41900

SECURITY FUNDAMENTALS

STUDY NOTES

2018

UTS 2018

CONTENTS

INTRODUCTION TO INFORMATION SECURITY

LECTURE 1

INFORMATION SECURITY

- Application of technology and processes to protect data from accidental or intentional misuse by known or unknown individuals, inside or outside of an organisation
- Technical aspects make up one-part Eg. Firewalls, encryption, access controls, etc.
- Increasingly important problem as hackers attempt to take advantage of an organisations network vulnerabilities

KEY TERMINOLOGY

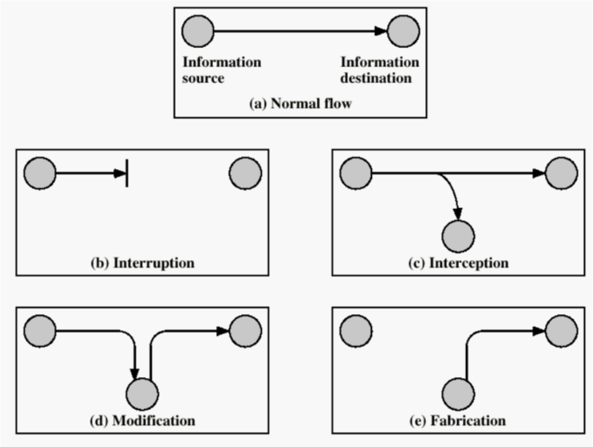
- Cryptography – Process of creation, development, application and testing of encryption methods
- Encryption – Converting original message into a form unreadable by unauthorised individuals
- Cryptanalysis – Process of breaking an encrypted message to obtain the original message
- Cryptology – Consists of both cryptanalysis and cryptography

CIA TRIAD (ASPECTS OF SECURITY)

- **C**onfidentiality – Accessible only to authorised users Eg. Encryption, Authentication, Access Controls, Location
- **I**ntegrity – Safeguarding accuracy/completeness Eg. Only entered/altered by authorised users, cannot be altered without detection Eg. Audit Trails, Checksums and Hashes
- **A**vailability – Ensuring authorised users have access to information when required, accessible from authorised locations, system resists failures and attacks Eg. Standby mechanisms, resistant to DoS attacks
- Authenticity – Proof of a message's origin, integrity and freshness ie. Message is not a replay
- Non-Repudiation – Authorship of a message cannot be disputed
- Covertness – Message existence secrecy

PASSIVE/ACTIVE ATTACKS

- Passive
  - Do not involve modification or fabrication of data
  - Confidentiality Eg. Release message contents
  - Covertness Eg. Traffic analysis
- Active
  - Fabrication – Attack on Authenticity
  - Interruption – Attack on Availability
  - Modification – Attack on Integrity



(a) Normal flow

(b) Interruption

(c) Interception

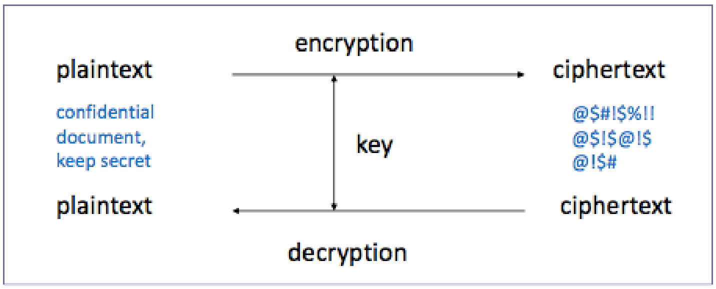
(d) Modification

(e) Fabrication

Figure 1.1 Security Threats

TYPES OF CRYPTOGRAPHY

- Classical
  - DES (Data Encryption Standard)
  - AES (Advanced Encryption Standard)
- Public Key
  - Diffe-Hellman
  - RSA (Rivest–Shamir–Adleman)
- Checksums
  - HMAC (Hash-based message authentication code)

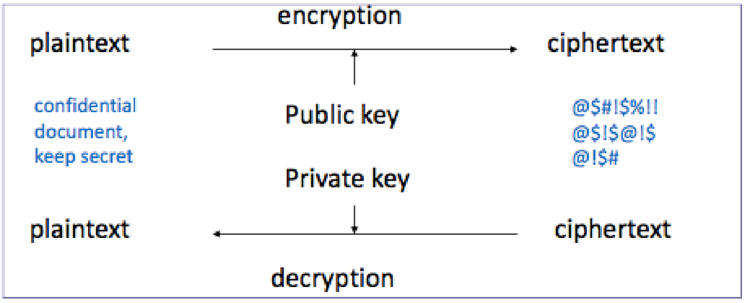


CLASSICAL CRYPTOGRAPHY

- Sender, receiver share common key
  - Keys may be the same or trivial to be derived from one another
  - Sometimes called Symmetric Cryptography
    - Using a single key for encryption/decryption
    - Plaintext and ciphertext are the same size
- Basic types:
  - Transposition Ciphers
  - Substitution Ciphers

