Module 8: Homework 8

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

October 13, 2023

Review Questions

1. **Define data loss prevention**

   Data loss prevention (DLP), also referred to as data leakage prevention, refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework.

   DLP is a holistic approach to data security that integrates technology, policies, and user awareness to prevent data loss or exposure. By addressing data protection across all stages and facets of data handling, DLP helps organizations proactively manage the risks associated with sensitive information and maintain data confidentiality and integrity.

2. **Discriminate between data at rest, data in motion, and data in use.**

   Discrimination between data are as follows:

   - **Data at rest:** Data that resides in databases, file systems, and other structured storage methods. Data at rest refers to data that is stationary and stored in a non-transient state on physical or digital storage devices, databases, or file systems. It is not actively being processed or transmitted.
   - **Data in motion:** Data that is moving through a network, including wireless transmission. Data in motion, also known as data in transit, is data that is actively moving from one location to another, typically over a network or communication channels. It is in a dynamic state during transmission.
   - **Data in use:** Data in the process of being created, retrieved, updated, or deleted. Data in use refers to data that is actively being processed, accessed, or manipulated by a software application, system process, or user. It is in a dynamic state during these operations.

   In summary, data at rest, data in motion, and data in use represent distinct states in the data lifecycle, each requiring specific security measures. Data at rest is static and stored, data in motion is actively transmitted, and data in use is actively processed. Organizations must adopt security strategies tailored to protect data in these different states to ensure comprehensive data security and privacy.

3. **Define the Internet of Things.**

The Internet of Things (IoT) refers to the network of physical objects or "things" that are embedded with sensors, software, and other technologies to connect and exchange data with other devices and systems over the internet where these objects can range from day to day appliances, vehicles, and wearable devices to industrial machinery and infrastructure components. These are physical things or devices outfitted with sensors, actuators, and other data collection and transmission gear. IoT devices can transmit and receive data because they are linked to the internet or other communication networks where these connectivity can be wired (for example, Ethernet) or wireless (for example, Wi-Fi, cellular, Bluetooth, LoRa, or Zigbee).

IoT devices take data from sensors and either process it locally or transmit it to centralized servers or cloud platforms for analysis and storage. The data generated by IoT devices may be utilized to develop a wide range of applications and services, ranging from consumer-oriented applications such as smart home automation and health monitoring to industrial applications such as predictive maintenance and supply chain optimization.Common communication and data exchange standards and protocols are required to ensure that IoT devices from various manufacturers may work together seamlessly.

4. **List and briefly describe the principal components of an IoT-enabled thing.**

- IoT devices are outfitted with a variety of sensors to collect data from the physical world where temperature sensors, motion sensors, humidity sensors are some kind of sensors. Sensors translate physical events into electronic data that may be processed.
- Microcontrollers or Microprocessors are the component that serves as the IoT device's brain, processing data, making decisions, and controlling the device's activities in which the firmware or software of the device is executed by microcontrollers or microprocessors.

- IoT devices require a way to send and receive data. Wi-Fi, Bluetooth, cellular, Zigbee, and other wireless technologies may be used in communication modules. These modules allow the gadget to talk with other devices or connect to the internet.
- To function, IoT devices require a power supply by depending on the device's design and application, it may be powered by batteries, solar panels, a cable connection, or another source of energy.
- Memory (RAM) and storage (flash memory or SD cards) are frequently used in IoT devices to store data, firmware, and configurations that are critical for efficient operation and retaining data even when the device is turned off.

5. **Define cloud computing.**

The access and use of a variety of computing resources, such as servers, storage, databases, networking, programs, and more, through the web is made available by a technology termed the cloud. Users can rely on providers of cloud services to supply these resources as a subscription service so they don't have to manage and maintain their own private hardware and software infrastructure. Users can now swiftly increase or decrease their computing needs while only paying for the resources they truly use. They can also use these resources from virtually any location with a web connection.

Agility and efficiency are two of the main benefits of using the cloud. This enables businesses to avoid the up-front expense of buying and keeping their own IT equipment as well as the regular operational expenses related to operating a data center. Likewise cloud services sometimes offer features like high reliability, security, and periodic updates, that may clear away critical time and resources for businesses to focus on their primary tasks. In general, cloud computing has changed the way we view and utilize the capabilities of computers through offering a practical and scalable solution for differed computing requests.

