Matthew Krieger

**Description for: CS 492 Homework**

Authentication and Authorization

**You must work individually**

**Authentication**

1. Passwords - A developer knows that security is only as strong as the weakest point in the system. Knowing this he wants to require users to have a password with enough characters that it should be theoretically as secure as his 2^96 bit crypto key. Assuming for each character they can choose there are 256 possibilities.
   1. [10pts] Theoretically, what is the minimum number of characters he has to require to make sure the password could be as strong as the crypto key he is trying to protect?

296 = 7.9228163e+28

25612 = 7.9228163e+28

296 = 25612

12 characters

* 1. [10pts] Explain in your own words why his goal will not be achieved if he allows users to pick their own passwords even if he requires at least one symbol and number in the password

Users generally do not select random passwords and an attacker would need to try much less than 263 different passwords

1. [20pts] Give 5 different real examples (i.e. different elements or combinations used – not just 5 different web sites) of where 2-factor authentication is used and explain what each factor in the examples
2. **Google**: two-step authentication is often used at different times to confirm the user’s identity. To login, Google requires a **password** (something you know) and it has to be able to **recognize the computer/device** (something you have)
3. **Smartcard** (something you have) & **Password** (something you know)
4. **Banks/ATM**:
   1. **Bank Card** – Something you have
   2. **Pin** – Something you know
5. Using a **credit card** (ie. Visa) to make a purchase in a store (Macy’s)
   1. **Credit Card** – Something you have
   2. **Signature** – Something you are
6. **LinkedIn** – Login
   1. **Password** – Something you know
   2. **SMS** – Something you have

**Authorization**

1. Advantages
   1. [5pts] What are 2 advantages of capabilities over ACL
      1. Easy to delegate & avoid confused deputy
      2. Simple to add/delete users
   2. [5pts] What are 2 advantages of ACL over capabilities – access is considered on a file-by-file OR resource-by-resource basis.
      1. Easier to implement
      2. Runs quicker
      3. Easy to modify the rights to a resource
      4. Protection is data oriented
2. Delegation
   1. [10pts] Describe what the confused deputy problem is

In a nutshell, the confused deputy problem is when a process/resource is tricked into doing any action (or not doing an action) that it doesn’t have permission to do.

For example: If Alice has access to execute a compiler and the compiler has permissions to read/execute itself & to read & write bil, but Alice does NOT have permission to write the bill. So if Alice executes the compiler and “tells” it to write the bill, which confuses the operating system.

In this situation, the compiler(deputy) becomes confused by the permission conflict and (more specifically), the compiler confused it’s permissions with Alices’.

Client

Resource

“Deputy”

1. [40pts] MLS compartments
   * Alice has the following clearances TopSecret, Secret{A}, Classified{B}
   * Bob has the following clearances TopSecret{A}, Secret{B}

Draw the full tree and indicate which files Alice and Bob each can read (don’t forget Unclassified)



