to read and save a RAM snapshot from the board's SoC. We took the snapshot after the firmware was initialized to acquire the firmware patches applied at runtime. We use the memory maps from the board's SDK to extract the various segments from the snapshot including the ROM, the RAM, and the scratchpad segments. As expected, the firmware was in the ROM segment and was a stripped ARM binary containing 16-bit Thumb instructions.

To reverse-engineer the firmware, we loaded the ROM, RAM, and scratchpad segments in Ghidra (a free and open-source decompiler and disassembler). In our first reverse-engineering pass we isolated the libc functions (e.g., `malloc` and `calloc`) by looking at the signatures and the code patterns of the functions that are called the most. Then, we found the firmware debugging symbols in the board's SDK and loaded them into Ghidra. Using the debugging symbols we isolated functions and data structures relevant for the BLUR attacks. Then, we wrote assembly patches to change their behaviors and we apply those patches at runtime using internalblue [30]. Our set of patches allow modifying crucial capabilities and parameters declared by the controller including the Bluetooth address and name, device class, Secure Connections support, and authentication requirements (as shown in Table 3).

5.3 Re-Implementing CTKD

Our BLUR attacks leverage CTKD, so the first step of our evaluation requires to confirm that the devices under test support and (correctly) implement it. As CTKD is an optional feature and it is not negotiated with a dedicated flag, we can only speculate that a device supports it if it declares Secure Connections support for BT and BLE. Furthermore, there are no available tools to check the correctness of the keys derived via CTKD.

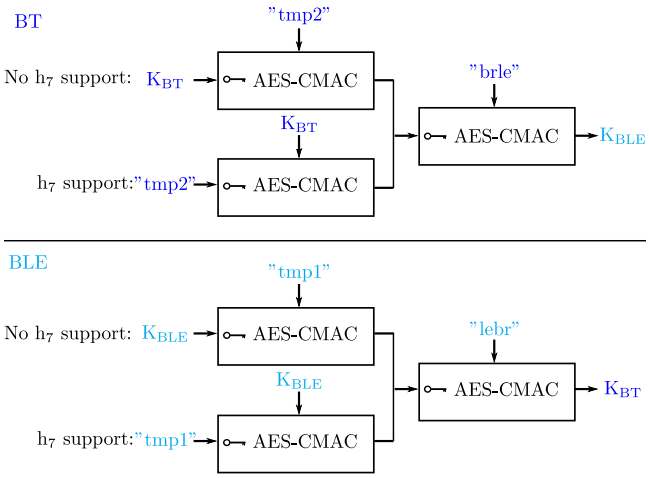

Figure 11: CTKD function for BT (top) and BLE (bottom). The functions are the same but use a sequence of two AES-CMAC with different input quantities. In the first AES-CMAC, the devices use a constant string as key and the pairing key as input if they support the h7 conversion function, otherwise, they swap the two. In the second AES-CMAC, the devices use the MAC from the first stage as key and a constant string as the input to derive the cross-transport pairing key.

To address those issues we implemented the CTKD derivation function based on the Bluetooth standard [11, p. 1401]. Our implementation uses the PyCA cryptographic module [8], was successfully tested against the standard's test vectors and the CTKD keys produced during our attacks. To enable other researchers to investigate CTKD we will open-source our implementation.

We now describe the CTKD key derivation function implementation details. The Bluetooth standard specifies a single CTKD function (see Section 2.2) that is used with different parameters for BT and BLE. Figure 11 shows the CTKD key derivation function for BT (top) and BLE (bottom). Both use a chain of two AES-CMAC blocks in sequence with different keys and 4-byte constant strings. AES-CMAC is a message authentication code (MAC) based on the AES block cipher [17]. In particular, BT uses K_{BT}, "`tmp2`" and "`brle`" and derives K_{BLE}, while BLE uses K_{BLE}, "`tmp1`" and "`lebr`" and derives K_{BT}.

In the first AES-CMAC, if both devices support the h7 conversion function in the Bluetooth standard [11, p. 1634], the long term key is used as key and the string as input, otherwise, the string (padded with 12 zeros) is used as key and the long term key as input. In the second AES-CMAC, the 128-bit (16-byte) output of the first AES-CMAC is used as key and the string as input. The 128-bit (16-byte) output of the second AES-CMAC is the derived long term key.

