CINEC CAMPUS
Beyond A Graduate

BSc (Hons) in Software Engineering

Course Code: GS3207
Security
Ethics & Professionalism

Security

Objectives

Introduction to security

Learning Outcomes

- Understanding security
- Understanding security in Ethical Frameworks
- Understanding security in professional Frameworks

Definition : Security

- Security means to prevent unauthorized access, use, alteration, and theft or physical damage to property.
- Security involves three elements:
  - Confidentiality
  - Integrity
  - Availability

Security Elements

- Confidentiality:
  - Prevent unauthorized disclosure of information to third parties.
  - Vital for protecting personal data, including medical, financial, academic, and criminal records.
- Integrity:
  - Prevent unauthorized modification of files and maintain the status quo.
  - System, information, and personnel integrity.
  - Alteration of information for personal gain or revenge.
- Availability:
  - Prevent unauthorized withholding of information from those who need it, when they need it.
  - Information is accessible to authorized users at all times.

Security imposement

- Two types of security
  - Physical security
    - Prevention of access to physical facilitates like computer systems.
  - Information security
    - Prevention of access to information by encryption, authentication, and other means.

Physical Security

- Physical security can be guaranteed if the following mechanisms are in place:
    - Deterrence:
        - First line of defense
        - A creating an atmosphere intended to scare intruders.
    - Prevention:
        - Second line of defense
        - Trying to stop intruders from gaining access.
    - Detection:
        - Third line of defense
        - Assumes the intruder has succeeded or is in the process of gaining access to the system
        - “see” that intruder who has gained or who is trying to gain access.

Physical Security-cnt

- Response:
  - An aftereffect mechanism
  - Trying to stop and/or prevent damage or access to a facility.

Physical Security

- Use electronic barriers to secure the system
    - Firewall
    - Password

Physical Access Controls

- A regime of access controls must be put in place.
- Create both physical barriers and electronic protocols
    - Physical Security Barriers
    - Electronic Access Controls
- It will authenticate the user of the resource .

Physical Security Barriers

- The physical barrier can be a fence made of barbed wire, brick walls, natural trees, mounted noise or vibration sensors, security lighting, close circuit television (CCTV), buried seismic sensors, or different photoelectric and microwave systems
- The area surrounding the facility can be secured using locks and keys, window breakage detectors, infrared and ultrasonic detectors, interior microwave systems, animal like dogs, and human barriers like security guards and others.

Electronic Access control

- With advances in technology, move from the physical barriers to electronic controls.
- They are:
  - Password
  - Firewall

Password

- It verify a user to an information system such as computer system.
- It contains string of usually six to eight characters with restrictions on length and start character.
- Password security greatly depends on the password owner.
- Hence;
    1. Never publicize a password.
    2. Never write a password down anywhere.
    3. Never choose a password that is easy to guess.
    4. Never keep the same password for an extended period of time.

Firewall

- A firewall is hardware or software used to isolate sensitive portions of an information system facility from the outside world.
- Limit potential damage by malicious intruders.
- There are three types of firewall:
  - Packet Filters
  - Proxy Servers
  - Stateful Inspection

Firewall

- Packet Filtering Firewall:
  - They are packet level filters.
  - Inspects packets based on predefined rules.
  - Allows or blocks packets based on source, destination, port, and protocol.
- Proxy Server
  - Acts as an intermediary between internal (client) and external (web site) systems.
  - When a client makes a request to access a resource on the internet, it sends that request to a proxy server instead of directly to the destination server.
  - The proxy server then forwards the request to the destination server on behalf of the client.
  - Ex: HTTPS Proxy

Firewall

- Stateful Inspection Firewall:
  - These firewalls combine both the filter and proxy functions.
  - Monitor and control network traffic based on the state of active connections and the context of the data packets.
  - Tracks the state of active connections.
  - Makes decisions based on the context of the traffic flow.

Information Security

- Information security ensure the integrity, confidentiality, and availability of information at the servers.
  - Information means information in files and databases and in transition between servers, and between clients and servers.