  - Combination – Product Cipher

PUBLIC KEY CRYPTOGRAPHY



- Two keys
  - Private key – Known to one individual
  - Public key – Available to anyone
    - Public key, private key inverses
- Confidentiality – Encipher using public key, decipher using private key
- Integrity/Authentication – Encipher using private key, decipher using public key
- Sometimes referred to as Asymmetric Cryptography
- Public Key Cryptography requirements:
  - Computationally easy to encipher or decipher a message given the appropriate key
  - Computationally infeasible to derive the private key from the public key
  - Computationally infeasible to determine the private key from a chosen plaintext attack

CRYPTOGRAPHIC CHECKSUMS

- Mathematical function to generate a set of k bits from a set of n bits (where $k \leq n$)
- Example: ASCII parity bit:
  - Has 7 bits; 8th bit is a 'parity' bit
    - Even parity – Even number of 1 bits
    - Odd parity – Odd number of 1 bits

HMAC

- Make keyed cryptographic checksums from keyless checksums
- Keyless cryptographic checksum function, h, takes data in blocks of b bytes and outputs blocks of l bytes
- K' is cryptographic key length b bytes
  - If short, padded with 0 bytes; If long, hash to length b
    - *ipad* is 00110110 repeated b times
    - *opad* is 01011100 repeated b times
- HMAC – $h(k, m) = h(k' \oplus opad \,||\, h(k' \oplus ipad \,||\, m))$

BASIS FOR ATTACKS

- Mathematical attacks
  - Based on analysis of underlying mathematics
- Statistical attacks
  - Make assumptions about models of the language
    - Distribution of letters, pairs of letters (Di-grams), triples of letters (Tri-grams)
  - Examine ciphertext, correlate properties with assumptions

DIGITAL SIGNATURES

- Encrypted messages that can be mathematically proven to be authentic
- Created in response to rising need to verify information transferred via electronic systems
- Asymmetric encryption processes used to create digital signatures

DIGITAL CERTIFICATES

- Electronic document containing key value and identifying information about entity that controls key
- Digital signature attached to certificate's container file to certify file is from entity it claims to be from

MANDATORY SECURITY

- Bell and La Padula Security Policy
  - Security levels – Subjects have clearance levels, Objects have sensitivity levels
    - Unclassified < Confidential < Secret < Top Secret
  - Compartments also possible, combined to form partially ordered lattice
  - Security Properties:

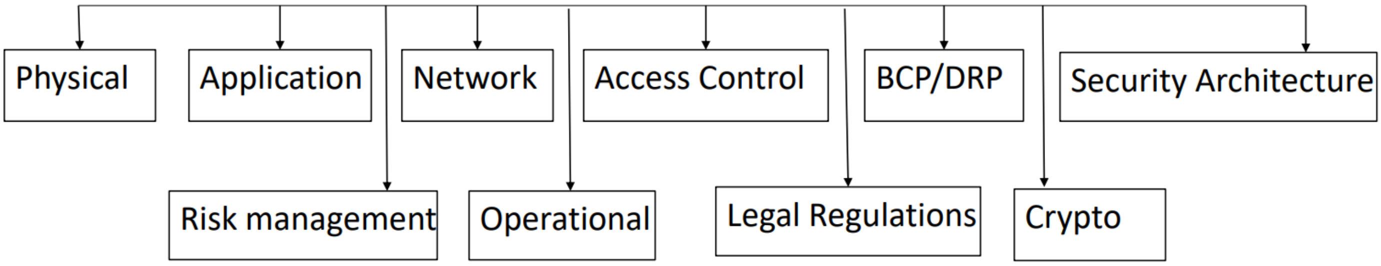
        - Simple Security Property – Subject may not READ an object at a higher security level
        - Star * Property – Subject may not WRITE to any object at a lower security level

CRYPTO ATTACK METHODS

- Brute Force
    - Goes through all available keys, testing each until the correct key is found
    - Main defence is to make at least 2128 possible keys, makes too time consuming to find key
    - Effectiveness of attack can be enhanced by using more hardware
- Exploit
    - Finding a weakness within the system
    - Encryption standards with known weaknesses are dropped quickly
    - Networks exchanging encrypted data allow attackers to collect encrypted information to possibly mount an attack

INFORMATION ASSURANCE

- Combination of all security principles to ensure information security



PHYSICAL SECURITY

DATA CENTER

- Designed to include physical safeguards, each facilities needs are unique
- Physical access trumps ALL other forms of security

SECURITY PROCESS AND PLAN

- Effectiveness is ensured by making certain:
    - Threats have been identified
    - Associated vulnerabilities are characterised, prioritised and addressed
- Supervised and enforced by consistent and ongoing management
- Example:
    - Numerous layers of: Alarms, Video Cameras, Armed Guards, Electrical Fences
    - Has separate emergency power plant, water system, and other facilities

APPLICATION SECURITY

- Data and critical business information is being exposed through:
    - Lack of Testing
    - Insecure Applications
    - Human Error Eg. Sticky Notes
- Security must be an integral part of the application lifecycle
- Golden Rule – You cannot test security! It must be designed into the application and verified throughout development

NETWORK SECURITY

- Network protocols are not secure:
    - Port scan/direct attack
    - Malicious websites
    - Social engineering
    - Phishing/Pharming
    - Denial of Service attacks
    - Insider attacks
    - Viruses/Worms
    - Information leakage
- Network hubs are insecure