Introduction to Information Security

Deepak Puthal

Email: Deepak.Puthal@uts.edu.au

41900 – Fundamentals of Security

Information Security

- The application of technology and processes to protect data from accidental or intentional misuse persons known or unknown inside or outside of an organization.

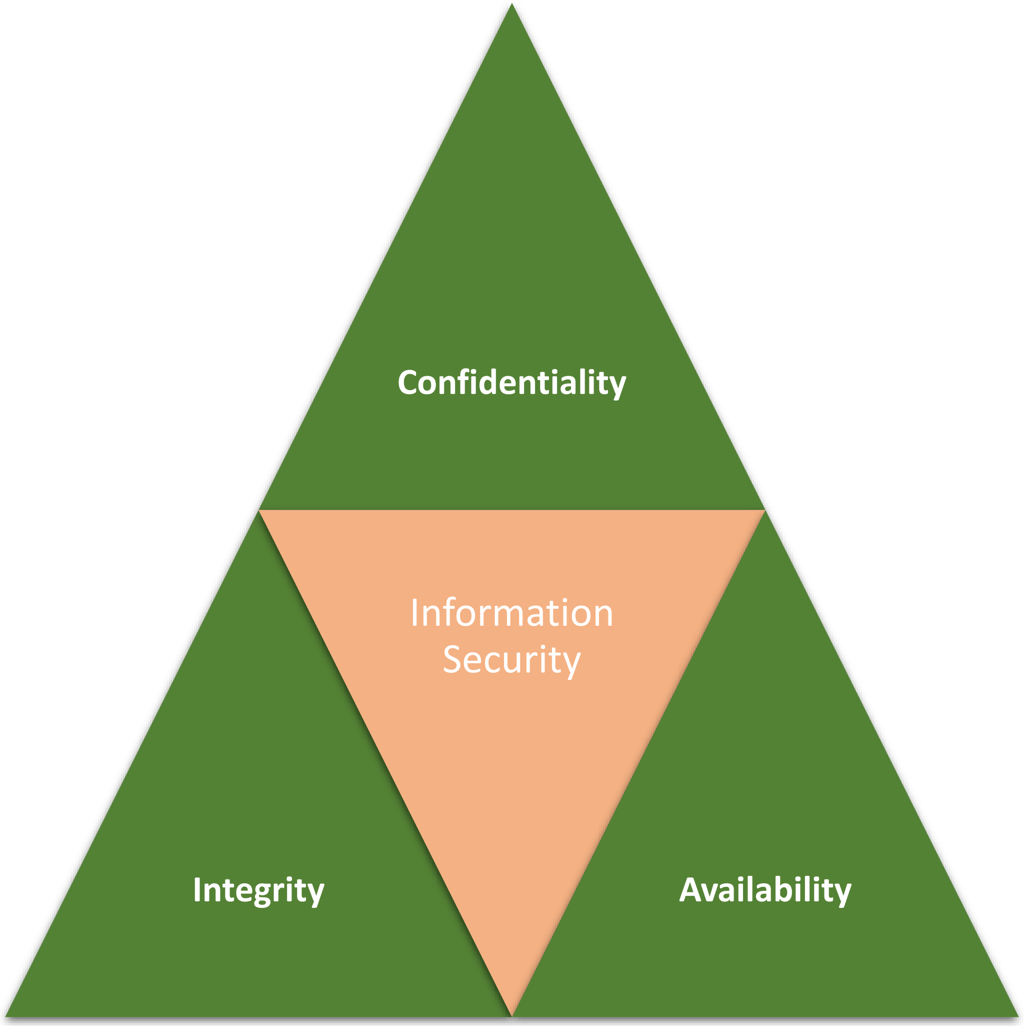
- By no means strictly a technical aspect, its technical aspects (firewalls, encryption, access controls, etc.) are important, but so are processes applied to ever varying situations.

- An increasingly high-profile problem as hackers (or crackers) take advantage of vulnerabilities against parts of an organization's network either Internet accessible or internal.

