ALL Bluetooth devices SPY ON YOU

Undocumented "backdoor" found in Bluetooth chip used by a billion devices

By

Bill Toulas

The ubiquitous ESP32 microchip made by Chinese manufacturer Espressif and used by over 1 billion units as of 2023 contains an undocumented "backdoor" that could be leveraged for attacks.

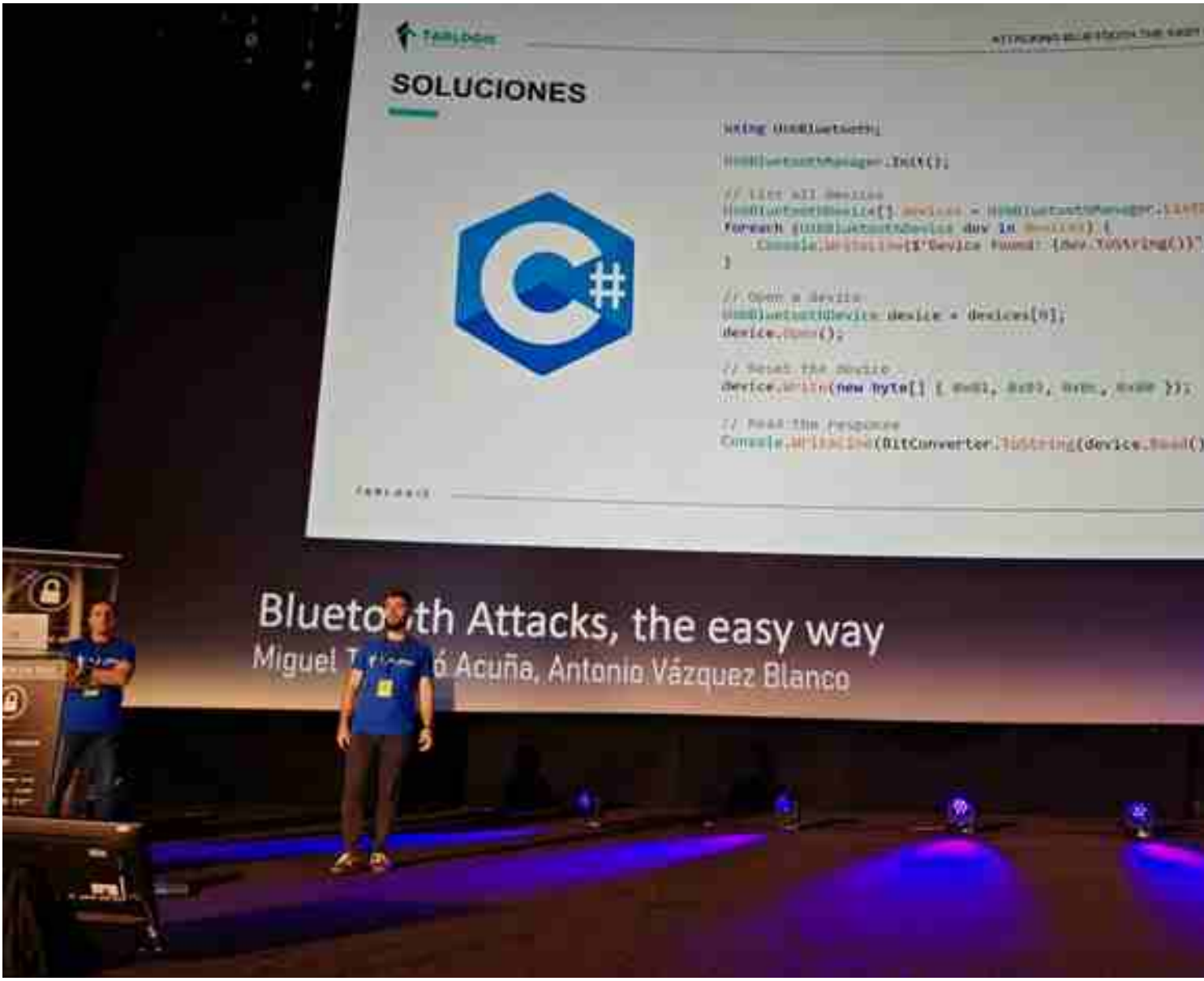
The undocumented commands allow spoofing of trusted devices, unauthorized data access, pivoting to other devices on the network, and potentially establishing long-term persistence.

