Evan Jester

I130- Intro to Cybersecurity

Professor J Duncan

December 12, 2023

RFID Paper Summary

Hackers Can Steal a Tesla Model S in Seconds by Cloning Its Key Fob

This paper described how a group of researchers from the University of Leuven in Belgium discovered a way to duplicate Tesla Model S key fobs with only $600 in equipment, allowing for immediate car theft. Because of the weak 40-bit cipher encryption on the key fobs, hackers were able to intercept and decrypt codes that looked like the key fob. In response, Tesla improved the encryption on the key fob and added a PIN code feature for extra security. Due to the use of similar keyless entry systems, vehicles from McLaren, Karma, and Triumph motorcycles may also be affected by the vulnerability. Tesla encouraged owners of older models to upgrade their keychains or utilize the PIN feature, and it paid a bug bounty to the researchers.

Source-

A. Greenberg, "Hackers Can Steal a Tesla Model S in Seconds by Cloning Its Key Fob," Wired, 10-Sep-2018. [Online]. Available: https://www.wired.com/story/hackers-steal-tesla-model-s-seconds-key-fob/. [Accessed: 12-Dec-2023].

Auto theft on the rise in Toronto area, and a security expert thinks he knows why

The article discussed how thieves are utilizing "relay theft" tactics, which involve boosting the signal from key fobs inside of homes to unlock and start cars, to cause an increase in auto thefts in the Toronto area. Car thefts have significantly increased as a result of this

technique; Toronto reports a 30% increase over the previous year. To prevent theft, security expert Jeff Bates advises car owners to use signal-blocking devices like Faraday cages and to keep their key fobs away from the front door. The difficulty is finding a balance between security requirements and the simplicity of use of keyless entry systems.

Source-

T. Simmons, "Auto theft on the rise in Toronto area, and a security expert thinks he knows why," CBC News, 04-Dec-2018. [Online]. Available: https://www.cbc.ca/news/canada/toronto/car-thefts-rising-1.4930890. [Accessed: 12-Dec-2023].

Crooks are stealing cars using previously unknown keyless CAN injection attacks

The study provided information on CAN injection attacks, a recently developed type of keyless vehicle theft. By altering with the car's Controller Area Network (CAN), the thief's device can be made to appear to the car as a genuine key fob. This technique was uncovered by cybersecurity researcher Ian Tabor following the theft of his Toyota RAV4. The device that thieves use to connect to the car's CAN bus is usually hidden as a common object, such as a speaker, and is usually accessed through the headlights. Through the use of signals mimicking a working key, the device enables thieves to unlock and operate the vehicle. This technique has developed as a result of manufacturers' and car owners' increased security measures, which have rendered traditional relay attacks—which amplify key fob signals—less effective.

Source-

D. Goodin, "Crooks are stealing cars using previously unknown keyless CAN injection attacks," Ars Technica, 07-Apr-2023. [Online]. Available:

https://arstechnica.com/information-technology/2023/04/crooks-are-stealing-cars-using-previously-unknown-keyless-can-injection-attacks/. [Accessed: 12-Dec-2023].

To steal today's computerized cars, thieves go high-tech

The paper discussed how the growing computerization of cars has led to a high-tech rise in car thefts nowadays. Millions of lines of code and multiple computers are now commonplace in cars. Keyless entry systems and remote starts are targeted by thieves, who use methods such as listening in on digital codes and constructing electronic bridges to intercept and replicate these signals. An alternative approach entails breaching the vehicle's internal network, particularly the controller area network bus, in order to manipulate the engine or replicate key codes. Some robbers even turn to antiquated techniques like the USB hack, taking advantage of weaknesses in specific car designs. Updating car software and adhering to fundamental security protocols are crucial for thwarting these sophisticated thefts.

Source-

D. Jacobson, "To steal today's computerized cars, thieves go high-tech," The Conversation, 14-Aug-2023. [Online]. Available: https://theconversation.com/to-steal-todays-computerized-cars-thieves-go-high-tech-210358. [Accessed: 12-Dec-2023].

Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars

The paper conveys relay attacks against contemporary automobiles' Passive Keyless Entry and Start (PKES) systems. In order to allow an attacker to start and unlock a car by relaying messages between the car and its key fob, the researchers developed two types of relay setups (wired and wireless). Their tests on ten different car models from eight different manufacturers demonstrated the viability of such attacks, exposing a serious security flaw in

PKES systems. In order to reduce the danger of these relay attacks, the paper also suggests countermeasures.

Source-

A. Francillon, B. Danev, S. Capkun, "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars," Department of Computer Science, ETH Zurich, 8092 Zurich, Switzerland. [Online].