Common approaches for ensuring Information Security

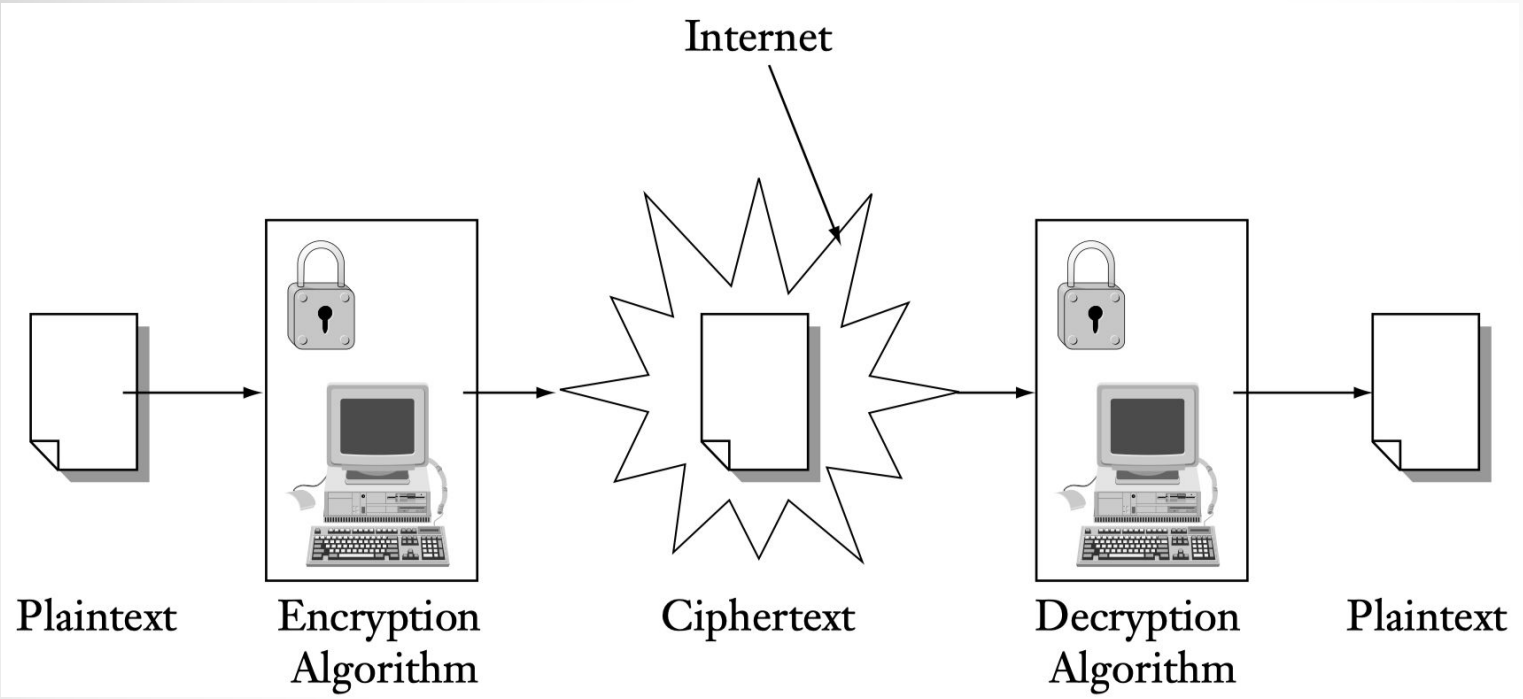
- Cryptography for secure transmission and authentication.
- Audit trails at information source and destination servers.

Cryptography

Cryptography: Securing Information Transmission

- Cryptography is the science of writing and reading coded messages.
- Cryptography functions:
    - Symmetric Encryption
    - Asymmetric Encryption
    - Hash Functions

