CSCI-1380: Distributed Computer Systems
Homework #2
Assigned: 03/06/2018
Due: 03/13/2018

1 Security

1. In class, we discussed a variety of interesting attacks on cryptographic primitives and frameworks. Two of these interesting attacks are *reflection* and *replay* attacks. While similar, there is a fundamental difference between these attacks. What is the fundamental difference? What is the solution to these attacks?

2. Both symmetric and asymmetric key cryptography leverage a trusted third party for key distribution. With asymmetric key, this third party is the certificate authority. Whereas, for symmetric key, the third party is the key distribution center (KDC). Why is the distribution of symmetric keys a fundamentally more challenging problem than the distribution of asymmetric keys?

3. We saw, in class, that the Diffie-Helman key exchange (DH) enables two parties that communicate over an insecure network (where all messages can be examined by an adversary) to generate a shared secret. While DH is vulnerable to a man-in-the-middle attack, DH is still used today in HTTPS (HTTP over TLS, or secured HTTP).

    - How can an adversary perform the man-in-the-middle attack on DH?
    - How is HTTPS/TLS able to overcome the man-in-the-middle attack?

2 Security in Practice

1. You have been asked to consult for a FinTech (financial technology) startup. The CEO is dead-set on implementing a simple capability-based authorization framework to control access to their customer database. However, the CIO is worried that ex-employees can misuse their authorization after they've been laid-off.

   (a) How can ex-employees retain access to the system under the capability-based framework?

   (b) How would you augment the capability-based framework to prevent unauthorized access by ex-employees?

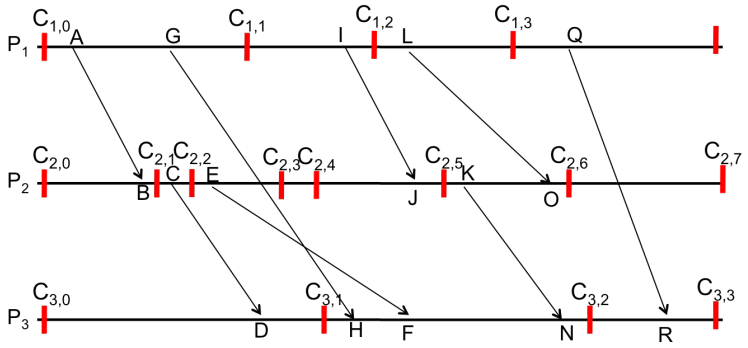
2. Having recently discovered that SHA-1 has been broken, the FinTech startup comes up with a new hash function, *EliteHash-1*, that extracts the last 50 bits of the document and XoRs it with a 50bit key. They plan to use this *EliteHash-1* function to create digital signatures for all future contracts. You have been consulted to discuss the strength and viability of their new hash function. Is this hash cryptographically strong? Explain your answer.

3. The FinTech startup would like to design an asymmetric key-based authentication scheme to authenticate customers. How would you design an asymmetric key-based authentication system? Specifically, what information is required from the customers? What is the fundamental assumption being made by such a scheme?

3 Time and Global State

1. For the process timeline below, provide the vector timestamps of the following events: A, C, E, H, J, N. Assume all processes start with (0,0,0), and that they occupy indices 0,1,2 from top to bottom. Recall, sending and receiving a message counts as a distinct event.

2. For the process timeline below, provide the logical timestamps of the following events: A, C, E, H, J, N. Assume all processes start with 0. Recall, sending and receiving a message counts as a distinct event.



3. List all potential consistent shapshots, i.e., consistent cuts. For example ($C_{1,0}$,$C_{2,0}$, $C_{3,0}$) is one consistent shapshot and ($C_{1,4}$, $C_{2,7}$, $C_{3,3}$) is another.

4. Consider the Chandy-Lamport algorithm for consistent global snapshots that we discussed in class. Explain why it may break down if the channel is not FIFO (i.e., if the channel can reorder messages).

4 Handing In

Once finished, you should hand in a PDF with your answers on Gradescope. Gradescope will allow you to select which pages contain your answers for each part of each question.

Please do not put your name on any page of your handin! This will allow us to do fully anonymized grading through Gradescope.

Please let us know if you find any mistakes, inconsistencies, or confusing language in this or any other CS138 document by filling out the anonymous feedback form:
http://cs.brown.edu/courses/cs138/s18/feedback.html.