Security & Privacy Analysis Framework For TOTP 2FA apps

Case-Study: Authy 2FA

Conor Gilsenan, Noura Alomar
CS261N - Spring 2020
Agenda

• Research Questions

• Background & Motivation
  – Related work

• Analysis framework
  – Case-study: Authy 2FA
Research Questions
1. What security and privacy issues exist in the backup & recovery functionality of prevalent TOTP 2FA apps?
2. How can they be fixed?
Research Questions

1. What security and privacy issues exist in the backup & recovery functionality of prevalent TOTP 2FA apps?

2. How can they be fixed?
Research Questions

1. What security and privacy issues exist in the backup & recovery functionality of prevalent TOTP 2FA apps?

2. How can they be fixed?
Research Questions

1. What security and privacy issues exist in the backup & recovery functionality of prevalent TOTP 2FA apps?

2. How can they be fixed?
Background & Motivation
Two-Factor Authentication (2FA)

• Knowledge (something you know)
• Possession (something you have)
• Inherence (something you are)
Two-Factor Authentication (2FA)

- Knowledge (something you know)
- Possession (something you have)
  - Inherence (something you are)
2FA Methods

• SMS

• Time-based One-time Passwords (TOTP)
  – e.g. Google Authenticator

• Push notifications
  – e.g. Duo Push

• WebAuthn
  – e.g. USB security keys
2FA Methods

• SMS

• Time-based One-time Passwords (TOTP)
  – e.g. Google Authenticator

• Push notifications
  – e.g. Duo Push

• WebAuthn
  – e.g. USB security keys
TOTP

1. Alice starts 2FA registration

Alice

Service Provider

Manual action
HTTPS connection
TOTP

1. Manual action
   HTTPS connection

2. Service provider shows a QR code in Alice's browser

Alice

Service Provider

Computer

Browser

Trusted Device

Alice
3 Alice scans QR code with authenticator app to obtain shared secret
TOTP

Alice

Service Provider

1. Manual action
2. HTTPS connection
3. Alice
4. Alice manually types OTP from trusted device into browser
TOTP: QR Code

Please use the TOTP protocol

Alice's email address or username

The shared secret

The service provider

otpauth://totp/alice@example.com?secret=SomeSecret&issuer=SomeCompany
Anyone can build a TOTP 2FA app!
Dozens of TOTP Apps

- Blizzard Authenticator
  Blizzard Entertainment, Inc.
- 2FA Authenticator (2FAS)
  2FAS
- LastPass Authenticator
  LogMeIn, Inc.
- FreeOTP Authenticator
  Red Hat
- andOTP - Android OTP Authenticator
  Jakob Nixdorf
- Salesforce Authenticator
  Salesforce.com, Inc.
- Duo Mobile
  Duo Security, Inc.
- SAAPASS Authenticator 2FA App & Password Manager
  SAAPASS
- Microsoft Authenticator
  Microsoft Corporation
- Authy 2-Factor Authentication
  Authy
- TOTP Authenticator – 2FA with Backup & Restore
  BinaryBoot
- Google Authenticator
  Google LLC
How should our app generate the OTP?
RFC says:

\[ \text{OTP} \approx \text{HMAC-SHA-1 (shared secret + time)} \]

How should our app backup the secret?
TOTP: Generate & Verify OTP

RFC says:

🤔 😐 😪 😴

❌ No backup capability by design!
Authy 2-Factor Authentication

1. Alice provides her Password.
2. The device generates a Key using PBKDF2(Password).
3. Authy receives ENC_key(TOTP Secret).

https://authy.com/blog/how-the-authy-two-factor-backups-work/
Related Work
Related Work

Password research

2FA authenticator apps

Mobile app security analysis

Security architecture and workflow analysis
Quantifying password guessability

• Password research shows
  – people pick **mostly weak** passwords
  – passwords are easy for attackers to crack


Password Managers
Bhargavan and Delignat-Lavaud (2012)

- Analyzed several “host-proof” systems
  - ideal: all data is encrypted on the clients
  - reality: flaws in client side crypto
Bhargavan and Delignat-Lavaud (2012)