Symmetric Encryption

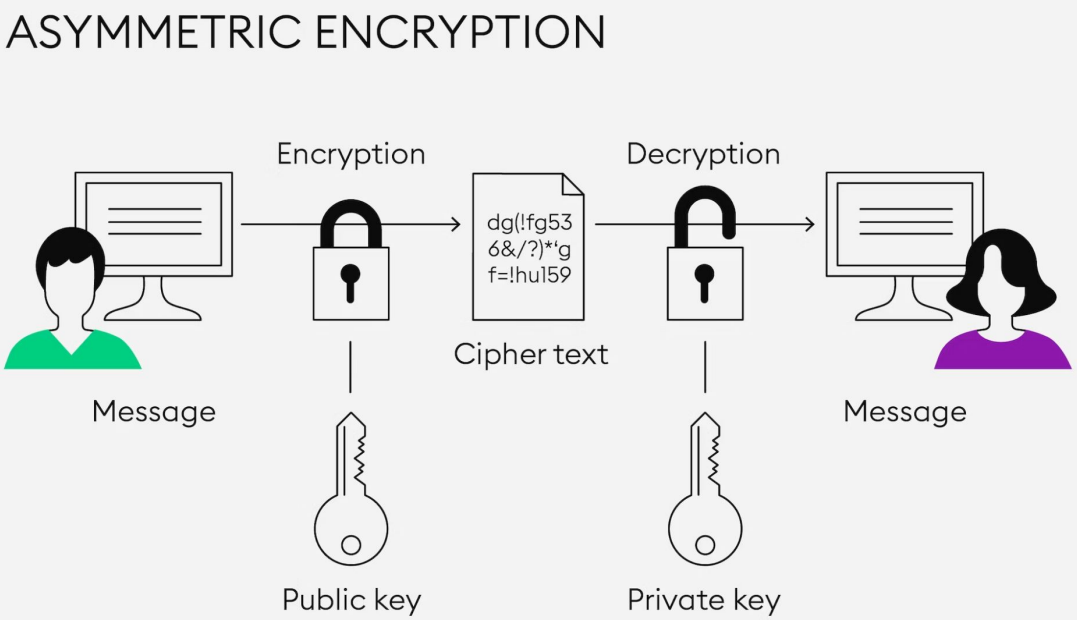


keys must be passed from the sender to the receiver.

Uses a common key and the same cryptographic algorithm to code and decode the message

Guest with no knowledge of the key are unable to read the message.

Asymmetric Encryption

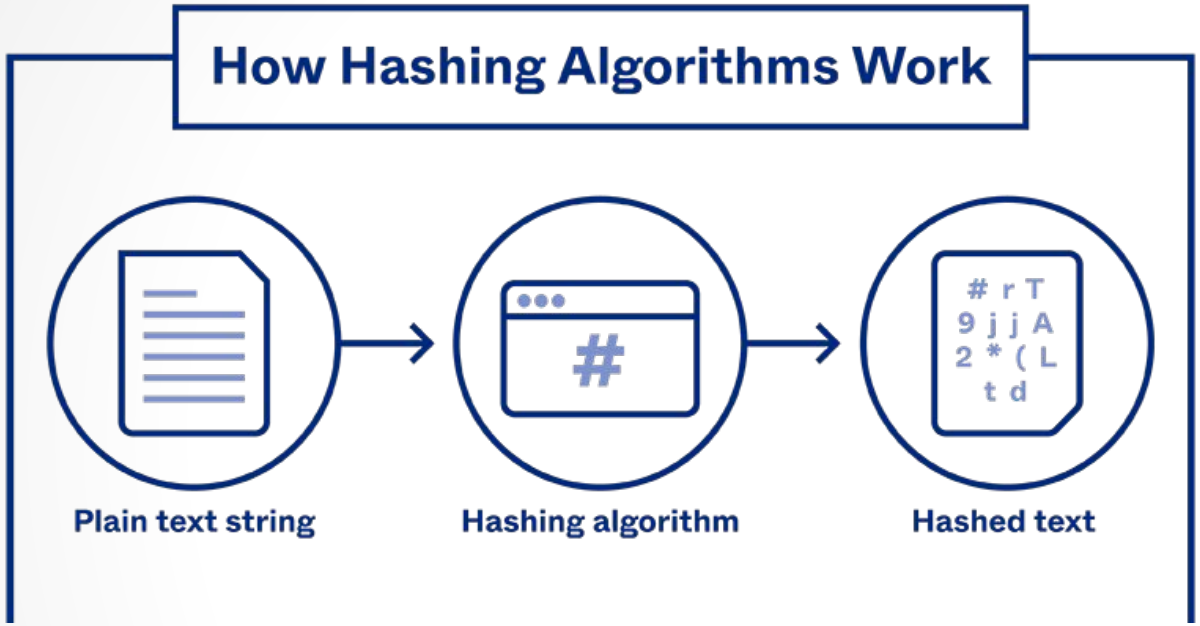


public key can be freely shared, the private key must remain secret.

a private key known by only the sender and the receiver and public key known by both.

