Institution: University of Oxford		
Unit of Assessment: 11 Computer Science and Informatics		
Title of case study: Resolution of Multiple Critical Design Flaws in Bluetooth Standard		
Period when the underpinning research was undertaken: January 2018 – August 2019		
Details of staff conducting the underpinning research from the submitting unit:		
Name(s):	**Role(s) (e.g. job title):**	**Period(s) employed by submitting HEI:**
Kasper Rasmussen	Associate Professor	Oct 2013 – present
Period when the claimed impact occurred: November 2018 – July 2020		
Is this case study continued from a case study submitted in 2014? N		

1. Summary of the impact

Oxford University research on weaknesses in wireless protocols uncovered critical flaws in multiple parts of the Bluetooth standard, as implemented in billions of devices worldwide (almost 3,000,000,000 Bluetooth BR/EDR devices were shipped in 2019 alone). The research demonstrated how both the Bluetooth session key establishment and the authentication procedures can be completely compromised by an external adversary, allowing attackers to circumvent the protections between devices to intercept, monitor, or manipulate communication at will and to impersonate previously-paired devices. The research team's coordinated disclosure to industry of each vulnerability in turn underpinned substantial efforts to remedy them before they could be discovered and misused by malicious parties. The work led to changes to the Bluetooth Core Specification, and to mitigations applied by major manufacturers (including Intel, Microsoft, Apple, Cisco, Google, and Huawei). These have protected Bluetooth-enabled devices that were previously vulnerable, preventing significant harm to both manufacturers and consumers.

2. Underpinning research

The claimed impact results from a programme of research investigating low-level communication interfaces for mobile devices, in particular the initialisation of communication sessions and mutual authentication of communicating parties. The research was led by Professor Rasmussen, in collaboration with researchers from Singapore University of Technology and Design (Nils Ole Tippenhauer and Daniele Antonioli, both of whom have since changed their affiliation). Secure communication between two devices requires a secret channel to be established and the identity of each party to be verified. Major technologies such as Bluetooth must ensure that these requirements are met throughout the provision of useful services, because they are critical to safe use of the technology by the public. If a secret channel is not properly established, then a malicious party can steal private information and forge data or instructions. If participants' identities cannot be verified, then a malicious party can masquerade as a legitimate one, sidestepping the benefits of a secret channel. For example, by breaking a secure channel, a file sent between devices can be stolen or altered, a password entered on a wireless keyboard can be monitored, or a typed account number can be changed. Through impersonation of a legitimate device, a vehicle can be unlocked and driven away, a mobile phone opened, or a smart home-security system deactivated.

Work led by Kasper Rasmussen investigated the twin challenges of secure session initialisation and mutual authentication in the systematic security analysis of existing systems [**R1**–**R4**]. This work led first to the identification of previously unknown deficiencies in location services used by Android mobile devices [**R1**]. A particular concern was the ability for an attacker to 'downgrade' communication security by manipulating parameters in a session initialisation. These insights were then applied in the security analysis of ubiquitous Bluetooth technology – ultimately identifying a critical design flaw allowing the downgrade of a key security parameter, and thus the compromise of the secure channel. This was the Key Negotiation of Bluetooth (KNOB) attack [**R2**, **R4**]. Further work on Bluetooth then discovered that a malicious party could masquerade as a trusted device by misleading a victim device in several ways during the session initialisation protocol. These attacks collectively became known as Bluetooth Impersonation AttackS (BIAS) [**R3**].

The paper presenting the first Bluetooth vulnerability (KNOB) [**R2**] described an attack on the session key negotiation protocol of Bluetooth BR/EDR. The paper was published in August 2019, following an embargo period to support the responsible disclosure process. The attack allows a third party, without knowledge of any secret material (such as link and encryption keys), to force a downgrade by making two (or more) victims agree on a session key with only 1 byte (8 bits) of entropy. Such low entropy enables the attacker to easily brute force the negotiated keys (only 256 values), decrypt the eavesdropped ciphertext, and inject valid encrypted messages (in real-time). The attack is stealthy because the key negotiation is transparent to the Bluetooth users. The attack is standard-compliant because all Bluetooth BR/EDR versions are required to support session keys with entropy between 1 and 16 bytes and do not properly secure the key negotiation protocol. Due to the support of Bluetooth for simple and low-power devices, there is no known implementation that applies any security protocols above the communication encryption.

