OWASP
AppSec EU
Belfast
8th to 12th
of May
2017
Waterfront
Conference
Center

The Key Under the Doormat

Design Flaws and Vulnerabilities in Android Password Manager Applications

Stephan Huber, Steven Arzt, Siegfried Rasthofer

Stephan

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

Steven

- Researcher (Security & Code Analysis)
- Maintainer of FlowDroid and Soot
- Twitter: @teamsik

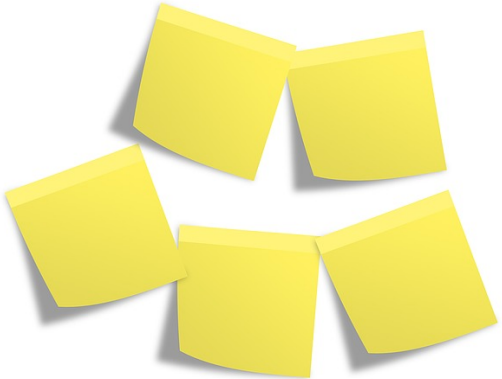
Fraunhofer SIT

team [SIK]

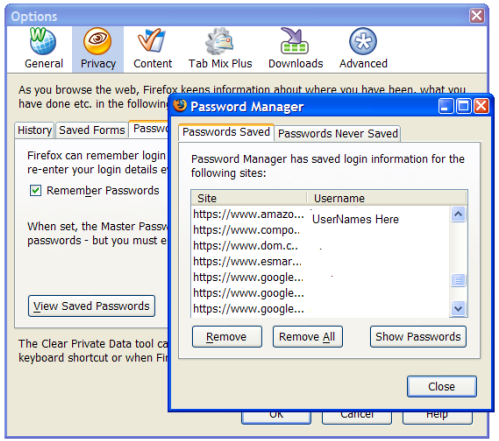
Acknowledgements

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

*https://thycotic.com



Note



Internal Password Manager

3rd Party 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

No break, but bypass !

App	Google Play Downloads
Keeper	10 – 50 m
Keepsafe	10 – 50 m
1Password	1 – 5 m
Dashlane	1 – 5 m
Lastpass	1 – 5 m
Avast	0.5 – 1 m
MyPasswords	0.5 – 1 m
F-Secure	100 – 500 k
PasswordManger	50 – 100 k

Secure Synchronization

Confidential Password Storage

Password Manager

Autofill

Comfort Feature (PIN login)

Custom Browser

Secure Synchronization

Confidential Password Storage

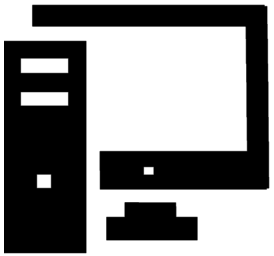
Autofill

Comfort Feature (PIN Login)

Password Manager

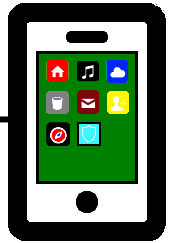
Custom Browser

Backup Problem



adb

backup com.passmger.app



AndroidManifest.xml:
android:allowBackup="true"

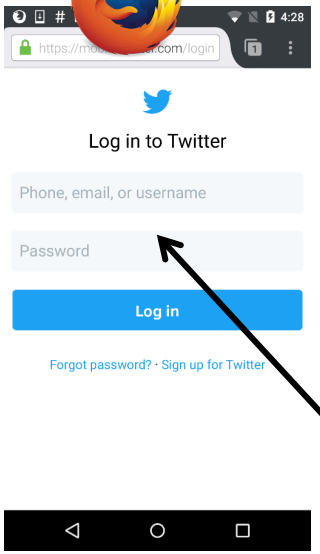
*

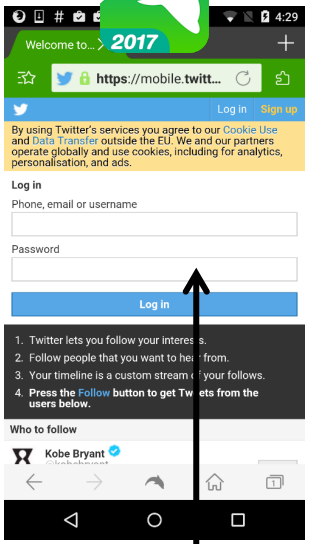
```
tar -xvf mybackup.tar
cat KeyStorage.xml
```

