COMPUTER SECURITY FINAL EXAM AUTUMN 2015

LECTURE 1 – INTRODUCTION TO SECURITY

PRINCIPLES

- **Easiest Penetration:** Intruder expected to use any available means of penetration.
- **Weakest Link:** Security can be no stronger than its weakest link.
- **Adequate Protection:** Protected only until they lose their value.
- **Effectiveness:** Controls must be used properly. Efficient, Easy to use and appropriate.

TYPES OF THREATS

- **Interception:** Unauthorized party has gained access to asset.
- **Interruption:** Asset of system becomes lost, unavailable or unusable.
- **Modification:** Unauthorized party not only access but tampers with asset.
- **Fabrication:** Unauthorised party create a fabrication of counterfeit objects on a system.

SECURITY GOALS

- **Confidentiality:** Accessed by Authorised parties only.
- **Integrity:** Only be modified by authorised parties and in authorised ways.
- **Availability:** Only be authorised by authorised parties at appropriate times.

SECURITY CONTROLS

- Encryption
- Software Control
- Hardware Control (locks, biometric, firewall)
- Policies and Procedures

LECTURE 2 - AUTHENTICATION

FUNDAMENTAL TOOLS

- **Authentication:** Act of proving the claimed identity.
  - ➔ Something the user knows
  - ➔ Something the user has
  - ➔ Something the user is

PASSWORD

Is a mutually agreed-upon code word, assumed known only to user and system

- Most common user authentication method.
- Drawbacks include: Lost, disclosure and revocation, attackable
- Can be brute forced, calculated using a^5 e.g.
  - ➔ All combinations of 5 lower case letter words $26^5 = 11,881,376$ combinations
  - ➔ All combinations of <= 5 letter (inc number) words $62^0 + 61^1 \ldots 61^5 = 931,151,403$

PASSWORD STORAGE

Cryptographic Hash Function: takes a value and return a fixed-size alphanumeric string (hash).

- Hash function that is easy to compute and hard to reverse.
- Same output values for same input values.
- Hard to find two input messages that produce same output values
- Examples include MD4/5 (Message Digest) and SHA/SHS (Secure Hash Algorithm/Standard)
- Used for
  - ➔ Integrity Checks
  - ➔ Password Verification
  - ➔ File indexing (file hashing)
  - ➔ Message Authentication
- Can use Salt to make same passwords hash value unique.

LECTURE 3 - CYPTOGRAPHY

KEY CONCEPTS

- Substitution vs Transposition(Permutation)
  - ➔ **Substitution** changes the text whereas transposition rearranges the text.
- Confusion vs Diffusion
  - ➔ **Confusion** scrambling in the code space
    - Interceptor should not be able to predict what happens by changing single character.
  - ➔ **Diffusion** scrambling in the location
    - Distribution of information from single symbols in the plaintext over the entire output.
- Stream vs Block Ciphers
  - ➔ **Stream Ciphers** convert each symbol of plaintext immediately into a symbol of cipher text e.g. Caesar Cipher
  - ➔ **Block Cipher** converts a group of plaintext symbols into a group of cipher text e.g. Columnar Cipher

KEYS

- **Private Key:** A user's secret key that should not be shared.
- **Public Key:** A user's key that can be shared to one or more users.

ENCRYPTION

- **Symmetric Encryption:**
  - ➔ Private/Public Key Encryption
  - ➔ Same key for encryption/decryption
  - ➔ Keys kept secretly
- **Asymmetric Encryption:**
  - ➔ Public Key Encryption
  - ➔ Use a pair of different keys for encryption/decryption
  - ➔ Private Key kept secretly, public key public or vice versa.

LECTURE 4 - CRYPTOGRAPHY

USE OF ENCRYPTION

- **Digital Signature**
  - ➔ Authentication of e-messages.
  - ➔ Valid digital signatures satisfy
    - **Authenticity:** message was created by sender
    - **Non-forgeable**: message cannot be forged
    - **Non-alterable:** message cannot be altered
    - **Non-repudiation:** sender can't deny having sent the message.
- **Key exchange**
  - ➔ **Coupled Approach:** Sender S encrypts the message with his private key, followed by the receiver's public key. Receiver R decrypts the message with her private followed, by the sender's public key.
  - ➔ **Decoupled Approach:** Sender signs the message with his private key and encrypts message with receiver's public key. Receiver decrypts the message with her private key, accept if signed message is equal to decrypted message.
  - ➔ Use key exchange to distribute an encryption key between two parties.
  - ➔ Ensure message is only seen between two parties.
  - ➔ Generate and use Random Key if message exceeds size limit
  - ➔ **Large Message Delivery** – if sender needs to send large message that exceeds size limit.
    1. Generate a random key used for symmetric encryption
    2. Encrypt the message with the random key using a symmetric cipher (e.g AES)
    3. Encrypt the random key with receivers public key using a public-key algorithm (e.g. RSA)
    4. Send encrypted message and encrypted key to receiver.
- **Digital Certificates**
  - ➔ Electronic document to prove ownership of a public key.
  - ➔ Includes: Owner information, owner public key, digital signature of the trusted body
  - ➔ Trusted body can be
    - **Public Key Infrastructure (PKI):** Central Authority known as Certificate Authority (CA)
    - **Web of Trust:** Trusted person that knows owner