• Analyzed several “host-proof” systems
  – ideal: all data is encrypted on the clients
  – reality: flaws in client side crypto

• Relationship to our work
  – considered offline brute force attacks out of scope
  – which data is encrypted?
  – how to circumvent client-side crypto?
Password Managers

Lie et al. (2014)

• Systematic security analysis
  – 5 web-based password managers

Password Managers

Lie et al. (2014)

- Security goals
  - Master account security
  - Credential db security
    - sharing features
  - Unlinkability

Password Managers

**Lie et al. (2014)**

- **Security goals**
  - Master account security
  - Credential db security
    - sharing features
  - Unlinkability

- **Attack surface**
  - Bookmarklet
  - Web
  - Authorization
  - User Interface

Password Managers

Lie et al. (2014)

• Relationship to our work
  – identified attacks to obtain password ciphertexts
  • CSRF

Password Managers

Lie et al. (2014)

• Relationship to our work
  – identified attacks to obtain password ciphertexts
    • CSRF

• “Systematic”
Password Managers

Lie et al. (2014)

• Relationship to our work
  – identified attacks to obtain password ciphertexts
    • CSRF
• “Systematic”

• Our goals
  – systematic analysis of TOTP 2FA apps
  – more technical detail to allow replication

Belenko and Sklyarov (2012)

• Analyzed 16 password managers
  – iOS & Blackberry
• **Goal**: brute force master passwords
  – attacker has password database

Belenko and Sklyarov (2012)

• **Findings**: takes only **one day** to brute force master passwords up to 10-15 characters

<table>
<thead>
<tr>
<th>Name</th>
<th>Password verification complexity</th>
<th>Password rate, passwords/sec (est.)</th>
<th>Password length</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keeper® Password &amp; Data Vault</td>
<td>1x MD5</td>
<td>CPU 60 M, GPU 6000 M</td>
<td>14.7</td>
</tr>
<tr>
<td>Password Safe - iPassSafe free version</td>
<td>1x AES-256</td>
<td>CPU 20 M, GPU N/A</td>
<td>12.2</td>
</tr>
<tr>
<td>Strip Lite - Password Manager</td>
<td>4000x PBKDF2-SHA1 + 1x AES-256</td>
<td>CPU 5000, GPU 160 K</td>
<td>10.1</td>
</tr>
</tbody>
</table>

Belenko and Sklyarov (2012)

• Relationship to our work
  – offline brute force attacks
  – attacker has ciphertext

Chatterjee et al. (2015)

- Proposed a novel defense scheme of “Plausible looking decoys”
### Bonneau’s Authentication Framework

