COMS 4180 Network Security Spring 2018 Written Assignment 2

Due Wednesday Feb 21, 2018, 10:00pm Eastern time.

- This assignment is to be done individually.
- NO LATE SUBMISSIONS WILL BE ACCEPTED.

Submission Instructions

- Assignments will be submitted in Courseworks.
- Submit one file containing all of your answers. The file formats accepted are pdf, word (.docx, .doc) and plain text with a .txt extension.
- The file name will be <your uni>.<extension> example: jld2017.pdf
- Please put your name on the first line of the file.

50 points

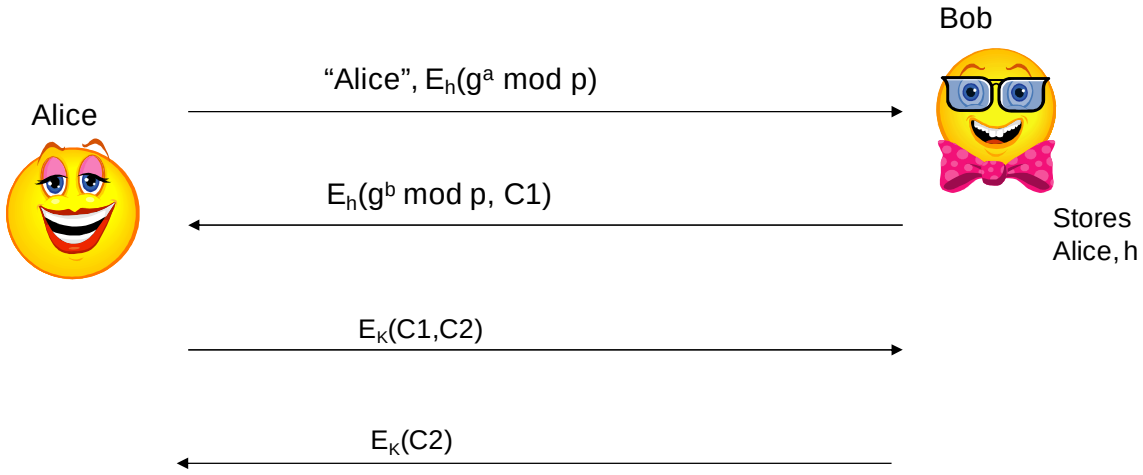
1. (15 points total) In the following protocol, h is a hash of Alice's password for server Bob. Alice and Bob do a Diffie-Hellman (DH) exchange to compute a shared secret K, but are encrypting the messages in the DH exchange instead of sending them in the clear. They are also exchanging nonces (random values), C1 and C2. Bob chooses C1, Alice chooses C2. Anything of the form $E_x(Z)$ means encrypt Z using a symmetric key encryption algorithm with key x. The exact encryption algorithm does not matter for this problem.

a. (5 points) At the end of this exchange, what has been achieved (it may be multiple things) and why?

b. (2 points) What is the benefit of encrypting the DH exchange?

c. (3 points) While the exact symmetric key algorithm does not matter, what restrictions are necessary on how the symmetric key algorithm is used?

d. (5 points) Is this protocol subject to any attack other than a passive man-in-the-middle attack? Explain your answer.

