ENPM 809W – Introduction to Secure Software Engineering

Homework 3

Date Due: October 5th, 2021, by 11:59 PM EST.

Please read the article attached in this week's (Week 5) module on 'Card Brand Mixup Attack Bypassing the PIN in non-Visa Cards by Using Them for Visa Transactions' and answer the following questions.

1. The attack outlined in the paper talks about a vulnerability in the EMV protocol. What does EMV stand for?
2. For online authorization, the payment terminal sends an authorization request to the card issuer carrying transaction details and what else?
3. What threat would you categorize the attack the authors outline in the paper as related to the CTQ data object?
4. How many contactless EMV protocols exist?
5. As part of the Combined Dynamic Data Authentication (CDDA) cryptographic protocol shown in Figure 3, how is the Application Cryptogram computed? Please explain using specifics including which key is used and how that key is derived.
6. What is the AID for Visa cards and how is it used during the CDDA protocol? What is the AID for Mastercard cards?
7. What threat would you categorize the attack from how the AID is used?
8. What countermeasures do the authors propose to fix just the PIN bypass attack?
9. What countermeasures do the authors propose to fix the EMV-wide to secure the protocol?
10. Do you agree with the authors on whether the countermeasures are enough? Please explain why.