6 Evaluation

In this section we present how we conducted the BLUR attacks and our evaluation results on 13 unique devices (see Table 4). The tested devices represent popular laptops, phones, headphones, and an embededd platform. The devices are from a broad set of device producers (Samsung, Dell, Google, Lenovo, and Sony), run different operating systems (Android, Windows, Linux, and proprietary OSes), use different Bluetooth chipsets (from Broadcom, CSR, Cypress, Intel, Qualcomm, and Samsung).

6.1 Realizing the Attacks

The BLUR attacks, presented in Section 4, include master impersonation, slave impersonation, man-in-the-middle, and unintentional session attacks. In the next paragraphs, we describe how we conducted them using our custom attack device described in Section 5.2.

Laptop (master) impersonation attack To impersonate the laptop, we configure our attack device to clone the laptop Bluetooth features, including Bluetooth address, Bluetooth name, device class, BT and BLE "Secure Connections" support, and advertised services. We accomplish this task by patching the attack device's Bluetooth firmware and configuring the attack laptop accordingly. Once the attack device looks like the impersonated laptop, we ask the headphones to pair over BLE using "Just Works" and CTKD.

The malicious BLE pairing request is sent using `btmgmt`'s text-based user interface (TUI). The headphones accept the request to pair over BLE, update the BLE long term key, run CTKD for BT, update the BT long term key, and establish a secure BLE session with the attack device. Then, the headphones terminate the BT session with the impersonated laptop and establish a secure BT session with the attack device. The impersonated laptop cannot connect back with the headphones as it does not possess the new BT and BLE long term keys.

Headphones (slave) impersonation attack To impersonate the headphones, we configure our attack device to clone the headphones Bluetooth features using the same technique adopted for the laptop impersonation. Once the attack device looks like the impersonated headphones we ask the laptop to pair over BT using "Just Works" and CTKD. The malicious BT pairing request is sent using `btmgmt`'s TUI. The laptop accepts to pair over BT, updates the BT long term key, and runs CTKD for BLE. Then, we establish a secure BT session with the headphones.

To evaluate master and slave impersonation attack experimentally, we used the attack device both as the attacker and as one of the victims. For example, in a master impersonation attack we pair the attack device with the slave victim device, we disconnect them, we "forget" the victim device on the attack device and we run the master impersonation attack from the attack device. This setup is efficient, because it allows us to quickly test many slave victims. For the slave impersonation, we use the same procedure and quickly test many master victims.

Man-in-the-middle attack By using our BLUR implementation with two development boards connected to the same attack laptop, we can impersonate the laptop and the headphones at the same time, and man-in-the-middle them. In particular, we run the laptop (master) impersonation attack first, and then the headphone (slave) impersonation attack. As a result, the attack device positions itself in the middle between the victims.

If a victim device is vulnerable to the master or slave impersonation attack, then is also vulnerable to the man-in-the-middle attack, as the latter requires a vulnerable master device and a vulnerable slave device.

Unintended sessions attack To perform the unintended sessions attacks, we configure the attack device to impersonate an arbitrary device with arbitrary services over BT and BLE. Then we send a malicious pairing request to the headphones over BLE and one to the laptop over BT. Both pairing requests declare support for CTKD and "Just Works". The attack device establishes new BT and BLE keys both with the headphones and the laptop and starts unintended sessions with both over BT and BLE.

We test this attack by connecting the target victim to a third device and then by trying to establish unintended sessions with the victim as an arbitrary device over the transport that is not used by the legitimate connection. For example, if the victim is a pair of headphones that is connected with a laptop over BT then we run the unintended session attacker over BLE.

6.2 Evaluation Results

We evaluated the BLUR attacks on 13 devices, the results are summarized in Table 4. The first six columns indicate the device producer, device model, OS, chip manufacturer, chip model, and supported Bluetooth version. The seventh column indicates the attacker role. The last three columns contain a checkmark (✓) if a device is vulnerable to the master impersonation attack (MI), slave impersonation attack (SI), man-in-the-middle attack (MitM), or unintended session (US) attack. The master and slave impersonation attacks are grouped in one column (MI/SI column). If the victim's role is slave then we test it against a master impersonation attack, otherwise, we test it against a slave impersonation attack. As shown by the last three columns, all the 13 devices (10 unique Bluetooth chips) that we tested are vulnerable to all relevant BLUR attacks.

