Information Security

P.Charan

Asst Professor, Dept of CSE

Acharya Nagarjuna University

Information security:

It is the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.

- Information security's primary focus is the balanced protection of the confidentiality, integrity and availability of data (also known as the CIA triad)

Threat

Information security threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Most people have experienced software attacks of some sort. Viruses, Worms, Phishing Attacks, and Trojan horses are a few common examples of software attacks

Confidentiality

In information security, confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes. While similar to "privacy," the two words aren't interchangeable. Rather, confidentiality is a component of privacy that implements to protect our data from unauthorized viewers. Examples of confidentiality of electronic data being compromised include laptop theft, password theft, or sensitive emails being sent to the incorrect individuals

Integrity

In information security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle. This means that data cannot be modified in an unauthorized or undetected manner

Availability

For any information system to serve its purpose, the information must be available when it is needed. This means the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial of service attacks, such as a flood of incoming messages to the target system, essentially forcing it to shut down

Non-repudiation

In law, non-repudiation implies one's intention to fulfill their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction, nor can the other party deny having sent a transaction.

Digital Signatures:

*"A **digital signature** is a mathematical scheme for verifying the authenticity of digital messages or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non repudiation), and that the message was not altered in transit (integrity)"*

Malware:

- Hostile, intrusive, or annoying software or program code (“malicious” +”software”)
- Includes computer viruses, worms, trojan horses, bots, spyware, adware, etc
- Software is considered malware based on the intent of the creator rather than any particular features

Internet bot:

- also known as **web robots**, are automated internet applications controlled by software agents
- These bots interact with network services intended for people, carrying out monotonous tasks and behaving in a humanlike manner (i.e., computer game bot)
- Bots can gather information, reply to queries, provide entertainment, and serve commercial purposes.
- Botnet - a network of "zombie" computers used to do automated tasks such as spamming or reversing spamming

Adware:

- **Advertising-supported software** is any software package which automatically plays, displays, or downloads advertising material to a computer after the software is installed on it or while the application is being used.
- Adware is software integrated into or bundled with a program, typically as a way to recover programming development costs through advertising income

Spyware:

- A broad category of software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user
- In simpler terms, spyware is a type of program that watches what users do with their computer and then sends that information over the internet

Spam:

- **Spamming** is the abuse of electronic messaging systems to send unsolicited, undesired bulk messages
- Spam media includes:
  - E-mail spam
  - Instant messaging spam
  - Web search engine spam
  - Spam in blogs
  - Mobile phone messaging spam

Phishing:

- A criminal activity using social engineering techniques.
- An attempt to acquire sensitive data, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication.
- Typically carried out using email or an instant message

Phishing Example

Keystroke Logging:

- Keystroke logging (often called keylogging) is a diagnostic used in software development that captures the user's keystrokes
- Widely available on the internet and can be used by anyone for the same purposes
- Can be achieved by both hardware and software means
- Writing software applications for keylogging is trivial, and like any computer program can be distributed as malware (virus, trojan, etc.)

Attacks

- Compromise systems in ways that affect services of information security
  - attack on confidentiality:
    - unauthorized disclosure of information
  - attack on integrity:
    - destruction or corruption of information
  - attack on availability:
    - disruption or denial of services

Prevention, detection, response

- proper planning reduces risk of attack and increases capabilities of detection and response if an attack does occur

Prevention

- Establishment of policy and access control
  - who: identification, authentication, authorization
  - what: granted on “need-to-know” basis
- Implementation of hardware, software, and services
  - users cannot override, unalterable (attackers cannot defeat security mechanisms by changing them)
  - examples of preventative mechanisms
    - passwords - prevent unauthorized system access
    - firewalls - prevent unauthorized network access
    - encryption - prevents breaches of confidentiality
    - physical security devices - prevent theft
- Maintenance

Detection

- Determine that either an attack is underway or has occurred and report it
- Real-time monitoring
  - or, as close as possible
  - monitor attacks to provide data about their nature, severity, and results
- Intrusion verification and notification
  - intrusion detection systems (IDS)
  - typical detection systems monitor various aspects of the system, looking for actions or information indicating an attack
    - example: denial of access to a system when user repeatedly enters incorrect password

Response

- Stop/contain an attack
  - must be timely!
    - incident response plan developed in advance
- Assess and repair any damage
- Resumption of correct operation
- Evidence collection and preservation
  - very important
    - identifies vulnerabilities
    - strengthens future security measures

