COMP3355 Cyber Security

Assignment 4

(Due on 6 Dec 2019, 23:55)

Q1. The following questions are about an e-commerce shop website.

(a) The shop website has implemented a set of "shopping cart" features on its website with the following functionalities:

(F1) It allows customers to select items they would like to buy from their website and put them in the shopping cart.

(F2) After finishing browsing and shopping, customers click on "Pay for Items" to checkout and pay for the items they put in the shopping cart.

The current implementation for the shopping cart stores the selected items and their associated prices in files on the server with one file per customer. Furthermore, the website identifies customers base on their IP addresses and https is used for all connections.

The website has experienced frequent DoS attacks. Explain why the existing design can easily be exploited by attackers to launch DoS attacks. [10%]

Suggest an alternative for the shopping cart implementation that provides the same functionalities (Fl) and (F2) but minimizes the risk of DoS attacks. [10%]

(b) Design an e-payment protocol without using Public Key Cryptography for the following scenario. The e-commerce shop allows users to purchase items through the Internet. You can assume the communication between any 2 parties is secure. At the end of a shopping session, the shop will calculate the total cost of the purchase based on items in the user's shopping cart. The user is then requested to pay the amount to the shop's banking account. You are required to design a payment protocol such that:

(1) The bank does not know what items are purchased by the customer.

(2) The shop does not know how the customer make the payment, e.g. the bank account details of the customer.

(3) At the end of the payment, the user should have a proof that he has paid the specified amount into the shop's banking account.

(4) The bank does not need to communicate with the shop directly during the process of payment.

You can assume that the shop has an account with the bank. The customer can make a payment into the shop's bank account either using his bank account or any other payment method. You can also assume that secret keys are available between the following parties:

(i) The shop and the bank (K_{shop})
(ii) The customer and the bank (K_{cust})

Show your designed protocol and explain how the above four requirements are satisfied. [30%]

Q2. Cryptography can be used to pass secret messages among a group of Internet users. Consider this case: a website owner, Bob, wants to send individual secret messages· to his twenty subordinates. Note that some messages are meant to be seen by one subordinate, but some other are meant to be seen by many subordinates. Bob wants to place the secret message into his web site, and let his subordinates use cyber cafe PCs in foreign countries to access the web site. Also, assume that Bob will give each subordinate a USB thumb disk, which may be used to store an individual secret (e.g. an encryption key), and any software that may not exist in the cyber cafe PCs. Design a system for Bob to achieve his goal. You need to focus on the cryptographic operations, and you can be very brief in describing the use of network/Internet technology.

You have to describe how he needs to prepare the messages in his website, what content he should place in the USB thumb disks, what procedures the subordinates have to follow to extract the secret messages, and any other necessary information.

As this is an open-ended question, you can state any additional assumptions as you prefer. Also, you need to design at least one additional functionality, for example: "If one subordinate reports to Bob that he has lost the USB thumb disk, what will be the remedy action that Bob can carry out, and what is the impact?". [50%]