Key terminologies

- **Cryptography:** process of creation, development, application and testing of encryption methods
- **Encryption:** converting original message into a form unreadable by unauthorized individuals
- **Cryptanalysis:** process of breaking of encrypted message to obtain original message
- **Cryptology:** it consists of two sections i.e. cryptanalysis and cryptography

C I A Triad


Confidentiality
Information Security
Integrity
Availability

C I A Triad (Aspects of Security)

- **Confidentiality** – only authorized people, resources, processes have access
- **Integrity** – protect data from intentional or accidental changes
- **Availability** – Data or system is available by authorized users when needed

- **Authenticity –** proof of a message's origin Integrity plus freshness (i.e. message is not a replay)
- **Non-Repudiation –** message enciphered with private key came from someone who knew it
- **Covertness –** massage existence secrecy (related to anonymity)

Passive/Active Attacks

- Passive Attack
  - Those that do not involve the modification or fabrication of data.
  - An unauthorised party gains access to an asset
  - Release of message contents → an attack on confidentiality
  - Traffic analysis → an attack on covertness

- Active Attack
  - Fabrication → an attack on authenticity
  - Interruption → an attack on availability
  - Modification → an attack on integrity

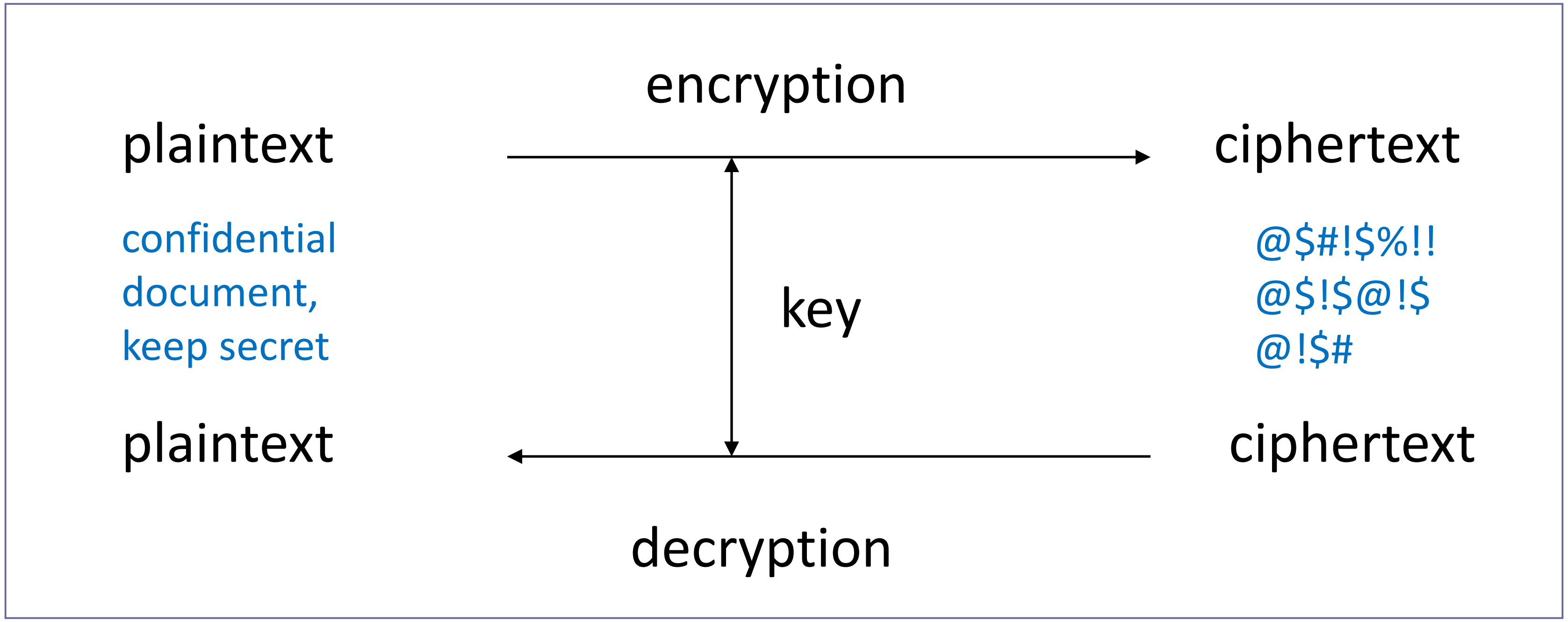
Types of Cryptography

- Classical Cryptography
  - DES (Data Encryption Standard)
  - AES (Advanced Encryption Standard)
- Public Key Cryptography
  - Diffie-Hellman
  - RSA
- Cryptographic Checksums
  - HMAC

