Defeating the Secrets of OTP Apps

Dr.-Ing., Michael Spreitzenbarth, Friedrich-Alexander-Universität, Erlangen
// Agenda

- Introduction
- Forensic Use
- Background
- Research
- Results
- Conclusion
// Introduction

• **Information age** requires secure authentication
Introduction

- **Information age** requires secure authentication
- "Bitkom" sets damage caused by **data theft** at yearly € **55** billion (2017, Germany only)
// Introduction

- **Information age** requires secure authentication
- "Bitkom" sets damage caused by **data theft** at yearly **€ 55** billion (2017, Germany only)
- August 2013: Three Billion **Yahoo Accounts** affected
Introduction

- **Information age** requires secure authentication
- "Bitkom" sets damage caused by **data theft** at yearly €**55** billion (2017, Germany only)
- August 2013: Three Billion **Yahoo Accounts** affected
- April 2015: IS Hackers capture **TV5Monde** and spread own messages (password was readable on TV)
// Introduction

• **Information age** requires secure authentication

• "Bitkom" sets damage caused by **data theft** at yearly **€ 55** billion (2017, Germany only)

• August 2013: Three Billion **Yahoo Accounts** affected

• April 2015: IS Hackers capture **TV5Monde** and spread own messages (password was readable on TV)

• July 2017: BKA reports database with 500 million „stolen“ e-mail addresses (incl. passwords)
// Introduction

- **Information age** requires secure authentication
- "Bitkom" sets damage caused by **data theft** at yearly € 55 billion (2017, Germany only)
- August 2013: Three Billion **Yahoo Accounts** affected
- April 2015: IS Hackers capture **TV5Monde** and spread own messages (password was readable on TV)
- July 2017: BKA reports database with 500 million „stolen“ e-mail addresses (incl. passwords)
- May 2018: **Twitter** prompts users to change their passwords (as they saved these **unencrypted**).
// Introduction

- **Information age** requires secure authentication
- "Bitkom" sets damage caused by **data theft** at yearly €55 billion (2017, Germany only)
- August 2013: Three Billion **Yahoo Accounts** affected
- April 2015: IS Hackers capture **TV5Monde** and spread own messages (password was readable on TV)
- July 2017: BKA reports database with 500 million „stolen“ e-mail addresses (incl. passwords)
- May 2018: **Twitter** prompts users to change their passwords (as they saved these **unencrypted**).
- —> Weak PW (user) / **unsalted** Hashes (provider)
// Introduction
Introduction

Wednesday, May 9th, Hamburg
// Introduction

Wednesday, May 9th, Hamburg
// Introduction

„lemotdepassedeyoutube“
Introduction
// Introduction

- **Multi-factor Authentication (MFA)** provides options to overcome the risks presented
// Introduction

- **Multi-factor Authentication (MFA)** provides options to overcome the risks presented
- Factors can be divided into three categories
Introduction

- Multi-factor Authentication (MFA) provides options to overcome the risks presented
- Factors can be divided into three categories
  - "Knowledge" (passwords, user names, PINs)
  - "Being" (e.g. fingerprint, biometric features)
  - "Possession" (hardware token, credit card, key)
// Introduction

- **Multi-factor Authentication (MFA)** provides options to overcome the risks presented
- Factors can be divided into three categories
  - "**Knowledge**" (passwords, user names, PINs)
  - "**Being**" (e.g. fingerprint, biometric features)
  - "**Possession**" (hardware token, credit card, key)
- Classic implementation is **SecurID** token from "RSA"

Wednesday, May 9th, Hamburg
Introduction

- Multi-factor Authentication (MFA) provides options to overcome the risks presented.
- Factors can be divided into three categories:
  - "Knowledge" (passwords, user names, PINs)
  - "Being" (e.g. fingerprint, biometric features)
  - "Possession" (hardware token, credit card, key)
- Classic implementation is SecurID token from „RSA“.
- "Tokenless" MFA is implemented by software.
// Introduction

- **Multi-factor Authentication (MFA)** provides options to overcome the risks presented
- Factors can be divided into three categories
  - "Knowledge" (passwords, user names, PINs)
  - "Being" (e.g. fingerprint, biometric features)
  - "Possession" (hardware token, credit card, key)
- Classic implementation is **SecurID** token from "RSA"
- "Tokenless" MFA is implemented by software
- Popular forms are so-called **2FA** apps für smartphones that generate **OTPs** ("one-time password")
Multi-factor Authentication (MFA) provides options to overcome the risks presented.

