COMS 4180 Network Security Spring 2016 Written Assignment 2

Due Wednesday Feb 24, 2016, 10:00pm Eastern time.

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

Submission Instructions

- Assignments will be submitted in Canvas.
- 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.

5 problems, 50 points

1. (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, timestamp), r_B} to Alice
• Alice sends { E_K_{AB} (r_B, timestamp)} Bob
The timestamp is only accepted if it is within +/- 0.5 seconds of the receiving host's clock. 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? Either justify why or show why not and how to fix the protocol.

2. Kerberos (10 points total)
In an environment using Kerberos v5, suppose Alice is a client and Bob is a server with services Alice uses.
a. (5 points) What in the exchanges verifies to Alice that she is really connected to Bob and the real KDC was involved?
b. (5 points) Can the KDC impersonate Bob to Alice or impersonate Alice to Bob? If yes, why? If no, why not?

3. (5 points total)
a. (2 points) What is a major usability issue with the use of fingerprints for authentication in place a password? (it is something that can likely apply to any individual at some point in his/her lifetime)
b. (3 points) Suppose some biometric method is used for authenticating users when they log into a system. If a deterministic authentication method is needed as a backup because the biometric is not 100% accurate, how can this eliminate any additional security gained by using the biometric method?

4. Certificates (15 points total)
a. 3 points The last piece of information on a certificate is the signature. What is the purpose of this signature?
b. 8 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.
c. 4 points In addition to the signature, what else should the browser verify before accepting the certificate?

5. wireshark (10 points) (2 points each for c, d and e, 1 point for a,b,f and g)
For this problem you will either need to use the centos VM which has wireshark installed or 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. **Do not include the pcap file in your submission, but save it in case the TAs request it to verify your answers.**

Use Wireshark to monitor the HTTPs connection when opening the web page https://ssol.columbia.edu/ (do not log in, only use the traffic needed for bringing up the login page)
a. How many algorithm combinations (cipher suites) does your browser propose? Just provide the number and do not the list of names.
b. What algorithms (cipher suite) does the Columbia server select to use?
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?