The second Bluetooth vulnerability (BIAS) [**R3**], published after embargo in May 2020, allows an attacker to downgrade the use of the Bluetooth Secure Connections mode to an insecure Legacy mode by falsely claiming that Secure Connections are not available (even if the genuine link was originally established with Secure Connections). The Legacy mode authentication only requires authentication of one party (the Master device) in the communication. The paper further shows that an attacker can trigger a Master-Slave role switch to avoid undertaking even the one-way authentication, thereby masquerading as a trusted, paired device despite having no knowledge of the long-term link key. The use of both attacks in sequence allows complete compromise of any established trust relationship between devices and the secrecy of communicated data – entirely breaking Bluetooth BR/EDR security without being detected.

In both cases, the attacks target the firmware of the Bluetooth chips because the firmware (Bluetooth controller) implements all the security features of Bluetooth BR/EDR. As standard compliant attacks, they are effective on any firmware, and on any device, that follows the specification. The KNOB attack [**R2**] was implemented on more than 14 Bluetooth chips from popular manufacturers such as Intel, Broadcom, Apple, and Qualcomm, with all tested devices being vulnerable. The BIAS attack [**R3**] was conducted against more than 28 unique Bluetooth chips, which were all found to be vulnerable.

3. References to the research

[**R1**] D. Antonioli, N. O. Tippenhauer, K. Rasmussen: Nearby Threats: Reversing, Analyzing, and Attacking Google's 'Nearby Connections' on Android. Network and Distributed System Security Symposium (NDSS), 2019: https://dx.doi.org/10.14722/ndss.2019.23367. *Submitted to REF 2021*.

[**R2**] D. Antonioli, N. O. Tippenhauer, K. Rasmussen: The KNOB is Broken: Exploiting Low Entropy in the Encryption Key Negotiation Of Bluetooth BR/EDR. USENIX Security Symposium, 2019: http://tiny.cc/cfv0tz.

[**R3**] D. Antonioli, N. O. Tippenhauer, K. Rasmussen: BIAS: Bluetooth Impersonation AttackS. IEEE Symposium on Security and Privacy (IEEE S&P), 2020: https://doi.org/10.1109/SP40000.2020.00093. *Submitted to REF 2021.*

[**R4**] D. Antonioli, N. O. Tippenhauer, K. Rasmussen: Key Negotiation Downgrade Attacks on Bluetooth and Bluetooth Low Energy. ACM Tr. on Privacy and Security (TOPS), 2020: https://doi.org/10.1145/3394497. *Submitted to REF 2021*.

4. Details of the impact

Our research exposed critical failures in the security of Bluetooth that nullified the confidentiality and authentication properties of the technology. Bringing these facts to light carries direct impacts: in making unknown security risks known, in allowing informed choices to be made by manufacturers and users of Bluetooth, and in directing the development of commercial communication systems. However, the most profound impact of this programme has come from the research team's coordinated disclosure process, which has repeatedly allowed the most serious risks to be mitigated before they can be abused – thereby preventing their potential harm. As Bluetooth is in use at enormous scale (almost 3,000,000,000 Bluetooth BR/EDR devices were shipped in 2019 alone [**E4**.1]), and the exposed vulnerabilities affected all standard-compliant devices, the steps taken to remedy the deficiencies found by the research team have helped protect the security and privacy of a substantial proportion of the world's population.

The coordinated disclosure of security vulnerabilities is a pillar of beneficial security research. Once discovered, a vulnerability is reported to the affected standards bodies and manufacturers so that they can remedy it before it becomes publicly known. The research team provides details of their discovery and analysis, interacting with industry security specialists as they devise an appropriate countermeasure. One researcher typically acts as the point-of-contact between the research team and the industry parties. Papers describing vulnerabilities are embargoed from public release before a given publication deadline to allow the remediation to take place in secret. During this process, vulnerabilities are assigned a Common Vulnerabilities and Exposures (CVE) Identifier and evaluated for severity using the Common Vulnerability Scoring System (CVSS). This provides a clear and common format for controlled distribution to affected manufacturers, along with a measure of criticality for prioritising fixes. Typically, researchers will have proposed potential mitigations in their papers, which can form the starting point for practical fixes. When successfully executed, the coordinated disclosure process allows critical vulnerabilities to be fixed for the majority of users before the vulnerabilities can be maliciously exploited. This provides an obvious benefit to the users themselves, be they individuals or businesses, and also to the manufacturers who avoid the costs and liability of security breaches resulting from the vulnerability. As such, firms often operate Bug Bounty programmes to reward researchers for their efforts.

