Frankenstein: Advanced Wireless Fuzzing to Exploit New Bluetooth Escalation Targets

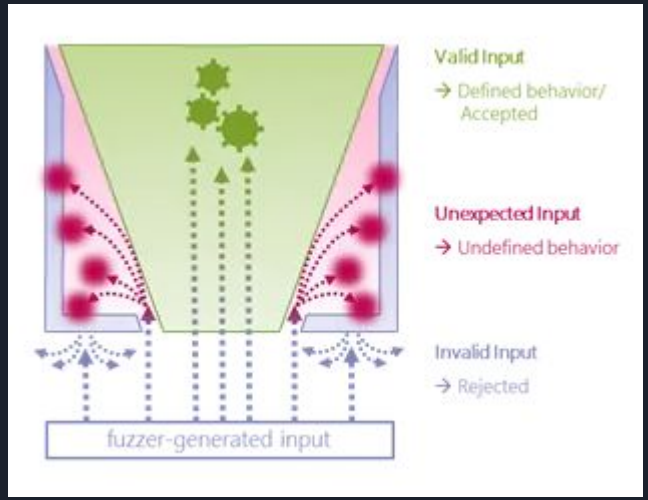
COMPSCI 702 - Reuben Speirs

What was the motivation behind the research?

- Large amount of smartphone users.
- Bluetooth connectivity in vast majority.
- Large attack surface.
- Connectable once bluetooth on and by default.

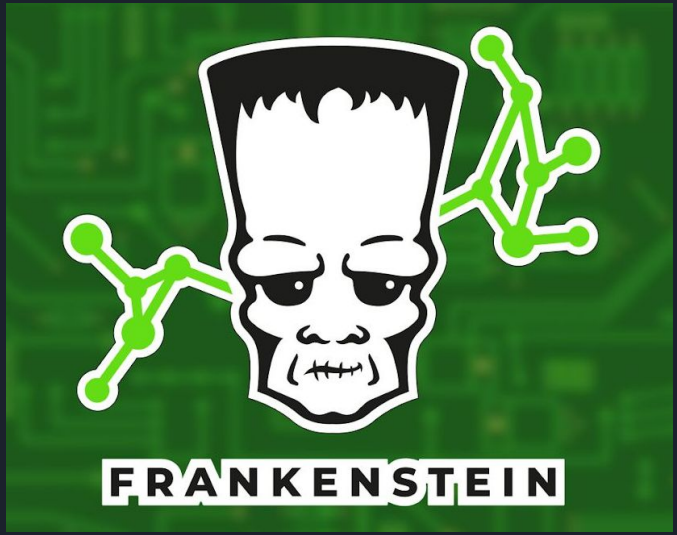
What is fuzzing?

- Inputs into an app to find bugs
- Often automated and random.
- Used as part of dynamic analysis.



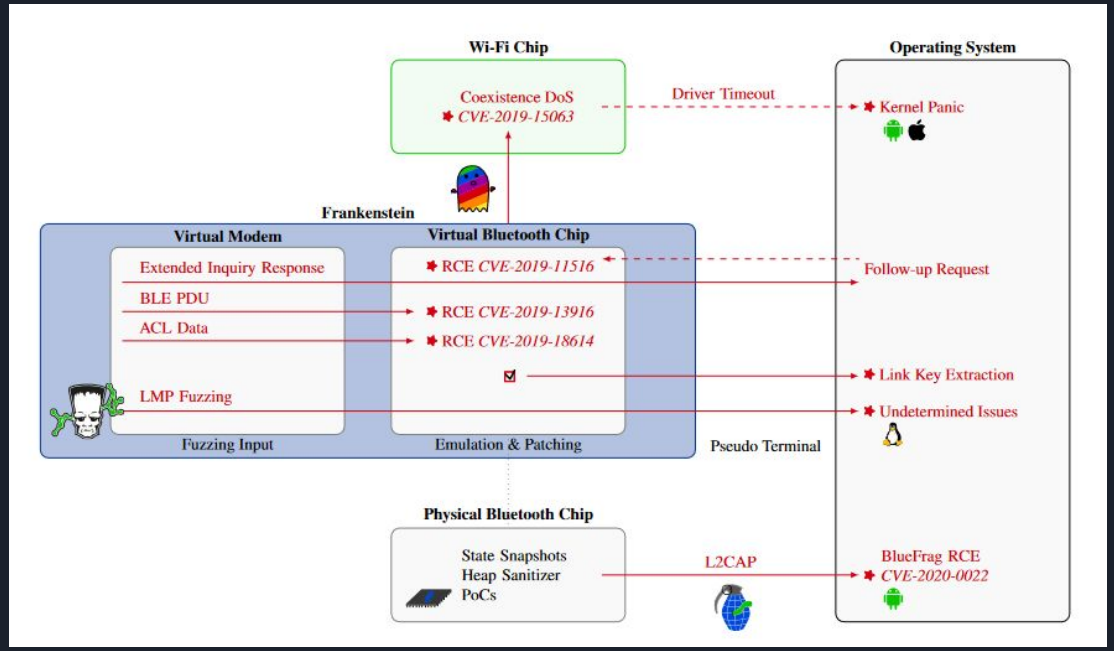
How does frankenstein work?

