16- Explaining Data Privacy and Protection Concepts

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Outlines

16.1- Explain Privacy and Data Sensitivity Concepts

16.2- Explain Privacy and Data Protection Controls

16.1- Explain Privacy and Data Sensitivity Concepts

16.2- Explain Privacy and Data Protection Controls

PRIVACY AND SENSITIVE DATA CONCEPTS

- The value of information assets can be thought of in terms of how a compromise of the data's security attributes of the confidentiality, integrity, and availability (CIA) triad would impact the organization.
- When surveying information within an organization, it is important not to solely judge how secretly it might need to be kept, but how the data is used within workflows.
- Data must be kept securely within a processing and storage system that enforces CIA attributes.
- In practice, this will mean a file or database management system that provides read or read/write access to authorized and authenticated accounts or denies access otherwise (by being encrypted, for instance).

PRIVACY VS. SECURITY

- While data security is important, privacy is an equally vital factor.
- Privacy is a data governance requirement that arises when collecting and processing personal data.
- Personal data is any information about an identifiable individual person, referred to as the **data subject**.
- Where data security controls focus on the CIA attributes of the processing system, privacy requires policies to identify private data, ensure that storage, processing, and retention is compliant with relevant regulations, limit access to the private data to authorized persons only, and ensure the rights of data subjects to review and remove any information held about them are met.

DATA ROLES AND RESPONSIBILITIES

- A data governance policy describes the security controls that will be applied to protect data at each stage of its life cycle.
- There are important institutional governance roles for oversight and management of information assets within the life cycle:
  - ✓ Data owner—a senior (executive) role with ultimate responsibility for maintaining the confidentiality, integrity, and availability of the information asset.
  - ✓ Data steward—this role is primarily responsible for data quality, This involves tasks such as ensuring data is labeled and identified with appropriate metadata and that data is collected and stored in a format and with values that comply with applicable laws and regulations.
  - ✓ Data custodian—this role handles managing the system on which the data assets are stored. This includes responsibility for enforcing access control, encryption, and backup/recovery measures.
  - ✓ Data Privacy Officer (DPO)—this role is responsible for oversight of any personally identifiable information (PII) assets managed by the company.

DATA CLASSIFICATIONS

- A data classification schema is a decision tree for applying one or more tags or labels to each data asset.
- Many data classification schemas are **based on the degree of confidentiality required**:
  - ✓ Public (unclassified)—there are no restrictions on viewing the data, Public information presents no risk to an organization if it is disclosed but does present a risk if it is modified or not available.
  - ✓ Confidential (secret)—the information is highly sensitive, for viewing only by approved persons within the owner organization, and possibly by trusted third parties under NDA.
  - ✓ Critical (top secret)—the information is too valuable to allow any risk of its capture, Viewing is severely restricted.

DATA CLASSIFICATIONS (cont.)

- Another type of classification schema **identifies the kind of information asset**:
  - ✓ Proprietary—proprietary information is information created and owned by the company, typically about the products or services that they make or perform.
  - ✓ Private/personal data—information that relates to an individual identity.
  - ✓ Sensitive—this label is usually used in the context of personal data, Privacy-sensitive information about a person could harm them if made public.

DATA TYPES

- Personally Identifiable Information (PII)
  - ✓ **Personally identifiable information (PII)** is data that can be used to identify, contact, or locate an individual.
  - ✓ A **Social Security Number (SSN)** is a good example of PII.
  - ✓ Others include name, date of birth, email address, telephone number, street address, biometric data, and so on.
  - ✓ Some bits of information, such as a SSN, may be unique; others uniquely identify an individual in combination (for example, full name with birth date and street address).
  - ✓ Some types of information may be PII depending on the context.
  - ✓ **For example**, when someone browses the web using a static IP address, the IP address is PII.
  - ✓ An address that is dynamically assigned by the ISP may not be considered PII.
  - ✓ PII is often used for password reset mechanisms and to confirm identity over the telephone.

DATA TYPES (cont.)

- Health Information
  - ✓ **Personal health information (PHI)—**or protected health information—refers to medical and insurance records, plus associated hospital and laboratory test results.
  - ✓ PHI may be associated with a specific person or used as an anonymized or deidentified data set for analysis and research.
  - ✓ An anonymized data set is one where the identifying data is removed completely.
  - ✓ PHI trades at high values on the black market, making it an attractive target.
  - ✓ Criminals seek to exploit the data for insurance fraud or possibly to blackmail victims.
  - ✓ PHI data is extremely sensitive and its loss has a permanent effect.
  - ✓ Unlike a credit card number or bank account number, it cannot be changed.
  - ✓ Consequently, the reputational damage that would be caused by a PHI data breach is huge.

