Trends in Mobile Authentication

cnlab security ag, obere bahnhofstr. 32b, CH-8640 rapperswil-jona
esther.haenggi@cnlab.ch, +41 55 214 33 36
E-banking authentication
E-banking authentication: mTAN

User

Browser

Bank

Code for login: 73G833
Last login: 31.03.2014 16:47

Theft of credentials ✓

Phishing passiv ✓

Man-in-the-Middle ×

Malware ×

password

mTAN

mTAN

mTAN

mTAN

account information
E-banking authentication: mTAN

Code for transaction:
3EH878
50 CHF to Account Nr. 01-145-6

User
password
mTAN
mTAN
mTAN
mTAN
mTAN

Browser
password
mTAN
mTAN
mTAN
mTAN
mTAN

Bank
Account information
transaction
Man-in-the-Middle
Session hijack
Session riding
Malware
Comparison of different authentication methods

- **Scratch list**
- **One-time password**
- **Challenge-Response Token**
- **mTAN (SMS)**
- **PhotoTAN/QR-Code**
- **Kobil AST 2 devices**

### Theft Credentials
- **Measures**:
  - Different device
  - Limited validity, Non-static credential
  - Client certificate, hardened trust store
  - Hardened Browser

### Phishing passive

### Man-in-the-Middle

### Malware

### Session hijack

### Session riding

### Man-in-the-Middle

### Malware

- Additional authorization
- Transaction-dependent
- Visibility of transaction
Strong authentication: definition(s)

- No transmission of password over network  
  (Fermilab)

- Challenge-response identification  
  (Handbook of Applied Cryptography)

- 2 different authentication methods  
  (BSI)

- At least 2 factors:
  • Something the user knows (e.g., password, PIN);
  • Something the user has (e.g., ATM card, smart card);
  • Something the user is (e.g., biometric characteristic, such as a fingerprint).

  ENISA definition +
  • mutually independent
  • at least one
    - non-reusable
    - non-replicable (except inherence)
    - cannot be stolen via the internet

  Network interception not sufficient.
  Hard to steal.

Frequent additional requirement in banking: 2 device, not only 2 factor!
Mobile banking

Code for login: 73G833
Last login: 31.03.2014 16:47
Single device authentication methods

- **Scratch list**
- **One-time password**
- **Challenge-Response Token**
- **mTAN (SMS)**
- **Mobile ID**
- **PhotoTAN/QR-Code**
- **Kobil AST 2 devices**

### Theft Credentials
- **Login + Reading Access**
- **Transaction**
- **2 device solution**
- **1 device solution**
- **1 device with hardening**

- **Phishing passive**
- **Man-in-the-Middle**
- **Malware**

- **Session hijack**
- **Session riding**
- **Man-in-the-Middle**
- **Malware**
Strategies for secure mobile banking

Hardened single device:
Full functionality on a single device - Mitigate risk through technical measures

Multiple authentication levels:
Limit the functionality depending on strength of authentication
Hardened single device (1/4): Technical measures make attacks harder

Actually, the situation is not as bad as it seems…

- Theft Credentials
- Phishing passive
- Man-in-the-Middle
- Malware

- Session hijack
- Session riding
- Man-in-the-Middle
- Malware

Measures

- App’s own trust store
- Hardened App
Hardened single device (2/4): Example 1
Raiffeisen integrated PhotoTAN App

Properties of credentials:
• 2 Factors
• Non-reusable
• Non-replicable
• Cannot be abused by MitM

strong authentication can be reached on one device!

• Full E-Banking from smartphone
• Single device
• Technical hardening mechanisms
Hardened single device (3/4): Technical measures

Advantages of mobile devices compared to desktop devices

- Sandboxing of Apps (processes and data)
- Distribution of programs (Apps) through store
- Access protection through PIN (optional)
- Encrypted file system (iOS: standard, Android: some)

Possible hardening mechanisms for Apps:

- Check certificates against specific trust store
- Protect data through keychain protection mechanisms (iOS) (incl. binding to hardware)
- Protect files through OS access protection mechanisms (iOS)
- Exclude files from backup
- Prevent screenshots
- Jailbreak / rooting detection
- Version control of App / OS
Hardened single device (4/4): Example 2
Kobil AST 1 device (simplified)
Strategies for secure mobile banking

Hardened single device:
Full functionality on a single device - Mitigate risk through technical measures

Multiple authentication levels:
Limit the functionality depending on strength of authentication
Multiple authentication levels (1/3): Limit functionality

1st step
Authentication of user
e.g. through login

- Account data +
  ‘plausible’ Transactions

2nd step
Additional authorization
e.g. through mTAN,…

- All transactions+
  Important changes

User

Bank

Login

Account data

‘plausible’ Transactions

Transaction

Transaction authorization
Multiple authentication levels (2/3): Example 1
Mobile Banking UBS

Banking on smartphone
- General Information
- Read-only access to account + cards
- Personal finance assistant
- Trades on stock exchange
- Virtual portfolios
- E-bills
- Register transactions
- Execute whitelisted transactions

Full E-Banking
- Execute pre-registered transactions
- Register and execute all transactions
- Change of customer data
Multiple authentication levels (3/3): Example 2

E-banking with long-term cookie

1. **First login using mTAN**
   - User enters login credentials
   - Bank sends login cookie

2. **Login cookie**
   - X&kk13847eronnhf

3. **Password + login cookie**
   - User enters password
   - Bank verifies account information

4. **Account information**
   - User receives account information

5. **Some transactions still need to be confirmed using mTAN**
   - User confirms transactions using mTAN

Diagram showing the flow of authentication steps between User, Browser, and Bank.
Trends

- Smartphones are no different from computers
- Read access is considered less sensitive than transactions
- Technical hardening mechanisms
- Several levels of authentication
Thank you