Spring 2022 April 27, 2022

Final review sheet

Instructor: Roopa Vishwanathan *CS 478/513: Computer Security*

Syllabus, etc.: Syllabus is:

1. CS 8, 11, 12, 13, 18, 19

Exam will consist of mostly short-answer questions, objective-style (T/F) questions, and a few problems. You can use calculators. The purpose of this review sheet is to give you an idea of the kind of questions you can expect to see on the midterm, but this isn't an exhaustive list of questions for the exam.

Questions:

1. What are the main properties of a hash function?
2. On an avg. how many preimages (inputs) do you need to try for successfully brute-forcing a hash function and recovering a putative password?
3. Attack vectors on passwords.
4. Be familiar with characteristics of ideal biometric, biometric modes and phases, fraud rate, insult rate.
5. Possible problem on C-lists and ACLs.
6. Why is ACL better than ACM, and why is C-List better than ACLs?
7. Confused deputy problem.
8. Be familiar with Bell-LaPadula and Biba properties.
9. Possible problem on Bell-LaPadula, Biba: given a certain classification/clearance/compartmentalization system, who can read/write what files?
10. Possible inference control problem, and ways to mitigate it.
11. Problem on authentication using nonces, replay attacks, etc. and suggest ways to solve it.
12. Password-based problems: salted, unsalted, with/without dictionary, and probability of finding one in the dictionary (see class notes and assignment 3).
13. On a particular system, all passwords are 8 characters, there are 128 choices for each character, and there is a password file containing the digests of 2^{10} passwords. Trudy has a dictionary of 2^{30} passwords, and the probability that a randomly selected password is in her dictionary is $\frac{1}{4}$. Work is measured in terms of the number of hashes computed.

(a) Suppose that Trudy wants to recover Alice's password. Using her dictionary, what is the expected work for Trudy to crack Alice's password, assuming the passwords are not salted?

(b) Repeat part a, assuming the password are salted.

(c) What is the probability that at least one of the passwords in the password file appears in Trudy's dictionary?

14. Suppose that all passwords on a given system are 8 characters long, and that each character can be any one of 64 different values. The passwords are hashed (with a salt) and stored in a password file. Now suppose Trudy has a password-cracking program that can test 64 passwords per second. Trudy also has a dictionary of 2^{30} common passwords and the probability that any given password is in her dictionary is $\frac{1}{4}$. The password file on this system contains 256 digests.

(a) How many different passwords are possible?

(b) How long, on average, will it take Trudy to crack the administrator's password?

(c) What is the probability that at least one of the 256 passwords in the password file is in the dictionary?