Angel Velazquez

Identity and Authentication

1. What is the difference between identity and authentication?
   1. Identity the username to an account; authentication is the password for the username.
2. In what situation should each of these be used or not used?
   1. These should be used to access a personal account on a web service. However, certain web services would be better suited to use something other than personal accounts, such as reading articles online.

Authentication Methods

1. Name three types of authentication methods used today.
   1. Two-factor authentication
      1. Verify using phone number
      2. Verify using email
      3. Verify using security question

AES and DES

1. How are AES and DES both different than the Caesar encryption model?
   1. AES and DES split the text into separate blocks before encrypting, whereas Ceasar encryption only performs a letter shift.
2. Explain the differences between AES and DES
   1. DES divides the text into two halves before encrypting, whereas AES uses multiple rounds of substitutions and critical verifications to create an encrypted block, making AES more secure
3. Explain XOR
   1. XOR is an exclusive or logic gate that only activates if the two signal inputs are opposite, so 0 and 1 or 1 and 0 would only activate an XOR block. In encryption, this adds another level of complexity.
4. What alternatives are there to block ciphers?
   1. Stream ciphers
      1. Encrypts data within 8 bits
   2. Public key cryptography
      1. Encrypts using a public key
      2. Decrypts using a private key
   3. Block ciphers
      1. Encrypts blocks to 64, 128, or 256 bits of data.
      2. More complex but slower

Symmetric vs. Asymmetric Encryption

1. Explain the differences between symmetric and asymmetric encryption.
   1. Symmetric uses a single key to encrypt and decrypt
   2. Asymmetric uses a public and a private key
2. What are the pros and cons?
   1. Symmetric encryption only requires one key, so one key fits all, but this is a security risk since everyone may know the key.
   2. Asymmetric encryption uses a public key to encrypt but a private key to decrypt. So, private keys can be shared between the sender and the receiver.
3. Explain the difference between a public and private key
   1. With a public key, a single key may be shared among multiple users to access data.
   2. With a private key, only that specific key will work to decrypt the data.
4. Explain the role of prime numbers in creating a public and private key.
   1. In theory, every whole number is a product of prime numbers, but finding the prime factors of a large key takes time and effort.

Hashing vs. Encryption

1. Explain the purpose of a hashing algorithm.
   1. Hashing can be used to authenticate sensitive data. For example, users may want to compare their results with some hashed data; they can hash their data and see if the two compare.
   2. Encryption is used to hide sensitive data using keys. Only people with the key may access the readable contents of the data.
2. Explain how a computer system can use hashing to ensure passwords are private.
   1. There is always a risk of a system’s database being breached. If so, the stored passwords are already hashed, which makes it incredibly difficult to decipher into the actual password; it is simply another security measure against security breaches.
3. Explain how hackers use a rainbow table and how you can defeat them.
   1. If hackers access the hashed passwords, they can run them through a rainbow table with the hash value for all plain text characters.
   2. Rainbow table attacks may be mediated by inserting random data through the hash function and plain text.