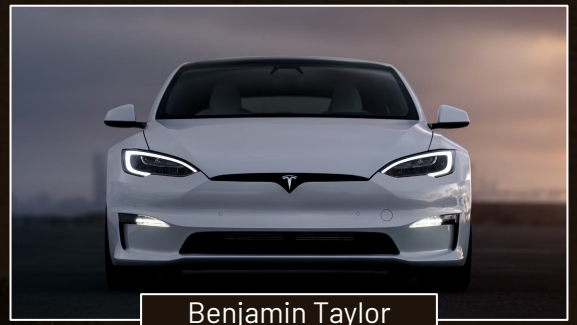
2015 Tesla Model S Hack

Case Study on Automotive Cybersecurity



Benjamin Taylor
Fall 2024 - ITCS-3166

Agenda Overview

01 Understanding the Risk

I. Why Automotive Cybersecurity Matters

II. What is the Tesla Model S Hack

III. Timeline of the Attack

02 Analyzing the Impact

I. Impact of the Tesla Model S Hack

II. How the Attack Worked

03 Lessons and Future Outlook

I. Lessons Learned

II. Conclusion (Future of Automotive Security

III. References

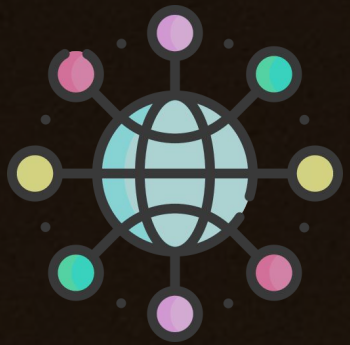
**to jump to a slide, *click the title*

01

Understanding the Risk

Why Automotive Cybersecurity Matters

- Modern vehicles are increasingly becoming more reliant on software and connected systems
- The more advanced they get, the more connected they are - and that comes with serious risks
- The 2015 Tesla Model S Hack showed some of the risks, helping to raise awareness about securing connected vehicles (with vulnerabilities ranging from the brakes to the wipers)
- This case study analyzes the attack, its impact, and key lessons for the future of automotive cybersecurity. It was a essentially a wake-up call for everyone about how crucial cybersecurity is in this space



What is the Tesla Model S Hack?

- In 2015, security researchers Marc Rogers and Kevin Mahaffey found and pointed out some critical vulnerabilities in the Tesla Model S software
- Demonstrated at DEF CON 23, the hack showed how attackers could exploit the car's systems to take control of major functions. They found their way in through a diagnostic port and tweaked the cars firmware to give themselves control over some major functions:
  - Brakes *(applying or releasing them even while vehicle was moving)*
  - Radio and Displays *(adjusting volume, changing settings, displaying fake information)*
  - Windshield Wipers *(turning them on or off at will)*
  - Trunk *(remotely opening and closing)*
- Tesla responded to this by quickly releasing an over-the-air software update that fixed the vulnerabilities

Timeline of the Attack

Pre-2015

- Researchers Marc Rogers and Kevin Mahaffey started investigating Tesla Model S systems
- Focused on analyzing vulnerabilities in the car's firmware and diagnostics
- Identified initial points of entry via the Ethernet diagnostic port

Mid-2015

- Discovered the ability to exploit firmware vulnerabilities
- Demonstrated control over key functions during testing (the brakes, wipers, and displays)
- Prepared for a public demonstration at DEF CON 23.

August 2015

- Hack revealed at DEF CON 23
- Researchers showcased the ability to remotely control the Tesla Model S
- Highlighted the risks of connected vehicle vulnerabilities

Post-DEF CON

- Tesla issued an over-the-air update to fix the vulnerabilities
- Introduced stricter security measures to prevent future attacks
- The incident pushed the automotive industry to prioritize cybersecurity

02

Analyzing the Impact

Impact of the Tesla Model S Hack

Control Over Critical Systems

Researchers demonstrated remove control over:

- Brakes: Applied while the car was in motion
- Infotainment System: Adjusted displays, radio, and settings
- Windshield Wipers: Activated unexpectedly
- Trunk: Opened and closed remotely

Safety Concerns

- Highlighted the potential for accidents or driver distractions
- Raised questions about the safety of connected vehicles