Classical Cryptography

- Sender, receiver share common key
  - Keys may be the same, or trivial to derive from one another
  - Sometimes called *symmetric cryptography*
- Two basic types
  - Transposition ciphers
  - Substitution ciphers
  - Combinations are called *product ciphers*

Symmetric cryptography

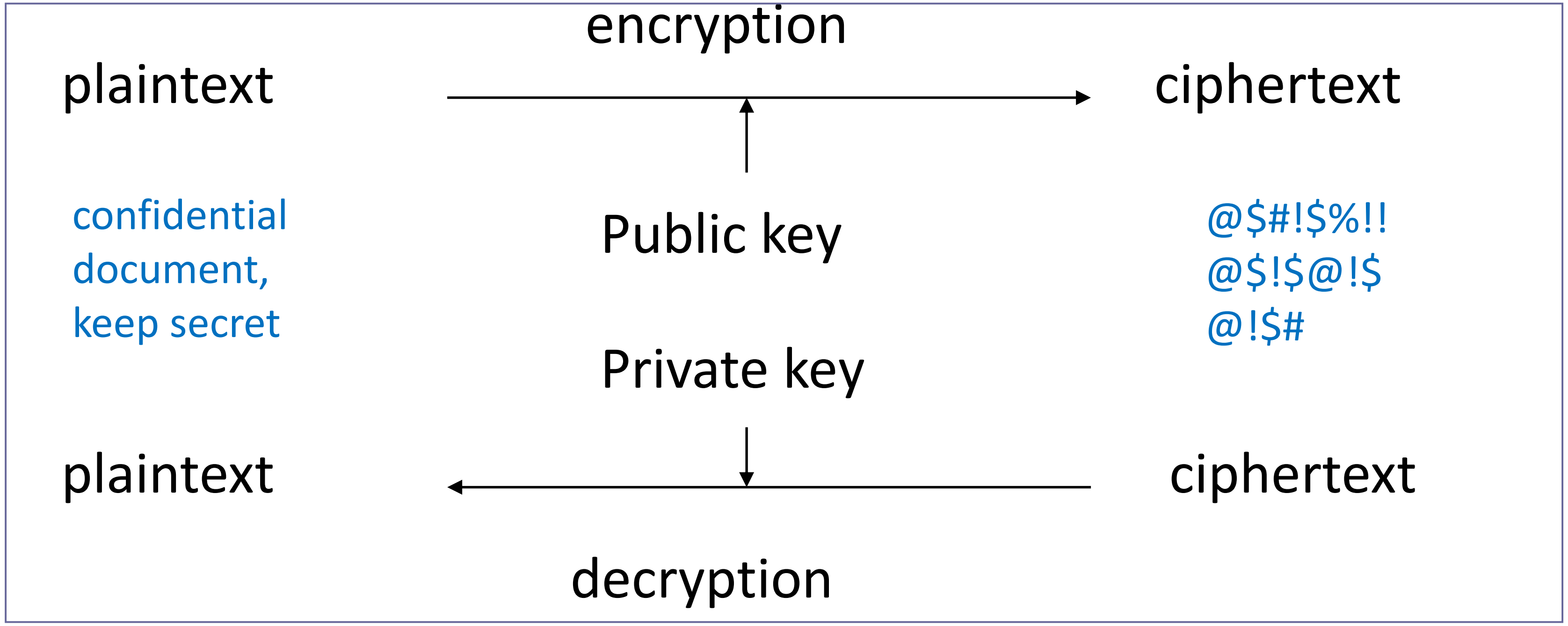


- Using a single key for encryption/decryption.
- The plaintext and the ciphertext having the same size.

