Module 7: Homework 7

Harsh Manishbhai Siddhapura

Vaibhavi Nitin Honagekar

Arunava Lahiri

Thembelihle Shongwe

Sai Shashank Nagavaram

Anandha Krishnan Senthooraan

Group: Class96958 4

Ira A. Fulton School of Engineering, Arizona State University

IFT 520: Advanced Information Systems Security

Prof. Upakar Bhatta

September 25, 2023

Review Questions

1. **What are the main elements of the online ecosystem for personal data?**

   The main elements of the online ecosystem for personal data are:

   - **Data Collectors:** These entities, often websites or apps, collect and process user data. They can be categorized as first-party data collectors (those that collect data directly from users) and third-party data collectors (those that obtain data from other sources, such as advertising networks or data brokers).
   - **Data Brokers:** Entities that collect, aggregate, and sell user data to third parties for various purposes, such as marketing and analytics.
   - **Data Users:** Individuals who use online services and websites. Users generate personal data through their interactions, such as browsing, searching, social media activity, and online transactions.

   These elements collectively form the intricate online ecosystem for personal data, where the balance between data-driven services, user privacy, and regulatory compliance is continuously evolving and subject to scrutiny.

2. **What security features are built into HTTPS?**

   HTTPS (Hypertext Transfer Protocol Secure) is a secure communication protocol used to protect the integrity and confidentiality of data exchanged between a user's web browser and a website's server. It incorporates several key security features to achieve these goals:

   - **Encryption:** Encryption is one of the primary security features of HTTPS. It ensures that data transmitted between the user's browser and the server is encrypted, making it extremely difficult for unauthorized parties to intercept and decipher the information. HTTPS uses cryptographic algorithms to encode the data, rendering it unreadable without the appropriate decryption key.
   - **Data Integrity:** HTTPS employs mechanisms to maintain the integrity of data during transmission. This means that the data cannot be tampered with or altered by malicious actors

while it's in transit. To achieve data integrity, HTTPS uses cryptographic hash functions to generate unique checksums (hashes) of the data. These checksums are sent alongside the data, allowing the recipient to verify that the data has not been modified during transmission.

- **Authentication:** HTTPS ensures that users are communicating with the legitimate website or server they intend to visit. It uses digital certificates issued by trusted Certificate Authorities (CAs) to verify the authenticity of the server. When a user connects to an HTTPS-enabled website, the server presents its digital certificate, which contains information about the server's identity and its public key. The user's browser checks the certificate's validity by verifying it against a list of trusted CAs. If the certificate is valid and matches the website's domain, the user can be reasonably assured of the website's authenticity.

In summary, HTTPS combines encryption, data integrity checks, and authentication mechanisms to create a secure and trustworthy connection between users and websites. These features collectively protect sensitive data from eavesdropping, tampering, and unauthorized access, enhancing the security of online communications and transactions.

3. **How does a web application firewall function?**

A web application firewall (WAF) plays a critical role in safeguarding web applications and websites from a wide range of online threats, including web-based attacks and vulnerabilities. Here's an extended explanation of how a web application firewall functions:

- **Traffic Inspection:** A WAF acts as a gatekeeper, intercepting and inspecting all incoming and outgoing HTTP/HTTPS traffic between users and web applications. This traffic inspection occurs in real-time as data packets are transmitted.
- **Rule-Based Analysis:** At the core of a WAF's functionality is a set of rules or policies designed to identify and mitigate potential threats. These rules are often based on known attack patterns, signatures, and heuristics. As traffic passes through the WAF, it compares the data against these rules to detect malicious patterns or suspicious activities.
- **Protection Against Common Attacks:**

  - **SQL Injection:** WAFs can detect attempts to inject malicious SQL code into web application forms or query strings and block such attempts.
  - **Cross-Site Scripting (XSS):** WAFs identify and block scripting attacks that attempt to inject malicious code into web pages viewed by other users.
  - **Cross-Site Request Forgery (CSRF):** WAFs can help prevent CSRF attacks by verifying that incoming requests have the proper token.
- **Protection from Zero-Day Attacks:** WAFs can provide a degree of protection against zero-day vulnerabilities. While they may not have specific rules for unknown attacks, they can often detect anomalies and unusual behavior that could indicate an attack in progress.
- **Rate Limiting:** WAFs can implement rate-limiting rules to prevent abuse, such as limiting the number of requests from a single IP address within a certain time frame. This helps protect against brute force attacks and DDoS attempts.
- **Session Management:** Some WAFs assist in managing user sessions and ensuring that sessions are properly authenticated and authorized, reducing the risk of session hijacking.
- **Logging and Monitoring:** WAFs maintain detailed logs of web traffic, rule violations, and security incidents. This information is invaluable for security teams in analyzing and responding to threats.
- **Virtual Patching:** WAFs can provide virtual patches for known vulnerabilities in web applications. This is particularly helpful when applying actual patches to a web application might take time, allowing organizations to reduce the window of exposure.
- **Positive Security Model:** In addition to negative security (blocking known attacks), some WAFs use a positive security model, which defines the allowed behavior of a web application. Any requests that do not conform to this model are blocked, helping protect against unknown threats.
- **Learning Mode:** Many modern WAFs have learning modes where they observe traffic and generate rules dynamically based on legitimate traffic patterns. This adaptive approach helps reduce false positives and ensures effective protection.

