SecureNet by GlobalBank - DFD with Threat Analysis

Owner: Athena Parsa Kayin
Reviewer: Mamoona Homayun
Contributors:
Date Generated: Wed Nov 20 2024

Executive Summary

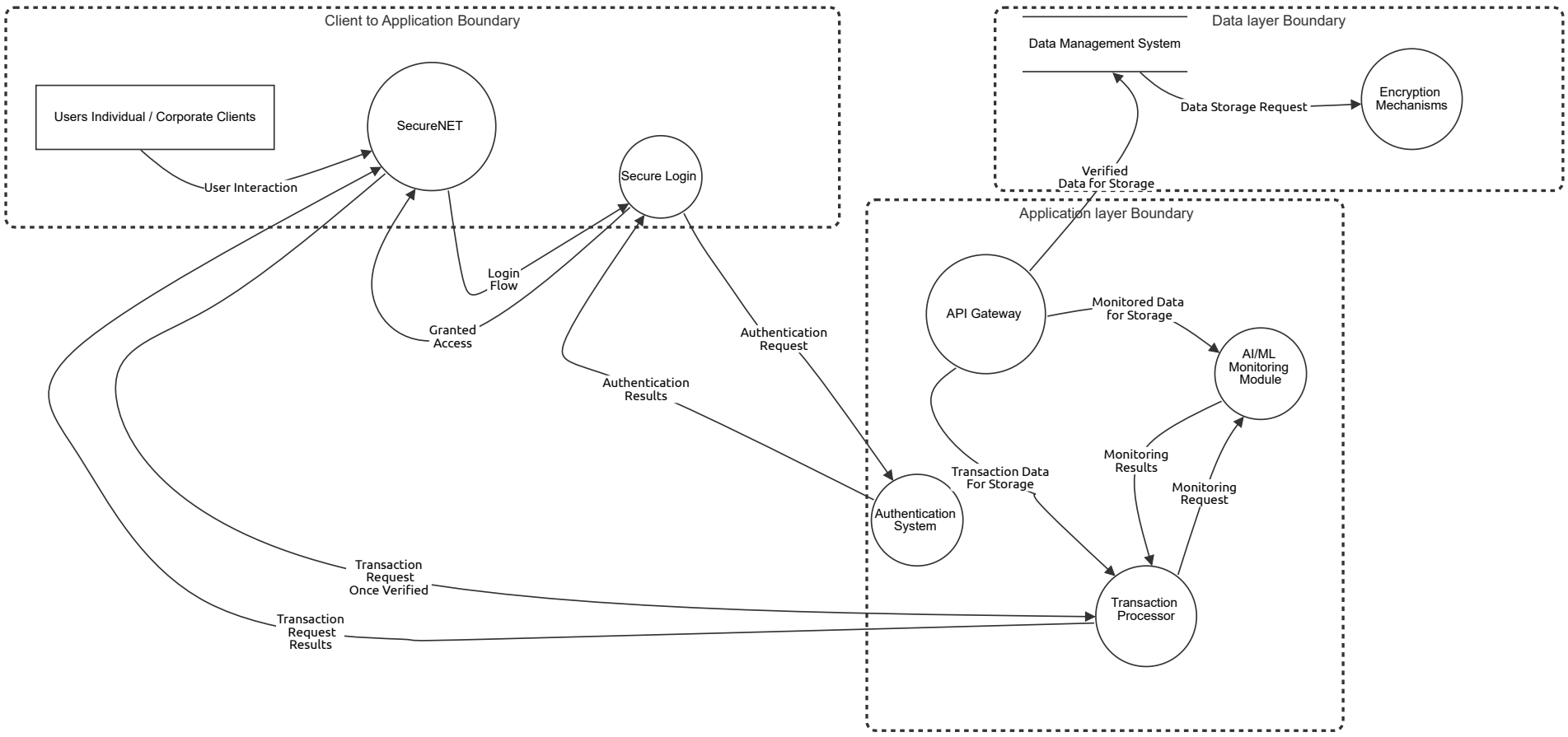
High level system description

SecureNet by GlobalBank is a secure digital banking platform with a three-tier architecture. It enables clients to manage accounts, perform transactions, and monitor activities through a web/mobile interface. The system includes a Presentation Layer for user interaction, an Application Layer for authentication and transaction processing, and a Data Layer for secure data storage. Security features like Multi-Factor Authentication, encryption, and real-time monitoring protect against unauthorized access and fraud