public key for encryption and a private key for decryption

Hash Encryption

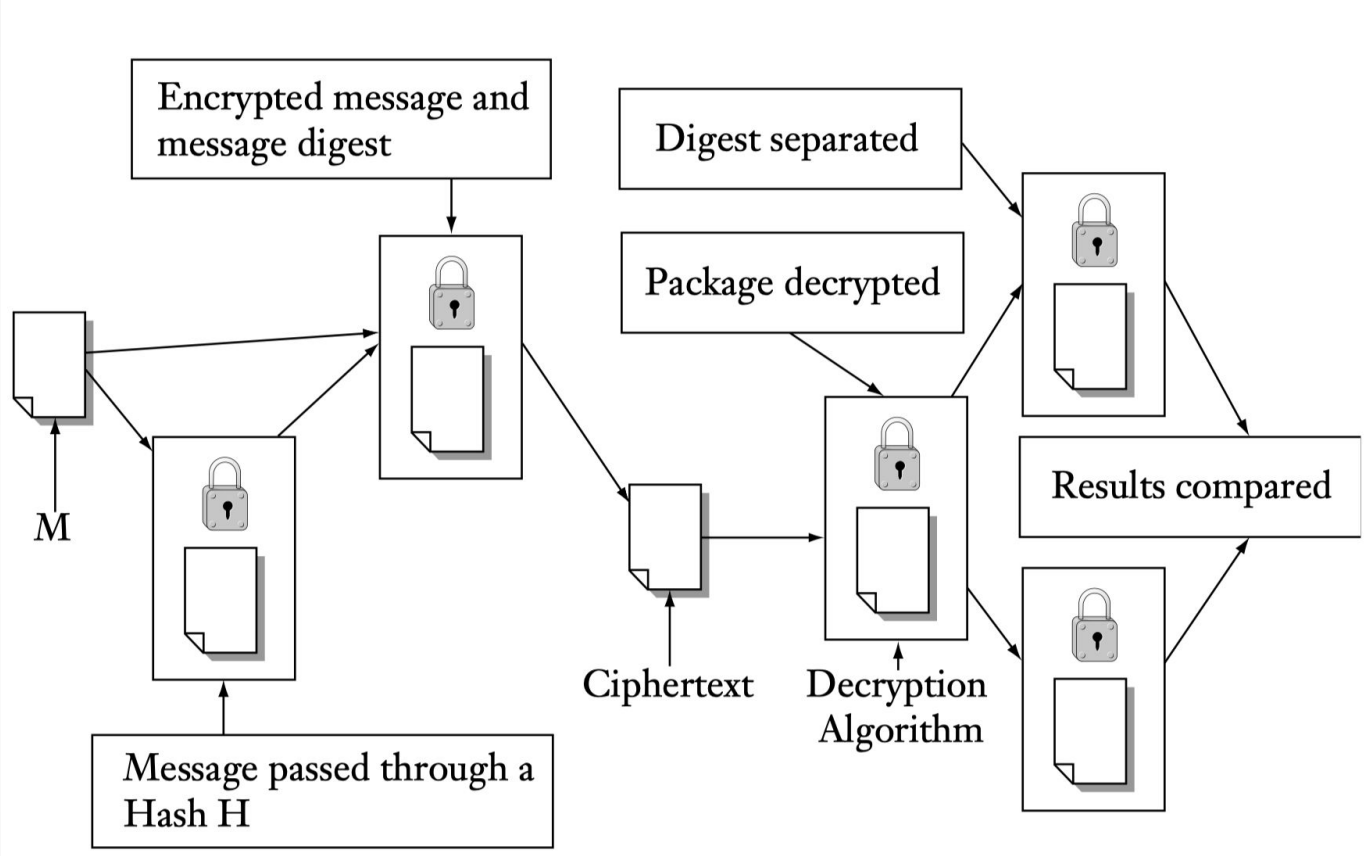


Cryptographic hash functions take input data and produce a fixed-size string of characters(in hexadecimal), known as a hash or digest.

Hashes are used to verify data integrity and authenticity. Even a small change in the input data results in a significantly different hash.

Authentification

Process whereby the system gathers and builds up information about the user to assure that the user is genuine.


Encrypted message and message digest
Digest separated
Package decrypted
Results compared
M
Ciphertext
Decryption Algorithm
Message passed through a Hash H

Authentification

Physical Authentication Methods:

- User name
- Password
- Retinal images
- Fingerprints
- Physical location
- Identity cards

Operational Security

- Operation security involves policies and guidelines that organizations including all employees must do to safeguard the assets of the organization including its workers.
- These policy guidelines are spelt out in a document called security policy.
- It also includes guidelines for security recovery and response in case of a security incident

What is Security in ethics and professionalism?

- Security in ethics and professionalism refers to the **practice of safeguarding sensitive information, upholding ethical principles, and maintaining the trust and integrity associated with a particular profession or field**.
- It is not a one-time action but an ongoing commitment.
- It requires continuous **training**, **awareness**, and **adaptation** to evolving threats and ethical dilemmas.