- **Deployment Options:** WAFs can be deployed as hardware appliances, software running on servers, or cloud-based services. Cloud-based WAFs offer scalability and easy deployment without the need for physical infrastructure.
- **Continuous Updates:** WAF rule sets are regularly updated to protect against new threats and attack techniques. Keeping the WAF up-to-date is essential for effective security.

In summary, a web application firewall serves as a crucial security layer that continuously monitors web traffic, applies predefined rules, and employs various techniques to identify and mitigate threats. By doing so, it helps organizations protect their web applications and sensitive data from a wide range of security risks, ensuring a safer online experience for users and minimizing the risk of data breaches and cyberattacks.

4. What are the main elements of the mobile app ecosystem?

- Mobile apps are designed to work with specific operating systems that are iOS and Android that are the two main mobile operating systems where the app developers create separate versions of their apps for each platform.
- Individuals or companies that are responsible for designing the user interface, functionality and overall user experience of the user mobile applications are known as app developers.
- App stores are platforms where users can discover, download and update mobile applications where Apple App Store (for iOS) and Google Play (for Android) are two popular app stores.
- Mobile app end users who download and use it for various purposes where success comes from user behavior and preferences.
- App User Devices: Specific hardware and software settings of users devices, such as screen size, resolution, and OS version, that app developers should consider when designing their apps
- Mobile applications typically request access to device functions such as camera, microphone, location, and contacts where users can grant or deny certain rights, which have implications for application functionality and privacy.

- The methods that generate revenue for mobile apps such as in-app advertising, in-app purchases, subscription models, or pre-purchased prices.

5. List major security concerns for mobile devices.

- Unauthorized access to personal data such as contacts, messages, photos and location information can lead to identity theft and privacy violations
- Malicious programs (malware) and viruses can infect mobile devices to steal data, monitor activities, or harm the device.
- Phishing attacks delivered through email, SMS, or malicious programs can trick users into revealing sensitive information or login credentials.
- Malicious or poorly written apps can reveal vulnerabilities that attackers can exploit to compromise device security or user data.
- Connecting to insecure or public Wi-Fi networks leaves mobile devices vulnerable to theft, holes and middleware attacks.
- If a mobile device is lost or stolen, unauthorized data can be accessed if the device is not secured properly.
- Failure to maintain an updated version of the operating system and apps on the device can result in vulnerabilities being unpatched and vulnerable to exploitation.
- Changing device settings to comply with restrictions imposed by the manufacturer (jailbreaking for iOS and rooting for Android) can introduce additional security threats
- While it may be convenient to store data in the cloud, it can also pose security risks, such as unauthorized cloud accounts, if not properly configured
- Attackers can use fraudulent SMS messages or phone calls to trick users into revealing sensitive information or engaging in actions which they do not want.

6. **What is mobile app vetting?**

Mobile applications undergo scrutiny and examination in the course of the mobile app vetting process to make sure they comply with a set of guidelines, security requirements, and customer requirements. This thorough assessment involves assessing an app's performance, usability, achievement, and security, among other aspects. Mobile app vetting's main objective is to find ways to minimize dangers that might result from downloading and employing apps, like malware, hacking of data, or breaches of privacy.

Before starting their apps, app developers can do vetting, and app shops or other organizations in charge of distribution can also undertake this. Code evaluation, security testing, and compliance checks with app store policies are frequently involved. In order to determine client happiness and reliability, user reviews and ratings may be taken into account throughout the evaluation procedure. In the end, however, screening mobile applications is essential to providing users with a safe and reliable mobile app surroundings.

7. **List and briefly define major privacy risks for web applications.**

Apparently the most significant privacy concerns for web apps are:

- **Data Breach**: Information breaches may occur when unauthorized access is provided to sensitive user data, such as personal or financial information. These breaches could be caused by lax security controls or coding vulnerabilities in the application.
- **Tracking and profiling**: Utilizing cookies, tracking scripts, or analytical instruments, web apps can gather a lot of user information. The building of complex user profiles using the above data could violate users' privacy and enable intrusive targeted advertising.
- **Cross-Site Scripting (XSS)**: XSS attacks include introducing malicious scripts into web pages that are being viewed by other users. This could end up in a breach of user session data, enabling attackers an opportunity to pose as actual users.
- **Cross-Site Request Forgery** (CSRF): CSRF attacks encourage users to access a web application without their knowledge or permission. Attackers can control these operations to alter user choices or carry out transactions on the victim's behalf.