Public Key Cryptography

- Two keys
  - *Private key* known only to individual
  - *Public key* available to anyone
    - Public key, private key inverses
- Idea
  - Confidentiality: encipher using public key, decipher using private key
  - Integrity/authentication: encipher using private key, decipher using public one
- Sometimes called *asymmetric cryptography*

Asymmetric cryptography



- Each individual has two keys
  - a private key: need not be reveal to anyone
  - a public key: preferably known to the entire world

Public Key Cryptography Requirements

- It must be computationally easy to encipher or decipher a message given the appropriate key
- It must be computationally infeasible to derive the private key from the public key
- It must be 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* ≤ *n*).
  - *k* is smaller then *n* except in unusual circumstances
- Example: ASCII parity bit
  - ASCII has 7 bits; 8th bit is "parity"
  - Even parity: even number of 1 bits
  - Odd parity: odd number of 1 bits

HMAC

- Make keyed cryptographic checksums from keyless cryptographic checksums
- *h* keyless cryptographic checksum function that takes data in blocks of *b* bytes and outputs blocks of *l* bytes. k' is cryptographic key of length *b* bytes
    - If short, pad with 0 bytes; if long, hash to length *b*
- *ipad* is 00110110 repeated *b* times
- *opad* is 01011100 repeated *b* times
- HMAC-$h(k, m) = h(k' \oplus opad \mid\mid h(k' \oplus ipad \mid\mid m))$
    - $\oplus$ exclusive or, $\mid\mid$ concatenation

Basis for Attacks

- Mathematical attacks
    - Based on analysis of underlying mathematics
- Statistical attacks
    - Make assumptions about the distribution of letters, pairs of letters (digrams), triplets of letters (trigrams), *etc.*
        - Called *models of the language*
    - Examine ciphertext, correlate properties with the assumptions.

Digital Signatures

- Encrypted messages that can be mathematically proven to be authentic
- Created in response to rising need to verify information transferred using 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
  - Subjects have clearance levels, Objects have sensitivity levels; clearance and sensitivity levels are also called security levels
  - Unclassified < Confidential < Secret < TopSecret
  - Compartments are also possible
  - Compartments and Security levels form a partially ordered lattice
- Security Properties
  - Simple Security Property: Subject has READ access to an object of the subject's security level dominates that of the objects
  - Star (*) Property: Subject has WRITE access to an object if the subject's security level is dominated by that of the objects

Two Crypto attack methods

- Brute Force: This method goes through all the available keys, testing each one until the correct key is found.

- Exploit a weakness in the encryption algorithm.

Brute Force Attack

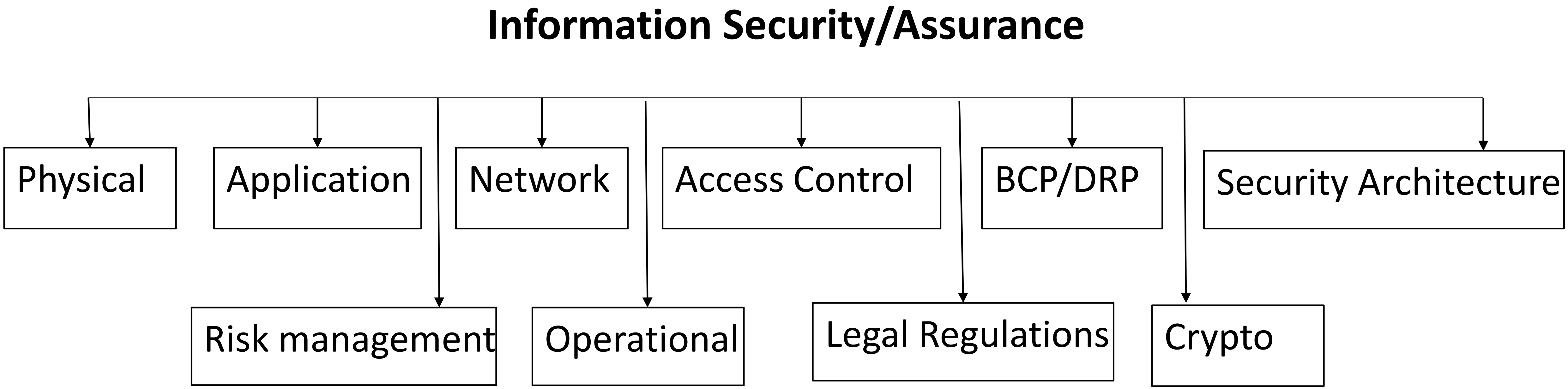
- Brute Force attack will always find the key eventually.
- Main defence is to make the number of possible keys a large number – at least 2128. This makes the search for the key time-prohibitive.
- The effectiveness of brute force attacks can be enhanced by adding more hardware. Purpose designed hardware can be even more effective.

