**2023/2024 4062/3010 Computer Security**

**Authentication/Password Tutorial**

1. Is it always a bad idea to write down your password? Is there a way to do it more safely?



1. (a) Verify the computational complexity of these 3 entries: 10 character lower case alphanumeric, 9 character alphanumeric, 8 character printable keyboard characters in slide 16 of the Password Slides. What do you notice?



(b) The fastest Software Password crackers has cracking speed of up to 16 million passwords per sec (take it as 2^24) on a 3GHz PC. Estimate the time taken to compute cracking time of



(i) 10 numeric characters passwords



(ii) 8 character lower case alphanumeric passwords

(iii) 8 character alphanumeric passwords



(iv) 8 character all 95 printable characters passwords

1. Do you think passwords such as Methuselah78 is safe?



1. How long should a password be if it is to achieve 128-bit security?



1. Alphanumeric, (b) alphanumeric case-sensitive (c) Printable
2. Supposedly you are the CISO (chief info security officer) of a big company and you are about to launch a new e-commerce website. What do you think are his best ways to ensure his website is ready to face the public?



1. Calculate the time needed to crack a 8 char, 9 char & 10 char password unsing a 3GHz PC, for both mixed case alphanumeric and printable chars. This means there are 6 calculations in total.



Qn1: No it is not always a bad idea to write down passwords since it is difficult to memorise complex passwords, deal with frequent password changes and to avoid reusing the same passwords

Passphrases can be used where the user enters sentences that are easy to remember and the system hashes the phrase to get the password

Write down your difficult passwords on paper. Lock it in a safe or locked office drawer. Hackers will not be able to access your office and open your safe in a locked drawer

BUT if he can install keyloggers into your pc through your careless ness, your secure passwords can be captured by it and render your long secure passwords useless.

Qn2: a)i) 10 characters lower case alphanumeric: 2^k = 36^10. k = lg(36^10)/lg(2) = 51.69925001

ii) 9 character alphanumeric: 2^k = 62^9. K = lg(62^9)/lg(2) = 53.58776679 = 53.6

iii) 8 keyboard characters: 2^k = 95^8. K = lg(95^8)/lg(2) = 52.55884487

They have around the same computational complexity. With more variation in characters, the password can be shorter.

b)i) 10 numeric characters passwords:2^k = 10^10. K = lg(10^10)/lg(2) = 33.21928095

2^33.22/2^24 = 596.34s = 9.939mins

ii)8-character lower case alphanumeric passwords: k=41.4

2^41.4/2^24 = 172950.54s = 2882.5mins = 48hrs

iii)8-character alphanumeric passwords: k=47.6

2^47.6/2^24 = 12714752.12s = 211912.5353mins = 3531.87hrs = 147.16days

iv)8 character all 95 printable characters passwords: k=52.6

2^52.6/2^24 = 406872067.7s = 6781201.128mins = 113020.0188hrs = 4709.16745days = 12.9years

Qn3: No passwords like Methuselah78 is not safe as it is easily guessable due to the use of common terms/slang like Meth, use and lah, the placement of only one capital letter at the front of the password, and the placement of numbers at the end of the password.

Although password is alphanumeric 12 character, attacker does not need to bruteforce them and only needs a dict of names.

Qn4: 128 bit security = 2^128

1. alphanumeric: 2^128 = 36^n. n=lg(2^128)/lg(36) = 24.759 ~= 25
2. alphanumeric case sensitive: 2^128 = 62^n. n = lg(2^128)/lg(62) = 21.497 ~= 22
3. Printable: 2^128 = 95^n. n = lg(2^128)/lg(95) = 19.483 ~= 20

Qn5:

The website should salt passwords, hashing them and not encrypting them. The website has to ensure that the server security is well protected so that it cannot be hacked and that traffic cannot be sniffed using keyloggers. There should be careful selection of hash algorithms which slow down offline attacks through being as resource intensive as possible.

The website forces users to set passwords and change the default password. It also ensures that guessable passwords are avoided while setting a expiry date on passwords. Users are also prevented from using a list of previously used passwords. There should be a limit in the number of login attempts and inform the user whenever he logs in

Ask own security team to test system BUT depends on skillsets of small team and internal conflicts possible

Contract experts in penetration testing BUT depends on skillsets of small team, how hard they work on it, and cost.

Open Competition, talent from world wide, all bugs fixed asap

Qn6:

1. 8 character
2. Mixed case alphanumeric: k= 47.6 = 147.16 days
3. printable characters: k = 52.6 = 12.9 years
4. 9 character
5. Mixed case alphanumeric:53.6

2^53.6/2^24 = 813744135.4s = 13562402.26mins = 226040.0376hrs = 9418.3349days = 25.8years

1. printable characters:59.1

2^59.1/2^24 = 3.682585576 x 10^10 s = 1167.74years

1. 10 character
2. Mixed case alphanumeric:59.5

2^59.5/2^24 = 4.8592008 x 10^10 s = 1540.84years

1. printable characters:65.7

2^65.7/2^24 = 3.572323818 x 10^12s = 113277.65years