DATA TYPES (cont.)

- Financial Information
  - ✓ Financial information refers to data held about bank and investment accounts, plus information such as payroll and tax returns.
  - ✓ Payment card information comprises the card number, expiry date, and the three-digit card verification value (CVV).
  - ✓ Cards are also associated with a PIN, but this should never be transmitted to or handled by the merchant.
  - ✓ Abuse of the card may also require the holder's name and the address the card is registered to.
  - ✓ The Payment Card Industry Data Security Standard (PCI DSS) defines the safe handling and storage of this information (pcisecuritystandards.org/pci_security).

DATA TYPES (cont.)

- Government Data
  - ✓ Internally, government agencies have complex data collection and processing requirements.
  - ✓ In the US, federal laws place certain requirements on institutions that collect and process data about citizens and taxpayers.
  - ✓ This data may be shared with companies for analysis under strict agreements to preserve security and privacy.

PRIVACY BREACHES AND DATA BREACHES

- A data breach occurs when information is read, modified, or deleted without authorization.
- "Read" in this sense can mean either seen by a person or transferred to a network or storage media.
- A data breach is the loss of any type of data (but notably corporate information and intellectual property), while a privacy breach refers specifically to loss or disclosure of personal and sensitive data.

16.1- Explain Privacy and Data Sensitivity Concepts

16.2- Explain Privacy and Data Protection Controls

DATA PROTECTION

- Data can be described as in one of **three** states:

1. Data at rest

- ✓ This state means that the data is in some sort of persistent storage media.
- ✓ **Examples** of types of data that may be at rest include financial information stored in databases, archived audiovisual media, operational policies and other management documents, system configuration data, and more.
- ✓ In this state, it is usually possible to **encrypt** the data, using techniques such as whole disk encryption, database encryption, and file- or folder-level encryption.
- ✓ It is also possible to apply permissions—**access control lists (ACLs)**—to ensure only authorized users can read or modify the data.

DATA PROTECTION (cont.)

2. Data in transit (or data in motion)
   - ✓ This is the state when data is transmitted over a network.
   - ✓ **Examples** of types of data that may be in transit include website traffic, remote access traffic, data being synchronized between cloud repositories, and more.
   - ✓ In this state, data can be protected by a transport encryption protocol, such as **TLS** or **IPSec**.
3. Data in use (or data in processing)
   - ✓ This is the state when data is present in volatile memory, such as system RAM or CPU registers and cache.
   - ✓ **Examples** of types of data that may be in use include documents open in a word processing application, database data that is currently being modified, event logs being generated while an operating system is running, and more.
   - ✓ When a user works with data, that data usually needs to be decrypted as it goes from in rest to in use, **trusted execution environment (TEE)** mechanisms, such as Intel Software Guard Extensions are able to encrypt data as it exists in memory.

DATA EXFILTRATION

- Data exfiltration attacks are one of the primary means for attackers to retrieve valuable data, such as personally identifiable information (PII) or payment information, often destined for later sale on the black market.
- Data exfiltration can take place via a wide variety of mechanisms, including:
  - ✓ Copying the data to removable media or other device with storage, such as USB drive, the memory card in a digital camera, or a smartphone.
  - ✓ Using a network protocol, such as HTTP, FTP, SSH, email, or Instant Messaging (IM)/chat.
  - ✓ By communicating it orally over a telephone, cell phone, or Voice over IP (VoIP) network. Cell phone text messaging is another possibility.
  - ✓ Using a picture or video of the data—if text information is converted to an image format it is very difficult for a computer-based detection system to identify the original information from the image data.

DATA EXFILTRATION (cont.)

- While some of these mechanisms are simple to mitigate through the use of security tools, others may be much less easily defeated.
- You can protect data using mechanisms and security controls that you have examined previously:
  - ✓ Ensure that all sensitive data is encrypted at rest, If the data is transferred outside the network, it will be mostly useless to the attacker without the decryption key.
  - ✓ Create and maintain offsite backups of data that may be targeted for destruction or ransom.
  - ✓ Restrict the types of network channels that attackers can use to transfer data from the network to the outside, Disconnect systems storing archived data from the network.
  - ✓ Train users about document confidentiality and the use of encryption to store and transmit data securely.

DATA LOSS PREVENTION

- Data loss prevention (DLP) products automate the discovery and classification of data types and enforce rules so that data is not viewed or transferred without a proper authorization.
- Such solutions will usually consist of the following components:
  - ✓ Policy server—to configure classification, confidentiality, and privacy rules and policies, log incidents, and compile reports.
  - ✓ Endpoint agents—to enforce policy on client computers, even when they are not connected to the network.
  - ✓ Network agents—to scan communications at network borders and interface with web and messaging servers to enforce policy.