CYBR372 - Week 2: Introduction to Cryptography

Terms in this set (18)

Encryption notation	Secret key = Kc Message = m (plaintext) Ciphertext = c Encryption function = E(Kc, m) Decryption function = D(Kc, c)
Kerckhoff's Principle	Security of the encryption scheme must depend on the key, not the algorithm (only keep the key as the secret) -have to distribute algorithms to everyone using it (potentially hundred of thousands) - Hard to get it right - Hard to update, it may have a long lifecycle - Good to have open source (peer review and testing) - Security through obscurity is weak
Authentication notation	Authentication key = Ka Message authentication code function (MAC) = h(Ka, m)
Weaknesses of just using authentication	Exposed to replay attacks and denial of service With sequence numbers implemented, deletion or delaying messages still occur.

Public-key encryption (asymmetric encryption)	A type of encryption that uses two different keys, a public key and a private key Public key is published, encrypt message with public key of recipient, recipient decrypts message with their private key. D(s, E(p, m)) = m
Public-key encryption drawbacks	Expensive and less efficient Have to distribute keys Have to sign keys to authenticate
Digital signature	Signing a public key to ensure authentication Public key verifies, the secret key is used to create a new signature. Signing = o(S, m, s) Verification = v(p, m, S)
Digital signature drawbacks	An individual doesn't compute the signature themselves, their computer does - exposure to malware and hijacking.
Public key infrastructure (PKI)	Central authority (certificate) signs authentic public keys. They verify the public key with their own secret key. Multiple levels of CAs - Top and bottom levels, may have to verify at least two.
PKI drawbacks	CA must be trusted. Liability issues - CA can issue false certificate or the secret key is stolen.

CYBR372 - Week 2: Introduction to Cryptography

Cipher-text-only attack	Attacker only knows the cipher. The hardest attack with the least amount of info.
Known-plaintext attack	Attacker knows both plaintext and ciphertext. Is able to learn about the key. Gives more info than Cipher-text-only.
Chosen-plaintext attack	Attacker is able to choose plaintexts with correlating ciphertexts. Offline - Choose a list of plaintexts before before receiving ciphertexts. Online - Choose new plaintexts depending on recieved ciphertexts. Online more powerful than offline.
Chosen-ciphertext attack	Attacker is able to choose both ciphertext and plaintext at all times. More powerful than chose-plaintext attack.
Distinguishing attack	Attacker has a non-trivial method that detects the difference between an ideal encryption scheme and the actual encryption scheme. They find imperfections in the implementation. Involves information leakage and side-channel attacks.

CYBR372 - Week 2: Introduction to Cryptography

Birthday attacks	Based on birthday paradox - if there are enough people in the room, there is a 50% chance they have the same birthday. Based on collisions - where a hash is generated twice. A collision is possible when over 50% of combinations have been achieved. Root over n, where n bits = 2 to the power of n = root of 2 to the power of n = 2 to the power of n over 2. eg. 64 bits = 2 to the power of 64 combinations, only 50% combinations are needed for a key to generate the same hash, therefore min is 2 to the power of 32.
Meet in the middle attack	Build a table of possible keys If computed hash is in created table correlating to a key, it is likely to work. Birthday - wait for a collision. Meet in the middle - wait for an overlap. n = possible values Computed set = p elements Computing set = q elements Birthday - p = q = root of n Meet in the middle - p = n to the power of 1/3, q = n to the power of 2/3
Exhaustive search attack (brute force)	Go through all combinations. eg. 64 bit = 2 to the power of 64 combinations.