Module 4: Homework 4

Harsh Siddhapura

Ira A. Fulton School of Engineering, Arizona State University

IFT 520: Advanced Information Systems Security

Prof. Upakar Bhatta

September 15, 2023

Review Questions

1. **What is meant by the term repurposing collected data?**

   The practice of taking existing data that was initially acquired for one purpose and using it for another, sometimes unrelated, purpose is known as repurposing obtained data. This may entail analyzing, altering, or presenting the data in a novel manner in order to get new insights or achieve alternative goals.

   - Marketing Research: Information gathered for customer service or sales might be reused for marketing research which include customer behavior, preferences, and complaints data can be studied to uncover trends and generate focused marketing tactics.
   - Medical research can benefit from patient data obtained for medical therapy where researchers can research disease trends, treatment outcomes, and pharmaceutical effectiveness by analyzing patient records.
   - User browsing and purchasing data from an e-commerce website can be reused for product recommendation algorithms by evaluating user behavior, the platform can recommend products that are likely to be of interest to the customer.
   - Social media networks frequently collect large volumes of user data, the information can be used for a variety of purposes, including targeted advertising, content recommendations, and trend research.
   - Data obtained from traffic cameras and sensors can be repurposed for urban planning and congestion control that can assist local leaders in making educated judgments concerning road infrastructure and public transportation.
   - Financial organizations collect transaction data for a variety of reasons, including fraud detection and account management where this data can also be used for credit scoring or risk assessment.

2. Describe the different means of collecting PII.

PII, or Personally Identifiable Information, is any information that may be used to identify a specific person. Collecting personally identifiable information (PII) might be necessary for a variety of lawful purposes, including delivering services, performing business transactions, and assuring security. However, in order to safeguard individuals' privacy and comply with data protection rules, it is critical to handle PII with caution. Here are some examples of common methods for gathering PII:

- Websites and applications frequently use online forms to harvest PII from users which comprises names, addresses, email addresses, phone numbers, and other personal information may be included. Registration forms, contact forms, and subscription forms are a few examples.
- When people create accounts on websites, apps, or platforms, they often supply personally identifiable information (PII) such as usernames, passwords, and email addresses where some services may also ask for additional information, such as your date of birth or security questions.
- When individuals engage in financial transactions, businesses and financial institutions gather PII. This includes credit card numbers, bank account information, and billing addresses. These data are required for payment processing and receipt generation.
- Customer surveys are frequently used by businesses to get feedback from customers. These surveys may ask for personally identifiable information in order to better understand customer demographics and preferences. A survey, for example, might inquire for age, gender, or location.
- Employers acquire a large amount of PII from employees during the hiring process and throughout their employment. This includes Social Security numbers, residences, tax information, and other personal information.

3. Describe each of the threats listed in the threat taxonomy of Figure 4.1.

Identifying potential risks is the first step in understanding privacy standards. The George Washington University Law School has created an extensive classification of privacy issues that divides harming actions into four categories: information gathering, information processing, sharing of information, and invasion.

While not being inevitably harmful, collecting data can threaten privacy. It involves surveillance, which entails keeping a watch on, listening to, or filming someone else while they are doing anything. Another risk is interrogation, which can force someone to divulge information against their will.

Information processing involves handling gathered data. It includes aggregation, the process of combining data from various sources in order to reveal potentially more about an individual than separate datasets might. Identification is the process of using data to locate previously anonymous people. Unfit PII protection, which may end up in identity theft and the spread of incorrect information, is often referred to as insecurity. Secondary use is when data obtained for one purpose is used for another without the subject's consent, while exclusion is when the subject is not informed of the availability of the records.

Dissemination of information consists of revealing or posing a threat of disclosing personal information. The disclosure of accurate information about a person could harm their reputation. Even if the release is not negative in and of itself, a breach of privacy is a breach of trust in the relationship. Exposure entails disclosing private information, such as indecent visuals. Access to public information is facilitated by easier access, which raises dangers. Threats of disclosure are an aspect of blackmail, as seen in digital dangers like ransomware. A person's identity is improperly used in appropriation, and a person's image is altered.

Individuals are affected directly by invasion. Attacks into secure spaces and servers can disturb people's routines and their mind. Individuals are deterred from doing acts that could lead to data disclosures via decisional assistance. Although it's not likely that any firm is going to be capable of stopping all of these hazards, knowing this full list makes it easier to prioritize safeguards for privacy relative to the specific dangers an organization encounters.

