Extracting All Your Secrets: Vulnerabilities in Android Password Managers

Stephan Huber, Siegfried Rasthofer, Steven Arzt

Fraunhofer SIT
Stephan

- Mobile Security Researcher at Fraunhofer SIT
- Enjoys teaching students in Android (app) hacking
- Twitter: @teamsik

Siegfried

- Malware and Vulnerability Researcher at Fraunhofer SIT
- Founder of CodeInspect
- Web: www.rasthofer.info
- Twitter: @teamsik
Acknowledgements

• Benedikt Hiemenz
• Daniel Hitzel
• Daniel Magin
• Joseph Varghese
• Julien Hachenberger
• Max Kolhagen
• Michael Tröger
• Philipp Roskosch
• Wittmann Andreas
90 Accounts

*https://thycotic.com
Password Manager

Everything you put in Keepsafe is encrypted on your device using the cipher AES-256, considered among the most secure in the world and labeled “bank-level” or “military-grade” by many. Our back-ups are also encrypted and there are multiple layers of encryption keys, which are managed by your device and by the back-up system. No Keepsafe employee will access or view your content and we have systems in place that prevent this.

Source: https://www.getkeepsafe.com/about.html
<table>
<thead>
<tr>
<th>App</th>
<th>GooglePlay Downloads</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keeper</td>
<td>10 – 50 m</td>
</tr>
<tr>
<td>Keepsafe</td>
<td>10 – 50 m</td>
</tr>
<tr>
<td>1Password</td>
<td>1 – 5 m</td>
</tr>
<tr>
<td>Dashlane</td>
<td>1 – 5 m</td>
</tr>
<tr>
<td>Lastpass</td>
<td>1 – 5 m</td>
</tr>
<tr>
<td>Avast</td>
<td>0.5 – 1 m</td>
</tr>
<tr>
<td>MyPasswords</td>
<td>0.5 – 1 m</td>
</tr>
<tr>
<td>F-Secure</td>
<td>100 – 500 k</td>
</tr>
<tr>
<td>PasswordManger</td>
<td>50 – 100 k</td>
</tr>
</tbody>
</table>
Password Manager

- Secure Synchronization
- Confidential Password Storage
- Comfort Feature (PIN login)
- Autofill
- Custom Browser
Internet App Account Manager (master password)

File (master password)

Database

user1:pw1
user2:pw2
...

Account Manager (master password)

PW-Manager App

PC

Fraunhofer SIT

team[SIK]
“No-root scenario”
Internet

App

Account Manager (master password)

File (master password)

PW-Manager App

user1:pw1
user2:pw2
...

Database

File

App

PW-Manager App

Internet
Manual Filling

Password Manager

user
****
user1
****
user2
****
user3
****

Clipboard

http://twitter.com/login

Log in to Twitter
Phone, email, or username
Password
Log in

Forgot password? · Sign up for Twitter
Manual Filling - Attack

Password Manager

user:pass

clipboard „sniffer“- app
(no permissions required)

Receiver Apps
Automatically Filling

Password Manager

- user ****
- user1 ****
- user2 ****
- user3 ****
“An accessibility service is an application that provides user interface enhancements to assist users with disabilities, or who may temporarily be unable to fully interact with a device. For example, users who are driving, taking care of a young child, or attending a very loud party might need additional or alternative interface feedback.”
Automatically Filling

Password Manager

user
****

user1
****

user2
****

user3
****

Twitter-App
(com.twitter.android)
Automatically Filling

Password Manager

Name of website
Twitter

Website address
twitter.com

Username
tmstest1

Password

GENERATE PASSWORD

Twitter-App (com.twitter.android)
Automatically Filling - Attack

Name of website
Twitter

Website address
twitter.com

Username
tmstest1

Password
...........

GENERATE PASSWORD

com.twitter.twitterleak

find field
textPassword

inject credentials

prefix matches

com.twitter

reverse
DEMO TIME!
File (master password)

Database

user1:pw1
user2:pw2
...

PW-Manager App

Account Manager (master password)

Internet

App

PC
Use Backup Function

```
adb backup com.fsecure.key

* https://github.com/nelenkov/android-backup-extractor

tar -xvf mybackup.tar

cat KeyStorage.xml

<string name="master_password">secretpass</string>
```
File (master password)

PW-Manager App

user1:pw1
user2:pw2
...

Database

Account Manager (master password)