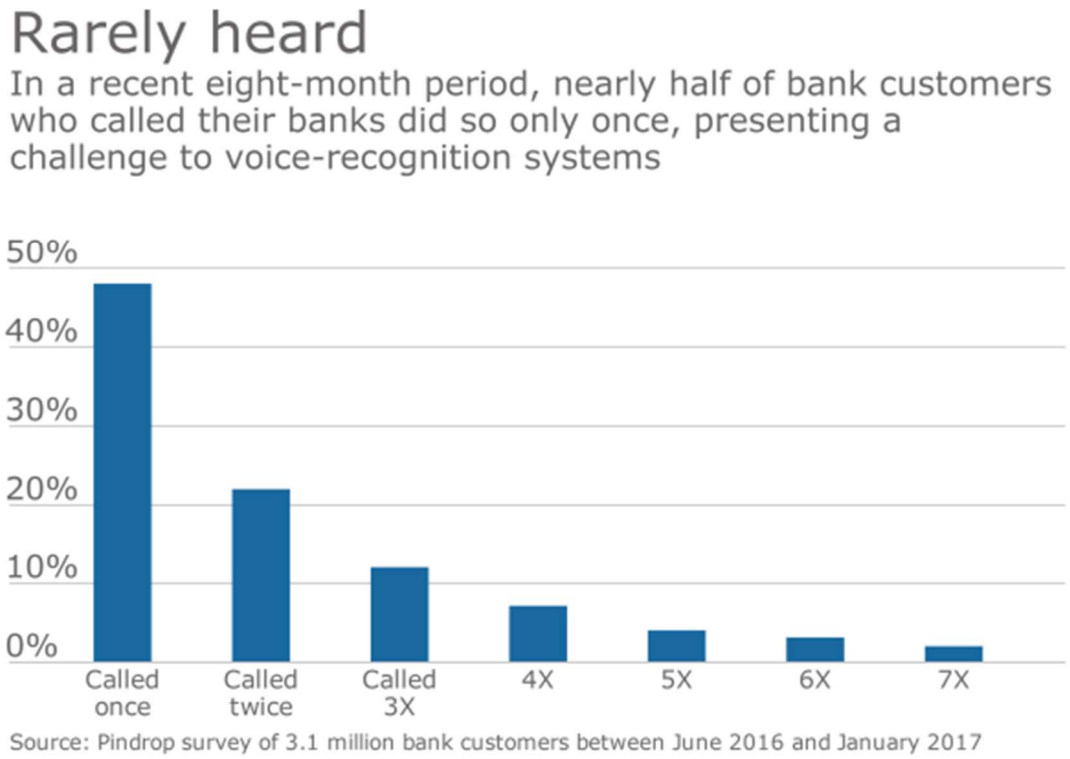


2. (10 points) Suppose Alice and Bob share a secret key K_{AB} and wish to authenticate each other. Alice always initiates contact with Bob. Consider the following protocol for mutual authentication between Alice and Bob.
Let rA and rb be nonces. E_K_{AB}{X} means X is encrypted with a symmetric key cipher using K_{AB} as the key.

• Alice sends r_A to Bob
• Bob sends {E_K_{AB}(r_A), r_B} to Alice
• Alice sends { E_K_{AB} (r_B)} to Bob

When the three messages have been exchanged, can Alice be sure that she is talking to Bob? Can Bob be sure he is talking to Alice? If yes, justify your answer (why is no attack possible). If no, explain why not and describe what, if any, attacks are possible.

3. (5 points total)
Suppose a bank uses voice authentication to authenticate customers when they call the bank. The following graph shows the % of customers that call their bank X times in an 8 month period.
Given that a person's voice changes as a person ages, how can the frequency of calling impact the false negative rate of the authentication?



4. Certificates (5 points)
Suppose when a user visits a web site, the site uses HTTPs and sends a certificate chain containing the website's certificate and CA's certificate. How does the browser verify that the certificate it received for the website is valid? The answer must be as detailed as possible.

5. TLS 1.3 (5 points)
From the the blog.cloudfare in the assigned reading in lecture 4, summarize (at most ½ page single space, <= 12 point font) what issues have prevented widespread deployment of TLS 1.3 and resulted in the need for additional drafts of the RFC.

6. wireshark (10 points) (2 points each for c, d and e, 1 point for a,b,f and g)
For this problem you will need to download and install Wireshark on a machine you have admin or root privileges in order to capture live traffic. It is recommended that you close any other applications you have running, including other instances of the browser and email, when capturing the data to minimize the amount of extraneous traffic captured. Your answers for some parts may differ from that of others depending on what version of TLS your browser supports. **Do not include the pcap file in your submission, but save it in case the TA requests it to verify your answers.**

Use Wireshark to monitor the HTTPs connection when accessing https://ssol.columbia.edu/ (either use your browser's refresh button or clear your browser history and visit the web site again if you do not see a TLS exchange). Save the packets to a pcap file and retain the file until your assignment is graded.

a. How many cipher suites are proposed? Just provide the number and do not include a list of all the algorithm combinations.

b. What algorithms (cipher suite) are selected to be used for the connection?

c. How many certificates are in the chain returned? For each, who is the certificate issued to and what algorithm was used to sign it.

d. What is the name of the root CA?

e. Are either any Diffie-Helman parameters observed (if so, which ones) or a premaster secret used?

f. How many application data packets are sent from the server to the browser?

g. What version of TLS was used?