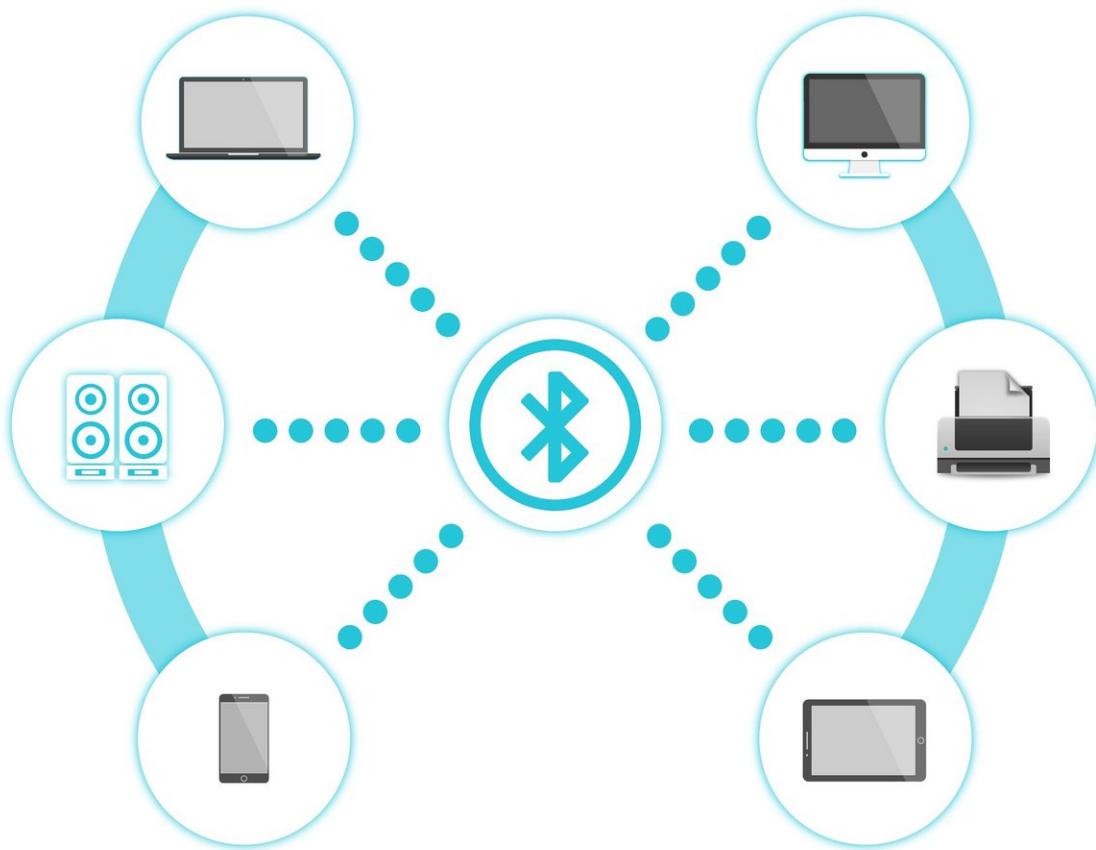


# Specification vulnerability in devices that speak Bluetooth is addressed

August 18 2019, by Nancy Cohen

---



Credit: CC0 Public Domain

The discovery of a flaw in Bluetooth specification that could enable an

attack to spy on your information made news this week; the attacker could be able to weaken the encryption of Bluetooth devices and snoop on communications or send falsified ones to take over a device, said *The Verge*.

The flaw was acknowledged by the group overseeing the Bluetooth standard, and the specification was changed.

The attack was dubbed KNOB and both identified and demonstrated by an international group of researchers. Daniele Antonioli, Singapore University of Technology and Design; Nils Ole Tippenhauer, CISPA Helmholtz Center for Information Security; and Kasper Rasmussen, University of Oxford, were the investigators.

This attack potential pertained basically to all devices that "speak Bluetooth", said the investigators; any standard-compliant Bluetooth device, they said, could be expected to be vulnerable.

"We conducted KNOB attacks on more than 17 unique Bluetooth chips (by attacking 24 different devices). At the time of writing, we were able to test chips from Broadcom, Qualcomm, Apple, Intel, and Chicony manufacturers. All devices that we [tested](#) were vulnerable to the KNOB attack."

In November 2018 they shared details of the attack with the Bluetooth Special Interest Group, the CERT Coordination Center and the International Consortium for Advancement of Cybersecurity on the Internet (ICASI), an industry led coordination body.

