Public Key Infrastructure

Objectives

- Discuss how PKI works
- Explain how PKI is used to secure systems
- Discuss how using PKI is better than using shared passwords

Encryption

- There are 2 kinds of encryption
  - Symmetric – Each party knows the same information
  - Asymmetric Each party knows enough information
- Public Key Encryption
  - Based on mathematical functions
  - Uses public and private key pairs
  - Needs some way of distributing the keys

Asymmetric Encryption Steps

1. User generates a key pair – this is typically done through software due to the key size
2. Each user publishes their public key. Each user keeps their private key private
3. If Bob wants to send a message to Alice, Bob encrypts the message with Alice’s public key and Bob’s private key
4. When Alice receives the message, Alice decrypts the message with Bob’s public key and Alice’s private key

Public Key Encryption

- First developed in 1976
- Is a way to encrypt and decrypt without knowing the private secret or key
- Requirements
  - Generated key pairs must encrypt and decrypt
  - Must be computationally easy to produce key pairs
  - Must be computationally easy to encrypt and decrypt
  - Must be computationally impossible for anyone else to decrypt message
  - Must be computationally impossible to decrypt using only the public key by itself
  - Must have some way to exchange keys

Why is it important?

- It is a reverse function that allows the sender and receiver to only share their public key
- It is very difficult to break because of prime factorization
- The size of the key is important
- This covers both confidentiality and integrity

RSA Algorithm

- It’s really a very simple algorithm
- To encrypt: C = M^e mod n
- To decrypt: M=C^d mod n
- Both the sender and receiver must know the values of n and e. Only the receiver knows the value of d
- Public key must be known.
  - PU = {e,n}
- Private key is private
  - PR = {d,n}

Example - 1

- Let’s say our message (m) is just a letter. The letter “A”. A in ASCII is the number 65.
- We need to select 2 prime numbers.
  - P = 61 and q = 53
- Calculate n
  - n=p*q = 61*53 = 3233
- Calculate the relative prime for e and select for e based off Eulers totient
  - (n) = (p – 1)(q – 1) = 60*52 = 3120.
  - Must be prime so we’ll pick 17

Example - 2

- Encrypt:
  - $C = M^e \bmod n$
  - $C = 65^{17} \bmod 3233$
  - $C = 6599743590836592050933837890625 \bmod 3233 = 2790$
  - So our ciphertext is 2790 for the letter A
- Decrypt
  - $M=C^d \bmod n$
  - $M = 2790^{2753} \bmod 3233$
  - $M = 65$

Why use public/private keys?

- In order to break it, you would have to try to brute force the private keys
- Mathematically, it’s very difficult to break, you have to factor primes
- It’s difficult to break period
- There are other attacks out there, but they are difficult to exploit and may take years to decrypt information