This was discovered by Spanish researchers Miguel Tarascó Acuña and Antonio Vázquez Blanco of Tarlogic Security, who presented their findings yesterday at RootedCON in Madrid.

"Tarlogic Security has detected a backdoor in the ESP32, a microcontroller that enables WiFi and Bluetooth connection and is present in millions of mass-market IoT devices," reads a Tarlogic announcement shared with BleepingComputer.

"Exploitation of this backdoor would allow hostile actors to conduct impersonation attacks and permanently infect sensitive devices such as mobile phones, computers, smart locks or medical equipment by bypassing code audit controls."

The researchers warned that ESP32 is one of the world's most widely used chips for Wi-Fi + Bluetooth connectivity in IoT (Internet of Things) devices, so the risk of any backdoor in them is significant.



Slide from the RootedCON presentation

Source: Tarlogic

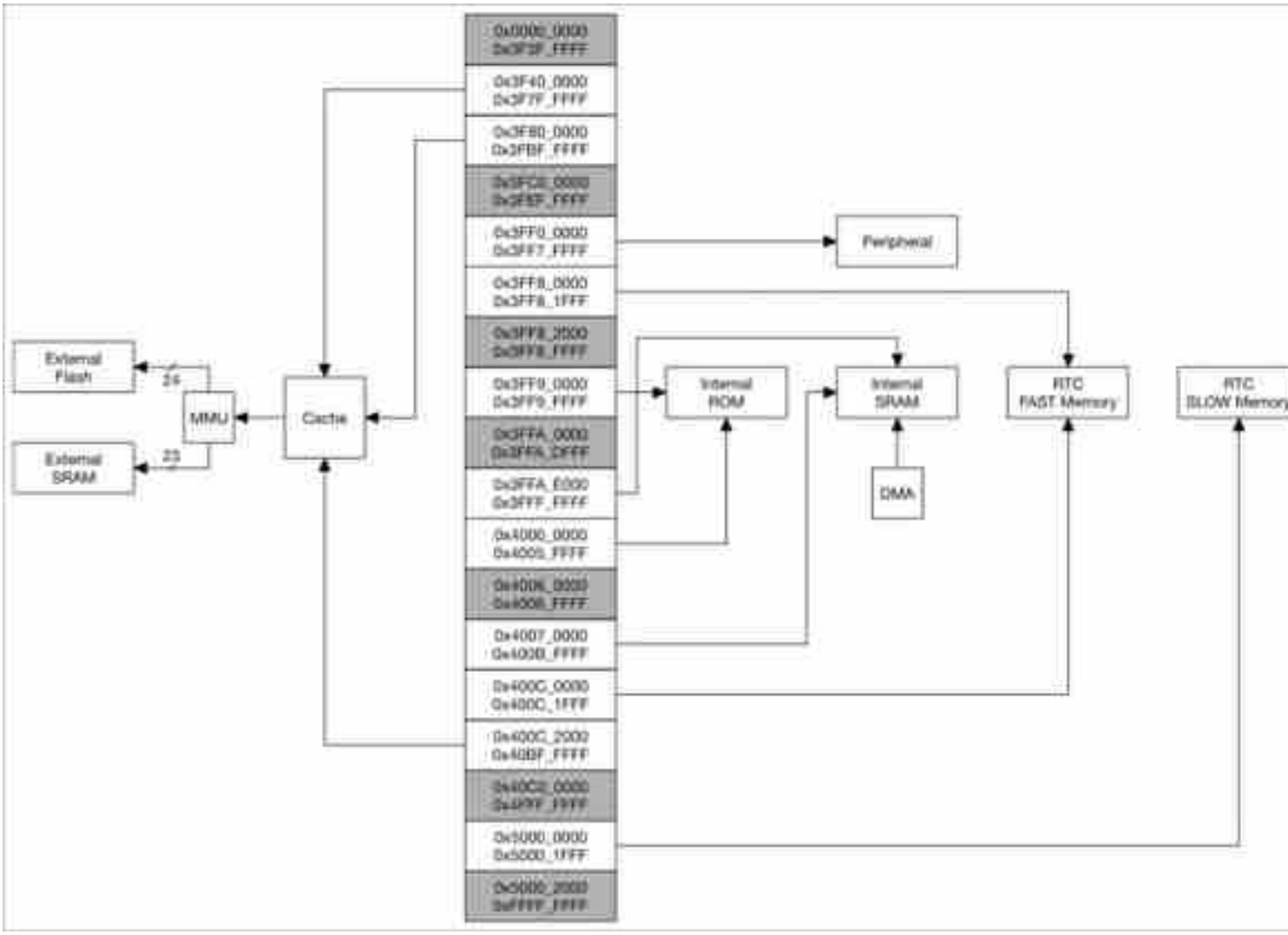
Discovering a backdoor in ESP32

In their RootedCON presentation, the Tarlogic researchers explained that interest in Bluetooth security research has waned but not because the protocol or its implementation has become more secure.

Instead, most attacks presented last year didn't have working tools, didn't work with generic hardware, and used outdated/unmaintained tools largely incompatible with modern systems.

Tarlogic developed a new C-based USB Bluetooth driver that is hardware-independent and cross-platform, allowing direct access to the hardware without relying on OS-specific APIs.

Armed with this new tool, which enables raw access to Bluetooth traffic, Targolic discovered hidden vendor-specific commands (Opcode 0x3F) in the ESP32 Bluetooth firmware that allow low-level control over Bluetooth functions.