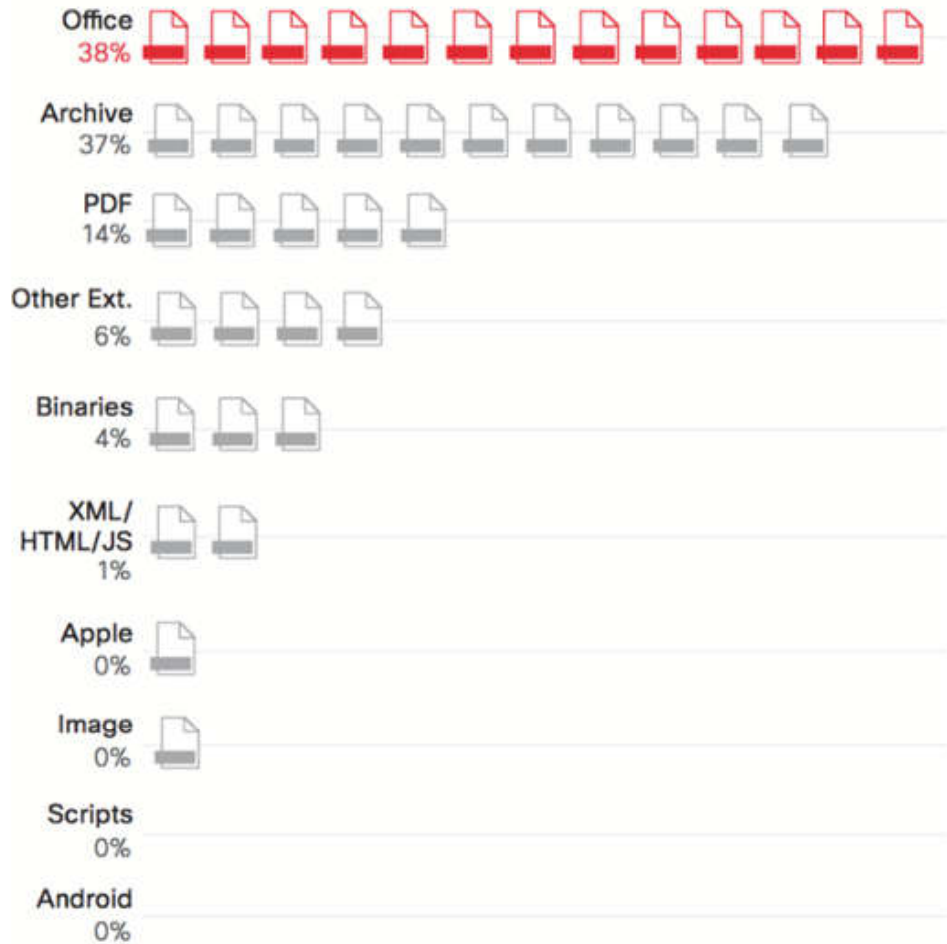
Importance of Information Security

- Over the last few years, the IT security threat landscape has changed significantly.
- Traditional malware threats hit an apparent wall in 2005
- However new threats (bots, spam, phishing) have stepped into the void.
- Unauthorized access (malware, spyware) limits our ability to protect the confidentiality of the data
- Malicious programs can alter the data values, destroying the integrity of the data
- Denial of Service (DoS) attacks can shut down a server and/or network, making the system unavailable.
- Efforts to correct costs corporations time and money!

Few snippets

- 76% of organizations say they experienced phishing attacks in 2017.
- By the end of 2017, the average user was receiving 16 malicious emails per month.
- 92.4% of malware is delivered via email.
- Fake invoices are the #1 disguise for distributing malware.

Figure 10 Top 10 malicious file extensions, January – September 2017



Source: Cisco Security Research

What Can We Do?

- Security Assessment
  - Identify areas of risk
  - Identify potential for security breaches, collapses
  - Identify steps to mitigate
- Security Application
  - Expert knowledge (train, hire, other)
  - Multi-layered Approach (there is no single solution)
  - Policies and Procedures

- Security Awareness
  - Not just for the geeks!
  - Security Training at all levels (external and/or internal)
  - Continuing education and awareness – not a one-time shot!
  - Make it part of the culture

Questions?