Team MorganState

Morgan State University

Robert Hill, Loic Jephson, Joy Falaye, Olufemi Agunbiade, Gregory Briscoe, Vinton Morris
Advised by: Dr. Kevin Korneygay, PhD
April 24, 2023

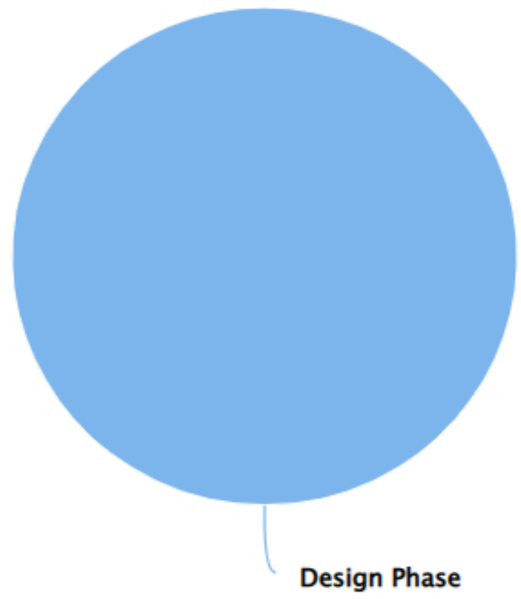
Design Overview

- For this project, a lightweight asymmetric encryption called **ASCON** was used to mask and protect communication mainly between the car and fob and across the design structure.
- The ASCON encryption protocol was used to ensure data authentication and data integrity.
- We also attempted to use hashing to protect the features from modification.

Defensive Highlight

- Our system uses encryption to protect sensitive Host secrets and device communication, and implement authentication and access controls. Our Design scheme uses Docker to store the symmetric keys for encryption and decryption.
- To protect the fob, anti-cloning and encrypted access credentials was implemented into our architecture. The implemented encryption also included salted or dummy variables to prevent data communications from snooping to create a randomized output.
- The access controls of our design protect the fob from root modification.
- In our fob/car architecture, the fob handles the encryption of information, while the car handles the decryption. The fob security architecture was designed to protect the system from possible intrusion while helping to facilitate the critical function of the fob/car pairing.
- When the fob sends a signal to the car, it receives the encrypted message and decrypts it using its cryptographic key. This allows the car to determine whether the signal is authentic and should take a particular action, such as unlocking the doors and starting the engine.
- Our system was susceptible to specific attacks. The fob/car architecture is vulnerable to cryptographic attacks. If an attacker can break the encryption used by the fob and car, they could potentially access and control the car.
- The effectiveness of the fob car architecture also depends on the implementation of the system. Even if the encryption was done right other weaknesses in the code allowed attackers to intrude into our systems. To improve our encryption, we would improve the randomness of the encryption. This involves adding a random element to the encryption algorithm to create unique keys each time the system is used. This makes it much more difficult for attackers to break the encryption. Another method would be to improve the use of obfuscation techniques to make it more difficult for attackers to reverse engineer the code; this includes code obfuscation, function inlining, and data obfuscation.

Solved Challenges Breakdown



Offensive Highlight

- Due to time constraints, we were, unfortunately, unable to participate in the attack stage of the competition. An attack that we planned to use but did not an opportunity to, was the Side-Channel Analysis attack.
- Side-channel analysis is a type of attack that targets the information a system leaks through various channels.
- In the context of a fob car pair architecture, side-channel analysis could extract secret information, such as the cryptographic keys used to secure the communication between the fob and the car, by analyzing the side-channel information generated during the communication.
- Power analysis involves monitoring the power consumption of the fob or car during communication and analyzing the power traces. Those traces can reveal secret information in the fob/car pair.
- For example, when the fob sends a command to unlock the car, the power consumption of the fob and the car would increase due to the encryption and decryption operations involved in the communication process. The attacker could extract the secret key used for encryption and decryption by analyzing the power traces.
- Several countermeasures can be taken to prevent power analysis attacks on a fob car pair architecture. For example, the system can implement random delays and noise in communication to make the power traces less predictable. Additionally, implementing secure cryptographic algorithms and keys can make it more difficult for attackers to extract the secret key through power analysis attacks. Of course, in doing so, it is also vital to refer to the time and space requirements set by MITRE for the competition.

References

1. Dobraunig, C., Eichlseder, M., Mendel, F., & Schläffer, M. (2021). Ascon v1.2: Lightweight Authenticated Encryption and Hashing. Journal of Cryptology, 34(3). https://doi.org/10.1007/s00145-021-09398-9
2. Schläffer, Christoph Dobraunig, Maria Eichlseder, Florian Mendel, Martin. “Ascon – Authenticated Encryption and Hashing.” Ascon.iaik.tugraz.at, ascon.iaik.tugraz.at/. Accessed 21 Apr. 2023.
3. Dobraunig, Christoph, et al. “ASCON AUTHENTICATED ENCRYPTION and HASHING.” NIST, NIST, 4 Nov. 2019, csrc.nist.gov/CSRC/media/Presentations/ascon-v1-2-analysis-of-security-and-efficiency/images-media/session2-mendel-analysis-of-security.pdf. Accessed 11 Feb. 2023.