KNOB stands for the Key Negotiation of Bluetooth ([KNOB](#)) Attack. The reason for that name became clear in seeing how the attack was described.

"The specification of Bluetooth includes an [encryption](#) key negotiation protocol that allows to negotiate encryption [keys](#) with 1 Byte of entropy without protecting the integrity of the negotiation process. A remote attacker can manipulate the entropy negotiation to let any standard compliant Bluetooth device negotiate encryption keys with 1 byte of entropy and then [brute force](#) the low entropy keys in real time."

A further detailed overview comes from Carnegie Mellon University Software Engineering Institute, CERT Coordination Center, sponsored by the Department of Homeland Security Office of Cybersecurity and Communications:

"The encryption key length negotiation process in Bluetooth BR/EDR Core v5.1 and earlier is vulnerable to packet [injection](#) by an unauthenticated, adjacent attacker that could result in information disclosure and/or escalation of privileges. This can be achieved using an attack referred to as the Key Negotiation of Bluetooth (KNOB) attack, which is when a third party forces two or more victims to agree on an encryption key with as little as one byte of entropy. Once the entropy is reduced, the attacker can brute-force the encryption key and use it to decrypt communications."

(Jacob Kastrenakes, *The Verge*, remarked Friday: "The vulnerability is pretty clever: instead of directly breaking the encryption, it allows hackers to force a pair of Bluetooth devices to use [weaker](#) encryption in the first place, making it far easier to crack.")

Moving forward, what has been done to address the flaw?

Zak Doffman, CEO of Digital Barriers, reported in *Forbes* that "To resolve the issue, the Bluetooth Core Specification has changed "to recommend a [minimum](#) encryption key length of 7 octets for BR/EDR connections."

Product developers were being told to update existing solutions.

Here are excerpts from the Bluetooth Security Notice.

"To remedy the vulnerability, the Bluetooth SIG [The Bluetooth Special Interest Group is the standards organisation that oversees the development of Bluetooth standards.] has updated the Bluetooth Core Specification to recommend a minimum encryption key length of 7 octets for BR/EDR connections. The Bluetooth SIG will also include testing for this new recommendation within our Bluetooth Qualification Program. In addition, the Bluetooth SIG strongly recommends that product developers update existing solutions to enforce a minimum encryption key length of 7 octets for BR/EDR [connections](#)."

The security notice also detailed some range and timing limitations governing whether or not such an attack could actually be carried out successfully.

"For an attack to be successful, an attacking device would need to be within wireless range of two vulnerable Bluetooth devices that were establishing a BR/EDR connection. If one of the devices did not have the vulnerability, then the attack would not be successful. The attacking device would need to intercept, manipulate, and retransmit key length negotiation messages between the two devices while also blocking transmissions from both, all within a narrow time window. If the attacking device was successful in shortening the encryption key length used, it would then need to execute a brute force attack to crack the encryption key. In addition, the attacking device would need to repeat the attack each time encryption gets enabled since the encryption key size negotiation takes place each time."

At the time of this writing, reports from various sites attempted to deliver updates on the flaw and which vendors were addressing it either

by actions or actions still in the wings.

The researchers, meanwhile, presented their findings at the USENIX Security Symposium. (USENIX began in 1975 as the original UNIX users group and since evolved to become the Advanced Computer Systems Association.)

The team's paper detailing their research was titled "The KNOB is Broken: Exploiting Low Entropy in the Encryption Key Negotiation Of Bluetooth BR/EDR" and included in the Proceedings of the 28th USENIX Security Symposium.

There's no evidence the attack has actually been used, said [Steven Melendez](#) on Friday in *Fast Company*.

*TechSpot's* [Adrian](#) Potoroaca addressed the status of the situation in a brief roundup. "While all current Bluetooth BR/EDR devices are susceptible to it, there is an easy fix that Microsoft and Apple are already rolling out. The Bluetooth Core Specification has also been changed to require manufacturers to hardcode a minimum encryption key length of seven octets (characters) in future devices."

Similarly, *Fast Company* had its report, saying that the industry group behind Bluetooth standards updated the specification to ban overly short [encryption keys](#) while companies including Microsoft and Apple rolled out operating system patches to fix the flaw in their rounds of updates.

**More information:** [knobattack.com/](http://knobattack.com/)

[www.usenix.org/conference/usenix19/presentation/antonioli](http://www.usenix.org/conference/usenix19/presentation/antonioli)

Citation: Specification vulnerability in devices that speak Bluetooth is addressed (2019, August 18) retrieved 20 March 2024 from <https://techxplore.com/news/2019-08-specification-vulnerability-devices-bluetooth.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.