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

† CTKD functionality was backported by the vendor to Bluetooth 4.1 for this device.

Table 4: BLUR attacks evaluation results. The last three columns contain a checkmark (✓) if a device is vulnerable to the master impersonation attack (MI), slave impersonation attack (SI), man-in-the-middle attack (MitM), or unintended session (US) attack. If the victim's role is slave then we test the victim against a master impersonation attack (Role = Master), otherwise, we test it against a slave impersonation attack (Role = Slave), and we group the attacks in one column (MI/SI column). As shown by the last three columns, all the tested 13 devices (10 unique Bluetooth chips) are vulnerable to all relevant BLUR attacks.

As we tested a wide range of devices that were all vulnerable, our evaluation demonstrates that the BLUR attacks are practical, standard-compliant, and affect all the Bluetooth versions that support CTKD. As the BLUR attacks are standard-compliant, potentially all standard-compliant devices supporting CTKD are also vulnerable. Based on our evaluation, we suggest that the Bluetooth SIG fix the issues that we uncover in CTKD and we provide our set of countermeasures for the Bluetooth standard in Section 7.2.

7 Discussion

We now discuss the lessons learned and our set of countermeasures to mitigate the BLUR attacks.

7.1 Lessons Learned

There are several lessons that we learned while analyzing CTKD and developing the BLUR attacks. In this section we report those lessons evaluating the BLUR attacks. In this section we report those lessons as they are useful for protocol designers who are dealing with cross-transport features and related security issues.

Cross-transport mechanisms need a cross-transport threat model Security mechanisms, such as CTKD, that cross the security boundary between two technologies with different threat models should be designed using a cross-transport threat model. For example, the Bluetooth standard should consider that an attacker might try to exploit BT from BLE via CTKD and vice versa. Unfortunately, at the time of writing, the Bluetooth standard lacks a cross-transport threat model. The lack of a threat model (along with a security analysis) is the main reason why we were able to uncover severe issues with CTKD.

Similar security mechanisms with different threat models do not provide the same security guarantees BT and BLE both provide their version of pairing and secure session establishment. One might think that pairing over BT and then establishing a secure session over BLE provides the same security guarantees of pairing over BT and establishing a secure session over BLE. However, this is not the case, as those mechanisms are similar but not equal and they are designed with different threat models in mind. Mixing those procedures actually enables more ways to attack BT and BLE (e.g., the BLUR attacks).

Properly weighting usability against security benefits is key CTKD was introduced to improve BT and BLE usability. In light of the presented issues and attacks, we learned that the usability benefits introduced with CTKD are not bal-

ancing the security issues introduced by CTKD. We agree that no-one wants to use complicated security mechanisms, but the Bluetooth standard should have introduced a secure and usable CTKD mechanism.

7.2 Countermeasures

We now present a set of countermeasures to address all the five cross-transport issues (CTI) that we present in Section 3.4. Our countermeasures can be implemented in the device's Bluetooth Host (i.e., device's OS), by storing and checking extra metadata about its state and trusted remote devices.

Align BT and BLE roles (CTI 1) The BLUR attacks take advantage of BT and BLE role asymmetries to act as a BT master while being a BLE slave. To fix this issue, a device should store the role that the remote device used while pairing and enforce it across re-pairings. In case of a role mismatch, the device should abort pairing.

Enforce Secure Connections (CTI 2) In our experiments, we can use CTKD with the WH-CH700N headphones even if they only support "Secure Connections" for BLE. This should not happen as CTKD should be used only when "Secure Connections" is provided by both BT and BLE and a device should enforce this condition before running CKTD and abort CTKD if this condition is not met.

Enforce strong association mechanisms (CTI 3) BT and BLE do not protect the negotiation of the association mechanism and CTKD allows two devices to use different association mechanisms on different transports when pairing and re-pairing. The BLUR attack exploits this fact to re-pair with a victim device using "Just Works" even if the victim supports "Numeric Comparison". A device should keep track of the remotes' strongest association mechanism used while pairing and enforce it for subsequent (re-)pairings.

Disable CTKD key overwrites (CTI 4) CTKD allows (over)writing BT long term keys from BLE and vice versa. This enables an attacker to impersonate a device and take over her existing session on one transport by attacking the other. To fix this issue, a device should disallow key overwrites with CTKD when a paired device wants to re-pair. For example, re-pairing over BT should not overwrite a BLE long term key that was securely established in the past. When a device has lost a long term key for a transport (e.g., device reset), it should explicitly re-pair on that transport.