Factors can be divided into three categories:

- **Knowledge** (passwords, user names, PINs)
- **Being** (e.g. fingerprint, biometric features)
- **Possession** (hardware token, credit card, key)

Classic implementation is the SecurID token from "RSA".

"Tokenless" MFA is implemented by software.

Popular forms are so-called 2FA apps for smartphones that generate OTPs ("one-time password").
// Introduction

- **Multi-factor Authentication (MFA)** provides options to overcome the risks presented.
- Factors can be divided into three categories:
  - "Knowledge" (passwords, user names, PINs)
  - "Being" (e.g. fingerprint, biometric features)
  - "Possession" (hardware token, credit card, key)
- Classic implementation is the **SecurID** token from "RSA".
- "Tokenless" MFA is implemented by software.
- Popular forms are so-called 2FA apps for smartphones that generate **OTPs** ("one-time passwords").
// Forensic Use
Forensic Use

- Central question of any criminal procedure is „Causality“
// Forensic Use

- Central question of any criminal procedure is „Causality“
- Computer forensic consideration proofs whether the
// Forensic Use

• Central question of any criminal procedure is „Causality“
• Computer forensic consideration proofs whether the court exhibit (i.e. PC) was used as an instrument of crime
// Forensic Use

• Central question of any criminal procedure is „Causality“
• Computer forensic consideration proofs whether the court exhibit (i.e. PC) was used as an instrument of crime
• Consideration literally stops at the „keyboard“
Central question of any criminal procedure is "Causality".
Computer forensic consideration proofs whether the court exhibit (i.e. PC) was used as an instrument of crime.
Consideration literally stops at the "keyboard".
2FA app examination puts the user (perpetrator) into focus.
Central question of any criminal procedure is “Causality“.
Computer forensic consideration proofs whether the court exhibit (i.e. PC) was used as an instrument of crime.
Consideration literally stops at the “keyboard“.
2FA app examination puts the user (perpetrator) into focus.
Otherwise defense strategy could be: “it wasn’t me“.
// Forensic Use

• Central question of any criminal procedure is „Causality“
• Computer forensic consideration proofs whether the court exhibit (i.e. PC) was used as an instrument of crime
• Consideration literally stops at the „keyboard“
• 2FA app examination puts the user (perpetrator) into focus
• Otherwise defense strategy could be: „it wasn’t me“
• However analyzing authentication process closes the gap
// Forensic Use

- Central question of any criminal procedure is "Causality"
- Computer forensic consideration proofs whether the court exhibit (i.e. PC) was used as an instrument of crime
- Consideration literally stops at the "keyboard"
- 2FA app examination puts the user (perpetrator) into focus
- Otherwise defense strategy could be: "it wasn’t me"
- However analyzing authentication process closes the gap
- Chain of evidence could be closed
// Forensic Use
// Forensic Use
// Forensic Use
// Forensic Use

