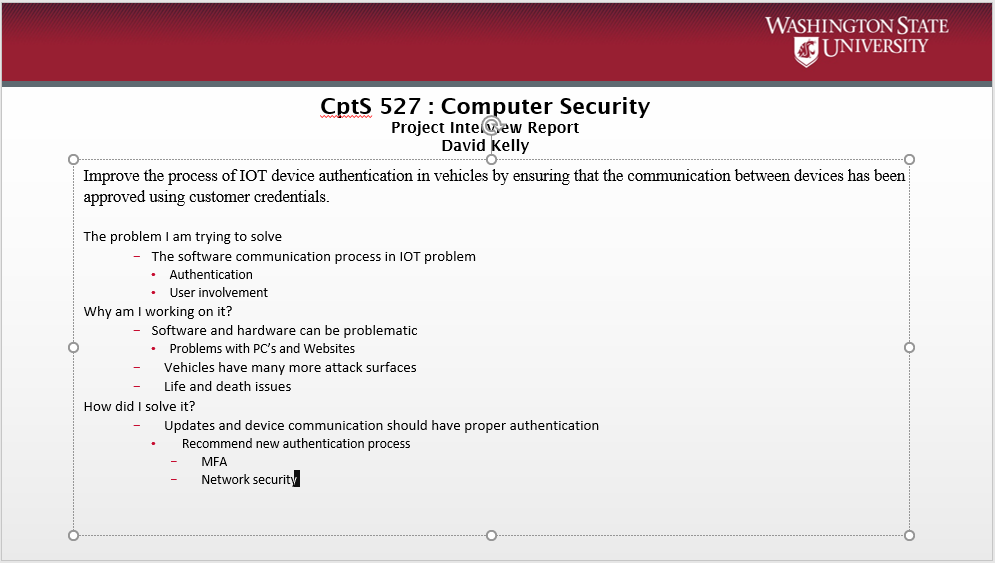
**Project Interview Report**

David Kelly

7/25/2021

**Power point for presentation:**



**Case study I analyzed:**

1. IOT and network security in Vehicles

**Validation experiments:**

**Connected to a 2002 ford taurus and 2008 VW Jetta**

1. Connect OBD code scanner Autophix OM126 into 16 pin data port
   1. This tool has its own screen and is not Bluetooth or Wifi enabled.
   2. The goal is to test clearing codes, getting VIN, CID, CVN codes, turn off codes (Violates Confidentiality, Integrity and Availability (CIA))
2. Connect OBD code scanner Veepeak Mini Bluetooth OBD2 Scanner for Android
   1. This tool is network capable. It is lower cost but can create a DoS attack on your battery if left in.
3. Connect OBD code scanner Veepeak OBDCheck BLE+ Bluetooth 4.0 OBD2 Scanner for iOS & Android into 16 pin data port.
   1. This tool is network capable – Bluetooth using the latest ELM327 command protocol for developers.
   2. I will install a 3rd party app on my Android phone called Torque and do the following tests. These tests can violate CIA by exposing driving data and creating a possible DoS attack. The test will be administered from another vehicle within range of the Bluetooth signal. The following tests will be run:
      1. Send GPS tagged tweets directly to twitter
      2. Send logging information to email CSV/KML for analysis
      3. Set warning and alarms
      4. More as available on app.

**Theory Outline**

1. Title
2. Abstract
   1. Authentication, IOT Devices and network in vehicles, threats. The increasing number of (wireless) interfaces available in today’s cars exposes it to new attack vectors. Automotive remote keyless entry systems have also been shown to use weak key management and cryptographic primitives, enabling an eavesdropping adversary to clone the car key [7]
3. Index Terms:
   1. Electronic control units, Controller area network (CAN), CAN Bus, Bluetooth interface, cyber-attack
4. Introduction
   1. State of the art - State of the art papers **reflect the present state of scientific or engineering development**. Review papers reflect a broader view: history, development, and present state of scientific development.
   2. Research problem
      1. Authentication is not standard or in existence in IOT devices and CAN networks
   3. Proposed solution/Contributions
   4. MFA in updates and IOT interoperability, Valet access.
      1. MAC – auth data and create session keys
      2. Certificate
      3. SessionID created when start
      4. TLS in the CAN
      5. UserId, password
      6. Biometric or temp code
   5. Outline of this Paper
5. Related Work
   1. A light weight protocol for CAN [8]
6. Contributions/Experiments/Results
   1. Connect OBD code scanner Autophix OM126 into 16 pin data port
   2. Connect OBD code scanner Veepeak Mini Bluetooth OBD2 Scanner for Android
   3. Connect OBD code scanner Veepeak OBDCheck BLE+ Bluetooth 4.0 OBD2 Scanner for iOS & Android
7. Future Work
   1. Electric Vehicle testing
8. Conclusion
   1. How this contribution will make vehicles safer.
9. Acknowledgment
   1. Assistance with helping to conduct experiments.
10. References

[3] C. Miller and C. Valasek, Remote exploitation of an unaltered passenger vehicle. Black Hat USA, 2015.