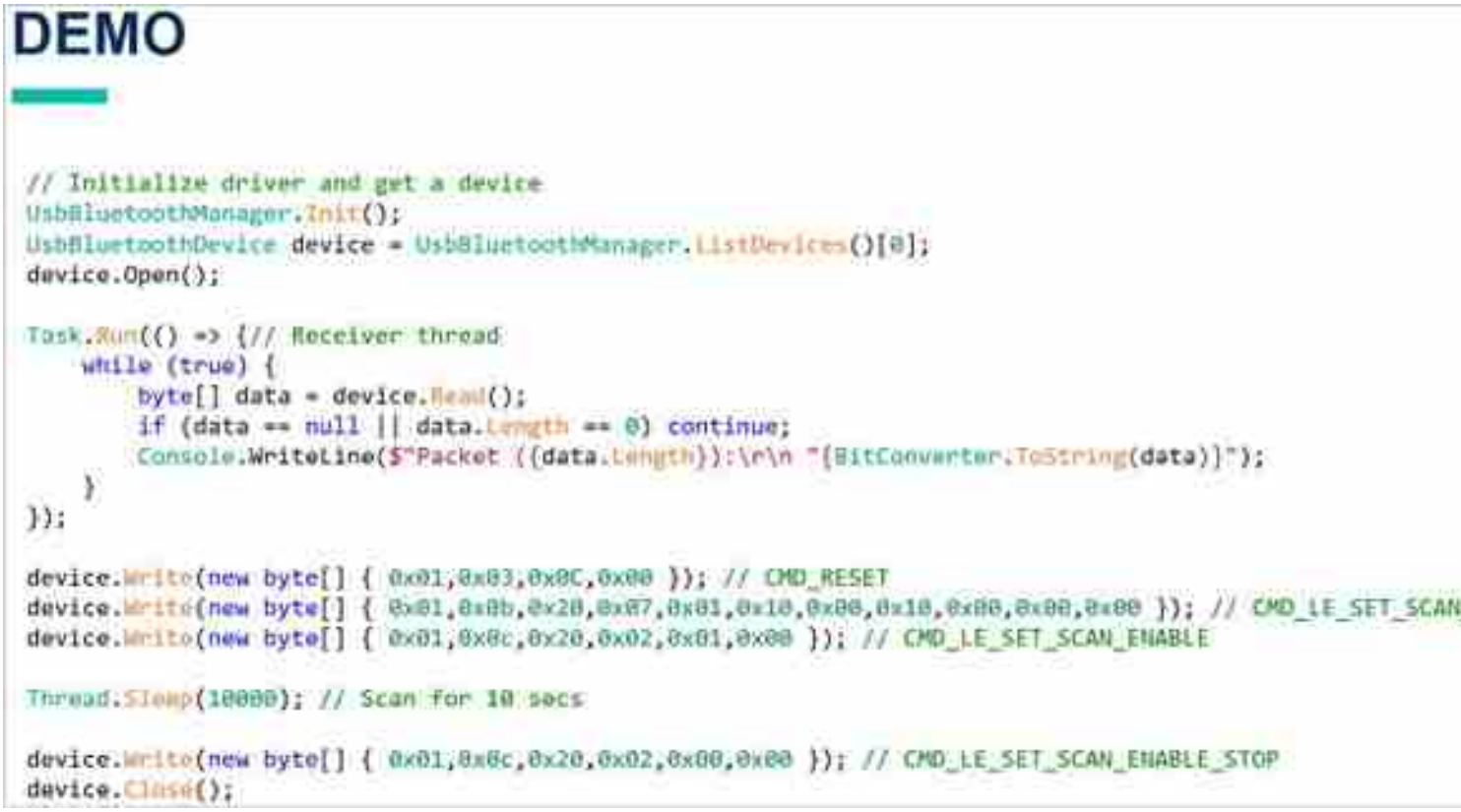


ESP32 memory map

Source: Tarlogic

In total, they found 29 undocumented commands, collectively characterized as a "backdoor," that could be used for memory manipulation (read/write RAM and Flash), MAC address spoofing (device impersonation), and LMP/LLCP packet injection.

Espressif has not publicly documented these commands, so either they weren't meant to be accessible, or they were left in by mistake.



Script that issues HCI commands

Source: Tarlogic

The risks arising from these commands include malicious implementations on the OEM level and supply chain attacks.

Depending on how Bluetooth stacks handle HCI commands on the device, remote exploitation of the backdoor might be possible via malicious firmware or rogue Bluetooth connections.

This is especially the case if an attacker already has root access, planted malware, or pushed a malicious update on the device that opens up low-level access.

In general, though, physical access to the device's USB or UART interface would be far riskier and a more realistic attack scenario.

"In a context where you can compromise an IOT device with as ESP32 you will be able to hide an APT inside the ESP memory and perform Bluetooth (or Wi-Fi) attacks against other devices, while controlling the device over Wi-Fi/Bluetooth," explained the researchers to BleepingComputer.

"Our findings would allow to fully take control over the ESP32 chips and to gain persistence in the chip via commands that allow for RAM and Flash modification."

"Also, with persistence in the chip, it may be possible to spread to other devices because the ESP32 allows for the execution of advanced Bluetooth attacks."

BleepingComputer has contacted Espressif for a statement on the researchers' findings, but a comment wasn't immediately available.

Related Articles:

Privacy tech firms warn France's encryption and VPN laws threaten privacy

New Auto-Color Linux backdoor targets North American govts, universities

Zyxel won't patch newly exploited flaws in end-of-life routers

Backdoor found in two healthcare patient monitors, linked to IP in China

Chinese cyberspies use new SSH backdoor in network device hacks