Key Aspects

- It encompasses several key aspects:
  - Confidentiality
  - Data Protection
  - Ethical Conduct
  - Compliance with Laws and Regulations
  - Trust and Reputation
  - Client and Stakeholder Interests
  - Preventing harm
  - Long-Term Success

Understanding Security Ethics

- Information Technology (IT) and Cybersecurity:
  - Security ethics in IT involves protecting digital assets, data privacy, and cybersecurity.
  - IT professionals are responsible for safeguarding sensitive information, and ethics guide their actions in areas such as responsible disclosure of vulnerabilities, respecting user privacy, and ensuring the security of systems and networks.
- Finance and Banking:
  - In the financial sector, ethical behavior and security measures are essential for maintaining the integrity of financial transactions and safeguarding customer assets.
  - Banking professionals must adhere to ethical standards when handling financial data and ensuring secure transactions.

Understanding Security Ethics

- Healthcare:
    - In healthcare, security ethics are essential for maintaining patient confidentiality and trust.
    - Healthcare professionals must handle medical records and sensitive patient information with the utmost care, following ethical standards to protect patient privacy and ensure the security of health data.
- Legal and Judiciary:
    - Security ethics are integral to the legal profession.
    - Attorneys are bound by ethical codes that require them to protect client confidentiality, ensure a fair legal process, and uphold the rule of law.
    - Ethical dilemmas in areas like attorney-client privilege are common.

Importance of Security at working place

- Trust and Reputation
- Protection of Sensitive Information
- Legal Compliance
- Ethical Responsibility
- Client and Customer Expectations

Importance of Security at working place

- Professionals across various fields have significant ethical responsibilities when it comes to handling sensitive information.
- These responsibilities are essential for maintaining trust, respecting privacy, and upholding the integrity of their respective professions
- Professionals must respect the principle of confidentiality.
- Professionals should obtain informed consent from individuals before collecting, using, or sharing their sensitive information.
- Professionals take measures to protect the privacy of sensitive information by securing physical records, using encryption for digital data, and implementing access controls.

How to ensure security in your profession?

- Confidentiality:Professionals must respect the principle of confidentiality.
- Informed Consent: Professionals should obtain informed consent from individuals before collecting, using, or sharing their sensitive information.
- Privacy Protection:Professionals take measures to protect the privacy of sensitive information by securing physical records, using encryption for digital data, and implementing access controls.
- Honesty and Transparency: Professionals should provide clear information about what data is being collected, why it's collected, and how it will be used.
- Ethical professionals must be aware of and comply with relevant laws and regulations pertaining to sensitive information.
- Accountability: Professionals are accountable for their actions regarding sensitive information.

Dilemma

Edward Snowden and the NSA Surveillance Leaks:

- In 2013, Edward Snowden, a former National Security Agency (NSA) contractor, leaked classified documents revealing extensive global surveillance programs. This case raises questions about the ethics of whistleblowing, government surveillance, and individual privacy.

Equifax Data Breach:

- In 2017, Equifax, one of the largest credit reporting agencies, suffered a massive data breach that exposed sensitive personal information of over 147 million people. This case illustrates the ethical responsibilities of organizations to secure customer data.

Dilemma

Cambridge Analytica and Facebook Data Scandal:

- In 2018, it was revealed that Cambridge Analytica, a political consulting firm, obtained and misused Facebook user data for political purposes. This case highlights ethical concerns related to data harvesting, consent, and the responsibility of tech companies.

Stuxnet Worm and Cyber Warfare:

- Stuxnet was a computer worm reportedly developed by nation-states to target Iran's nuclear facilities. This raises ethical questions about the use of cyberweapons, collateral damage, and the blurred lines between cyber warfare and traditional warfare.

Dilemma

Uber's Handling of a Data Breach:

- Uber faced criticism for concealing a data breach that exposed the personal information of 57 million users. The ethical dilemma here is whether Uber's decision to hide the breach was justified.

Ethical and Legal Framework for Information

The Need for Frameworks

- An ethical framework is essential for addressing moral issues in information management.
- A legal framework is necessary to establish rules and regulations that protect privacy and data security.
- Both frameworks complement each other in addressing the complex issues surrounding information ethics.

Ethical and Legal Framework for Information

Development of Frameworks

- The question of who will develop these frameworks arises.
- Collaboration between governments, technology experts, legal professionals, and ethicists is required.
- Multidisciplinary efforts can lead to comprehensive and balanced frameworks.

Ethical and Legal Framework for Information

Enforcement of Frameworks

- Ensuring adherence to these frameworks is crucial for their effectiveness.
- Law enforcement agencies, regulatory bodies, and international cooperation play vital roles in enforcement.
- Properly defined penalties for violations are necessary to deter unethical or illegal behavior.

Brief of the Next Lecture

Cybercrimes

- Define cyber-crimes
- Type of cyber-crimes

Reference

Joseph Migga Kizza, Ethical and Social issues in the information age,1997

Q & A

Thank You.