Password-less Authentication System for Mobile Banking Apps

Introduction

Overview

In today's digital landscape, the increasing sophistication of cyberattacks has rendered traditional password-based authentication methods insufficient. Banking applications are high-value targets for malicious actors who exploit weak or reused passwords using phishing, brute force, or credential stuffing attacks. To address these vulnerabilities, our project introduces a secure, password-less authentication system designed specifically for mobile banking apps.

Motivation

Passwords are not only a security risk but also a burden for user experience. Users often forget them, reuse them across platforms, or fall victim to phishing schemes. These limitations call for a new approach—one that eliminates passwords entirely while maintaining or even enhancing security. Our goal is to build a system that users trust, enjoy using, and that financial institutions can confidently adopt.

Our Solution

We propose a multi-factor, password-less authentication mechanism powered by a BBKey hardware token, backed by biometrics and OTPs as secondary methods. The BBKey acts as a physical authenticator, offering the highest level of security through cryptographic key pairs stored securely on a tamper-resistant chip. Authentication is quick, intuitive, and seamless—requiring just a tap or a plug-in action.

Key Objectives

Our solution is designed with the following core objectives:

- **Security:** Eliminate passwords and use cryptographic hardware (BBKey) to prevent phishing and unauthorized access.
- **User Experience:** Provide a frictionless, intuitive login experience with fast biometric fallback and OTP options.
- **Scalability:** Ensure the system can support thousands of concurrent users without compromising speed or reliability.

- **Compliance:** Adhere to local and international data protection regulations like PDPL and GDPR.

Authentication Techniques Chosen

Primary Method: BBKey (Hardware Token)

Our primary method of authentication is the BBKey, a secure hardware token that uses public key cryptography (FIDO2/WebAuthn) to authenticate users without passwords. Each BBKey device stores a private key securely and generates a unique cryptographic signature during login, which is verified by the server using the corresponding public key.

Key Features

- **Tamper-proof:** Resistant to cloning and extraction.
- **Phishing-proof:** Not vulnerable to fake websites or man-in-the-middle attacks.
- **Portable:** Can be carried and used across devices.

How it Works

- Stores a private key securely inside tamper-proof hardware.
- Generates a unique cryptographic signature during login.
- Verifies the user by matching the signature with the public key on the server.

Recovery Options for BBKey Loss

First Recovery Method: Magic Link Authentication

As an immediate backup, the app supports magic link authentication via the user's registered email address.

How It Works

1. The user taps "Lost your BBKey?" on the login screen.
2. A secure, time-limited magic link is sent to their verified email address.
3. Clicking the link automatically authenticates the user and grants access to their account.
4. The link expires after a short duration or after a single use.

Security Features

- Magic links are cryptographically signed and time-bound.
- Only deliverable to the user's verified email address.
- Device fingerprinting and IP validation can be used to detect suspicious activity.
- Optionally, the system may require OTP or additional verification for high-risk actions post-login.

Second Recovery Method: One-Time Use Passwords (Provided by Bank)

As a more robust recovery mechanism, each user is issued a set of 10 one-time-use passwords (OTPs) during registration or upon request.

How It Works

1. Users receive 10 unique codes, delivered digitally or as a printed secure sheet.
2. When BBKey is unavailable, the user can log in using any unused OTP.
3. After a code is used, it becomes invalid and marked as used.
4. When the list is exhausted, the app prompts the user to request a new set from the bank.

Security Features

- OTPs are tied to the user and device.
- Codes are hashed and securely stored on the backend.
- Real-time notifications are sent when an OTP is used.

User Sign-Up & Registration Flow

Step 1: Enter Personal Information

The user begins by filling in essential details required for account creation and identity verification:

- Phone Number
- Email
- Location
- Home Address
- Government-issued ID Verification:
  - Upload a front and back photo of their ID card or passport.
  - Perform a live selfie or short video for face matching.