Attacks based on a weakness

- All of the commonly used protocols have been extensively analysed.
- Encryption standards with known weaknesses are dropped fairly quickly.
- Networking protocols that exchange encrypted data allow attackers to collect encrypted data and from there possibly mount an attack.

Information Assurance

- Pulling all the principles together and applying them in a structured, ever evolving method results an more accurate term:



Physical Security: Data Center

- Facility must be designed to include physical safeguards
- Physical access trumps ALL other forms of security (exception being cryptography if properly implemented)
- No one solution: Each facility needs are unique

Physical Security Process and Plan

- Physical security process
  - Effectiveness is ensured by making certain that:
    - Threats have been identified
    - Associated vulnerabilities have been accurately characterized, prioritized, and addressed
  - Implemented through planning
  - Supervised and enforced by consistent and ongoing management

Example

- The facility is protected by numerous layers of
    - physical security
    - alarms
    - video cameras
    - armed guards
- Has a separate emergency power plant, water system, and other necessary facilities.
- The facility is ringed with several electrified fences and is under armed guard

Application Security

- Average sized organization has hundreds of in-house and externally developed applications.
- Business process are continually moving towards web services
- However, data and critical business services are being exposed:
    - Lack of testing
    - Insecure applications
    - Human error (leaving things where they shouldn’t be)

Application Security

- Security must be an integral part of application lifecycle:
    - from initial concept to final disposal

- A golden rule of application security:
    - You cannot test in security! It must be designed into the application and verified each step of the lifecycle.

Network Security

- Network protocols are not secure.
  - Port scan/direct attack
  - Malicious Web Sites
  - Social Engineering
  - Phishing/Pharming
  - Denial of Service attacks
  - Insider attacks
  - Viruses/Worms
  - Information Leakage
  - Others

Network Hubs

- Insecure!
- No traffic isolation or traffic control
- All data is replicated to all ports
- Any station on the hub can examine ALL traffic
- Collision problems on busy network

Network Security

- Switches are vulnerable
  - MAC address Flooding
- Other issues on local network
  - ARP Poisoning
  - Rogue DHCP Servers
  - Physical access to wiring closets

Access Control

- A key principle to preserve Confidentiality
- Properly implemented Access Controls ensures only authorized access and denies all else.
- Several methods are used
  - Mandatory Access Control
  - Discretionary Access Control
  - Role Base Access Control

BCP/DRP

- Business Continuity Planning/Disaster Recovery Planning
- An extremely important and rapidly growing part of Information Assurance!
- A proper security program is deficient if there isn’t business continuity and disaster recovery planning

Security Architecture

- Framework unifies reusable services and process to implement policy standards and risk management decisions.
- Strategic framework that allows the development and operations staff to align efforts
- Parameters
  - Policies
  - Standards
  - Guidelines
  - Baselines
  - Procedures

Risk Management

- Identifying and mitigating risks
- What is risk?
  - Risk = Threat * Vulnerability
- Mitigation can take three forms:
  - Accept the risk
  - Mitigate the risk
  - Transfer the risk
- Residual Risk

Operations Security

- Processes and controls placed around your operations.
- Assures Confidentiality/Integrity
- Can help assure availability
- Provides mitigation for incidents
- Includes HR processes (background checks)!

Audits

- Only good way to find out if controls are working as designed
- Internal vs. External
- Legal requirements

Legal, Regulations, Compliance and Investigations

- We are in the “Regulation Age”
- There are certain legal requirements and regulations which apply to many businesses
  - HIPPA, SOX, GLBA, FERPA, HEA, PCI DSS, PATRIOT Act, more!
- Compliance with these requirements and regulations are not optional
- Passing Audits necessary. Understanding the requirements and compliance now imperative

Investigations

- Log analysis
- Network analysis
- Digital Forensics
- Evidence handling
- eDiscovery

Cryptography

- Understanding how and when cryptography is used is not optional
- Encrypting data is required for eCommerce
- Sending certain types of data must be done securely and only cryptography is the solution.
- Implementing it correctly is essential
- Many poor implementations have resulted in breaches

Cryptography

- PKI – provides for nonrepudiation
    - Sending party later cannot deny they sent it*
        - *can you think of an exception
- Symmetric key management
- Asymmetric (PKI) management