Internet

PC
Log in to Twitter

Phone, email, or username

Password

Log in

Forgot password? · Sign up for Twitter

API accessing browser elements

PW Manager

credentials
API accessing browser elements

Pw Manager

credent...
Password Manager

Custom Browser

http://twitter.com/login

Log in to Twitter

user1

****

Log in

Forgot password? · Sign up for Twitter
Password Manager

Custom Browser

http://twitter.com/login

Log in to Twitter

Phone, email, or username

Password

Log in

Forgot password? · Sign up for Twitter
Details about the Browser

• Browser is part of the app

• Running in the same process, part of the sandbox

• Based on WebView API

• Supports file:/// URI *

*until Android 6
NOT A COOKIE, CREDENTIALS!
This XML file does not appear to have any style information associated with it. The document tree is shown below.

```xml
<map>
  <boolean name="9e907907d6f425ba97f7203533ea1204" value="true"/>
  <string name="edbbbc9eb6fe5b240cf4d8a084d9ef0a">PLAYSTORE</string>
  <boolean name="9e7df400f05775f556fd2b442cdc557" value="true"/>
  <int name="2f489516ce7edc99ef89d888ec9f3f9a1" value="0"/>
  <boolean name="bcffca8558d146de09ad1b1a1cc069fc" value="true"/>
  <long name="credentials_timestamp" value="1474018940377"/>
  <string name="2e5d8aa3d6a8ef34ca513120f9dad51">mDBu6bclc+n+TKCboLzp}ZqoeRdrRxUK/8JqMV7c1LV0MzD/j32tWdQdr36iwL4yuR45VAwb/6t3Hq20jCr1t5AQA=</string>
  <long name="3164a9674a6ff29071c3d43f08caaed" value="147401841304"/>
  <boolean name="04dc344efa56535cbbe1631bcb2dde1" value="true"/>
</map>
```

\[ \text{md5(,,pincodeValue,,)} \ast \text{base64(\text{encr(key, PIN)})} \]

*obfuscated attribute values (for this example)
ALL THE STUFF IS ENCRYPTED

WHERE IS THE KEY ??
public abstract class LPCommon {
    // first part of the key
    protected static String aA = "ldT52Fjsnjd4390";
    // second part of the key
    protected static String aB = "89y23489h989fFFF";

    AES-Key: ldT52Fjsnjd439089y23489h989fFFF
Account Manager (master password)

File (master password)

Database

user1:pw1
user2:pw2
...

PW-Manager App

Internet

App

PC
Android AccountManager

• „This class provides access to a centralized registry for the user’s online accounts ...“

• SQLITE Database for storing tokens or temporary Credentials

• API provides access for Application

/data/system/users/0  # ls -l accounts.db
-rw-rw---- system system 241664 2017-04-03 10:58 accounts.db
“With this in mind, you shouldn't pass the user's actual password to AccountManager.addAccountExplicitly(). Instead, you should store a cryptographically secure token that would be of limited use to an attacker.

If your user credentials are protecting something valuable, you should carefully consider doing something similar.”

Quote google developer (AccountManager)
https://developer.android.com/training/id-auth/custom_auth.html
DEMO TIME!
Target App

com.dashlane
email:passwd

AccountManager

accounts.db
Target App

com.dashlane
email:passwd

Attacker App

com.dashlane
mail1:pass1

account type

android

AccountManager

UID:123
accounts.db

email:passwd

*https://thenounproject.com/term/grab/121228/
Attacker App

com.dashlane
mail1:pass1

Target App

com.dashlane
eMail:passwd

AccountManager

System

android

accounts.db

email:passwd

UID:123

UID:456

COLLISION!

account type

account type
Attacker App

com.dashlane

mail1:pass1

account type

android

System

AccountManager

accounts.db

email:passwd

Fraunhofer

SIT

43
Read Account Data

Attacker App

com.dashlane
email:passwd

account type

android System

AccountManager

UID:456

accounts.db

email:passwd
Writing into AccountManager

```java
try {
    Account account = new Account("teamsiksm3@gmx.de", "com.dashlane");
    AccountManager acmanager = AccountManager.get(getApplicationContext());

    //requires permission android.permission.AUTHENTICATE_ACCOUNTS
    acmanager.addAccountExplicitly(account, "DUMMY", null);
}
```

Reading form AccountManager

```java
try {
    AccountManager acmgr = AccountManager.get(getApplicationContext());
    Account[] accounts = acmgr.getAccountTypesByType("com.dashlane");
    for (Account a : accounts) {
        String password = AccountManager.get(getApplicationContext()).getPassword(a);
        ...
    }
} catch (Exception e) {
    e.printStackTrace();
}
```
Further Fails

• **Custom** crypto-algorithm
• AES in ECB mode for database encryption
• Delivered *browser* do not consider *subdomains* in form fields
• **Data leakage** in browser
• **Custom** transport security
Improvements

• Use Android **KeyStore** (since Android 6 AES key support)
• Use **key derivation** function (e.g. API **PBKDF2**, **FB conceal**)
• **NO** hardcoded keys
• Use **AES/CBC** or **AES/GCM**
• **Do not** abuse **AccountManager**
<table>
<thead>
<tr>
<th></th>
<th>Keeper</th>
<th>Lastp</th>
<th>1Pass</th>
<th>MyPass</th>
<th>Avast</th>
<th>F-Sec</th>
<th>Keeps.</th>
<th>PwMgr</th>
<th>MyPass</th>
<th>Dash</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master/PIN</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Hardcoded Key</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Sandbox Bypass</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Side channel</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Subdomain</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Data leakage</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Partial encryption</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broken sync.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

www.sit4.me/pw-manager
Summary

• We showed several **non root** attacks on Android password managers

• **Convenience** functions **weaken or destroy** security

• All findings were **reported** and **fixed**
Stephan Huber  
Email: stephan.huber@sit.fraunhofer.de

Dr. Siegfried Rasthofer  
Email: siegfried.rasthofer@sit.fraunhofer.de

Twitter: @teamsik  
Website: www.team-sik.org