Summary

Total Threats	7
Total Mitigated	7
Not Mitigated	0
Open / High Priority	0
Open / Medium Priority	0
Open / Low Priority	0
Open / Unknown Priority	0

New STRIDE diagram



New STRIDE diagram

Users Individual / Corporate Clients (Actor)

This model focuses on the SecureNet banking platform, covering individual and corporate user interactions and the system's secure data flows/Business clients with access to advanced banking features

Number	Title	Type	Priority	Status	Score	Description	Mitigations

SecureNET (Process)

Main interface for user interaction, enabling account management, transaction initiation, and viewing account details. Acts as a bridge between users and the application layer

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Secure Login (Process)

Implements Multi-Factor Authentication (MFA) to verify user identify, Providing secure access control for all user actions

Number	Title	Type	Priority	Status	Score	Description	Mitigations
2	Unauthorized Account Access	Spoofing	High	Mitigated	8	An attacker may attempt to impersonate a legitimate user by leveraging stolen credentials, phishing attacks, or brute-force techniques. This spoofing could result in unauthorized access to user accounts, leading to potential financial fraud, unauthorized transactions, and data breaches	Multi-Factor Authentication (MFA): Enforce MFA for an additional layer of security beyond passwords. Strong Password Policies: Require complex passwords and enforce regular password updates. Account Lockout Policies: Lock accounts after a certain number of failed login attempts to prevent brute-force attacks. Session Monitoring: Implement session monitoring to detect and alert unusual access patterns. Category: Reduce

Authentication System (Process)

Handles user authentication, enforcing Multi-Factor Authentication (MFA) for secure access. Manages user sessions and flags suspicious activity for security monitoring

Number	Title	Type	Priority	Status	Score	Description	Mitigations
3	Altered Authentication Configuration	Tampering	High	Mitigated	8	An attacker might attempt to tamper with the authentication system by altering access control parameters, such as Multi-Factor Authentication (MFA) requirements or user privileges. This could allow unauthorized access to restricted parts of the system, posing a serious security risk	Cryptographic Integrity Checks: Use HMAC (Hash-based Message Authentication Code) or similar techniques to ensure data integrity. Configuration Hardening: Restrict access to authentication settings and secure configuration files. Audit Logging: Maintain detailed logs for any changes made to authentication configurations and review them regularly for suspicious activity Category: Reduce

Transaction Processor (Process)

Processes financial transactions, enforces business rules, and ensures compliance. Validates transactions and sends data to storage securely

Number	Title	Type	Priority	Status	Score	Description	Mitigations
4	Disputed Transactions	Repudiation	Medium	Mitigated	7	A user may deny initiating a transaction, claiming it was unauthorized. This repudiation could result in disputes and financial losses if the system cannot verify the legitimacy of the transaction	Digital Signatures: Implement digital signatures to authenticate and validate each transaction. Non-Repudiable Logging: Log transactions with cryptographic methods that make it infeasible for users to deny actions. Audit Trail: Maintain a secure audit trail that includes details such as user identity, IP address, and timestamp for all transactions Category: Reduce

AI/ML Monitoring Module (Process)

Monitors transactions in real-time, detecting suspicious patterns using AI algorithms to prevent fraud and unauthorized activities