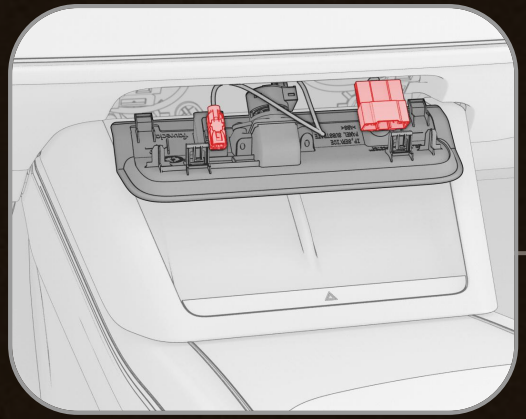
Public Awareness

- Brought global attention to the importance of cybersecurity in vehicles
- Demonstrated how software vulnerabilities could lead to physical consequences

Tesla's Response

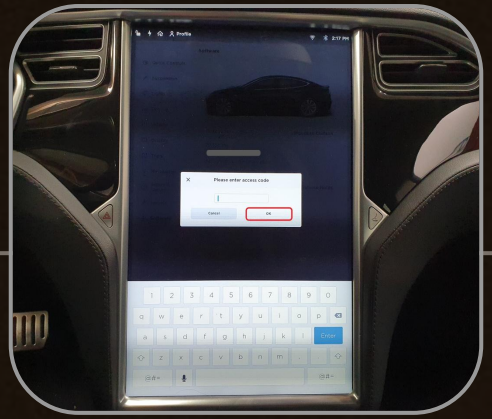
- Released a quick over-the-air update, addressing all of the vulnerabilities
- Set a new industry standard for quick response to cybersecurity threats

How the Attack Worked



Step 1: Physical Access

- Researchers connected to the car's diagnostic port via an Ethernet cable
- The provided access to the car's internal systems for initial exploration



Step 2: Firmware Exploitation

- Vulnerabilities in the car's firmware were identified and modified
- Enabled control over critical systems such as brakes, wipers, and infotainment

Step 3: Remote Access

- Once the firmware was compromised, remote control was demonstrated
- Researchers controlled the car over a wireless network as well, to show how the attack could be scaled

03

Lessons and Future Outlook

Lessons Learned

1. **Importance of Regular Software Updates**
   - Tesla's quick software update showed the value of staying ahead of vulnerabilities
   - Shows how proactive updates can address cybersecurity risks before they even escalate
2. **Comprehensive Security Testing**
   - Rigorous testing of vehicle systems is essential to uncover potential flaws.
   - Manufacturers should simulate attacks in order to identify vulnerabilities early on
3. **Collaboration with Researchers**
   - Tesla's collaboration with researchers demonstrated the value of external audits
   - Demonstrated the value of bug bounty programs or external audits
4. **Securing Connected Systems**
   - Emphasized the need to protect all connected components, from diagnostic ports to wireless communication
   - Reinforced the importance of encryption, authentication, and access controls

Conclusion (Future of Automotive Security)

- The 2015 Tesla Model S hack was a huge moment and turning point in the automotive industry, and it showed people the real-world risks of software vulnerabilities in connected vehicles
- It highlighted the importance of:
  1. Regular software updates to address potential exploits
  2. Comprehensive security testing to uncover weaknesses before attackers do
  3. Collaboration between manufacturers and researchers to enhance vehicle security
- As vehicles become more autonomous and connected, cybersecurity will definitely need to stay a critical focus to ensure people are safe and there is that aspect of public trust throughout the process

References

- https://www.youtube.com/watch?v=KX_0c9R4Fng&ab_channel=DEFCONConference
- https://en.wikipedia.org/wiki/Automotive_hacking
- https://www.wired.com/2015/08/researchers-hacked-model-s-teslas-already
- https://money.cnn.com/2015/08/06/technology/tesla-hack
- https://service.tesla.com/docs/ModelS/ServiceManual/Palladium/en-us/GUID-334598EE-397C-4BEF-B952-F331F87C3551.html
- https://service.tesla.com/docs/ModelS/ServiceManual/en-us/GUID-0DC534D7-A4B8-417F-8E42-DF1560E970C2.html
- https://grahamcluley.com/watch-teslas-hacked-drive-20-away/

References cont.

- https://www.businessinsider.com/tesla-model-3-minimalistic-interior-again-2017-8
- https://www.tuev-nord.de/en/company/traffic/manufacturers/electronic-system-and-car-it/automotive-cybersecurity/
- https://companieslogo.com/tesla/logo/
- https://www.topspeed.com/how-tesla-could-make-model-s-better/
- https://www.wirelesscar.com/connected-car-essentials-puts-car-makers-on-the-road-to-better-digital-services/
- https://www.flaticon.com/free-icon/network_5321845
- https://www.teslarati.com/tesla-advanced-summon-remote-control-mode-regulator-approval-elon-musk/