Design Philosophy

- Define a comprehensive threat model, especially for buffer overflows and side-channels
- Avoid over-engineering our protocols, to reduce risk of introducing vulnerabilities
- Limit the impact and scope of exploits, even if compromise does occur

Protocol Overview

- **Car Unlock**
  - Randomized challenge-response by car to fob
  - Symmetric key AEAD Encryption using Ascon

- **Fob Pairing**
  - Salted and Hashed 6-digit pairing PIN
  - Persistent 4 sec. timeout on each PIN attempt

- **Feature Package**
  - Unique 32-bit feature password for each car
  - Salted and Hashed feature stored on car

<table>
<thead>
<tr>
<th>Attacker Goal / Capability</th>
<th>Brute forcing pairing PIN</th>
<th>Unauthorized car unlock</th>
<th>Unauthorized car features</th>
<th>Unauthorized fob duplication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access to car</td>
<td>No PIN on car</td>
<td>Symmetric keys on car/fob</td>
<td>Unique feature passwords</td>
<td>No PIN on car</td>
</tr>
<tr>
<td>Temporary fob access</td>
<td>Delay</td>
<td>Unique challenge-response</td>
<td>Unique feature passwords</td>
<td>Salt-then-hash pairing PIN</td>
</tr>
<tr>
<td>Access to car with features</td>
<td>No PIN on car</td>
<td>Symmetric keys on car/fob</td>
<td>Unique feature passwords</td>
<td>No PIN on car</td>
</tr>
</tbody>
</table>

Attacks

- **Shared Secrets**:
  - Shared secrets allowed reusing fobs on other cars.
- **Brute Force**:
  - No limits on the number of attempts allowed to brute force the PIN on the fob.

Buffer Overflow:

- We wrote exploits to leak flags and pins from various teams.

Replay Attacks:

- Weak or predictable random number generation allowed replay attacks.

Defensive Highlight

EEPROM Layout Randomization (ELR):

- Our manufacturing process involves the creation of a randomized EEPROM layout for each car produced. This security measure ensures that any attacker who gains access to the EEPROM will be unable to discern the location and content of stored data.

Offensive Highlight

Stack Leaks:

- Boards with flags can only run signed firmware images. However, the attacker can flash any correctly signed firmware at any point on the car/fob. By flashing a vulnerable and a victim firmware on the car/fob, we leveraged the vulnerable firmware to extract sensitive data left behind from victim firmware images. This attack is shown in the figure below:

By leveraging these leaks, we successfully extracted private keys and pairing pins on the test boards. However, this attack did not work on keyed boards since the bootloader clears the SRAM and removes any sensitive data left by the victim team.

References

1. https://ascon.iaik.tugraz.at/
2. NIST SP 800-90A Rev. 1