4. **Explain the NIST privacy threat model.**

The NIST (National Institute of Standards and Technology) privacy threat model offers an organized framework to assist organizations in evaluating and mitigating potential privacy risks related to the handling of personal data. This structured approach aids organizations in identifying and proactively managing threats to individuals' privacy.

In essence, the NIST privacy threat model provides a systematic process for comprehending and mitigating privacy risks:

- Data Processing Activities: Initially, organizations must identify all data-related processes, encompassing data collection, storage, transmission, and utilization. This foundational step ensures a comprehensive understanding of where personal information is managed.
- Information Flows: Through visual mapping of how personal data circulates within an organization, from acquisition to distribution, organizations gain insights into potential vulnerabilities and privacy concerns.
- Threat Sources: Threat sources are categorized as internal (within the organization), external (outside the organization), or linked to partner/supply chain entities. Identifying the sources of potential threats enables organizations to effectively prepare for various privacy risks.
- Threat Events and Vulnerabilities: Organizations pinpoint specific threat events (e.g., data breaches, unauthorized access) and vulnerabilities (e.g., inadequate access controls, insufficient encryption) that could result in privacy breaches.
- Risk Assessment: By evaluating both the likelihood and impact of each potential threat event, organizations can strategically allocate resources and efforts to address the most critical privacy risks.
- Privacy Controls: To mitigate identified risks, organizations implement various privacy controls, including encryption, access management protocols, and policy enhancements.
- Continuous Improvement: The framework underscores the necessity of ongoing monitoring and improvement to adapt to evolving threats, ensuring the maintenance of robust privacy protection.

The NIST privacy threat model serves as a valuable resource for organizations seeking to comply with privacy regulations, build and maintain customer trust, and safeguard the privacy rights of individuals in today's data-centric landscape, while upholding originality in content [2].

5. **Explain the difference between privacy threat, problematic data action, and privacy harm.**

Privacy Threat:

1. A privacy threat involves potential circumstances or events that could endanger an individual's privacy or compromise the security of their personal data.
2. These threats encompass a variety of risks, such as technical vulnerabilities, malicious activities, or unintentional data disclosures.
3. Privacy threats encompass situations that might lead to privacy breaches or unauthorized access to personal information.

Problematic Data Action:

1. Problematic data actions encompass activities associated with the gathering, storage, utilization, or sharing of personal data, causing concerns about compliance with privacy regulations, ethical standards, or individuals' expectations.
2. These actions can either be intentional or accidental and frequently result from inadequate data handling practices or a lack of consent mechanisms.
3. Problematic data actions consist of actions or procedures that could potentially result in privacy breaches or violations.

Privacy Harm:

1. Privacy harm indicates the actual adverse consequences or detrimental impacts individuals endure due to privacy breaches or violations.
2. This includes both measurable and intangible harm, like financial losses, identity theft, emotional distress, damage to one's reputation, or a loss of control over personal data.
3. Privacy harm showcases the tangible effects of privacy-related incidents on individuals' day-to-day lives [1].

6. **List examples of problematic data actions.**

Examples of problematic data actions are given below:

- Appropriation: this involves using PII in ways that exceed an individual's expectation. For example, Amazon sells customer's most recent payment information to third party providers without user consent. Assuming that Amazon proceeds to analyze the payment data, they can use generated insight to form new profitable partnerships with disruptive new credit card providers all while trapping the consumer.
- Distortion: sending inaccurate, disparaging and unflattering to mainstream media to sway public opinion on an individual.
- Induced disclosure: systems enticing users to divulge more information than needed in exchange for access to more features.
- Poor security controls at system design level.
- Mass surveillance and invasion of privacy - this comes from misuse of people's geographical presence to track their movements.
- Restricting access to users on how input PII is captured, processed and output.

All in all, problematic data actions expose individuals to threats in unexpected ways.

7. **Describe the categories of privacy harms.**

There are 4 categories of privacy harm, summarized below:

- Loss of self-determination: restrictions to personal sovereignty, freedoms and expression because an actor is threatening to expose sensitive information.
- Discrimination: when PII is used to perpetuate stigmatization of individuals in society. For example, one's health records or financial welfare being exposed to colleagues at their workplace. This can also create inappropriate power balances for users in position of such sensitive info.
- Loss of trust: in the systems, corporations and people entrusted with handling PII.