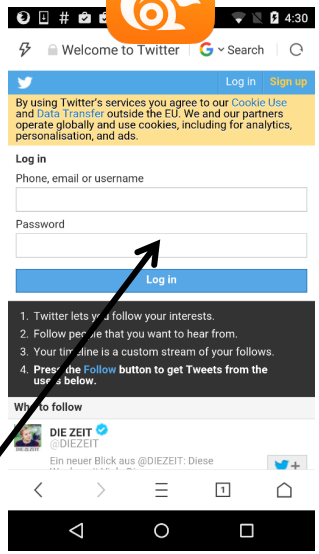
```
<string name="master_password">secretpass</string>
```

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

Sandbox Bypass



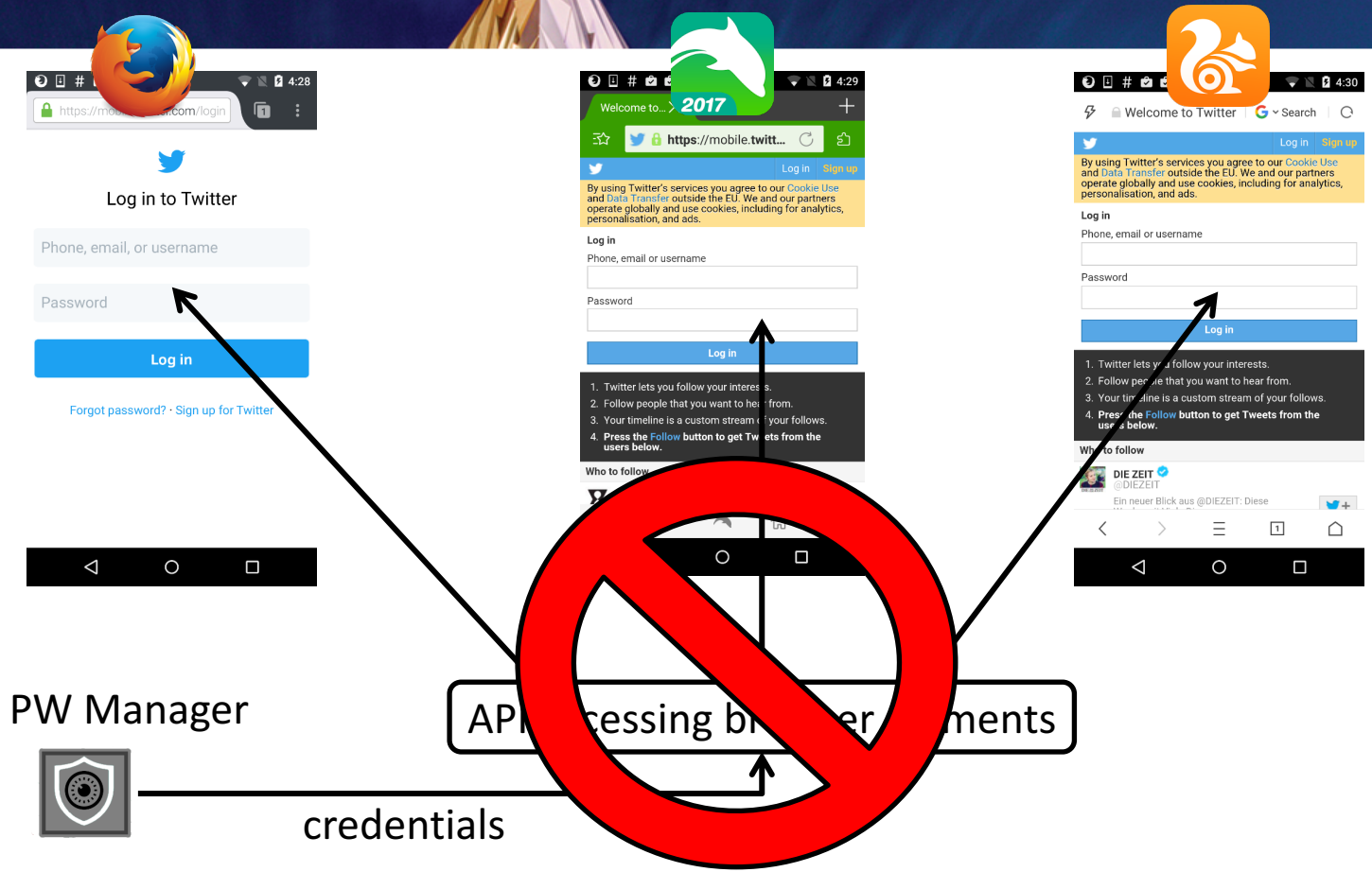




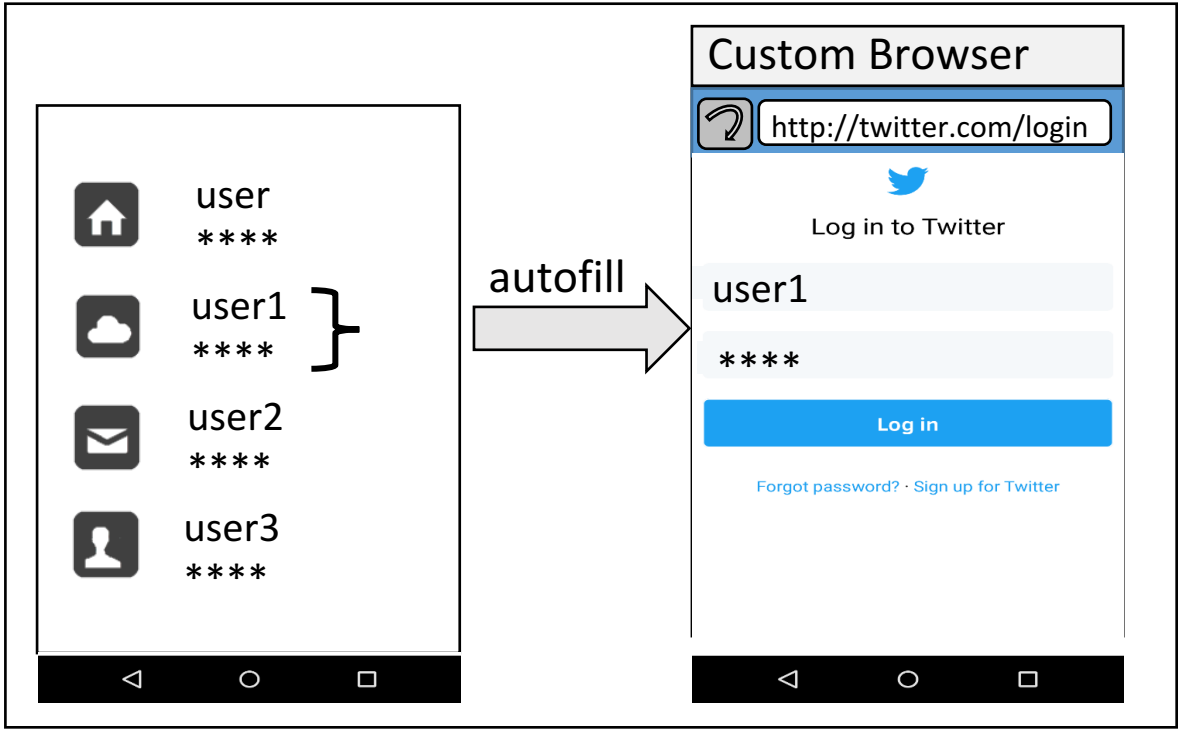
PW Manager

API accessing browser elements

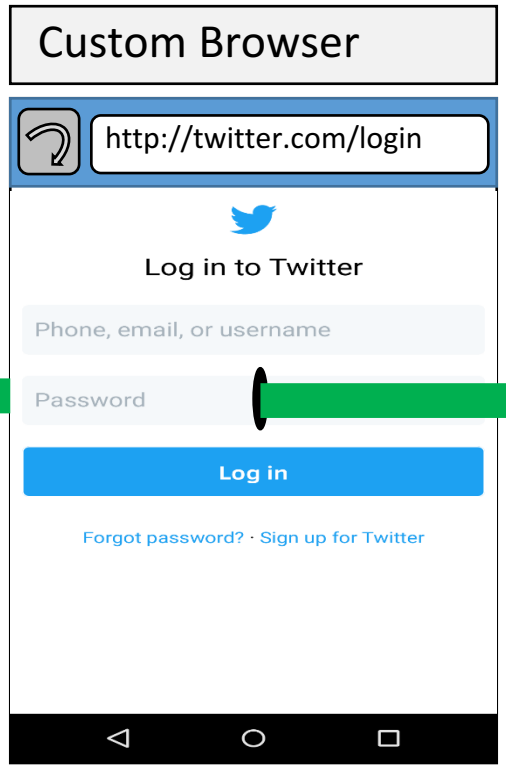
credentials


Log in to Twitter
Phone, email, or username
Password
Log in
Forgot password? · Sign up for Twitter
Welcome to...
https://mobile.twitt...
Log in
Sign up
By using Twitter's services you agree to our Cookie Use and Data Transfer outside the EU. We and our partners operate globally and use cookies, including for analytics, personalisation, and ads.
Log in
Phone, email or username
Password
Log in
1. Twitter lets you follow your interests.
2. Follow people that you want to hear from.
3. Your timeline is a custom stream of your follows.
4. Press the Follow button to get Tweets from the users below.
Who to follow
Welcome to Twitter
Search
Log in
Sign up
By using Twitter's services you agree to our Cookie Use and Data Transfer outside the EU. We and our partners operate globally and use cookies, including for analytics, personalisation, and ads.
Log in
Phone, email or username
Password
Log in
1. Twitter lets you follow your interests.
2. Follow people that you want to hear from.
3. Your timeline is a custom stream of your follows.
4. Press the Follow button to get Tweets from the users below.
Who to follow
DIE ZEIT
@DIEZEIT
Ein neuer Blick aus @DIEZEIT: Diese
PW Manager
credentials

Password Manager



Password Manager



- Browser is **part** of the app
- => it is running in the **same process**, it is part of the **sandbox**
- Browser is based on **WebView**
- **WebView** supports **file://** URI

