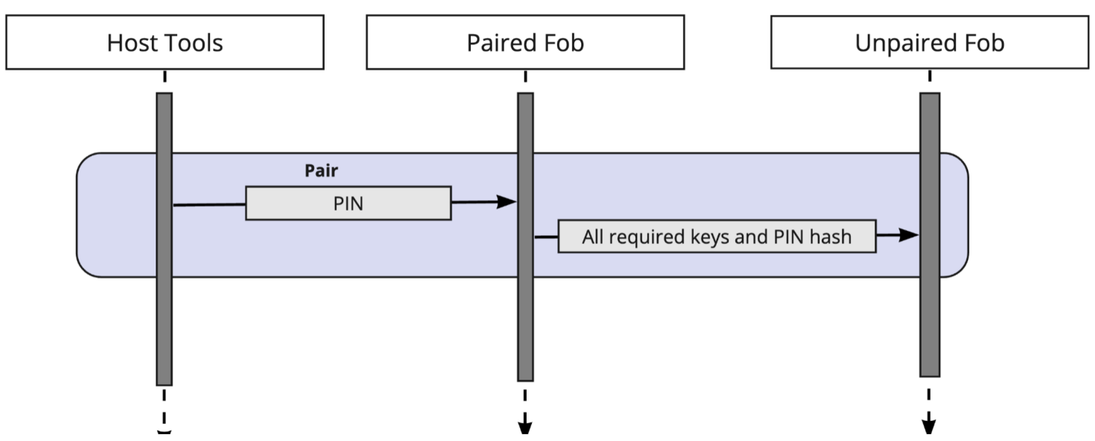
Plaid Parliament of Pwning

Carnegie Mellon University

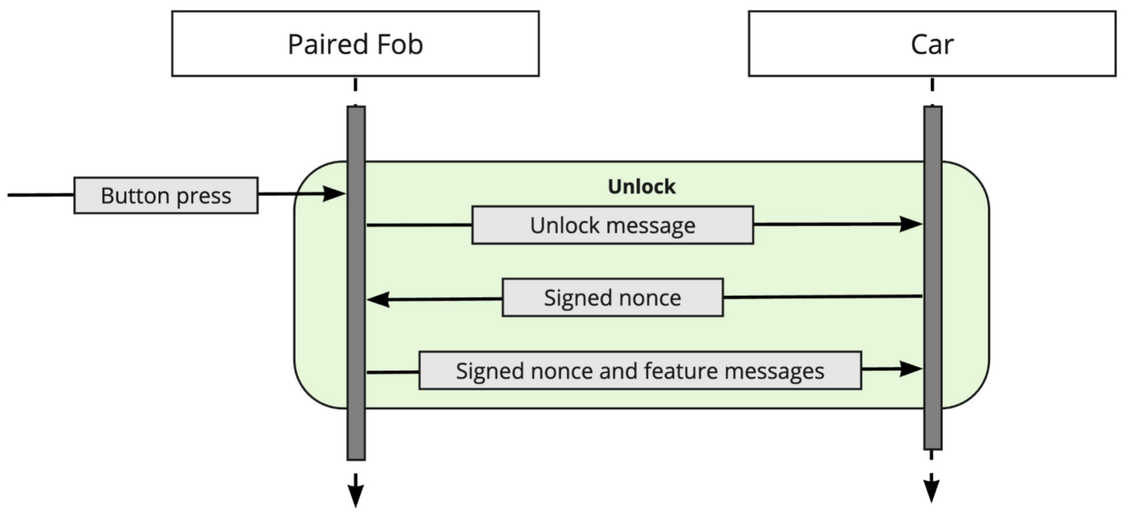
Eliana Cohen, Aditya Desai, Nandan Desai, Neha Gautam, Henry Howland, Ray Huang, Harrison Leinweber (Lead)
Ethan Oh, Palash Oswal, Anish Singhani, Carson Swoveland, Madeline Tasker-Fernandes, Suma Thota, Hanjie Wu
Advised by: Anthony Rowe, Patrick Tague, Maverick Woo
April 24, 2023

Design Overview

- **Package Feature**: Features are signed using deployment key to prevent tampering.
- **Enable Feature**: To enable a feature, the paired fob verifies the package signature with the public deployment key and also checks for a matching Car ID.
- **Pair Fob**: When a paired fob receives the correct pairing pin from the host computer, the paired fob information is securely sent to the unpaired fob.



- **Unlock Car**: Unlocking a car involves a secure and random challenge/response protocol between the car and the paired fob.



- Encryption and signatures combine to ensure message confidentiality, integrity, and authenticity between devices.
- Security requirements are met through robust encryption/signature schemes, secure EEPROM storage of secrets, and a strong RNG.

Defensive Highlight

EEPROM Encrypt	Compiler Countermeasures	Anti-glitching
Power analysis protection	Protections Against Bruteforce	Protections Against Replay

- We built a TRNG (True Random Number Generator) based off the ADCs' least significant bit.
- We used Von Neumann's whitening method to debias the ADC output, and used both ADCs for redundancy.
- Ideally, we would have used additional entropy sources, or a proper TRNG/Hardware crypto chip.

Offensive Highlight

- One important set of attacks performed were the timings attacks that were possible due to the use of functions such as `memcmp` and `strcmp`. These functions compare one character at a time and return when the first incorrect character is encountered, making the execution time vary based on the number of correct characters in the given input.
- Our attack involved trying all possible values for the first character, and identifying the correct character based on the one that takes the longest execution time. The same process is repeat for all other characters.
- In order to defend against this attack, all comparisons should be performed in constant time, so that a wrong input is indistinguishable from the correct one.

Images showing the extraction of first and second bytes of a PIN using timing attacks