15-440/15-640: Homework 4

Due: December 6, 2016 10:30am

Name:
Andrew ID:

1 RAID (16 points)

Raj has designed a new database system which he wants run on a RAID setup.

1. Which RAID configuration (from among the basic 5) should Raj use if he wants to optimize the database system for workloads consisting of small random reads and writes and why? [**4 points**]
2. Using a 10 disk RAID setup and each disk is capable of average throughput of 100 MB / sec (read and write) and an average latency of 10 ms (again, for both, reads and writes), what is the latency and throughput of random reads and writes of Raj's RAID scheme? [**8 points**]
3. What is the mean time to data loss of the setup in part 2 if the mean time to failure of a disk is 100 years and there are 10000 disk arrays of 10 disks each (assume no rebuild)? [**4 points**]

2 Virtual Machines (18 Points)

1. In no more than 5 sentences, describe the difference between Type I (Hypervisor) and Type II (Hosted) VMMs. [**4 points**]
2. In virtualization, can the hypervisor (or VMM) allocate and assign more than the actual physical resources it has available at its disposal (memory, processors) to individuals actual Virtual Machines (VMs)? Please explain. [**4 points**]
3. When does inflation of memory ballooning happen? And what problem might it cause? [**4 points**]
4. You are a data center engineer. Explain two (2) advantages and one (1) disadvantage of using system virtualization in the data center to your manager. [**6 points**]

3 Byzantine Fault Tolerance (16 Points)

In this question, we'll explore the links between replication for fail-stop failure resilience and replication for byzantine failure resilience. Recall that Paxos—an algorithm for fault tolerant replication under non-byzantine failures—requires $2f+1$ replicas to handle f failures. BFT, on the other hand, requires $3f+1$.

1. Why is it sufficient in Paxos to use a majority vote among $2f+1$ nodes to ensure consistency? (In other words, what property of a majority are we relying on?). [**4 points**]
2. Prove by providing a contradicting example that normal Paxos using 3 replicas cannot handle a byzantine fault in an asynchronous network. Use three replicas A, B, and C. For a proof, we want you to sketch a series of communication in which two clients observe an inconsistent result (which violates the requirement of a consistent answer from the system) when there's a single byzantine ("evil") node among the replica set. [**8 points**]

3. Why can BFT succeed with using $3f + 1$ replicas and requiring a consistent answer from $2f + 1$ of the nodes? (2 sentences) [**4 points**]

4 Security Protocols (18 points)

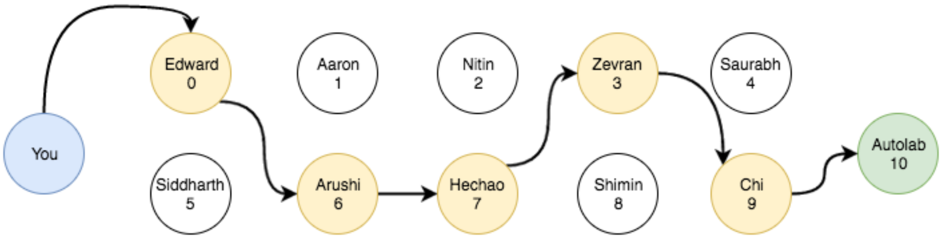
Yuraj and Srini wants to discuss the final exam questions through email. They decided to encrypt their emails to avoid being attacked by genius students like you. The first thing they have to do is to agree on a secret key. A TA suggests that they can use Diffie-Hellman key exchange protocol.

1. Suppose they have agreed on g = 23 and p = 5 (g and p are public). Now Yuraj picks his secret number 6 and Srini picks his secret number 8. What should Yuraj sends to Srini? What should Srini sends to Yuraj? And what is secret key they agree on? [**6 points**]
2. Assuming they use cryptographically secure primes, why can the final exam questions still be stolen by an attacker? Give an example of an attack using the parameters from part 1. [**8 points**]
3. What is the fundamental problem of this protocol (i.e. what security property is missing)? What different protocol or variation in this protocol can protect the final exam?? [**4 points**]

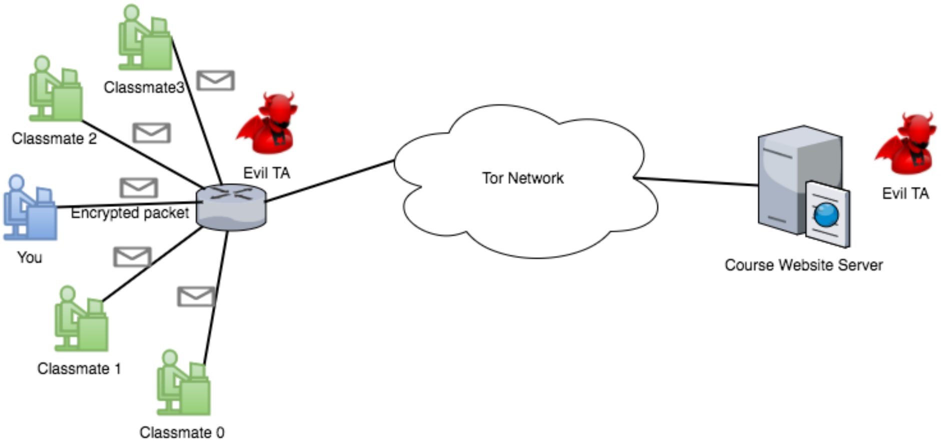
5 Anonymous Routing (12 points)

Recall that Tor, or "The Onion Router" (`https://www.torproject.org/`) is a decentralized system that allows people to anonymously browse the Internet. After learning about that, 440 TAs decided to set up a Tor network for students to submit homework on autolab. Each TA has an ID with him / her which works as the IP.

1. In the Tor circuit below, what is the packet that you send out? What is the packet that Hechao sees? Suppose that each packet is in the form [Next hop TA ID, data], M is your original message, K_i is the public key of TA i and E(K_i, m) denotes *encrypted data m using key K_i*. [**4 points**]



2. Suppose you use HTTP protocol in which your data is not encrypted. In the Tor circuit above, who may see your user name and password and why? [**4 points**]
3. As you may know, Tor does not provide perfect anonymity. It is vulnerable to an attack called "traffic analysis". Suppose you are asked to submit an anonymous feedback through the course website. You decide to use the Tor network to access the page. However, there is an evil TA who controls both the router right before the Tor entry point and the website server. Describe how can the TA distinguish you from your classmates.[**4 points**]


Classmate3
Classmate 2
Evil TA
Encrypted packet
You
Classmate 1
Classmate 0
Tor Network
Evil TA
Course Website Server