- Emulation of the firmware during execution.
- Snapshots of the hardware using the CYW2073 bluetooth controller.
- Named Frankenstein as emulation of snapshot used to bring firmware to life in another environment specifically host PC.
- Frankenstein allows for RCE.
- Saving state and injecting code.
- Debugging calls.



What was found

- Several vulnerabilities were found including:
  - Link key extraction
  - Interchip escalation
  - Bricking devices



Link key extraction

- Link key extraction used for encryption.
- Key can be used to eavesdrops on communication between devices.
- In some cases view shared private information such as phone contacts.
- Link keys from inactive devices can be retrieved for use at a later data

Interchip escalation

- Wifi and Bluetooth functionality on same chip.
- Escalation from Bluetooth to access Wifi.
- Cant software patch.
- Disabling Bluetooth functionality when Wifi is connected solves the issue.

Examples of interchip escalations effects on devices.

Chip	Device	OS	Build Date	Address	Value	Effect
BCM4335C0	Nexus 5	Android 6.0.1	Dec 11 2012	0x650440, 0x650600	0x00	Disconnects from 2.4 GHz and 5 GHz Wi-Fi, Wi-Fi can be re-connected.
BCM4345B0	iPhone 6	iOS 12.4	Jul 15 2013	0x650000–0x6507ff		Disables 2.4 GHz Wi-Fi until restarting Bluetooth.
BCM4345C0	Raspberry Pi 3+/4	Raspbian Buster	Aug 19 2014	0x650000–0x6507ff	Random	Full and partial Wi-Fi crashes, including Secure Digital Input Output (SDIO), ability to scan for Wi-Fis, speed reduction. Re-boot required to restore functionality.
BCM4358A3	Nexus 6P	Android 7.1.2	Oct 23 2014	0x650000–0x6507ff		Disables all Wi-Fi until restarting Bluetooth.
BCM4358A3	Samsung Galaxy S6	Lineage OS 14.1	Oct 23 2014	0x650000–0x6507ff		Disables all Wi-Fi until restarting Bluetooth.
BCM4345C1	iPhone SE	iOS 12.4–13.3.1	Jan 27 2015	0x650200	0xff	Kernel panic, resulting in a reboot.
BCM4355C0	iPhone 7	iOS 12.4–13.3.1	Sep 14 2015	0x650200		Kernel panic, resulting in a reboot.
BCM4347B0	Samsung Galaxy S8	Android 8.0.0	Jun 3 2016	0x650200		Disables 2.4 GHz and 5 GHz Wi-Fi, kernel panic and reboot when re-enabling Wi-Fi.
BCM4347B0	Samsung Galaxy S8	LineageOS 16.0	Jun 3 2016	0x650200		Temporarily disables 2.4 GHz and 5 GHz Wi-Fi, freezes system for a couple of seconds when re-enabling Wi-Fi.
BCM4347B1	iPhone 8/X/XR	iOS 12.4–13.3.1	Oct 11 2016	0x650200		Kernel panic, resulting in a reboot.
BCM4375B1	Samsung Galaxy S10/S10e/S10+	Android 9	Apr 13 2018	0x650200		Disables 2.4 GHz and 5 GHz Wi-Fi. Reboot required to re-enable Wi-Fi.
BCM4377B3	MacBook Pro/Air 2019–2020	macOS 10.15.1–10.15.5	Feb 28 2018	0x650400		Kernel panic, resulting in a reboot.
BCM4378B1	iPhone 11	iOS 13.3	Oct 25 2018	0x650400		Kernel panic, resulting in a reboot.

Brick devices

- Bluetooth chip uses read only memory to store firmware and patches.

- Non volatile random access memory used during manufacturing to store device specific information.

- Could be written to to brick devices.

Ineffective solutions: Disabling bluetooth

- Newer devices not disabled.
- Not hard reset on disable/flight mode.
- Some devices such as iPhones do not hard reset while the S10e does during flight mode.
- Reliance on bluetooth always on for connectivity makes attacking more convenient.

Issues take a long time to patch

- Slow times to fix report issues by Broadcom, Samsung and other vendors.
- Limit physical patchroms means patching vulnerabilities is limited.
- Chips usually a year old once they are release in off the shelf devices. So hard to test for vulnerabilities with limit access to hardware.
- Always being connected and devices not being reset means over the air attacks are more likely than ever.

Acknowledgement

[1] Frankenstein: Advanced Wireless Fuzzing to Exploit New Bluetooth Escalation Targets

Jan Ruge and Jiska Classen, Secure Mobile Networking Lab, TU Darmstadt; Francesco Gringoli, Dept. of Information Engineering, University of Brescia; Matthias Hollick, Secure Mobile Networking Lab, TU Darmstadt

https://www.usenix.org/conference/usenixsecurity20/presentation/ruge

Thank you for listening!!!

Questions?