- **Inadequate Authentication and Authorization**: Unwanted access to user accounts and data may be caused by weak authentication and authorization networks.
- **Vulnerabilities caused by third parties**: If external libraries or services are not adequately maintained or secured, integrating them with web apps can result in weaknesses.
- **Weak Data Protection**: If data is not secured with encryption when it is in use or in transit, it may be captured or exploited.

8. What are some of the major privacy/security threats for the use of mobile apps?

Some of the major privacy/security threats for the use of mobile apps are as follows:

- **Insecure Network Communications:** Mobile apps often rely on network communications to function, which can pose significant security threats if not implemented securely. Insecure data transmission can lead to eavesdropping and data interception by malicious actors. This vulnerability can expose sensitive user information, such as login credentials, personal data, and financial details. To mitigate this threat, mobile apps should use secure communication protocols like HTTPS and implement proper encryption mechanisms to protect data in transit.
- **Web Browser Vulnerabilities:** Many mobile apps incorporate web views or browsers for various purposes, such as displaying web content or enabling authentication through web pages. However, these embedded browsers can introduce security vulnerabilities if not properly configured and maintained. Browser vulnerabilities may allow attackers to execute malicious code, steal session cookies, or exploit Cross-Site Scripting (XSS) vulnerabilities. App developers should regularly update embedded browsers and follow best practices to secure web views.
- **Vulnerabilities in Third-Party Libraries:** Mobile app development often relies on third-party libraries and frameworks to streamline the development process. While these libraries can enhance efficiency, they can also introduce security risks if they contain vulnerabilities. Developers should stay vigilant and keep third-party components up to date to address known

security issues. Failure to do so may expose the app to risks like code execution exploits, data breaches, and unauthorized access.

- **Cryptographic Vulnerabilities:** Mobile apps often employ cryptography for various purposes, such as encrypting data, securing communications, and protecting user credentials. However, improper cryptographic implementation can lead to vulnerabilities that attackers can exploit. Common cryptographic vulnerabilities include weak key management, insufficient entropy, and improper use of encryption algorithms. To address this threat, app developers must adhere to cryptographic best practices, use strong encryption algorithms, and securely manage cryptographic keys.

9. What are the online privacy principles defined by the FTC?

The Federal Trade Commission (FTC) has established a set of fundamental online privacy principles to guide organizations in protecting individuals' privacy rights and ensuring responsible data handling practices. Here's an extended explanation of these principles:

- **Notice/Awareness:** This principle emphasizes transparency and requires organizations to inform individuals about their data collection and usage practices. When individuals visit a website or use an online service, they should be provided with clear and concise notices detailing what data is being collected, why it's being collected, how it will be used, and any third parties with whom it might be shared. This empowers users to make informed decisions about sharing their information.
- **Choice/Consent:** Choice and consent give individuals control over their personal data. Organizations should provide users with options to opt-in or opt-out of data collection and sharing practices. Users should have the freedom to choose whether their data is collected and used for specific purposes. Consent should be explicit, and individuals should not be forced into sharing their data as a condition of using a service unless it is necessary for that service's core functionality.

- **Access/Participation:** Access and participation principles grant individuals the right to access the data collected about them and to participate in its correction or deletion. Organizations should provide mechanisms for users to review, correct, or delete their personal data. This principle ensures that individuals can maintain the accuracy of their information and have control over their online profiles.
- **Integrity/Security:** Integrity and security principles emphasize the importance of safeguarding personal data. Organizations are required to implement robust security measures to protect collected data from unauthorized access, breaches, and other threats. Ensuring data accuracy and taking steps to prevent data tampering is crucial for maintaining trust with users.
- **Enforcement/Redress:** The enforcement and redress principle holds organizations accountable for complying with privacy commitments. The FTC has the authority to enforce privacy violations and impose penalties on non-compliant entities. Individuals should have avenues for seeking redress if their privacy rights are violated, including access to mechanisms for filing complaints and resolving disputes.

These online privacy principles established by the FTC form a comprehensive framework to guide organizations in responsible data handling practices. They underscore the importance of transparency, user control, data security, and accountability in the digital age. Adhering to these principles not only protects individuals' privacy but also helps organizations build and maintain trust with their customers and users.