Wednesday, May 9th, Hamburg
// Forensic Use

Wednesday, May 9th, Hamburg
// Forensic Use

Wednesday, May 9th, Hamburg
// Forensic Use

Wednesday, May 9th, Hamburg
// Forensic Use

Wednesday, May 9th, Hamburg
// Forensic Use

Wednesday, May 9th, Hamburg
// Forensic Use

Wednesday, May 9th, Hamburg
// Forensic Use

Wednesday, May 9th, Hamburg
// Forensic Use
// Forensic Use

Wednesday, May 9th, Hamburg
// Forensic Use

127.0.0.1
// Forensic Use

127.0.0.1

Wednesday, May 9th, Hamburg
// Forensic Use
// Forensic Use

Wednesday, May 9th, Hamburg
// Forensic Use

Wednesday, May 9th, Hamburg
// Forensic Use

Wednesday, May 9th, Hamburg
// Forensic Use

Wednesday, May 9th, Hamburg
// Forensic Use

Wednesday, May 9th, Hamburg
// Forensic Use

Wednesday, May 9th, Hamburg
// Forensic Use
// Forensic Use

127.0.0.1

2FA

Wednesday, May 9th, Hamburg
Forensic Use

127.0.0.1

2FA

Wednesday, May 9th, Hamburg
// Forensic Use

Wednesday, May 9th, Hamburg
// Forensic Use

Wednesday, May 9th, Hamburg
// Background
// Background

• Leslie Lamport formulated idea of using OTP in November 1981
// Background

- Leslie Lamport formulated idea of using OTP in November 1981
- $S = H(r_a \parallel ggKW)$, see RFC 2289
// Background

• Leslie Lamport formulated idea of using OTP in November 1981

• \( S = H(r_a \| ggKW) \), see RFC 2289

• Of central importance is the "shared secret" (ggKW), as an essential basis for calculating the OTP
// Background

- Leslie Lamport formulated idea of using OTP in November 1981
- \( S = H(r_a \parallel ggKW) \), see RFC 2289
- Of central importance is the "shared secret" (ggKW), as an essential basis for calculating the OTP
- Three different types can be distinguished:
  - time-controlled method
  - challenge-response controlled method
  - event-driven method
// Background

- Leslie Lamport formulated idea of using OTP in November 1981
- \( S = H(r_a \parallel ggKW) \), see RFC 2289
- Of central importance is the "shared secret" (ggKW), as an essential basis for calculating the OTP
- Three different types can be distinguished:
  - time-controlled method
  - challenge-response controlled method
  - event-driven method
- Security of the 2FA app strongly depends on integrity of the operating system
// Research

Wednesday, May 9th, Hamburg
Research

- The samples (2FA apps) were examined whether they
The samples (2FA apps) were examined whether they
// Research

- The samples (2FA apps) were examined whether they
  - analyse the environmental-integrity during setup
// Research

• The samples (2FA apps) were examined whether they
  • analyse the **environmental-integrity** during setup
  • **encrypt** the „shared secret“ (and how)
The samples (2FA apps) were examined whether they

- analyse the **environmental-integrity** during setup
- **encrypt** the „shared secret“ (and how)
- allow **cloning** of the database (with stored secrets)
The samples (2FA apps) were examined whether they

• analyse the **environmental-integrity** during setup
• **encrypt** the „shared secret“ (and how)
• allow **cloning** of the database (with stored secrets)
• disclose secrets due to **network-traffic** caused
// Research

- The samples (2FA apps) were examined whether they
  - analyse the **environmental-integrity** during setup
  - **encrypt** the „shared secret“ (and how)
  - allow **cloning** of the database (with stored secrets)
  - disclose secrets due to **network-traffic** caused
  - enable **stealing** of „shared secret“

Wednesday, May 9th, Hamburg
// Research
// Research

• Examination procedure
// Research

• Examination procedure
  • Determine most **popular 2FA** apps (cf. downloads)
// Research

• Examination procedure
  • Determine most **popular 2FA** apps (cf. downloads)
  • **Install** the apps via Google PlayStore
// Research

• Examination procedure
  • Determine most **popular 2FA** apps (cf. downloads)
  • **Install** the apps via Google PlayStore
  • Save "**zero evidence**" with a script (**before** execution)
// Research

- Examination procedure
  - Determine most **popular 2FA** apps (cf. downloads)
  - **Install** the apps via Google PlayStore
  - Save "**zero evidence**" with a script (**before** execution)
  - Record **network-traffic** **during** execution