Disable pairable state when not needed (CTI 5) In our experiment we confirmed that a device might remain pairable over BT and BLE even after it has paired and is communicating with a remote device. This is problematic as an attacker can target the transport that is not currently used by the two devices to launch the BLUR attacks. To address this issue, a device should automatically stop being pairable on a transport that is not currently in use. For example, a pair of headphones who are running a secure session over BT with a laptop should not answer pairing requests over BLE unless the user explicitly renters pairing mode.

8 Related Work

The Bluetooth provides a royalty-free and widely-available cable replacement technology [20]. Bluetooth standard compliant attacks are particularly dangerous as all Bluetooth devices are affected, regardless of version numbers or implementation details. Such standard-compliant attacks have appeared since the first versions of Bluetooth [24, 29]. Standard-compliant attacks on BT include attacks on legacy pairing [36], secure simple pairing (SSP) [10, 21, 37], Bluetooth association [22, 38], key negotiation [1], and authentication procedures [3, 28, 39]. Standard-compliant attacks on BLE include attacks on legacy pairing [35], key negotiation [4], SSP [10, 43], reconnections [41], and GATT [25]. Compared to the mentioned attacks that target either BT or BLE, the BLUR attacks are the first standard-compliant attacks targeting the intersection between BT and BLE.

We have seen attacks targeting specific implementation flaws on BT [6] and BLE [7, 19]. As our BLUR attacks target the specification level, they are effective regardless of the implementation details. Several surveys on BT and BLE security were published [16, 31, 32] but neither of those surveys nor the Bluetooth standard considers CTKD as a threat. We here demonstrate that CTKD is a serious threat and must be included in the threat model.

Cross-transport attacks were exploited for proximity technologies using Bluetooth and Wi-FI. Two prominent examples are attacks on Apple ZeroConf [9] and Google Nearby Connections [2]. Our BLUR attacks are the first cross-transport attacks for BT and BLE.

The cryptographic primitives used by Bluetooth have been extensively analyzed. For example, the E_0 cipher used by BT was investigated [18] and it is considered relatively weak [32]. SAFER+, used for authentication, was analyzed as well [27]. BT and BLE "Secure Connections" use the AES-CCM authenticated-encryption cipher. AES-CCM was extensively analyzed [26, 34] and it is FIPS compliant. Our BLUR attacks target key negotiation and not cryptographic primitives, and are effective even with perfectly secure cryptographic primitives.

9 Conclusion

We present the first security analysis of CTKD and identify novel standard-compliant and cross-transport issues and at-

tacks against BT and BLE. Our attacks show that CTKD enables an attacker to cross the security boundary between BT and BLE. In contrast to previously published attacks on the individual BT and BLE transports, our attacks on CTKD do not require the attacker to be present during pairing or secure session establishment. As a result, our attacks have lower requirements for the attacker while still allowing to break BT and BLE security guarantees.

We identify five cross-transport issues related to roles (CTI 1), "Secure Connections" (CTI 2), association (CTI 3), key overwrite (CTI 4), and pairing states (CTI 5). Based on those issues, we develop attacks against BT and BLE enabling impersonations, traffic manipulation, and malicious session establishment. We name our attacks BLUR attacks as they blur the security boundary between BT and BLE.

We provide and discuss a low-cost implementation of the BLUR attacks using off-the-shelf hardware and open-source software. To demonstrate that our attacks are practical, we successfully exploit 13 devices from different hardware and software manufacturers. Our devices range across all the Bluetooth versions supporting CTKD (e.g., versions greater or equal to 4.2) and also a version of Bluetooth 4.1 with backported CTKD features.

We discuss several lessons that we learned (e.g., the importance of a cross-transport threat model) and the major technical challenges that we faced (e.g., low-level modifications of a Bluetooth firmware). We present five countermeasures to mitigate the BLUR attacks. Each countermeasure addresses a specific cross-transport with a concrete fix that can be implemented at the Bluetooth standard level. We responsibly disclosed our vulnerabilities, attacks, and countermeasures to the Bluetooth SIG.

References

[1] Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen. The KNOB is broken: Exploiting low entropy in the encryption key negotiation of Bluetooth BR/EDR. In *Proceedings of the USENIX Security Symposium*. USENIX, August 2019.