Step 2: Select BBKey Package

Once identity verification is complete, the user moves to BBKey selection:

- Choose the number of BBKeys (e.g., 1 for personal, 2 for backup).
- Select features (e.g., USB-C, NFC, Bluetooth-enabled BBKey).
- Confirm order and shipping details.

Step 3: Track BBKey Delivery

The user gets a real-time delivery tracking interface. Estimated delivery time is within 1 hour. Notifications are sent when the BBKey is out for delivery and once delivered.

Step 4: Activate BBKey

Once received:

- The app guides the user to insert or tap the BBKey.
- The user enters the PIN for the BBKey.
- A one-time registration key from the BBKey is validated on the server.
- The device is then paired and marked as trusted.

Step 5: Choose Alternative Access Method

To ensure accessibility in case of BBKey failure, the user is prompted to choose at least one fallback method:

- Magic Link Authentication.
- 10 One-Time Backup Codes (delivered securely).
- Trusted Device Push Notification (optional).

Authentication Flow – Mobile App Login Process

Step 1: User Opens the App

The user taps "Login" on the mobile banking app.

Step 2: Primary Method – BBKey Authentication

- The app prompts the user to insert or tap their BBKey.
- BBKey generates a signed cryptographic challenge and sends it to the server.
- If valid, the server returns a session token (e.g., JWT), and the user is logged in securely.
- If BBKey is unavailable or fails, the user is redirected to a secure fallback options screen.

Step 3: Fallback Authentication Options

- **Option A: Magic Link Authentication.**
- **Option B: One-Time Backup Code.**

BBKey Protocols Explained

The BBKey is a small security device used to protect accounts using multiple authentication technologies such as FIDO2, PIV, OTP, and OpenPGP. This section explains the protocols supported by BBKey and how each one works.

FIDO2 / WebAuthn Protocol

- Used for passwordless login.
- A key pair (public and private) is generated inside the BBKey.
- The private key never leaves the device.
- The public key is used by websites to verify the login.

U2F Protocol (Universal 2nd Factor)

- Used alongside a password for added security.
- BBKey signs a challenge + domain combination.
- No additional software is required; works directly with the browser.

OTP Protocol (One-Time Password)

- BBKey generates temporary login codes.
- Two types: TOTP (time-based) and BBKey OTP (proprietary).
- Used with services that do not support FIDO2.

PIV Protocol (Personal Identity Verification)

- Used in enterprise environments for login and digital signing.
- Supports multiple slots like 9a for authentication, 9c for signing, and f9 for key attestation.
- Compatible with systems like Windows and macOS.

OpenPGP Protocol

- Used to sign messages and encrypt emails.
- BBKey holds the private key and signs internally.
- Ideal for developers and security-conscious users.

Cost

Implementing the proposed password-less authentication system involves the following cost considerations:

Hardware Costs

- **BBKey Devices:** Estimated cost per device ranges from $20 to $50, depending on features (e.g., NFC, Bluetooth).
- **Backup BBKeys:** Optional additional devices for users who opt for backups.

Development Costs

- **Software Development:** Includes integration of FIDO2/WebAuthn protocols, fallback mechanisms, and user interface design.
- **Backend Infrastructure:** Secure storage for public keys, OTPs, and compliance with data protection regulations.

Operational Costs

- **Customer Support:** Handling BBKey delivery, activation issues, and recovery requests.
- **Maintenance:** Regular updates to ensure compatibility with evolving security standards.

Total Cost Estimate

The total cost will vary based on the scale of deployment, number of users, and selected features. A detailed cost analysis can be conducted during the project planning phase.

Conclusion

In our proposed authentication system, we prioritize both security and user convenience by intelligently adapting the level of authentication required based on transaction risk. By introducing pre-set conditions that determine when the primary authentication method (BBKey) is necessary, we minimize friction for low-risk actions while maintaining robust protection for high-risk scenarios.