Wednesday, May 9th, Hamburg
// Research

- Examination procedure
  - Determine most popular 2FA apps (cf. downloads)
  - **Install** the apps via Google PlayStore
  - Save "**zero evidence**" with a script (**before** execution)
  - Record **network-traffic** **during** execution
  - **Re-backup** after execution and configuration
// Research

- Examination procedure
  - Determine most **popular 2FA** apps (cf. downloads)
  - **Install** the apps via Google PlayStore
  - Save "**zero evidence**" with a script (**before** execution)
  - Record **network-traffic** **during** execution
  - **Re-backup** after execution and configuration
  - Calculate the **differences** of both snapshots
Research

- Examination procedure
  - Determine most **popular 2FA** apps (cf. downloads)
  - **Install** the apps via Google PlayStore
  - Save "**zero evidence**" with a script (**before** execution)
  - Record **network-traffic** **during** execution
  - **Re-backup** after execution and configuration
  - Calculate the **differences** of both snapshots
  - **Analysis** of the collected data
Research

1. Examination procedure
   - Determine most popular 2FA apps (cf. downloads)
   - **Install** the apps via Google PlayStore
   - Save "zero evidence" with a script (before execution)
   - Record network-traffic during execution
   - **Re-backup** after execution and configuration
   - Calculate the **differences** of both snapshots
   - **Analysis** of the collected data
   - **Verification** of the results using tests in AVD

Wednesday, May 9th, Hamburg
### Results

Sample: „Google Authenticator“

<table>
<thead>
<tr>
<th>Icon</th>
<th>Anwendung</th>
<th>Version</th>
<th>Hash (MD5)</th>
<th>Größe</th>
</tr>
</thead>
<tbody>
<tr>
<td>![icon]</td>
<td>Google Authenticator</td>
<td>4.74</td>
<td>2658652deea2a274c90e111135634e1f</td>
<td>6,9 MB</td>
</tr>
</tbody>
</table>

**Programmpfad:** /data/data/com.google.android.apps.authenticator2

**UID:** u0_a128

**Ablage Shared Secret:** {app_verz}/databases/databases (SQLite)

**Format des TOTP:** Dezimal (6-stellig)

**Shared Secret:** rffl4xngz3bzhe5g7fhji4rza
Results

Sample: „Google Authenticator“

<table>
<thead>
<tr>
<th>Icon</th>
<th>Anwendung</th>
<th>Version</th>
<th>Hash (MD5)</th>
<th>Größe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Authenticator</td>
<td>4.74</td>
<td>2658652deea2a274c90e111135634e1f</td>
<td>6,9 MB</td>
<td></td>
</tr>
</tbody>
</table>

Programmpfad: `/data/data/com.google.android.apps.authenticator2`

UID: `u0_a128`

Ablage Shared Secret: `{app_verz}/databases/databases (SQLite)`

Format des TOTP: Dezimal (6-stellig)

Shared Secret: `rffl4xngz3bzhe5g7fhji4rzra`

```
42:GA philip$ adb pull /data/data/com.google.android.apps.authenticator2/databases/databases/
42:GA philip$ sqlite3 ./databases "select * from accounts" > google_authenticator_secret.txt

42:GA philip$ cat google_authenticator_secret.txt 1|Dropbox| rffl4xngz3bzhe5g7fhji4rzra|0|0|0||Dropbox
```

42:GA philip$
// Results

```bash
POST https://172.217.23.174/auth
  → 200 text/plain 266b 327ms

  → 200 application/x-protobuf 610b 426ms

GET https://172.217.23.1611/proxy/RmHevzGfWbmd87_FmcOWySSx1f5WGNu7rNiv7_Zq50Ys8UvbUmv9aQfdAqp
  → 200 image/png 18.5k 186ms

  → 200 application/x-protobuf 48b 151ms

POST https://172.217.23.174/auth
  → 200 text/plain 265b 238ms

GET https://66.102.1.102/history/api/lookup?client=web_app
  → 200 application/javascript 55b 235ms

GET https://66.102.1.102/history/api/lookup?client=device
  → 200 application/javascript 55b 220ms
```