[2] Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen. Nearby Threats: Reversing, Analyzing, and Attacking Google's "Nearby Connections" on Android. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, February 2019.

[3] Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen. BIAS: Bluetooth Impersonation AttackS. In *Proceedings of Symposium on Security and Privacy (S&P)*. IEEE, May 2020.

[4] Daniele Antonioli, Nils Ole Tippenhauer, and Kasper Rasmussen. Key Negotiation Downgrade Attacks on Bluetooth and Bluetooth Low Energy. *Transactions on Privacy and Security (TOPS)*, 2020.

[5] AOSP. Fluoride Bluetooth stack. https://chromium.googlesource.com/aosp/platform/system/bt/+/master/README.md, Accessed: 2020-01-27, 2020.

[6] Armis Inc. The Attack Vector BlueBorne Exposes Almost Every Connected Device. https://armis.com/blueborne/, Accessed: 2018-01-26, 2017.

[7] Armis Inc. BLEEDINGBIT: The hidden attack surface within BLE chips. https://armis.com/bleedingbit/, Accessed: 2019-07-24, 2019.

[8] Python Cryptographic Authority. Python cryptography. https://cryptography.io/en/latest/, Accessed: 2019-02-04, 2019.

[9] Xiaolong Bai, Luyi Xing, Nan Zhang, XiaoFeng Wang, Xiaojing Liao, Tongxin Li, and Shi-Min Hu. Staying secure and unprepared: Understanding and mitigating the security risks of apple zeroconf. In *2016 IEEE Symposium on Security and Privacy (SP)*, pages 655–674. IEEE, 2016.

[10] Eli Biham and Lior Neumann. Breaking the bluetooth pairing–fixed coordinate invalid curve attack. http://www.cs.technion.ac.il/~biham/BT/bt-fixed-coordinate-invalid-curve-attack.pdf, Accessed: 2018-10-30, 2018.

[11] Bluetooth SIG. Bluetooth Core Specification v5.2. https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=478726, Accessed: 2020-01-27, 2019.

[12] Bluetooth SIG. Bluetooth Markets. https://www.bluetooth.com/markets/, Accessed: 2019-10-23, 2019.

[13] BlueZ. Bluetooth 4.2 features going to the 3.19 kernel release. https://tinyurl.com/q9dzh2h, Accessed: 2020-01-27, 2014.

[14] Cypress. BLE and Bluetooth. https://www.cypress.com/products/ble-bluetooth, Accessed: 2020-01-27, 2019.

[15] Cypress. CYW920819EVB-02 Evaluation Kit. https://www.cypress.com/documentation/development-kitsboards/cyw920819evb-02-evaluation-kit, Accessed: 2019-11-16, 2019.

[16] John Dunning. Taming the blue beast: A survey of bluetooth based threats. *IEEE Security & Privacy*, 8(2):20–27, 2010.

[17] Morris Dworkin. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-38B.pdf, 2018. Recommendations of the NIST.

[18] Scott Fluhrer and Stefan Lucks. Analysis of the E0 encryption system. In *Proceedings of the International Workshop on Selected Areas in Cryptography*, pages 38–48. Springer, 2001.

[19] Garbelini, Matheus and Chattopadhyay, Sudipta and Wang, Chundong. SweynTooth: Unleashing Mayhem over Bluetooth Low Energy. https://asset-group.github.io/disclosures/sweyntooth/sweyntooth.pdf, Accessed: 2020-04-08, 2020.

[20] Jaap Haartsen, Mahmoud Naghshineh, Jon Inouye, Olaf J Joeressen, and Warren Allen. Bluetooth: Vision, goals, and architecture. *ACM SIGMOBILE Mobile Computing and Communications Review*, 2(4):38–45, 1998.

[21] Keijo Haataja and Pekka Toivanen. Two practical man-in-the-middle attacks on Bluetooth secure simple pairing and countermeasures. *Transactions on Wireless Communications*, 9(1):384–392, 2010.

[22] Konstantin Hypponen and Keijo MJ Haataja. "nino" man-in-the-middle attack on bluetooth secure simple pairing. In *Proceedings of the International Conference in Central Asia on Internet*, pages 1–5. IEEE, 2007.

[23] Intel. Intel Wireless Solutions. https://www.intel.com/content/www/us/en/products/wireless.html, Accessed: 2020-01-27, 2019.