<table>
<thead>
<tr>
<th>Category</th>
<th>Sub-Category</th>
<th>IV-A</th>
<th>IV-B</th>
<th>IV-C</th>
<th>IV-D</th>
<th>IV-E</th>
<th>IV-F</th>
<th>IV-G</th>
<th>IV-H</th>
<th>IV-I</th>
<th>IV-J</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password managers</td>
<td>Firefox</td>
<td>[22]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>LastPass</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Proxy</td>
<td>URRSA</td>
<td>[5]</td>
<td>[23]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Impostor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Federated</td>
<td>OpenID</td>
<td>[27]</td>
<td></td>
<td></td>
<td>[43]</td>
<td>[44]</td>
<td>[45]</td>
<td>[46]</td>
<td>[47]</td>
<td>[48]</td>
<td>[49]</td>
</tr>
<tr>
<td></td>
<td>MicrosoftPass</td>
<td></td>
<td></td>
<td></td>
<td>[49]</td>
<td>[50]</td>
<td>[51]</td>
<td>[52]</td>
<td>[53]</td>
<td>[54]</td>
<td>[55]</td>
</tr>
<tr>
<td></td>
<td>Passport</td>
<td></td>
<td></td>
<td></td>
<td>[50]</td>
<td>[51]</td>
<td>[52]</td>
<td>[53]</td>
<td>[54]</td>
<td>[55]</td>
<td>[56]</td>
</tr>
<tr>
<td></td>
<td>Facebook</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Connect</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>BrowserID</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>OTP</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>over email</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Graphical</td>
<td>PCCP</td>
<td>[7]</td>
<td>[47]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PassGo</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cognitive</td>
<td>Gridsure</td>
<td>[30]</td>
<td></td>
<td></td>
<td></td>
<td>[48]</td>
<td>[49]</td>
<td>[50]</td>
<td>[51]</td>
<td>[52]</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(original)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Weinshall</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hopper Blum</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Word Association</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Paper tokens</td>
<td>OTPW</td>
<td>[33]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>S/KEY</td>
<td>[32]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PIN+TAN</td>
<td>[31]</td>
<td>[51]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visual crypto</td>
<td>PassWindow</td>
<td>[52]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hardware tokens</td>
<td>RSA SecurID</td>
<td></td>
<td></td>
<td></td>
<td>[34]</td>
<td>[35]</td>
<td>[36]</td>
<td>[37]</td>
<td>[38]</td>
<td>[39]</td>
<td>[40]</td>
</tr>
<tr>
<td></td>
<td>YubiKey</td>
<td></td>
<td></td>
<td></td>
<td>[35]</td>
<td>[36]</td>
<td>[37]</td>
<td>[38]</td>
<td>[39]</td>
<td>[40]</td>
<td>[41]</td>
</tr>
<tr>
<td></td>
<td>IronKey</td>
<td></td>
<td></td>
<td></td>
<td>[36]</td>
<td>[37]</td>
<td>[38]</td>
<td>[39]</td>
<td>[40]</td>
<td>[41]</td>
<td>[42]</td>
</tr>
<tr>
<td></td>
<td>CAP reader</td>
<td></td>
<td></td>
<td></td>
<td>[37]</td>
<td>[38]</td>
<td>[39]</td>
<td>[40]</td>
<td>[41]</td>
<td>[42]</td>
<td>[43]</td>
</tr>
<tr>
<td></td>
<td>Pico</td>
<td></td>
<td></td>
<td></td>
<td>[38]</td>
<td>[39]</td>
<td>[40]</td>
<td>[41]</td>
<td>[42]</td>
<td>[43]</td>
<td>[44]</td>
</tr>
<tr>
<td>Phone-based</td>
<td>Phoolproof</td>
<td></td>
<td></td>
<td></td>
<td>[36]</td>
<td>[37]</td>
<td>[38]</td>
<td>[39]</td>
<td>[40]</td>
<td>[41]</td>
<td>[42]</td>
</tr>
<tr>
<td></td>
<td>Cronto</td>
<td></td>
<td></td>
<td></td>
<td>[37]</td>
<td>[38]</td>
<td>[39]</td>
<td>[40]</td>
<td>[41]</td>
<td>[42]</td>
<td>[43]</td>
</tr>
<tr>
<td></td>
<td>MP-Auth</td>
<td></td>
<td></td>
<td></td>
<td>[38]</td>
<td>[39]</td>
<td>[40]</td>
<td>[41]</td>
<td>[42]</td>
<td>[43]</td>
<td>[44]</td>
</tr>
<tr>
<td></td>
<td>OTP over SMS</td>
<td></td>
<td></td>
<td></td>
<td>[39]</td>
<td>[40]</td>
<td>[41]</td>
<td>[42]</td>
<td>[43]</td>
<td>[44]</td>
<td>[45]</td>
</tr>
<tr>
<td></td>
<td>Google 2-Step</td>
<td></td>
<td></td>
<td></td>
<td>[40]</td>
<td>[41]</td>
<td>[42]</td>
<td>[43]</td>
<td>[44]</td>
<td>[45]</td>
<td>[46]</td>
</tr>
<tr>
<td>Biometric</td>
<td>Fingerprint</td>
<td>[38]</td>
<td>[39]</td>
<td>[40]</td>
<td>[41]</td>
<td>[42]</td>
<td>[43]</td>
<td>[44]</td>
<td>[45]</td>
<td>[46]</td>
<td>[47]</td>
</tr>
<tr>
<td></td>
<td>Iris</td>
<td>[39]</td>
<td>[40]</td>
<td>[41]</td>
<td>[42]</td>
<td>[43]</td>
<td>[44]</td>
<td>[45]</td>
<td>[46]</td>
<td>[47]</td>
<td>[48]</td>
</tr>
<tr>
<td></td>
<td>Voice</td>
<td>[40]</td>
<td>[41]</td>
<td>[42]</td>
<td>[43]</td>
<td>[44]</td>
<td>[45]</td>
<td>[46]</td>
<td>[47]</td>
<td>[48]</td>
<td>[49]</td>
</tr>
<tr>
<td>Recovery</td>
<td>Personal knowledge</td>
<td>[58]</td>
<td>[59]</td>
<td>[60]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Preference-based</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Social re-auth.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Goals