Wednesday, May 9th, Hamburg
// Results

Sample: "Google Authenticator"

```bash
42:GA philip$ adb pull /data/data/com.google.android.apps.authenticator2/databases/databases/
42:GA philip$ sqlite3 ./databases "select * from accounts" > google_authenticator_secret.txt
42:GA philip$ cat google_authenticator_secret.txt
```

```
<table>
<thead>
<tr>
<th>Dropbox</th>
<th>rffl4xngz3bzhe5g7fhji4rzra</th>
</tr>
</thead>
</table>
```

Wednesday, May 9th, Hamburg
## Results

Sample: „Duo Mobile“

<table>
<thead>
<tr>
<th>Icon</th>
<th>Anwendung</th>
<th>Version</th>
<th>Hash (MD5)</th>
<th>Größe</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Duo Logo" /></td>
<td>Duo Mobile</td>
<td>3.16.1</td>
<td>afe74d12a8f4f9cb8e107727d0010727</td>
<td>12,3 MB</td>
</tr>
</tbody>
</table>

- **Programmpfad:** /data/data/com.duosecurity.duomobile
- **UID:** u0_a156
- **Ablage Shared Secret:** `{app_verz}/files/duokit/accounts.json`
- **Format des TOTP:** Dezimal (6-stellig)
- **Shared Secret:** hvwb64jexhst5xg2rg5j5nfwci
// Results

Sample: „Duo Mobile“

<table>
<thead>
<tr>
<th>Icon</th>
<th>Anwendung</th>
<th>Version</th>
<th>Hash (MD5)</th>
<th>Größe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duo</td>
<td>Duo Mobile</td>
<td>3.16.1</td>
<td>afe74d12a8f4f9cb8e107727d0010727</td>
<td>12,3 MB</td>
</tr>
</tbody>
</table>

Programmpfad: /data/data/com.duosecurity.duomobile/files/duokit/accounts.json

42:Duo philip$ adb pull /data/data/com.duosecurity.duomobile/files/duokit/accounts.json

42:Duo philip$ cat accounts.json

```json
[
  {
    "name": "philipevalu@wegwerfemail.info", "otpGenerator": {
      "otpSecret": "HVWB64JEXHST5XG2RG5J5NFWC1"
    },
    "logoUri": "android.resource://com.duosecurity.duomobile/drawable/ic_dropbox"
  }
]
```
Sample: „Duo Mobile“

42:Duo philip$ adb pull /data/data/com.duosecurity.duomobile/files/duokit/accounts.json

42:Duo philip$ cat accounts.json

```json
[
  {
    "name": "philipevalu@wegwerfemail.info",
    "otpGenerator": {
      "otpSecret": "HVWB64JEXHST5XG2RG5J5NFWCI"
    },
    "logoUri": "android.resource://com.duosecurity.duomobile/drawable/ic_dropbox"
  }
]
```