The coordinated disclosure process was conducted twice by Kasper Rasmussen's research team, with contact first made for the KNOB vulnerability described in [**R2** & **R4**] and the established relationships then used for the BIAS work in [**R3**]. The result of [**R2**] was initially reported to the Bluetooth Special Interest Group (SIG) and CERT Coordination Center (CERT/CC) in October 2018. This established communication with Intel, who were the responsible partner for the cross-industry Unified Security Incidence Response Process (USIRP) as defined by the International Consortium for Advancement of Cybersecurity on the Internet (ICASI) [**E1**]. The research team was in dialogue with Intel from January 2019 onwards regarding action to coordinate mitigation efforts, with Antonioli acting as the point-of-contact via email and telephone. The research paper was embargoed until August 2019 to aid these efforts. The later work in [**R3**] was reported in December 2019 through the same channels, with the associated paper embargoed until May 2020. In both instances, the research team provided detailed technical information, analysis, and potential countermeasures as derived from their work.

The main point of contact for the research team in both cases was with the Intel Product Security Incident Response Team (iPSIRT). In addition to chairing the USIRP, Intel also conducted their own vulnerability remediation, as a major manufacturer of Bluetooth devices. As the collaboration progressed, the research team was in direct contact with ICASI as well as through Intel, further working with CERT Coordination Center (CERT/CC) and the Bluetooth Special Interest Group (SIG) directly. CERT/CC is a non-profit body hosted by Carnegie Mellon University and funded by the US Government that coordinates security response events with industry. The Bluetooth SIG is the specification body for Bluetooth industry, representing over 36,000 member companies [**E4**.1]. These bodies in turn coordinated a response among their members.

The KNOB attack in [**R2**] was evaluated by Intel as "Critical", with a score of 9.3 (out of 10) [**E1**], which resulted in Intel awarding a Bug Bounty Firmware Payout of USD30,000 [**E1**], their maximum firmware payout [**E7**]. CERT/CC issued CVE Identifier, CVE-2019-9506, and a Vulnerability Note, VU#918987 [**E2**]. The attack was also evaluated at an industry-wide level as "High", with a score of 8.1 under CVSS v3.0 [**E2**]. For context, this score is higher than that for the well-known Spectre vulnerability (5.6, "Medium"), Heartbleed bug (7.5, "High") or WPA2 KRACK attack (6.8, "Medium"). This score therefore clearly indicated that the attack required a priority response. As documented below, industry acted very quickly to provide fixes, interrupting normal development schedules to ensure that timely mitigations were made available.

The subsequent BIAS attack in [**R3**] was issued CVE-2020-10135 by CERT/CC, who released Vulnerability Note VU#647177, and evaluated as 5.4 "Medium" under CVSS v3.0 [**E9**]. While this score is lower than for the earlier work, it only addresses the direct effects of the attack and does consider that it further enhances the power of the KNOB attack – a fact explicitly stated in the vulnerability note [**E8**] and discussed in the Bluetooth SIG response [**E4**.4].

Working together with the researchers and CERT/CC, ICASI subsequently led disclosures to the whole ICASI membership [**E1**]. They also coordinated with Apple and Lenovo through ICASI Collaborator NDAs. As ICASI noted of the handling of [**R2**]: "the goal of this coordination was for CERT/CC and the Bluetooth SIG to notify as many potentially impacted vendors as possible so that they could develop the appropriate fixes, while minimizing the risk that the vulnerability would be disclosed prior to a fix being available" [**E3**].

Industry acted quickly to provide fixes during the coordinated response process. Most major platform vendors released patches immediately following the public disclosure: Microsoft for Windows; Apple for macOS, iOS, and watchOS; Google for Android; Cisco for IP phones and Webex; Huawei for Android phones; and BlackBerry for Android-powered devices [**E5**]. Patches were similarly made available for popular Linux distributions such as debian, Red Hat and Ubuntu [**E5**]. Intel published a white paper and a statement in response to the disclosure of the research findings, recommending that "in all cases, components participating in a secure Bluetooth connection employ the highest level of encryption possible" [**E6**].

On 13 August 2019, the Bluetooth SIG announced that it had "updated the Bluetooth Core Specification to recommend a minimum encryption key length of 7 octets for BR/EDR connections" [**E4**.2] as recommended in [**R2**]. The SIG "strongly recommends that product developers update existing solutions to enforce" this minimum, and "is also broadly communicating details on this vulnerability and its remedy to our member companies and is encouraging them to rapidly integrate any necessary patches" [**E4**.3]. The SIG represents over 36,000 member companies [**E4**.1]. CERT/CC also issued an advisory referring Bluetooth host and controller suppliers to the updated specification and instructing downstream vendors to refer to their suppliers for updates [**E2**]. Both the Bluetooth SIG's technical update and CERT/CC's advisory describe the technical contribution of the paper [**R2**].

