Home Assignment 1
EITN41

Grading: $(0.7 + 0.9 + 0.8 + 0.8 + 1.0 + 1.0 + 1.0 + 0.6) =$**6.8**

A-4 *Give two common ways to prove/make probable that the person making a card-not-present transaction is in physical possession of the card. Compare the two alternatives in terms of security.*

Two efforts to increase security during a card-not-present transaction discussed during the course are SET and 3D Secure. These two methods provide authentication that the buyer is in fact the one registered to the card used. I find it redundant to explain the whole protocols in detail since the question in hand is just to compare the security of them which we can do without this. 3D Secure provides user authentication typically via the use of a password the cardholder must enter at the time of purchase. Other authentications can be chosen by the bank such as BankID (this author has touchID via BankID app for example). 3D Secure can also protect the cardholder against phising sites by allowing the display of a Personal Assurance Message set by the cardholder on card activation, so this person can verify that the pop-up box in which to enter the password is from the bank. I.e two factor authentication. To stop attackers from intercepting a card and choose a password or such before the user can, the enrollment into the 3D Secure system is fortified by a number of options. Either the bank can choose to let you activate the card face-to-face where they can check your ID, or via their website where its assumed only you can log into your personal pages/account management. Or a third option is available where the card is activated on the first purchase made and password is chosen at that time. This is protected by the use of personal questions assumed only the intended user knows.

SET, Secure Electronic Transaction, provides more than just two factor authentication but failed to gain traction on the market due to user friendliness issues. In this authentication method the merchant will never get a hold on the card details and the bank will never know the items ordered. The use of PKI and certificates are implemented, which is the user friendliness issues mentioned. This protocol relies on the use of the dual signature technique and encryption via the gateways public key to keep the order information from being read by the bank and the payment information from being read by the merchant. The dual signature consists a hash/digest of two already hashed parts, the payment information and the order information. with the usage of hashes and signatures this protocol also provides integrity of the data. In summary, 3D secure provides us with authentication of the cardholder, an optionally authentication of the bank. While SET provides us with two factor authentication, data integrity, and confidentiality of information. Since 3D Secure typically uses a password

the strength of this protocol lies on the cardholder. If a bad/easy password is chosen this is susceptible to guessing attacks, for example if the password is the name of the pet. Or if the personal questions are easy to guess. A possible security aw of the SET method is the breach of the PKI or loss of private key. PS sorry for this wall of text.

Grading motivation: *Conciseness is a virtue.*

I would argue that the 3D secure authentication with password by User and PAM by Issuer is not so much two-factor authentication as a mutual single-factor authentication.

Otherwise, this very extensive answer is good. It agrees with the lecture slides and notes.

Grade: 0.7

A-6 *In SET, why is the Payment Information first symmetrically encrypted and not immediately encrypted with the Gateway's public key?*

The payment information, PI, is symmetrically encrypted with DES in SET **due to the speed of this encryption algorithm**. Symmetric encryption is a lot faster than asymmetric, so encrypting everything with the gateways public key would take a lot more time. The key used by the cardholder is then encrypted with the use of the public key of the gateway and sent together with the encrypted PI. When the merchant then relays the information to the payment gateway after order verification the gateway can unwrap/decrypt the key used to encrypt PI. Then in turn decrypt the PI and verify this with OIMD in the dual signature.

Grading motivation: Good, encrypting with symmetric key and then encrypting the symmetric key with an asymmetric key is a classic technique for speeding up but still keeping it reasonably secure.

Grade: 0.9

A-12 *How is mutual authentication between issuer and cardholder achieved in VbV (3D Secure)?*

As mentioned in question **A-3** the 3D Secure protocol offers two factor authentication from the bank side via the use of a Personal Assurance Message to be displayed with each purchase, verifying the pop-up window was issued by the bank. And from the client side via the password entered by the cardholder, which is assumed secret to only this person.

Grading motivation: The description of the things provided by Issuer and User is correct, however (again) the use of two-factor authentication I do not agree with.

Grade: 0.8

A-14 *The multiplicative property of RSA provides for blind signatures. What is meant by "the multiplicative property of RSA"?*

This simply means that $E(m_1) * E(m_2) = E(m_1 * m_2)$. Where E(x) is the encryption of x and * is an arbitrary operation.

Grading motivation: I would say that "arbitrary operation" is not technically correct, but at least addition and multiplication fits in there (`http://www.eit.lth.se/fileadmin/eit/courses/eit060/lect/Lect2-3.pdf`, slide 23. Or, slide 6 of 'ElectronicPayments_2' in this course). Otherwise, good answer.

Grade: 0.8

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

...

Grading motivation: Correct, according to lecture notes.

Grade: 1.0

A-18 *When Alice buys something from Bob using the untraceable E-cash scheme, why is it impossible for Bob to learn the identity of Alice?*

...

Grading motivation: Correct, according to lecture notes, page 13: "Still, Bob can not compute ID since he does not have both a_j and $a_j \oplus ID$ for any j."

Grade: 1.0

A-28 *Compare the PayWord protocol and the Peppercoin-like protocol in the lecture notes from the point of view of the customers, both in terms of what they pay, and in terms of what they need to compute to make a purchase.*

...

Grading motivation: According to the lecture notes, page 16 and 17, this answer is correct.

Grade: 1.0

A-29 *What is meant by a probabilistic payment? How does the Electronic Lottery Tickets scheme differ from Peppercoin from the user's perspective? How do they differ from the Merchant's perspective?*

...

Grading motivation: Important distinction: In the example with Alice making 100 purchases, she will *on average* "be debited an amount of 100 SEK once and 99 times nothing". It is probable, but not guaranteed. In a larger timescale it will average out.

An important factor this answer does not treat is where the psychological load is placed: In (ELT), the psychological load is placed on the User in that they sometimes pay more than they have actually spent. In Peppercoin the User never pays more than they have actu- ally spent and the psychological load is taken by the Bank.

Otherwise the information seems correct according to the lecture slides.

Grade: 0.6