Page 35 - Jailbreaking Uconnect, update process. a USB stick (jailbreak) or access to the in-car Wi-Fi (exploiting the D-Bus vulnerability/functionality).

Command injection is quite typical when dealing with user input from supposed trusted sources

Page 47 Note: We did not actually exploit the vehicles, so we can’t say with 100% certainty that they are vulnerable but they do have a listening D-Bus service that we could interact with remotely without authentication. Note: The recall that resulted from this research affected 1.4 million vehicles. It seems our estimate above was a bit low.

Page 50 we see that the IOC can be re-flashed with firmware and that no cryptographic signatures are used to verify the firmware is legitimate. .

Page 64: Updates. Flashing the v850 without USB. The biggest complication for an attacker is that the system is only designed to perform the upgrade from a USB stick, which as remote as remote attackers we can’t assume exists. We want to flash the V850 from the OMAP chip without a USB stick.

Page 71: The entire exploit chain

Page 78 : security access keys not need for Fiat/chrystler. Are needed for Ford and Toyota.

Diagnostic CAN message: Diagnostic messages are more powerful than normal messages, however most ECUs will ignore diagnostic messages if the car is traveling at speed, usually faster than 5-10 mph. Therefore, these attacks can typically only be performed when the car is travelling rather slowly, unless the attacker can figure out how to forge a speed used to determine if diagnostic messages should be accepted.

Page 87: A fix was made by Chrysler for this issue and can be found in version 15.26.1. We did not extensively study this patch although the net result is that the vehicle now no longer accepts incoming TCP/IP packets. This is the result of an nmap scan before the patch (version 14.25.5)

Additionally, the Sprint network was reconfigured to block (at least) port 6667 traffic even within the same cellular tower. Therefore, the only way to attack a vulnerable, unpatched, vehicle is to either do it over Wi-Fi, if available, or over a femtocell connection. Both require close range to the vehicle

[CWE 798 Use of Hard-coded Credentials (cvedetails.com)](https://www.cvedetails.com/cwe-details/798/cwe.html)

[Tesla : Products and vulnerabilities (cvedetails.com)](https://www.cvedetails.com/vendor/16203/Tesla.html)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Notes

Tesla cars regularly receive over-the-air software updates that add new features and enhance existing functionality via Wi-Fi. When an update is available, you will be notified on your in-vehicle touchscreen display, with the option to install immediately or schedule for later.

https://www.tesla.com/en\_AE/support/software-updates

Audi does offer over the air updates, but only for its vehicle maps. Those sorts of updates are sent out regularly and can be done from home an a wifi connection. Unfortunately for current e-tron owners, any other software updates must be manually done at a dealership.

BMW began using OTA updates in 2018 and has slowly increased its presence since. The automaker does offer over-the-air software updates to most of its models, but not to the full extent as some other competitors. Currently, BMW’s OTA updates extend to infotainment systems and to purchase and install “optional equipment features.” Furthermore, updates to the Advanced Driver Assistance Systems (ADAS) can be updated OTA in a limited capacity.

Audi, BMW, BYD, Canoo, Faraday Future, Fiat Chrysler (FCA), Ford, General Motors (GM), Honda, Hyundai Motor Group (Hyundai/Kia/Genesis), Jaguar/Land Rover, Li Auto, Lucid Motors, Mercedes-Benz, NIO, Nissan, Polestar, Porsche, Rivian, Tesla, Toyota, Volkswagen (VW), Volvo, Weltmeister (WM Motor) and Xpeng.

Autonomous vehicle is self-driving

Tesla uses a digital key - https://www.cnbc.com/2019/11/09/the-demise-of-the-car-key-tesla-lincoln-ditch-keys-for-mobile-entry.html and an app as keys and to drive the car. They also give the customer a backup keycard or standard key fob for lost phones or for a valet.

Automakers such as Volkswagen are scheduled to release vehicles with “ultra-wideband” connections instead of Bluetooth that can communicate and respond in milliseconds.