Matthew Austin

Cryptography

Anwar

November 2018

Key Management

* 1.
  + Replay Attack. Countermeasure, ensure that r1 is sent and seen between each interaction
  + Man in the Middle. Countermeasure, the sender/client or in this case the website has to encrypt it with their private key.
  + Spoofing. The countermeasure is a preventative one, where the sender/client or website should prevent against a man in the middle attack by encrypting it with their private key in order to prevent a spoofing attack.
* 2.
  + A. What root certificate is needed?
  + Root 1: Company 1
  + B. One or two of the host certificates are faulty. Name the certificates that are faulty. How could this happen?
    - Hoost 1 and Host 4
* 3.
  + What are the signature chains that Bert can use to convince himself that Ernie's certificate is trustworthy?
    - Bert → Elmo → Count → Ernie
  + Which chain is the best proof? Why?
    - The Chain between Bert and Ernie, that has Elmo and Count involved. It is the best proof because every person has high level.
* 4.
  + How can a dishonest customer MM (who also has an account of Bank BB and a Card from Bank BB) steal money from CC (by withdrawing cash from the account of CC). Here we assume that MM knows CC’s account number. He also has a machine that can modify information on the magnetic strip. However, MM does not know the secret key of the Bank.
    - He can encrypt the Cc with his information thus making Cc’s account his, they Mm can use/create his own pin to get the money out of Cc’s account.
  + Explain how a dishonest customer MM can withdraw much more than the $200 daily limit from her own account. What would the bank have to do to make this impossible?
    - Since the transactions aren’t computed until the end of the day, the dishonest customer can go to different atms and withdraw $200 from each atm.