Spanalytics, LLC
01010010101010010

We Are:

- Leaders in the field of wireless cyber security
- Manufacturer of best-in-class IoT analysis tools
- Decades of experience in security audits and penetration testing
- One of the only companies to do deep dive training in IoT Wireless and Cyber Security
- Located in Richmond, Virginia
- A Veteran-Owned Small Business

Should I Worry About the Bluetooth and Wi-Fi in my Car?

Could your car's Bluetooth or Wi-Fi leave you vulnerable to attacks?

Discovered Vulnerabities

Spanalytics has perfomed Bluetooth and Wi-Fi evaluations on dozens of car makes and models, consequently finding a variety of problems, like:

- ➢ Bluetooth security was weak, such that a "beach-head" could be established with possible pivoting to another bus.
- ➢ Information leaks, like phone contacts left on the head unit
- ➢ A previous "trusted device" can be spoofed to gain wireless access

Identified Bluetooth and Wi-Fi Weakness:

Denial of Service:

Various levels of susceptibility to DoS attacks from remote devices. Additional vulnerabilities can exist when a DoS attack is performed.

SSP Debug Mode:

Allows SSP Debug Mode, which means all Bluetooth traffic can be decrypted by a Bluetooth sniffer.

Trusted Device Info:

BD_ADDR and link keys are available via the MMI. Spoofing these devices to perform DoS attacks then becomes easy.

Weak/No MITM Protection:

For legacy pairing, the unit does not force the user to validate the PIN code. This could result in a hacking device connection to the unit without the user's knowledge

Residual Phonebook Data:

Displays all of the phone book contacts of a trusted device when it is connected with a spoofing device.

Hot-Mike the Cabin:

Does not provide active MITM protection or security upon connection to the Hands Free Profile

Discoverability:

Always discoverable or is discoverable for "too long". The longer your device is discoverable the easier it is to identify by a hacker.

Connectability:

Always connectable or is connectable for "too long." This can lead to DoS, fuzzing, or other attacks. A unit should also limit the time it attempts to auto-connect to trusted devices.

Low Energy Pairing:

Bluetooth 4.0 devices use either Just Works or Passkey Entry association models during paring, neither of which provide protection against passive eavesdropping.

Weak Bluetooth Encryption:

Does not enforce 128-bit encryption key size or fails to initiate encryption when the connected device does not start encryption

Wi-Fi Range:

Wi-Fi hotspot range exceeds immediate area surrounding the vehicle

Wi-Fi Port Vulnerability:

An open IP port available for connection.

Wi-Fi Weak Encryption:

WEP encryption is allowed, which can be broken

Physical and Mailing Address: 4190 Innslake Dr., Glen Allen, VA, 23060
Phone: (804) 364-1050 **Email:** contact@spanalytics.com **Website:** Spanalytics.com