Bluetooth: It's complicated. Armis Labs researchers see pitfalls

13 September 2017, by Nancy Owano

(Tech Xplore)—If you ask two researchers what is the problem with Bluetooth they will have a simple answer.

"Bluetooth is complicated. Too complicated. Too many specific applications are defined in the stack layer, with endless replication of facilities and features." Case in point: the WiFi specification (802.11) is only 450 pages long, they said, while the Bluetooth specification reaches 2822 pages.

Unfortunately, they added, the complexity has "kept researchers from auditing its implementations at the same level of scrutiny that other highly exposed protocols, and outwards-facing interfaces have been treated with."

Lack of review can end up with vulnerabilities needing identification.

And that is a fitting segue to this week's news about devices with Bluetooth capabilities.

At Armis Labs, Ben Seri and Gregory Vishnepolsky are the two researchers who discussed the vulnerabilities in modern Bluetooth stacks—and devices with Bluetooth capabilities were estimated at over 8.2 billion, according to the Armis site's overview.

Seri and Vishnepolsky are the authors of a 42-page white paper detailing what is wrong and at stake in their findings. The discovery is being described as an "attack vector endangering major mobile, desktop, and IoT operating systems, including Android, iOS, Windows, and Linux, and the devices using them."

They are calling the vector BlueBorne, as it spreads via the air and attacks devices via Bluetooth. Attackers can hack into cellphones and computers simply because they had Bluetooth on. "Just by having Bluetooth on, we can get malicious code on your device," Nadir Izrael, CTO and cofounder of security firm Armis, told *Ars Technica*.

Let's ponder this, as it highlights a troubling aspect of attack: Lorenzo Franceschi-Bicchierai at *Motherboard*:

"'The user is not involved in the process, they don't need to be in discoverable mode, they don't have to have a Bluetooth connection active, just have Bluetooth on,' Nadir Izrael, the co-founder and chief technology officer for Armis, told *Motherboard*."

Their white paper identified eight vulnerabilities: (The authors thanked Alon Livne for the development of the Linux RCE exploit.)

1. Linux kernel RCE vulnerability - CVE-2017-1000251
2. Linux Bluetooth stack (BlueZ) information Leak vulnerability - CVE-2017-1000250
3. Android information Leak vulnerability - CVE-2017-0785
4. Android RCE vulnerability #1 - CVE-2017-0781

5. Android RCE vulnerability #2 - CVE-2017-0782
6. The Bluetooth Pineapple in Android - Logical Flaw CVE-2017-0783
7. The Bluetooth Pineapple in Windows - Logical Flaw CVE-2017-8628
8. Apple Low Energy Audio Protocol RCE vulnerability - CVE-2017-14315

Why do their discoveries matter?

The Armis Labs site overview pointed to what could go wrong.

The overview said, "The BlueBorne attack vector requires no user interaction, is compatible to all software versions, and does not require any preconditions or configurations aside of the Bluetooth being active. Unlike the common misconception, Bluetooth enabled devices are constantly searching for incoming connections from any devices, and not only those they have been paired with. This means a Bluetooth connection can be established without pairing the devices at all. This makes BlueBorne one of the most broad potential attacks found in recent years, and allows an attacker to strike completely undetected."

Zack Whittaker, security editor for *ZDNet*, had this to say about its nature. "Malware exploiting the attack vector may be particularly virulent by passing peer-to-peer and jumping laterally, infecting adjacent devices when Bluetooth is switched on."

He added, "A single infected device moving through a busy office past dozens of people with phones, tablets, or computers with Bluetooth switched on could cause a rapid infection across networks —leading to network infiltration, ransomware attacks, or data theft."

UK-based James Walker in *Digital Journal*:

"BlueBorne is so serious because it has an unusually high reach...An attacker doesn't need to craft special links, create email scams or hijack your Internet to distribute malware. They can just wait until you have Bluetooth turned on."

So what's next? Armis Security notified significant third parties after it discovered the vulnerability, said Walker. At the time of this writing: "Google and Microsoft have both already released security patches for their affected products, closing the vulnerability. The Linux kernel maintainers have acknowledged Armis' report and plan to release an update this week."

The Armis site said, "Information on Linux updates will be provided as soon as they are live."

Ars Technica weighed in: "Izrael said he expects Linux maintainers to release a fix soon."

The vulnerability was mitigated by Apple in iOS 10.

The authors stated that "We hope this paper will be an initial step for a wider and more inclusive audit of the security issues that might lie dormant in the various Bluetooth stacks that are part of the 8.2 Billion Bluetooth devices that are in use today. We encourage other researchers to use this paper as a guideline for the various pitfalls that might exist in implementations of Bluetooth stacks."

ZDNet summed up the situation: "Several companies, including software and device makers, were notified of the vulnerabilities in April and have since rolled out patches. The majority of newer phones, tablets, and some computers have already been fixed."

Older devices though could be vulnerable to such exploits. Nonetheless, *Motherboard* noted that "the fact that they depend on the limited range of Bluetooth and that would-be hackers would need to develop separate exploits for each different device and operating system makes them impractical to target victims at scale."

Russell Brandom in *The Verge* offered a similar explanation, saying "the specific exploit varies from system to system, making it difficult to write a single virus that would be able to target every vulnerable device. Bluetooth itself limits the bug even further: Blueborne can only target devices within range of the hackers, and only devices with Bluetooth turned on."

APA citation: Bluetooth: It's complicated. Armis Labs researchers see pitfalls (2017, September 13) retrieved 21 February 2018 from https://techxplore.com/news/2017-09-bluetooth-complicated-armis-labs-pitfalls.html