6. **List and briefly describe three cloud service models.**

The most common cloud service models are IaaS, PaaS and SaaS. A summary of them is below:

1. **IaaS** - also known as infrastructure as a service. This is backend IT infrastructure hosted in the cloud that organizations can access for a monthly fee to run applications and workloads in the cloud. It reduces company hardware expenses and losses from hardware depreciation as application and/or business functions evolve. Businesses using this model also have the ability to customize the infrastructure and receive full insights on how its clients are interacting with services delivered.
2. **PaaS** - also known as platform as a service. Refers to on-demand, ready-to-use virtual platforms for delivering applications. Unlike IaaS, the organizations on this platform do not have access to the host infrastructure and therefore, are not responsible for maintaining the infrastructure. This increases faster time to market and scale of delivering applications.
3. **SaaS** - also known as software as a service. An example is Microsoft 365. This is a full application rendered over the cloud, that businesses can use to perform a specific function. Just about any personal or business productivity application on the market today is available as a SaaS. Providers of SaaS are responsible for comprehensive development, maintenance and security of the application and platforms/infrastructure hosting it.

7. List and briefly define four cloud deployment models.

Four cloud deployment models are as follows:

- **Public cloud:** The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services. The CSP is responsible both for the cloud infrastructure and for the control of data and operations within the cloud.
- **Private cloud:** The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise. The CSP is responsible only for the infrastructure and not for the control.
- **Community cloud:** The cloud infrastructure is shared by several organizations and sup- ports a specific community that has shared concerns (e.g., mission, security requirements, policy, and

compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

- **Hybrid cloud:** The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

8. Describe some of the main cloud-specific security threats.

Some of the main cloud specific security threats are:

- **Responsibility ambiguity:** The enterprise-owned system relies on services from the CSP. The level of the service provided (SaaS, PaaS, IaaS) determines the magnitude of resourc- es that are offloaded from IT systems onto the cloud systems. Regardless of the level of service, it is difficult to define precisely the security responsibilities of the customer and those of the CSP. If there is any ambiguity, this complicates risk assessment, security control design, and incident response.
- **Loss of governance:** The migration of a part of the enterprise's IT resources to the cloud infrastructure gives partial management control to the CSP. The degree of loss of governance depends on the cloud service model (SaaS, PaaS, IaaS). In any case, the enterprise no longer has complete governance and control of IT operations.
- **Loss of trust:** It is sometimes difficult for a cloud service user to assess the CSP’s trust level due to the black-box nature of the cloud service. There is no way to obtain and share the CSP’s security level in a formalized manner. Furthermore, the cloud service users are generally unable to evaluate the security implementation level achieved by the CSP. This in turn makes it difficult for the customer to perform a realistic risk assessment.
- **Service provider lock-in:** A consequence of the loss of governance could be a lack of freedom in terms of how to replace one CSP with another. An example of the difficulty in transitioning is

if a CSP relies on proprietary hypervisors or virtual machine image formats, and does not provide tools to convert virtual machines to a standardized format.

- **Non-secure cloud service user access:** As most of the resource deliveries are through remote connections, unprotected APIs (mostly management APIs and PaaS services) are among the easiest attack vectors. Attack methods such as phishing, fraud, and exploitation of software vulnerabilities pose significant threats.
- **Lack of asset management:** The cloud service user may have difficulty in assessing and monitoring asset management by the CSP. Key elements of interest include location of sensitive asset/information, degree of physical control for data storage, reliability of data backup (data retention issues), and countermeasures for business continuity and disaster recovery. Furthermore, the cloud service users also have important concerns on exposure of data to foreign governments and on compliance with privacy laws.
- **Data loss and leakage:** This threat may be strongly related to lack of asset management. However, loss of an encryption key or a privileged access code will bring serious problems to the cloud service users. Accordingly, lack of cryptographic management information, such as encryption keys, authentication codes and access privilege, will lead to sensitive damages, such as data loss and unexpected leakage to the outside.

References

[1] Hannabuss, S. (2010, August 17). Understanding Privacy20103Daniel J. Solove. Understanding Privacy. Cambridge, MA and London: Harvard University Press 2008.

[2] Komninos, A. (2023, September 1). An Introduction to Usability. The Interaction Design Foundation. https://www.interaction-design.org/literature/article/an-introduction-to-usability#:~:text=While%20usability%20is%20concerned%20with,become%20useful%20to%20their%20users.