JAHANGIR NAGAR UNIVERSITY

Institute of Information Technology

Assignment 1 | Fall 2023 Semester
PMIT 6104 Database Security
Summer Semester 2023 Intake
Date of Submission: December 15, 2023

Submitted by
HASAN TAHSIN RAFSAN
Professional Masters in Information Technology (PMIT) Program
2nd Trimester Regular Batch - Section A
ID **232137**

Submitted to
MOHAMMAD ABU YOUSUF
Professor
Institute of Information Technology

ANS 1

A

Draft Outline for a Large Department Store Security Policy Document

Mission: Securely handle customer and company data.
Scope: Employees, systems, vendors.
Key Concepts: Data classification and access control.
Security controls: training, encryption, firewalls.
Incident response: identify, recover, report.
Compliance: relevant regulations.

Responsibilities:
Employees: reporting and awareness.
Management: oversight and resources.
Vendors: data protection.
IT: implementation and maintenance.

Continuous Improvement:
Regular monitoring and updates.
Commitment to data security.

This concise outline captures the core elements of the department store's security policy, offering a high-level overview for further development.

B

User Groups and Database Tables for an Airline Company

User Groups:
Booking Agents: Responsible for managing passenger reservations and ticketing.
IT Staff: Maintain and develop database systems and applications.
Operations Staff: Manage flight schedules, aircraft assignments, and gate operations.
Customer Service Representatives: Assist customers with inquiries, changes, and cancellations.
Revenue Management: Analyze booking data and optimize pricing strategies.
Accounting: Manage financial transactions, generate reports, and comply with regulations.
Marketing: Develop and execute marketing campaigns to attract passengers.
Executives: Access overall company data for strategic decision-making.

Major Database Tables:
Passengers: Stores passenger information including name, contact details, travel history, and loyalty program data.

Flights: Lists scheduled flights with details like route, aircraft, schedule, and fare categories.
Bookings: Tracks passenger reservations, including booking date, fare paid, seats assigned, and payment information.
Financial Transactions: Records all financial transactions related to ticket purchases, refunds, fees, and other revenue streams.
Sample Authorization Matrix:

User Group	Database Table	Access Privileges
Booking Agents	Passengers, Flights, Bookings	Read, Create, Update, Delete (booking records)
IT Staff	All Tables	Read, Create, Update, Delete (system administration)
Revenue Management	Bookings, Financial Transactions	Read, Analyze
Marketing	Passengers, Flights	Read, Analyze
Customer Service Representatives	Passengers, Flights, Bookings	Read, Update (booking records)
Accounting	Passengers, Bookings, Financial Transactions	Read, Create, Update (financial transactions)
Operations Staff	Flights, Bookings, Financial Transactions	Read, Create, Update (flight schedules, gate assignments)
Executives	Passengers, Flights, Bookings, Financial Transactions	Read, Analyze (aggregated data)

C

User views can be powerful security tools by offering granular access control and data segregation, enhancing data privacy, and simplifying audit trails. Here are three examples:

1. Enhanced Data Privacy:

By limiting user access to only the data they need, user views minimize the risk of data breaches and unauthorized data disclosure. This helps comply with data privacy regulations and protects user information.

2. Data Segregation:

In a database with financial data and product details. User views can restrict access based on roles. The marketing team might only see product details, while finance professionals have a separate view of financial data. This segregates sensitive data, minimizing exposure and potential breaches.

3. Simplified Audit Trails:

User views can simplify audit trails by logging user activity within the specific data they accessed. This makes it easier to track suspicious activity and identify potential security breaches or unauthorized access attempts compared to analyzing logs of the entire database.

D

I'll choose RSA for this example, as it's a more widely used and versatile encryption technique. Here's how data is exchanged using RSA:

Imagine Isha wants to send a secret message to Abisheikh securely.

1. Key Generation:
Isha and Abisheikh generate their own separate key pairs:
Private key: This is kept secret and used for decryption.
Public key: This is shared publicly and used for encryption.

2. Encryption:
Isha wants to send Abisheikh the message "Hello, Abisheikh!".
She uses Abisheikh’s public key to encrypt the message. This involves complex mathematical calculations that transform the message into seemingly random data.

3. Transmission:
Isha sends the encrypted data to Abisheikh through a public channel (e.g., email, internet).

4. Decryption:
Abisheikh receives the encrypted data.

He uses his own private key to decrypt the data. This reverses the mathematical transformation and reveals the original message: "Hello, Abisheikh!".

ANS 2

Applying Mandatory Access Control (MAC) to the Video Platform:

1. User Roles and Labels:
Define user roles: Parents, Uploaders, Viewers, and Mash-up creators.
Assign security labels to each role based on their clearance levels (e.g., using Biba model):
Parents: Highest Integrity (e.g., Integrity Level 4).
Uploaders: Intermediate Integrity (e.g., Integrity Level 3).
Viewers: Lowest Integrity based on age and belief configuration (e.g., Integrity Level 1, 2).
Mashup creators: Same Integrity level as the highest constituent video (no upward flow).

2. Metadata and Tags:
Enhance video meta-data with contentdescriptor tags and their associated sensitivity levels:
Tags: Cold drinks, BarbieAndKen, Disrespect, Evolution, IntelligentDesign, Sexuality, etc.

Sensitivity levels: Low, Medium, High (corresponding to appropriate age ranges).

3. Videoviewer program:
Read childviewingallowed.config:
Calculate child's age and derive minimum age clearance (e.g., Integrity Level 2 for 18+).
Extract allowed content descriptor list and their sensitivity levels.
Compare video's metadata:
Ensure video's Integrity level is less than or equal to the child's clearance.
Only display videos where all tags are allowed by the child's configuration.
Prioritize videos with tags matching the child's allowed sensitivity levels.

4. Mashup creation program:
Inherit tags and sensitivity levels from constituent videos.
Calculate new video's Integrity level:
Same as the highest Integrity level of any constituent video (no upward flow).
Combine tags from all constituent videos, ensuring no duplicates.
Assign the new video's sensitivity level based on the highest level of any constituent tag.

5. Access Control Enforcement:

Implement Biba style Mac mechanisms: Users can only access videos with Integrity levels less than or equal to their own. Mashup creation cannot increase the Integrity level of any constituent video. Uploading enforces downward information flow (videos cannot gain higher Integrity).