As described in their Security Notice [**E4**.4 & 5], the Bluetooth SIG made further fixes to the standard in direct response to the BIAS attack [**R3**]: "to remedy this vulnerability, the Bluetooth SIG is updating the Bluetooth Core Specification to clarify when role switches are permitted, to ensure a role switch in the middle of a secure authentication procedure does not affect the procedure, to require authenticating the peer device in legacy authentication, and to recommend checks for encryption-type to avoid a downgrade of secure connections to legacy encryption. These changes will be introduced into a future specification revision."

Due to the well-executed disclosure process, the final experience for most users was the seamless deployment of software patches to protect them [**E5**]. In the case of the KNOB attack [**R2**, **R4**], by the time the vulnerability information became public – and thus at greater risk of malicious exploitation – mitigations were already widespread. Further, there had been sufficient opportunity for industry to analyse the intricate technical details of the research papers and produce accessible guidance that users could readily act upon [**E3**, **E4**.2–5, **E6**].

As a fundamentally preventative activity, and while parts of the industry response are still ongoing, it is difficult to precisely quantify the investment in remedying the KNOB and BIAS vulnerabilities – or indeed the economic savings that pre-empting any malicious exploitation has yielded. However, for context, the costs associated with the WPA2 KRACK attack

(CVSS v.3.0 score of only 6.8, lower than the KNOB attack's 8.1) have been placed in the tens of millions of dollars [**E9**], while the cost of the Heartbleed bug (CVSS v.3.0 score of 7.5) has been estimated in the hundreds of millions of dollars [**E10**]. What is certain is that the researchers' coordinated disclosure allowed remediation to begin before malicious exploitation could take place, and that the corrections to the Bluetooth Core Specification guarantee that this work [**R2**–**R4**] will continue to have an industry-wide impact in the future, protecting many millions of Bluetooth users from malicious attacks and associated harm.

5. Sources to corroborate the impact

[**E1**] Coordinated disclosure emails regarding (1) the KNOB attack and (2) the BIAS attacks.
[**E2**] NIST National Vulnerability Database (NVD) entry for KNOB attack: http://tiny.cc/26auiz; Common Vulnerabilities and Exposures (CVE) entry for KNOB attack: http://tiny.cc/uyauiz;
CERT/CC advisory and vulnerability note on the KNOB attack: http://tiny.cc/70qqiz.
[**E3**] Statement from ICASI on the Bluetooth BR/EDR Vulnerability, 13 August 2019: https://www.icasi.org/br-edr-encryption-key-bluetooth-vulnerability/.
[**E4**] Bluetooth SIG (https://www.bluetooth.com/):
(1) SIG information and member numbers: https://www.bluetooth.com/about-us/; global market information in Bluetooth Market Update report 2020 (at p. 10): http://tiny.cc/u9v0tz.
(2) Expedited Errata Correction 11838 to the Core Specification.
(3) Security Notice regarding KNOB attack and Technical Update advising about the correction to the Core Specification: http://archive.ph/G1IVz.
(4) Response to BIAS attacks disclosure.
(5) Security Notice regarding BIAS attacks: https://tinyurl.com/y2j3pga5.
[**E5**] Patches announced in August 2019 by major platform vendors: Microsoft Windows – http://archive.ph/HaNVs; Apple macOS – http://archive.ph/Bbyb0, iOS – http://archive.ph/YqPvC, watchOS – http://archive.ph/UZ7pb; Google – http://archive.ph/3lpuJ; Cisco – http://archive.ph/6k9ZJ; Huawei – http://archive.ph/1Z1pG; BlackBerry – http://archive.ph/Yzjjf. Linux patches: debian –http://archive.ph/LdNhr; Red Hat – http://archive.ph/Emm4z; Ubuntu – http://archive.ph/jkTzY.
[**E6**] Intel Bluetooth Security – Encryption Key Size Recommendation statement and white paper, August 2019: http://archive.ph/ICUk2.
[**E7**] Information on Intel bug bounty payments from cybersecurity firm HackerOne: https://hackerone.com/intel. According to a HackerOne report (at p. 3) the average bug bounty payout for a critical vulnerability in 2019 was USD3,384: http://tiny.cc/4uqrsz.
[**E8**] NIST NVD entry for the BIAS attack: https://tinyurl.com/y5vku5to; CVE entry for the BIAS attack: https://tinyurl.com/y2uxe9eb (http://archive.ph/bcEAE); CERT/CC advisory and vulnerability note for BIAS attack: https://tinyurl.com/yxspma5m.
[**E9**] ZDNet article discussing WPA2 KRACK and costs: http://archive.ph/ik38B.
[**E10**] eWeek article estimating cost of Heartbleed: http://archive.ph/IMt3t.