CSCI 345, Spring 2019
Midterm Review

Topics to Study:

1. **Security mindset**
    a. Security pillars CIANA and applications
        i. Apply CIANA to the design and implementation of a smartphone application that manages contacts.
        ii. Explain why CIANA covers all security aspects in a software or hardware project.
        iii. How is CIANA implemented in decentralized banking?
    b. Asymmetric advantage
        i. Describe the security implementation on a campus network. How can an adversary gain an asymmetric advantage?
        ii. Explain recommendations to defenders that need to overcome the adversary's asymmetric advantage.
    c. Security in Depth
        i. Is two factor authentication security in depth?
        ii. Give an example of security in depth for a software development organization.
    d. Human Factors
        i. Discuss a strategy to help an organization strengthen their security of "humans" and overcome human weaknesses as they relate to systems security.
    e. Threat Modelling
        i. What is the threat model of a Man In The Middle (MITM) cryptographic attack?
        ii. What is the threat model of a side channel attack?
        iii. Given a specific attack, describe its threat model.
2. **Access Controls**
    a. Implementation
        i. Compare different access control implementations.
    b. Weaknesses
        i. Describe the pros and cons of access controls.
    c. Usefulness
        i. Why do we need access controls?
        ii. Is there an alternative to access controls?
3. **Authentication mechanisms**
    a. Passwords
        i. Defenses: How should we store passwords? What do passwords protect?
        ii. Attacks: How can we break passwords?
        iii. Information entropy: Find the information entropy of a specific password.
    b. Biometrics
        i. ROC: draw a Receiver Operating Characteristic curve (TPR vs FPR) for a specific biometrics example.

      ii. Sensitivity: calculate the sensitivity of a sensor.
      iii. Accuracy: calculate the accuracy of a sensor.

4. **Cryptography**
   a. Hashing
      i. How it works?
      ii. Why it works?
      iii. How it is used and why?
      iv. Weaknesses
      v. HMAC: what is this? How is it used?
   b. Kerckhov's Principle
   c. Symmetric Crypto
      i. Older crypto ciphers
      ii. DES
      iii. AES
      iv. Weaknesses and advantages of symmetric cryptography
   d. Asymmetric
      i. Diffie-Hellman Key Exchange
      ii. RSA
         1. How it works?
         2. Why it works?
5. **Computer Networking Basics**
   a. OSI stack
   b. Protocols: HTTP, DNS, TCP, UDP, DHCP
   c. Explain what happens in the application, transport layer when we try to access a webpage?
   d. (Why do we use NAT? Can we implement security with NAT? – Layer 3, not covered yet)
   e. (Find the subnet mask of a subnet from CIDR notation, find number of hosts in that subnet. – Layer 3, not covered yet)
   f. (What happens when we configure IPs manually? – Layer 3, not covered yet)

Sample Questions

1. WhatsApp is a free to download messenger app for smartphones. WhatsApp uses the internet to send messages, images, audio or video. The service is very similar to text messaging services however, because WhatsApp uses the internet to send messages, the cost of using WhatsApp is significantly less than texting. Whatsapp is adding passwords: what is the threat model that they want to protect their users from?
2. Recall that a symmetric-key cryptosystem consists of three functions: a key generator G, an encryption function E, and a decryption function D. For any pair of users, say Alice (A) and Bob (B), G takes as input a string of random bits and produces as output a shared key KAB. Either Alice or Bob can take a plaintext message x and produce a ciphertext message y ←− E(x, KAB). The ciphertext y can be sent over an insecure channel, and the recipient can recover x ←− D(y, KAB). a) Briefly explain three basic requirements for such a system to be secure. b) Why isn't symmetric-key cryptography sufficient as a foundation for secure Internet communication and, in particular, for secure Web-based commerce?

3. What is a one-way hash function?

4. How are one-way hash functions typically used in conjunction with public-key signature schemes, and why?

5. (When a new machine is attached to a network, it must be told the IP addresses of three machines if it is to be able to communicate with the rest of the Internet. Identify these three machines whose IP addresses are needed, and briefly explain the way in which the host uses each of these three IP addresses. – Layer 3, not covered yet)

6. What are the four primary layers in the Internet architecture?

7. How do the network-architectural principal of layering and the existence of open protocol standards foster a dynamic and fertile environment for innovation in electronic commerce and other Internet-based interaction?

8. What is the end-to-end principle of network design? Do you think that the end-to-end design of Internet protocols works for or against the privacy and security of Internet users? Briefly justify your answer.

9. Consider a program to accept and tabulate votes in an election. Describe the threat model and the vulnerabilities of the program that may be exploited.

10. Describe an example in which a complete denial of service to a user is a serious problem to the user.

11. Why do cryptologists recommend to change the encryption key from time to time? Is it the same reason security experts recommend to change the password from time to time? How can one determine how frequent to change keys or passwords?

12. Explain why hash collisions occur, i.e., when two different inputs to a hash function lead to the same output.

13. Design a protocol where two mutually suspicious parties can authenticate each other. Your protocol should be usable the first time these two parties try to authenticate each other.