1. Gather published technical details
   a. Do not start analysis blind
How Authy 2FA Backups Work

1. **Password**
   - Alice

2. **Key = PBKDF2( Password )**
   - Trusted Device

3. **ENC_{\text{key}}( \text{TOTP Secret} )**
   - Authy

https://authy.com/blog/how-the-authy-two-factor-backups-work
Goals

1. Obtain ciphertext.
2. Which fields are not encrypted?
3. Personal information required?
Network Capture

- Take specific actions using the app
  - Add 1\textsuperscript{st} TOTP secret
  - Enable backup
  - Add 2\textsuperscript{nd} TOTP secret
• Authy requires phone & email
  – Even if backup is not enabled
• mitmproxy + cert pinning = 😞
• Used lab-built Android image
  – Lesson learned: communicate early and clearly!
Goals

1. Which crypto is used?
   a. cipher, mode, etc

2. How is decryption verified?
   a. “Sorry, wrong recovery password!”
Static Analysis

Documentation Research
Phase 1

Static Analysis
Phase 3

Network Capture
Phase 2

APK

apktool ➔ .smali ➔ dex2jar ➔ .jar ➔ jd-cmd ➔ .java
Challenge: Obfuscation

- Documentation Research (Phase 1)
- Static Analysis (Phase 3)
- Network Capture (Phase 2)

Duo Mobile
Duo Security, Inc.
Challenge: Obfuscation

Documentation Research

Phase 1

Static Analysis

Phase 3

Phase 2

Network Capture

AUTHY
One App for All your Accounts
### Static Analysis

**Phase 1: Documentation Research**

**Phase 2: Network Capture**

**Phase 3: Static Analysis**

<table>
<thead>
<tr>
<th>Encrypted?</th>
<th>Key derivation</th>
<th>Cipher &amp; mode</th>
<th>Decryption verification?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>AES-CBC</td>
</tr>
<tr>
<td></td>
<td>- PBKDF2</td>
<td>1k rounds</td>
<td>Heuristic: Valid Base32?</td>
</tr>
</tbody>
</table>

**Key Derivation: PBKDF2 with 1k rounds.**
Goals

1. Difficulty of ciphertext => plaintext?
• Adapt password cracking tools to “crack” ciphertexts
  – e.g. Hashcat module framework
How many possible TOTP secrets?
- base32 format will match many key guesses
- attacker forced into an online attack
Goals

1. Diagram the recovery workflow
   a. How could an attacker access the ciphertext?
   b. Opportunities for user to identify/stop the attack?
Authy claims a 24 hour delay
- User sent SMS and email
- Recovery available after only ~10 hours
Recommend Fixes

- **Documentation Research**
  - Phase 1

- **Static Analysis**
  - Phase 3

- **Recovery Workflow Analysis**
  - Phase 5

- **Network Capture**
  - Phase 2

- **Offline ciphertext attack**
  - Phase 4

- **Recommend Fixes**
  - Phase 6
Recommend Fixes

- Encrypt name and issuer fields
- Strengthen key derivation
Thank you!

Please, ask us questions!