Number	Title	Type	Priority	Status	Score	Description	Mitigations
5	Unauthorized Privilege Escalation	Elevation of privilege	High	Mitigated	8	An attacker could attempt to gain higher privileges within the AI/ML Monitoring Module, potentially allowing them to modify detection parameters or disable fraud alerts. Unauthorized privilege escalation within this module could result in fraudulent activities going undetected	Role-Based Access Control (RBAC): Enforce strict role-based access controls to ensure that only authorized users have access to privileged functions. Privileged Access Monitoring: Log and monitor all privileged access actions, with alerts set up for unusual behavior. Separation of Duties: Ensure that users who manage monitoring configurations cannot access or alter the transaction data they are monitoring Category: Avoid

API Gateway (Process)

Manages communication between the application and data layers, ensuring secure data exchange. Handles incoming and outgoing API requests

Number	Title	Type	Priority	Status	Score	Description	Mitigations
6	Unsecured Data Transmission	Information disclosure	Medium	Mitigated	6	Sensitive data passing through the API Gateway may be intercepted by an unauthorized party if it is not properly encrypted, potentially leading to data exposure and breaches	SSL/TLS Encryption: Encrypt all data flows through the API Gateway using SSL/TLS to secure data in transit. Token-Based Authentication: Use secure tokens like OAuth or JWT to authenticate API requests and protect data. Access Control: Limit access to the API Gateway to authenticated and authorized users only. Category: Reduce

Data Management System (Store)

Stores verified transaction data, customer details, and compliance records securely in an encrypted environment. Ensures data availability for authorized access only

Number	Title	Type	Priority	Status	Score	Description	Mitigations
7	Overloading Transaction Systems	Denial of service	High	Mitigated	8	An attacker could attempt to overwhelm the Data Management System with excessive requests, leading to service unavailability for legitimate users	Rate Limiting: Implement rate limits to control the volume of requests from each source. Redundancy and Load Balancing: Use redundant systems and load balancers to manage high request loads and maintain service availability. Traffic Monitoring: Implement intrusion detection to monitor traffic patterns and identify suspicious activity indicative of a Denial of Service (DoS) attack. Category: Reduce

Encryption Mechanisms (Process)

Implements robust encryption protocols to protect sensitive data in transit (TLS/SSL) and at rest (AES-256). Ensures secure key management practices

Number	Title	Type	Priority	Status	Score	Description	Mitigations
8	Weak Encryption Standards	Information disclosure	High	Mitigated	9	Sensitive data could be exposed if encryption mechanisms fail due to weak algorithms, inadequate key management, or misconfigurations, resulting in unauthorized access to data at rest.	Strong Encryption Standards: Use robust encryption standards like AES-256 for data at rest and TLS 1.2 or higher for data in transit. Secure Key Management: Implement secure key management practices, such as using Hardware Security Modules (HSMs) to store encryption keys. Regular Encryption Audits: Conduct regular audits of encryption configurations to ensure compliance with security standards and to detect potential vulnerabilities. Category: Reduce

Login Flow (Data Flow)

Initiates Secure Login

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Granted Access (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Authentication Results (Data Flow)

Results of the User Authentication

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Authentication Request (Data Flow)

Authentication request

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Transaction Request Results (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Transaction Request Once Verified (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Monitoring Results (Data Flow)

If Clear, then continues

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Monitored Data for Storage (Data Flow)

Represents the monitored and analyzed transaction data that flows to storage.

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Monitoring Request (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Data Storage Request (Data Flow)

Ensures data is encrypted in transit and at rest

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Verified Data for Storage (Data Flow)

Number	Title	Type	Priority	Status	Score	Description	Mitigations

User Interaction (Data Flow)

Account Management, Transaction Requests

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Transaction Data For Storage (Data Flow)

Data containing verified transaction details securely transmitted from the application layer to the data layer for encrypted storage and compliance purposes

Number	Title	Type	Priority	Status	Score	Description	Mitigations