Wednesday, May 9th, Hamburg
### Results

X = Yes; O = No; - = unwanted behavior; + = wanted behavior

<table>
<thead>
<tr>
<th>2FA App Name</th>
<th>Cloning Possible</th>
<th>Encrypted Secret</th>
<th>Device Integrity Check</th>
<th>PIN Protection</th>
<th>Secure SSL-Connection</th>
<th>Secure OTP-Push</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Authenticator</td>
<td>X-</td>
<td>O-</td>
<td>O-</td>
<td>O-</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Microsoft Authenticator</td>
<td>X-</td>
<td>O-</td>
<td>O-</td>
<td>O-</td>
<td>X+</td>
<td>O-</td>
</tr>
<tr>
<td>Authy 2-Factor Authentication</td>
<td>O+</td>
<td>O-</td>
<td>O-</td>
<td>X+</td>
<td>X+</td>
<td>N/A</td>
</tr>
<tr>
<td>DUO Mobile</td>
<td>X-</td>
<td>O-</td>
<td>X+</td>
<td>O-</td>
<td>X+</td>
<td>X+</td>
</tr>
<tr>
<td>FreeOTP</td>
<td>X-</td>
<td>O-</td>
<td>O-</td>
<td>O-</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Sophos Authenticator</td>
<td>X-</td>
<td>O-</td>
<td>O-</td>
<td>O-</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Push Authenticator</td>
<td>X-</td>
<td>O-</td>
<td>O-</td>
<td>O-</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>OTP Authenticator</td>
<td>O+</td>
<td>O-</td>
<td>O-</td>
<td>O-</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Yandex.Key</td>
<td>O+</td>
<td>X+</td>
<td>O-</td>
<td>X+</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Symantec VIP Access</td>
<td>O+</td>
<td>X+</td>
<td>O-</td>
<td>O-</td>
<td>X+</td>
<td>X+</td>
</tr>
<tr>
<td>2FA Token</td>
<td>X-</td>
<td>O-</td>
<td>O-</td>
<td>O-</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Launchkey</td>
<td>X-</td>
<td>N/A</td>
<td>O-</td>
<td>X+</td>
<td>X+</td>
<td>N/A</td>
</tr>
<tr>
<td>CyAuth Cylocklite</td>
<td>X-</td>
<td>X+</td>
<td>O-</td>
<td>O-</td>
<td>X+</td>
<td>N/A</td>
</tr>
<tr>
<td>Topicus KeyHub</td>
<td>X-</td>
<td>O-</td>
<td>O-</td>
<td>O-</td>
<td>X+</td>
<td>N/A</td>
</tr>
<tr>
<td>Latch</td>
<td>O+</td>
<td>X+</td>
<td>O-</td>
<td>O-</td>
<td>O-</td>
<td>N/A</td>
</tr>
<tr>
<td>Okta Verify</td>
<td>O+</td>
<td>X+</td>
<td>O-</td>
<td>O-</td>
<td>X+</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Wednesday, May 9th, Hamburg
// Results
// Results

• Security implementations vary greatly
Results

- Security implementations vary greatly
- 50% of apps do **not** encrypt „shared secret“
// Results

- Security implementations vary greatly
- 50 % of apps do not encrypt „shared secret“
- 12.5 % of the apps only use other notation
Results

- Security implementations vary greatly
- 50% of apps do **not** encrypt „shared secret“
- 12.5% of the apps **only** use other **notation**
- Security strongly **dependent** on OS

Wednesday, May 9th, Hamburg
// Results

- Security implementations vary greatly
- 50% of apps do not encrypt „shared secret“
- 12.5% of the apps only use other notation
- Security strongly dependent on OS
- 56% of the apps allow copying the DB
Results

- Security implementations vary greatly
- 50% of apps do not encrypt „shared secret“
- 12.5% of the apps only use other notation
- Security strongly dependent on OS
- 56% of the apps allow copying the DB
- Only about 1/5 of the apps offer PIN protection
Results

- Security implementations vary greatly
- 50% of apps do **not** encrypt „shared secret“
- 12.5% of the apps **only** use other **notation**
- Security strongly **dependent on OS**
- 56% of the apps allow **copying the DB**
- Only about 1/5 of the apps offer PIN protection
- Only 44% do not generate **network traffic**
Conclusion
// Conclusion

- Pro 2FA-App
// Conclusion

• Pro 2FA-App

• Comprehensive use of 2FA is recommended
• 2FA app reduces number of devices to carry
• SM have more (transparent) data/sensors
// Conclusion

• Pro 2FA-App

• Comprehensive use of 2FA is recommended
• 2FA app reduces number of devices to carry
• SM have more (transparent) data/sensors

• Pro HW-Token
// Conclusion

• Pro 2FA-App

  • Comprehensive use of 2FA is recommended
  • 2FA app reduces number of devices to carry
  • SM have more (transparent) data/sensors

• Pro HW-Token

  • HW token self-sufficient -> no area of attack via remote
  • "Stealing" the "shared secret" undermines factor property
  • 2FA apps persuade to use a single device only
  • Spread of specific malware threatens 2FA apps
  • FIDO-Alliance combines secure hardware and PKI
Thank you for your attention
Questions? 42!