10. What are the elements and subelements of the FTC online privacy framework?

Four essential principles are laid out in the FTC's online privacy framework for businesses to follow in order to protect customers' online privacy:

- **Transparency**: Companies are obligated to publicly disclose their information practices, including the data they gather, the purposes for which they are used, and the recipients of their sharing.
- **Privacy by design**: Principles and procedural protections.

- **Simplified choice for business and consumers**: Practices that do not require choice, and practices that require choice.
- **Greater transparency:** Privacy notices, consumer access to data, and consumer education
- **Choice**: Consumers have the right to decide how their information is used. This includes the choice not to participate in a particular data gathering or data sharing activity.
- **Security**: Businesses are required to protect the privacy and personal information of their customers by putting in place safeguards to prevent unwanted access or breaches.
- **Accountability**: Businesses are accountable for their privacy practices and rules. They must be able to show compliance with the framework, demonstrating their dedication to protecting customer privacy.

11. **List and briefly describe the main factors that contribute to the ineffectiveness of current web privacy notices.**

The following are the key reasons why existing web privacy notifications are ineffective:

- **Length and complexity:** Privacy notifications are sometimes lengthy and intricate, written in legalese that is hard for most people to comprehend. Users find it challenging to make educated judgments regarding their privacy.
- **Lack of transparency:** Frequently, privacy notifications do not include brief, clear information about the data that is collected, utilized, and shared. Users find it challenging to comprehend the privacy consequences of utilizing a website or service as a result.
- **Lack of choice:** Users sometimes have extremely limited or no control over how their data is gathered and used when reading privacy notifications. This defeats the intent behind privacy notifications, which is to provide
- **Privacy notifications:** They are sometimes shown to consumers at inconvenient moments, such as when they are initially signing up for a service or downloading an app, and are frequently badly designed. Users are therefore more inclined to disregard or quickly scan privacy alerts as a result.

- **Lack of enforcement:** Because privacy rules and regulations are not consistently followed, businesses frequently get away with issuing poor privacy notifications. This deters businesses from devoting the time and money required to produce efficient privacy notifications.

12. List and briefly define the dimensions of a privacy notice design space.

- Depth of Content: The extent to which the privacy notice delves into specific details, which may range from concise summaries to comprehensive disclosures, tailored to suit the target audience and adhere to regulatory requirements.
- Clarity and Language Usage: The application of straightforward and easily understandable language in the privacy notice to effectively convey information in a clear and concise manner.
- Format and Arrangement: The visual layout of the notice, encompassing elements like headings, bullet points, visual aids, and the overall structure, all contributing to the ease of readability.
- Accessibility: Ensuring that the privacy notice is readily accessible to all users, including those with disabilities, through the use of appropriate fonts, colors, and provisions for alternative formats when necessary.
- Visual Design Elements: The incorporation of visual components such as icons, images, and color schemes to enhance the visual appeal and memorability of the privacy notice.
- User Engagement Features: The inclusion of interactive elements like collapsible sections or tooltips, which empower users to access supplementary information as required.
- Consent Mechanisms: The integration of functionalities like checkboxes or choices for opting in or out to facilitate the collection of user consent when it's a prerequisite.
- Personalization Options: The customization of the notice to accommodate individual user preferences, such as language choice, geographical location, or user category.
- Mobile Compatibility: Ensuring that the notice is optimized for viewing and interaction on mobile devices, acknowledging the prevalence of mobile browsing.
- Multilingual Support: Providing translations or language alternatives to cater to a diverse international audience.

- Navigation and Linking: Offering clearly marked and easily accessible links to related documents such as privacy policies, terms of service, and contact details for privacy-related queries.
- Dynamic Updates: Adapting the notice to incorporate alterations in privacy practices or regulations and effectively communicating these changes to users.

13. Define the various types of cookies.

- **Unidentified cookie:** The only identifying information associated with the cookie is a unique ID assigned by the server.
- **Identified cookie:** User information is associated with the cookie.
- **Session cookie:** Remains on the user system only while the user has an open window to that website.
- **Persistent cookie:** Includes an expiration date.
- **First-party cookie:** Set and read by the web server hosting the website the user is visiting.
- **Third-party cookie:** Belongs to a domain different from the one shown in the address bar.

References

[1] What are the Differences Between Anonymisation and Pseudonymisation - Blogpost. (n.d.). https://www.privacycompany.eu/blogpost-en/what-are-the-differences-between-anonymisation-and-pseudonymisation

[2] Wang, J., Du, K., Luo, X., & Li, X. (2018, June 29). Two privacy-preserving approaches for data publishing with identity reservation. Knowledge and Information Systems, 60(2), 1039–1080. https://doi.org/10.1007/s10115-018-1237-3