Home Assignment 1

November 9, 2017

1 A-2) Describe an attack that the CVV1 code on a credit card prevents. Why is it not effective against skimming?

The CVV1 code is used for ensuring that a given card is actually a valid card issued by an issuer. The code is encoded into the magnetic band on the card and is verified during card present transactions. If the code is invalid the transaction is denied. The code is computed by the issuer and it uses things like card number, expiration date and a private key as inputs. This means that if someone tries to create a completely new card by making up card details and claim that the card is issued by an issuer they should not be able to produce a correct CVV1 code since they do not know the issuers private key. This means that the CVV1 code protects against such an attack.

During skimming the information on the magnetic band is saved in order to be able to produce a clone. Since the CVV1 code is encoded onto the magnetic band this means that the skimmer will also clone the CVV1 code thereby bypassing the CVV1 code protection. This means that the CVV1 code is ot an effective protection against skimming.

2 A-5) How does the Merchant verify the dual signature in SET?

The cardholder sends its own certificate, encrypted PI, PIMD, OI and the dual signature to the merchant. The merchant has access to OI and PIMD. The merchant hashes OI in order to get OIMD. The merchant now takes the two hashes PIMD and OIMD and concatenates them to PIMD||OIMD. This concatenated hash is den hashed resulting in a new hash called h(x). The merchant now verifies the client certificate. If the verification was successful the merchant uses the public key in the certificate to decrypt the signature receiving h(x)'. The decrypted signature h(x)' is now compared to the merchant calculated hash h(x). If they match the verification is succesfull otherwise it fails.

3 A-8) How does the SET protocol provide non-repudiation?

Since the the concatenated hashes PIMD||OIMD is hashed then signed with the cardholders private key this is a signature that can be verified with the cardholders public key by both the merchant and the bank since they have access to the client certificate plus OI and PIMD or PI and OIMD. This provides non-repudiation.

4 A-11) The acronyms ACS and ADS are both related to VbV (3D Secure). Explain them briefly.

4.1 ACS(Access Control Server)

The server operated by the card issuer that is responsible for authenticating the cardholder and providing digitally signed messages. It is also possible for the bank to outsource the task of maintaining ACS to a third party. The ACS tells the network which URL that should be used for authenticating the cardholder.

4.2 ADS(Activate During Shopping)

Allows the cardholder to enroll to 3D Secure during payment. This is done as a part of the first payment done using 3D Secure. This feature is criticized since people tend to choose quite bad passwords during the purchase.

5 A-15) When requesting a blind signature, why must Alice keep r secret?

Lets assume RSA is used and n is the public modulus, d is the private signing key and e is the public verification key. Alice begins with generating a random number r that is kept secret from the signing party. The signing party is tasked with signing $r^e * h(x)$. Since the signing party does not know r it is impossible to derive h(x) from $r^e * h(x)$. Alice knows r and can extract the signature of h(x) by multiplying with the inverse of r. Now lets assume that Alice does not keep r private and instead happily shares this secret with the signing party. Then it is possible for the signing party to derive h(x) making it a non blind signature!

6 A-20) How is Alice's identity revealed if she double spends a coin in the untraceable E-cash scheme?

The coin consists of k quadruples $(a_1, c_1, d_1, r_1), (a_2, c_2, d_2, r_2), ..., (a_k, c_k, d_k, r_k)$ and an signature S. During the with drawl procedure it is checked(probabilistic) that Alice has generated the B_is used in generating the signature S by inserting her identity into the y_is. When Alice wishes to spend her coin Alice sends the signature S to the merchant. The merchant responds with a generated vector of length k where each element is either 0 or 1. Alice now returns $(x_j, a_j \oplus ID, d_j)$ if $z_j = 0$ or (y_j, a_j, c_j) if $z_j = 1$ for all j. Using this data the merchant can verify the signature. If Alice tries to use the same coin with another merchant her identity will be revealed since another merchant will use another vector z. When the bank receives the two spendings some index j will with very high probability be different meaning that for some j we have the two different versions $(x_j, a_j \oplus ID, d_j)$ and (y_j, a_j, c_j). This means that the ID can be extracted since $a_j \oplus ID \oplus a_j = ID$.

7 A-27) In the PayWord protocol, give the Bank's algorithm for verifying how much money should be taken from the user's account.

Alice selects some value w_n by for an example hashing a random number. This number is then used to create a hash chain according to the following formula $w_i = h(w_{i+1})$ for $i = n - 1..0$. This means that given some value w_k is is impossible to derive w_{k+1} since that would correspond to finding the preimage. Alice now commits to the value w_0 saying that yes w_0 is in my hash chain that will be used for payment to the merchant(M). This is done by signing $\{M, w_0, C\}_{PRI_A}$ by using Alice private key. When the merchant(M) wants to receive money from Alice the merchant sends (w_t, t) and $\{M, w_0, C\}_{PRI_A}$ to the bank. The bank now first verifies the signature $\{M, w_0, C\}_{PRI_A}$. By verifying that the bank knows that Alice has the hash value w_0 in a hash chain used for merchant M. Since it is not possible to go backwards in the hash chain from w_0 it means that if (w_t, t) received from the merchant results in w_0 when hashed t times it must mean that Alice has sent (w_t, t) to the merchant thereby meaning that Alice has agreed to pay t units. This means that Alice should be debited by t units and the merchant should receive money.

8 A-30) Compare the anonymity given by the untraceable E-cash scheme and Bitcoin.