ENPM809W – Introduction to Secure Coding

Homework – 3

Author – Syed Mohammad Ibrahim

UMD ID: iamibi

Email: iamibi@umd.edu

1. The attack outlined in the paper talks about a vulnerability in the EMV protocol. What does EMV stand for?

A. EMV is an acronym for Europay, Mastercard, and Visa. These were the three companies that created this technology.

2. For online authorization, the payment terminal sends an authorization request to the card issuer carrying transaction details and what else?

A. A cryptographic Message Authentication Code (MAC).

3. What threat would you categorize the attack the authors outline in the paper as related to the CTQ data object?

A. Tampering with Data. At the lowest level the attack is tampering with the CTQ data object by setting the value 0x0280 which makes the terminal to not use PIN based authentication for the user and that the user is verified on the consumer's device.

4. How many contactless EMV protocols exist?

A. There are six contactless EMV protocols.

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.

A. Application cryptogram (AC) is computed using a session key *s*, which is derived from the Application Transaction Counter (ATC) and a symmetric key *mk* only known to the issuer and the card. The symmetric key is computed in a function f(mk, ATC) that is a known key and ATC are passed in to the function to get a random NC. Application cryptogram uses MAC function as MACs(X,AIP,ATC, IAD).

6. What is the AID for Visa cards and how is it used during the CDDA protocol? What is the AID for Mastercard cards?

A. AID for Visa Cards:

Visa card	0xA0000000031010

Mastercard	0xA0000000041010

Usage in CDDA protocol: AID is used to activate supported applications aka kernels or protocols. Kernel 3 is used to activate a Visa AIDs and Kernel 2 is used to activate Mastercard AIDs.

7. What threat would you categorize the attack from how the AID is used?

A. Tampering of data

8. What countermeasures do the authors propose to fix just the PIN bypass attack?

A. The following two countermeasures were proposed by the authors for PIN bypass attacks:

1. The terminal must always set the bit 1 of byte 1 of the Terminal Transaction Qualifiers (TTQ).

2. The terminal must always verify the Signed Dynamic Authentication Data (SDAD).

9. What countermeasures do the authors propose to fix the EMV-wide to secure the protocol?

A. The following are the two countermeasures proposed by the authors:

1. All transactions must have the card generate the SDAD and the terminal verify it.

2. The selected AID must be part of the input to the SDAD.

10. Do you agree with the authors on whether the countermeasures are enough? Please explain why.

A. I agree with the authors that the countermeasures are enough even though one of them is a costly case for the card issuers, but it will safeguard their customers from attacks. The authors have verified their countermeasures and based on the attacks that they have carried out it would suffice to say that they are confident in their provided solution. As an add-on, it is always good to perform verifications at every stage possible where the performance is not hindered.