[24] Markus Jakobsson and Susanne Wetzel. Security weaknesses in Bluetooth. In *Proceedings of the Cryptographers' Track at the RSA Conference*, pages 176–191. Springer, 2001.

[25] Sławomir Jasek. Gattacking bluetooth smart devices. Black Hat USA Conference, 2016.

[26] Jakob Jonsson. On the security of CTR+ CBC-MAC. In *Proceedings of the International Workshop on Selected Areas in Cryptography*, pages 76–93. Springer, 2002.

[27] John Kelsey, Bruce Schneier, and David Wagner. Key schedule weaknesses in SAFER+. In *Proceedings of the Advanced Encryption Standard Candidate Conference*, pages 155–167. NIST, 1999.

[28] Albert Levi, Erhan Çetintaş, Murat Aydos, Çetin Kaya Koç, and M Ufuk Çağlayan. Relay attacks on Bluetooth authentication and solutions. In *Proceedings International Symposium on Computer and Information Sciences*, pages 278–288. Springer, 2004.

[29] Andrew Y Lindell. Attacks on the pairing protocol of Bluetooth v2.1. *Black Hat USA, Las Vegas, Nevada*, 2008.

[30] Dennis Mantz, Jiska Classen, Matthias Schulz, and Matthias Hollick. InternalBlue - Bluetooth binary patching and experimentation framework. In *Proceedings of Conference on Mobile Systems, Applications and Services (MobiSys)*. ACM, June 2019.

[31] Nateq Be-Nazir Ibn Minar and Mohammed Tarique. Bluetooth security threats and solutions: a survey. *International Journal of Distributed and Parallel Systems*, 3(1):127, 2012.

[32] John Padgette. Guide to bluetooth security. *NIST Special Publication*, 800:121, 2017.

[33] Qualcomm. Expand the potential of Bluetooth. https://www.qualcomm.com/products/bluetooth, Accessed: 2020-01-27, 2019.

[34] Phillip Rogaway. Evaluation of some blockcipher modes of operation. *Cryptography Research and Evaluation Committees (CRYPTREC) for the Government of Japan*, 2011.

[35] Mike Ryan. Bluetooth: With low energy comes low security. In *Proceedings of USENIX Workshop on Offensive Technologies (WOOT)*, volume 13, pages 4–4. USENIX, 2013.

[36] Yaniv Shaked and Avishai Wool. Cracking the Bluetooth PIN. In *Proceedings of the conference on Mobile systems, applications, and services (MobiSys)*, pages 39–50. ACM, 2005.

[37] Da-Zhi Sun, Yi Mu, and Willy Susilo. Man-in-the-middle attacks on Secure Simple Pairing in Bluetooth standard v5. 0 and its countermeasure. *Personal and Ubiquitous Computing*, 22(1):55–67, 2018.

[38] Maximilian von Tschirschnitz, Ludwig Peuckert, Fabian Franzen, and Jens Grossklags. Method Confusion Attack on Bluetooth Pairing. In *Proceedings of Symposium on Security and Privacy (S&P)*. IEEE, 2021.

[39] Ford-Long Wong, Frank Stajano, and Jolyon Clulow. Repairing the Bluetooth pairing protocol. In *Proceedings of International Workshop on Security Protocols*, pages 31–45. Springer, 2005.

[40] Joshua Wright. I Can Hear You Now - Eavesdropping on Bluetooth Headsets. https://www.willhackforsushi.com/presentations/icanhearyounow-sansns2007.pdf, Accessed: 2018-10-30.

[41] Jianliang Wu, Yuhong Nan, Vireshwar Kumar, Dave Jing Tian, Antonio Bianchi, Mathias Payer, and Dongyan Xu. BLESA: Spoofing Attacks against Reconnections in Bluetooth Low Energy. In *14th USENIX Workshop on Offensive Technologies (WOOT)*, 2020.

[42] Apple WWDC. What's New in Core Bluetooth. https://developer.apple.com/videos/play/wwdc2019/901, Accessed: 2020-01-27, 2019.

[43] Yue Zhang, Jian Weng, Rajib Dey, Yier Jin, Zhiqiang Lin, and Xinwen Fu. Breaking Secure Pairing of Bluetooth Low Energy Using Downgrade Attacks. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 37–54, 2020.