Implementing Zero Trust Architecture: Banking System

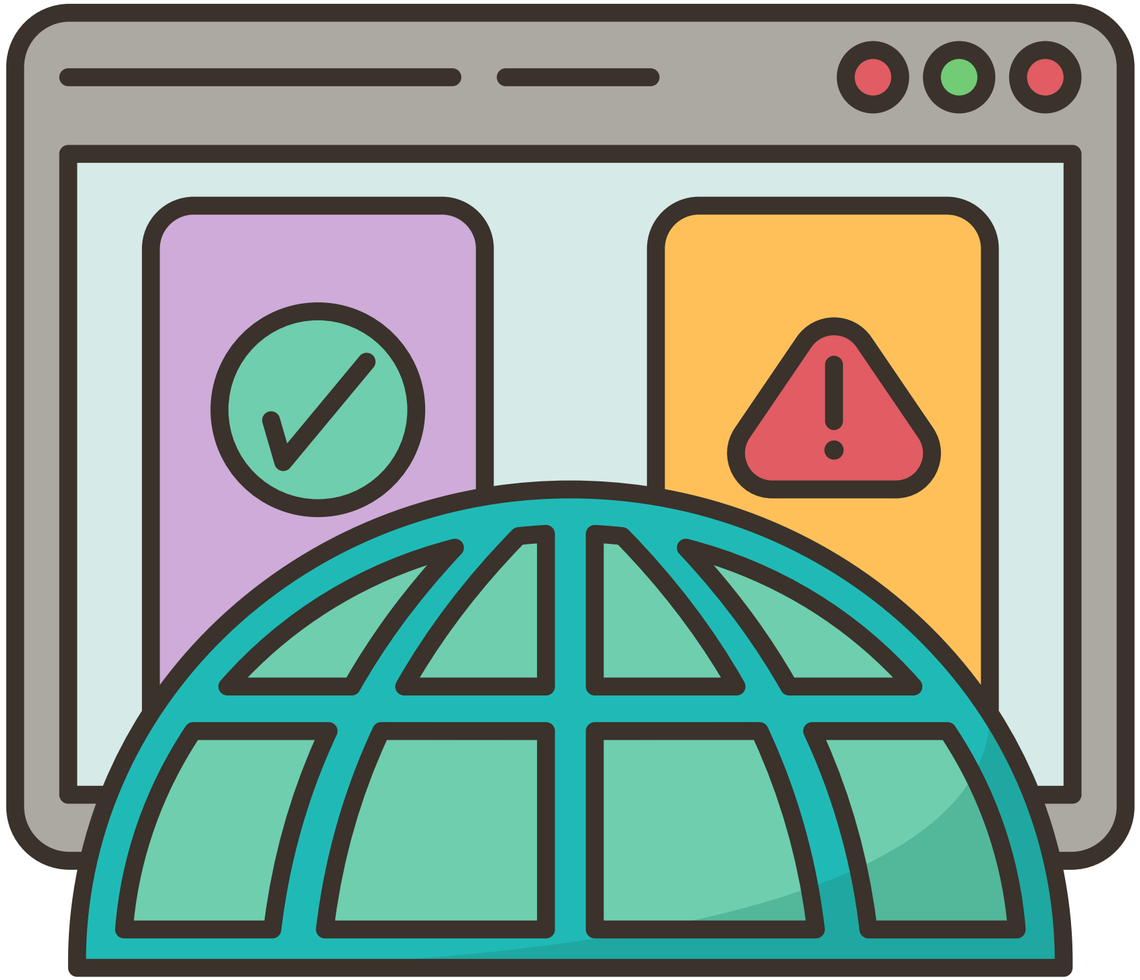
Never Trust, Always Verify

The Modern Threat Landscape

- **Rapid Evolution:** AI and technology are developing fast, but so are attackers.
- **High Stakes:** Data is the new currency (Financial systems, National Security, Military data).
- **Diverse Motives:** Attacks aren't just for money; they are for disruption, manipulation, and espionage.

Where Do Threats Come From?

- **External Threats:** Hackers trying to breach the system (Brute force, SQL Injection).
- **Internal Threats**: Authenticated users performing unauthorized actions.
- **The Reality:** We must stop outsiders, but also assume they will get in.



The Zero Trust Principle

- **The Problem:** Being "inside" does NOT mean you are trusted.
- **The Core Rule:** No Implicit Trust.
- **The Requirement:** Every request must be verified and authorized, regardless of origin.

Perimeter Defense: Identity

- Strong Authentication: Complex passwords (hashed, never plain text).
- MFA (Multi-Factor Authentication):
  Two-factor authentication using email-based OTP.
  OTP has 1-minute validity and is single-use enforced.
- Secure Login Flow:
  - Lock accounts after failed attempts.
  - CAPTCHA: Blocks bots and brute-force scripts.

Perimeter Defense: Firewalls & WAF

Firewall

- Filters traffic and blocks suspicious connections (The "Security Guard").

Security Headers

- Implemented CSRF protection, XSS protection, and HSTS enforcement

WAF (Web Application Firewall)

- Stops SQL Injection: Harmful database code prevented using Parameterized Queries and Strict Input Sanitization.
- Stops XSS: Malicious scripts (<script>, javascript:) in URLs.

Visibility: Scanning & Logging

- **Logged Events:** Login attempts, OTP generation/verification, Session timeouts

- **Log Details:** Records Timestamp, User ID, IP Address, User Agent, Action details, and Status

Enforcing Least Privilege

- **Least Privilege:** Give users only the permissions they truly need.
- **Result:** Limits the damage if an account is compromised.

Continuous Verification

- **Re-Authentication:** Require OTP/Password for sensitive actions (e.g., money transfers).
- **Behavioral Monitoring:** Detect suspicious internal actions:

  1.Repeated unauthorized attempts.

- **Response:** Block user, end session, send alerts.

Strict Session Security

Absolute Timeout: Sessions expire quickly (e.g., 5 minutes active).

Idle Timeout: Auto-logout after short idleness (e.g., 2 minutes).

Session Regeneration: Generate a new Session ID after every login.

Summary & Key Takeaways

- **Attackers are evolving;** we must defend against both External and Internal threats.
- **The Perimeter:** Use WAF, MFA, and Scanners to block outsiders.
- **Zero Trust:** Use Least Privilege, RBAC, and Monitoring to stop insiders.
- **Final Thought:** "Never Trust, Always Verify."

Live Demo

THANK YOU !

20226047, 20227005, 20226084, 20226093