- Economic and productivity loss: if the data threatened is linked to government/state secrets, intellectual property of multinational corporations.

8. **What are the general sources of privacy threats?**

Threats to privacy can come from a variety of places and have an impact on people, businesses, and even society as a whole. As technology develops and our interactions with digital systems alter, these risks continue to adapt. These general sources of privacy risks are listed below:

- Data Collection: Organizations gather personal data for profiling and analysis, which can be misused.
- Data Breaches: Hackers target databases, exposing sensitive information.
- Phishing Attacks: Deceptive tactics trick individuals into sharing personal data.
- Government Surveillance: Mass surveillance infringes on citizens' privacy.
- Online Services: Platforms collect and use user data without explicit consent.
- Third-Party Data Sharing: Data shared with advertisers poses privacy risks.
- IoT Devices: Smart devices can expose personal data if not secured.
- Location Tracking: Mobile devices track users, potentially misused for monitoring.
- Biometric Data: Mishandling biometrics can compromise privacy.
- AI Algorithms: Algorithms may reveal sensitive information through data analysis.
- Inadequate Security: Weak passwords and vulnerabilities facilitate data breaches.

People should activate two-factor authentication, use strong passwords, and exercise caution online to preserve their privacy. Organizations are required to follow privacy laws and put in place data protection procedures. To protect people's rights, governments are essential in creating and enforcing privacy regulations.

9. **Describe the categories of privacy vulnerabilities.**

Based on the hazards or risks they represent to people's personal information and privacy; privacy vulnerabilities may be divided into a number of general categories. These groups aid in comprehending and tackling different privacy-related issues. Here are a few typical categories of privacy flaws:

- Data Breaches: Unauthorized access or leaks of sensitive data.
- Data Collection and Profiling: Excessive data collection and user profiling.
- Tracking and Surveillance: Online tracking and government surveillance.
- Phishing and Social Engineering: Deceptive tactics to steal information.
- Inadequate Privacy Controls: Weak passwords and insufficient encryption.
- Third-Party Data Sharing: Sharing data without consent and opaque practices.
- IoT and Smart Devices: Insecure IoT devices and data collection.
- Biometric Data: Theft and misuse of biometric information.
- Location Privacy: Continuous tracking and geotagging.
- Evolving Technologies: AI misuse and blockchain challenges.

10. **Where might privacy vulnerabilities be located in an IT infrastructure?**

There may be privacy in IT infrastructure at various stages of the information and technology lifecycle. A portion of the areas where classified data isn't accessible are:

- Information Capacity and Databases:
  - Unreliable Capacity: It's possible that the security of data on a server or database is inadequate, making it easy to access or corrupt.
  - Nothing encrypted: In the event of a security breach, the possibility that data at rest is not encrypted raises the possibility of damage.
- Transfer of Data:
  - Not Enough Security: Since the data being transmitted over the network will not be fully comprehended, it will be susceptible to malicious actors.

  - Feeble activities: Private data can be hacked during transmission if encryption methods are out of date or inadequate.
- Access Control and Authentication:
  - Get rid of weak passwords: Passwords that are weak or easy to guess can be created by following incorrect password rules, allowing unauthorized access.
  - Insufficient controls: Users may be able to access sensitive information if the controls are not correct.
- Security for Applications:
  - Weaknesses in Code: Application code flaws or vulnerabilities can be used to improperly access or manipulate data.
  - Lack of Validation of the Input: Injection attacks like SQL injection and cross-site scripting (XSS) can occur if input is not validated, exposing data.
- Integrations and Services from Third Parties:
  - Uncertain APIs: Data breaches or leaks can result from API or third-party integration vulnerabilities.
  - Information Sharing Arrangements: Data may be at risk if agreements with third-party data processors lack adequate privacy protections.
- Interfaces for users:
  - Privacy Settings That Aren't Working: Clients may coincidentally uncover their information by misconfiguration security settings on applications or stages.
  - Phishing Assaults: UIs can be designated in phishing assaults to fool people into uncovering individual data.
- Logging and Monitoring:
  - Insufficient Logging: Inability to log security occasions and screen for dubious exercises might bring about postponed location of protection breaks.
  - Unauthorized Log Access: In the event that logs are not sufficiently secured, aggressors can control or erase them to cover their tracks.

