0xDACC

Delaware Area Career Center

**Sarah Ogden, Tony Ivanov, Diego Noria, Cooper Pflaum,
Nate Levenson, Ethan Agarwal, Afton Turner
Advised by: Eli Cochran**

April 24, 2023

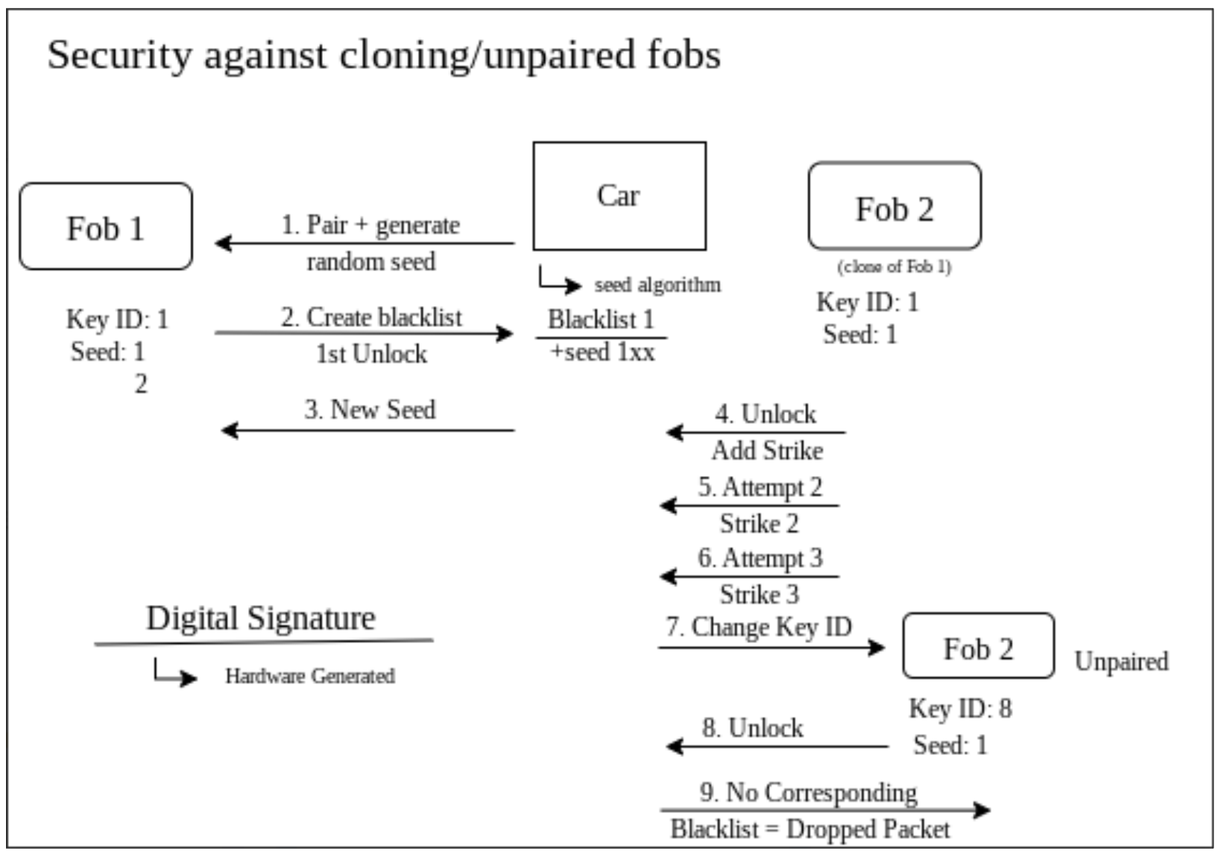
Design Overview

Our goal was to use Advanced Encryption Standard (AES) in CTR (Counter) mode, a symmetric key encryption cipher, to encrypt and secure data going over the board link.

We aimed to utilize AES encryption to secure our data; however, we were not able to include any other security features, software or otherwise.

Our design unfortunately does not meet the security requirements.

Our design planning layout →



Defensive Highlight

AES stands for Advanced Encryption Standard, and it is the encryption standard that replaced the Data Encryption Standard (DES) in 2001.
It is much more efficient, allows for variable key lengths, and uses the substitution–permutation network principle, meaning it is efficient in both software and hardware. It has a fixed block size of 128 bits, but a variable key size of 128, 192, or 256 bits.
We decided to use a 128-bit key.

We wanted to include it because it's efficient, lightweight, and there are plenty of references and examples of it. It's more effective than DES, RSA, and other encryption methods.

It was supposed to encrypt the data going over the board link using a 128-bit key.

Unfortunately, we couldn't get it to work fully. We were able to encrypt the unlock message, but not the enable features. We aren't entirely sure why it didn't work to its intended extent.

We could continue developing and make it work for the rest of the code and data, not just the unlock message.

Offensive Highlight

Unfortunately, we weren't able to make it into the attack phase, but if we had, we would have focused on cloning and replay attacks.

Cloning attacks can take advantage of a flawed authorization system and weak passwords.

We were not able to perform this attack, so we don't know if it would have been successful or not, or what we would need to fix/improve upon if it wasn't successful.

References

1. KOKKE's Tiny AES Library
2. https://www.nist.gov/publications/advanced-encryption-standard-aes
3. https://www.britannica.com/topic/AES
4. https://www.youtube.com/watch?v=UB2VX4vNUa0
5. https://crypto.stackexchange.com/questions/6029/aes-cbc-mode-or-aes-ctr-mode-recommended