Network Security Theory and Practice

Assignment

Due April 15, 2019

POLICIES:

1. **Coverage**
   Lectures 01-08
2. **Grade**
   100 points, 10% counted into the final grade
3. **Individual or Group**
   Individual based, but group discussion is allowed and encouraged
4. **Academic Honesty**
   Violation of academic honesty may result in a penalty more severe than zero credit for an assignment, a test, and/or an exam.
5. **Submission**
   Hard copy in class.
6. **Late Submission**
   20-point deduction for late submission till the lab session on April 16, 2019;
   Deduction ceases upon zero;
   Late submissions after April 16 15:55 will NOT be graded.

QUESTIONS:

1. 10 points: Cryptography

a. What is the difference between symmetric cryptography and asymmetric cryptography?

b. Given that both types of cryptography can protect security, why should we still need both of them?

c. What is the algorithm framework of RSA?

d. What is the key innovation of homomorphic encryption? Provide one use case.

e. How does proxy re-encryption work? What is the design goal?

[Grading Rubric: 2 points per sub-question.]

2. 10 points: Cryptanalysis

a. Given an n-bit password, what is the average trying time for cracking the password using a brute force attack? Provide the detailed derivation.

b. How to attack a one-time pad encryption?

c. How does a replay attack work? How to address it?

d. How does a man-in-the-middle attack work? How to address it?

e. How does a relay attack work in wireless communication? How does distance bounding work against a relay attack?

[Grading Rubric: 2 points per sub-question.]

3. 10 points: Secure Routing

a. What are the key features of the five typical delivery schemes?

b. What is the framework of the Dijkstra algorithm?

c. What is the framework of the Bellman-Ford algorithm?

d. How does prefix hijacking work?

e. How does RPKI work? Why is it insufficient for secure routing?

[Grading Rubric: 2 points per sub-question.]

4. 10 points: Secure Forwarding

a. What is the difference between routing and forwarding? Why is secure routing insufficient for secure forwarding?

b. In which scenarios should secure forwarding be enforced? If not, what are the security impacts?

c. How does a typical secure forwarding scheme, ICING, work?

[Grading Rubric: 10 points = 2 + 3 + 5.]

5. 10 points: Blockchain

a. What are the key cryptographic techniques used in blockchain? What are they used for therein?

b. How is double spending addressed in blockchain?

b. How does Proof of Stake work and save blockchain from intensive computation?

[Grading Rubric: 10 points = 2 + 5 + 3.]

6. 10 points: Secure Connection

a. How does a DNS hijacking attack affect network security?

b. What is the protocol framework of HTTPS?

c. How does a user verify a certificate for determining the authenticity of the website it connects to?

d. When is a certificate chain required? How to authenticate a certificate chain?

[Grading Rubric: 10 points = 2 + 3 + 2 + 3.]

7. 10 points: Wi-Fi Security

a. What key properties of wireless communication make it more vulnerable to attacks than wired communication?

b. Why is WEP insecure?

c. How does IEEE 802.11i provide a higher security guarantee than WEP?

[Grading Rubric: 10 points = 2 + 3 + 5.]

8. 10 points: Anonymous Communication

a. Why is current Internet communication vulnerable to anonymity or privacy leakage?

b. In which scenarios do users require the communication anonymity or privacy as concerned in sub-question a?
c. How to use proxies to secure communication anonymity? What are the possible limitations?
d. How does Onion Routing provide a better guarantee for anonymity?
e. How to infer anonymity or privacy of Onion Routing traffic?
[Grading Rubric: 2 points per sub-question.]

9. 10 points: Authentication Efficiency

Consider a time-consuming authentication scenario where a database records all secret keys of a large number of users. When the system authenticates a user, it first issues a challenge message to the user. The user then uses his/her key to encrypt the challenge and then returns the encrypted challenge to the system. The system then encrypts the challenge using one key in the database after another and compares the result with the received encrypted message. Once a match is found, the system accepts the user. Otherwise, the user is denied. This authentication protocol surely takes a lot of time and computation.

Design a possible solution to speed up the authentication process.

666.10 points: SHINE YOUR WAY

[Hmm, albeit the semester is ending, I'm still trying to seize every opportunity to make the class more fun.
This question should look familiar to mengxins who have studied Computer Architecture with me. I truly appreciate your believe in me for taking another course I teach.
For mengxins who study with me for the first time, I wish I would provide you with a better learning experience if it were not my first time teaching this course.
I sincerely thank each and every one of you for taking the "adventure" of Network Security with me, and for your continuing support, understanding, tolerance, and cooperation.
At the very best, I hope you will walk out of this class with not only some security highlights to master but also some fun moments to remember.
When you think of this class once in a while, this is the sweetest I can imagine: Smile because it happened.]

Design a question that you think is feasible as an exam question.
a. which topic among the lectures you would like to consider?
b. describe a (sufficiently complex) question;
c. provide also a *correct* sample solution, thanks.

Sample solution from one dalao in a previous Computer Architecture class:
a. Class
b. Who gives the class candies?

c. Solution: X W T

Warning: You can ask X W T for candies. You are, however, not expected to provide such "sweet" solutions.

[Finally, the last question of the first, yet last assignment of Network Security. Enjoy.]