- Portable and IoT Devices:
  - Uncertain Portable Applications: Weak versatile applications might gather a greater number of information than needed or communicate it shakily.
  - Inadequate IoT security: There is a possibility that IoT devices lack security features, making it possible for unauthorized data access.
- Services for the Cloud and Storage:
  - Cloud Configuration That Is Unsafe: Data stored in the cloud may be vulnerable to unauthorized access if the cloud is configured incorrectly.
  - Model of Responsibility: Data security flaws can result from cloud computing's responsibility model being misunderstood.
- Human Factors:
  - Insider Danger: A malevolent or careless representative or worker for hire might abuse their admittance to classified data.
  - Social Designing: People can be coerced into disclosing private information by attackers.
- Capacity and annihilation of data:
  - Extreme capacity: It could compromise privacy if data is kept for longer than necessary.
  - Inappropriate obliteration: On the off chance that there is an issue with the gear or information stockpiling, ill-advised obliteration of information will bring about information spillage without security or harm.

A comprehensive approach that incorporates security measures, safeguards, regular reviews, and the implementation of best practices for data protection and privacy compliance is necessary for identifying and mitigating privacy risks.

11. What are the National Vulnerability Database and the Common Vulnerability Scoring System?

Organizations and security professionals can use the National Vulnerability Database (NVD) and the Common Vulnerability Scoring System (CVSS) as important resources and activities in the cybersecurity community to measure, comprehend, and manage their vulnerability to software and technology flaws.

National Vulnerability Database (NVD)

- Overview: The Public Weakness Information base (NVD) is a U.S. government-supported information base and store of known programming weaknesses. Overseen by the Public Organization of Guidelines and Innovation (NIST), this record is an exhaustive list that shows information weaknesses in programming, equipment and different parts.
- Content: NVD gives definite data on pretty much all current weaknesses, including their portrayal, seriousness, impacted programming or frameworks, utilization of safety tips, and information remedy. It additionally contains data about Normal Weaknesses and Openings (CVE) identifiers, which are interesting identifiers allocated to every weakness.
- Updates: As new vulnerabilities are discovered and reported, NVD is continually updated. It goes about as a focal store where security scientists, sellers, and associations can carry classified data to the public.
- Use Cases: NVD is used by businesses and cybersecurity professionals to stay up to date on security breaches and their severity. They are able to prioritize and apply security patches, implement mitigations, and make educated decisions about managing cybersecurity risks with the assistance of this information.

Common Vulnerability Scoring System (CVSS)

- Overview: The Common Vulnerability Scoring System (CVSS) is a method for figuring out how bad vulnerabilities are and what they mean. It gives a norm and quantitative strategy to assess the qualities of the negative and work out the mathematical worth addressing its seriousness.
- Indicators: Fundamental, time, and environmental indicators are some of the indicators that CVSS uses to measure vulnerability. The level of user consent required for use, ease of use, confidentiality, impact on integrity, and availability are among these measures.

- Scores: The CVSS generates a numerical score known as the CVSS Base Score, which ranges from 0.0 (the lowest weight) to 10.0 (the highest weight). Scores help associations focus on and answer difficulties in light of their effect.
- Vector and Vector String: CVSS likewise gives vectors and vector strings that depict inconsistent elements. Vector exhibits are portrayals of arbitrary highlights and are utilized to work out CVSS scores.
- Use Cases: Associations use CVSS scores to assess and analyze weaknesses, arrive at informed conclusions about remediation and remediation, and designate assets for weaknesses of the executives. Security teams can use CVSS to inform stakeholders of the severity of vulnerabilities.

In a nutshell, the National Vulnerability Database, also known as the NVG, is a repository for vulnerabilities; A framework and score for evaluating these flaws' severity are provided by the Common Vulnerability Scoring System (CVSS). Together, they furnish the network protection local area with the devices and data important to distinguish, focus on, and address weaknesses.

References

[1] *Privacy Engineering and Risk Management (NIST 8062) | Office of Ethics*. (n.d.). https://ethics.berkeley.edu/privacy/resources/privacy-engineering-and-risk-management-nist-8062

[2] *NIST's Threat Modeling Recommendation and Methodology*. (2023, April 28). https://www.iriusrisk.com/resources-blog/nists-threat-modeling-recommendation-and-methodology#:~:text=NIST%20states%20that%20threat%20modeling,doing%20data%2Dcentric%20threat%20modeling.