HANDS-ON AUTOMOTIVE EXPLOITATION

BASIC BLUETOOTH BUFFER OVERFLOW

SPEAKER: KAMEL GHALI

SECURE OUR STREETS - 2022

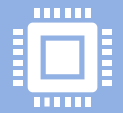
WHOAMI

- "Automotive Cybersecurity Technology Architect" at White Motion
  - Subsidiary of Marelli (International Automotive Tier1 Supplier)
  - Based in Tokyo
- Trilingual Car Hacking Enthusiast
  - English, Arabic, and Japanese
  - Ex-Admin of ASRG (Automotive Security Research Group) Detroit
  - Founder of ASRG Japan
- Jack of ~~all~~ some trades, master of none
- Recent areas of interest:
  - Bluetooth
  - USB
  - RF
  - Fighting with obscure Taiwanese microcontrollers
- Hobbies include fighting games, cooking, playing the ukulele, and getting lost

OBJECTIVES OF THIS TALK

- Short Explanation of Automotive Bluetooth
- Short Overview of Buffer Overflow Software Vuln.
- Short Real-Time Demo
- Q&A

SHORT BLUETOOTH INTRO



Short-range, cable replacement technology

Very widely used, used in almost all IoT devices worldwide

Sensor data, audio data, file transfers, media, etc.

Advertised ranges can be very long, but in practice most applications are within 30m.

WHAT IS A BUFFER OVERFLOW VULNERABILITY?

BUFFER OVERFLOW

- Software Vulnerability
  - Input Data > Allocated Buffer Size
  - Memory Corruption
  - Overwrite Variables
  - Execution Interference
- No Input Validation
- Mainly Affect C/C++

DEMO TIME!

*BUT FIRST, A SHORT DISCLAIMER

- The vulnerable program used in this demo is intentionally made to be VERY insecure
  - This is in no way reflective of Bluetooth applications used in any modern vehicle
- This vulnerability in no way reflects the security posture of any company's product(s)

DEMO PLATFORM

- Simple Password Input Over Bluetooth
  - Correct Password (HiKamel) → Root Privileges Granted!
  - Incorrect Password → Goodbye!

- Easy enough, right? Let’s do some trials!

DEMO TRIALS

TRIAL	Expected Outcome	Observed Outcome
INCORRECT PASSWORD		
CORRECT PASSWORD		
??????????????		

CONCLUSION

- The buffer overflow attack clearly invoked unintended functionality from the target
- This vulnerability was *an issue with the application running on the target – NOT the target's Bluetooth implementation itself*
- Attacking the Bluetooth protocol itself would be a different area of study entirely – but not impossible at all!

REFERENCES USED

- Bluetooth Specification RFCOMM V12
  - https://www.bluetooth.org/docman/handlers/DownloadDoc.ashx?doc_id=263754
- An Introduction to Bluetooth Programming
  - https://people.csail.mit.edu/albert/bluez-intro/index.html
- Keen Labs Lexus Research
  - https://keenlab.tencent.com/en/2020/03/30/Tencent-Keen-Security-Lab-Experimental-Security-Assessment-on-Lexus-Cars/
- Article About Tesla Fob Hack
  - https://www.wired.com/story/tesla-model-x-hack-bluetooth/
- Tesla BLE Relay Article
  - https://research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/

THANK YOU!

KAMEL.GHALI@WHITE-MOTION.COM

MKAMEL.GHALI@ASRG.IO

LINKEDIN: KAMEL GHALI