file:///data/data/package.name/shared_prefs/passwords_pref.xml

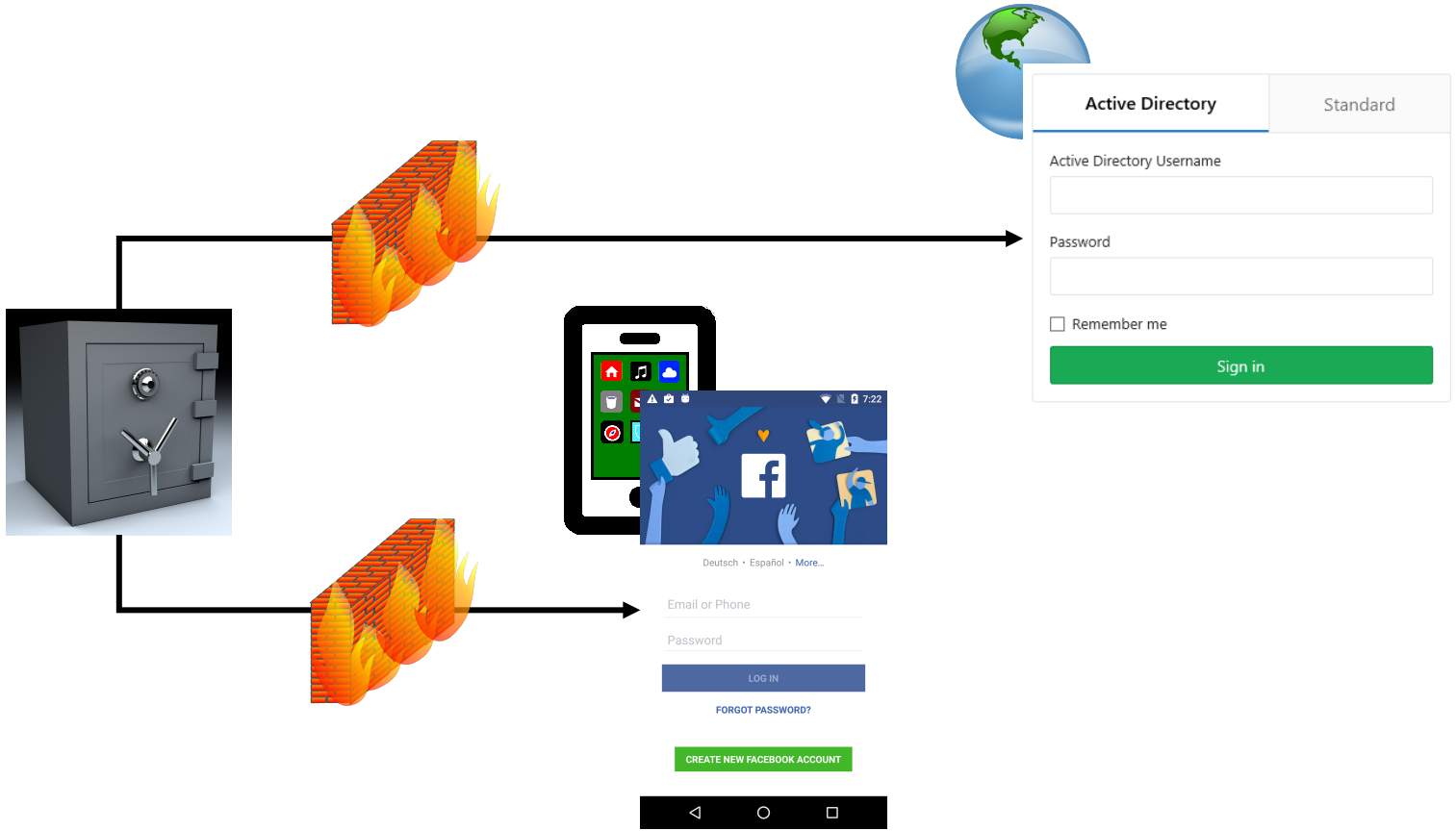
```
<map>
  <boolean name="9e907907d6f425ba97f7203533ea1204" value="true"/>
  <string name="edbbbc9eb6fe5b240cf4d8a084d9ef0a">PLAYSTORE</string>
  <boolean name="9e7dbf400f05775f556fd2b442cdc557" value="true"/>
  <int name="2f489516ce7edc99ef89d88ce9f3ffa1" value="0"/>
  <boolean name="bcffca8558d146de09ad1b1a1cc0e9fc" value="true"/>
  <long name="credentials_timestamp" value="1474018940377"/>
  <string name="2e5d8aa3dfa8ef34ca5131d20f9dad51">
    +F4dkegeBO2WMP8jheQkkSzfw237ztAZL6ne9RYV5jNLVOMz9xgSCLtvI/TVW/3NgrDOge4c8qsJhRSfpHNhWQvjwKbp8vJQYd5AwhVCtGlk6
  </string>
  <long name="3164a9674a6ff29071c3d43f0d8caaed" value="1474018411304"/>
  <string name="d2d8e0ab85be1ce1b690efac17be5b16">
    NBDBu6bclc+n+TKCbzLzpjZqoerErdRxUK/8JqMV7C1LVOMzD/j32tWdQdr36iWL4yuR4SVAWb/6t3Hq2OjCrit5AQA=
  </string>
  <boolean name="04dc344eefa56535cbbe1631bcb2dde1" value="true"/>
```

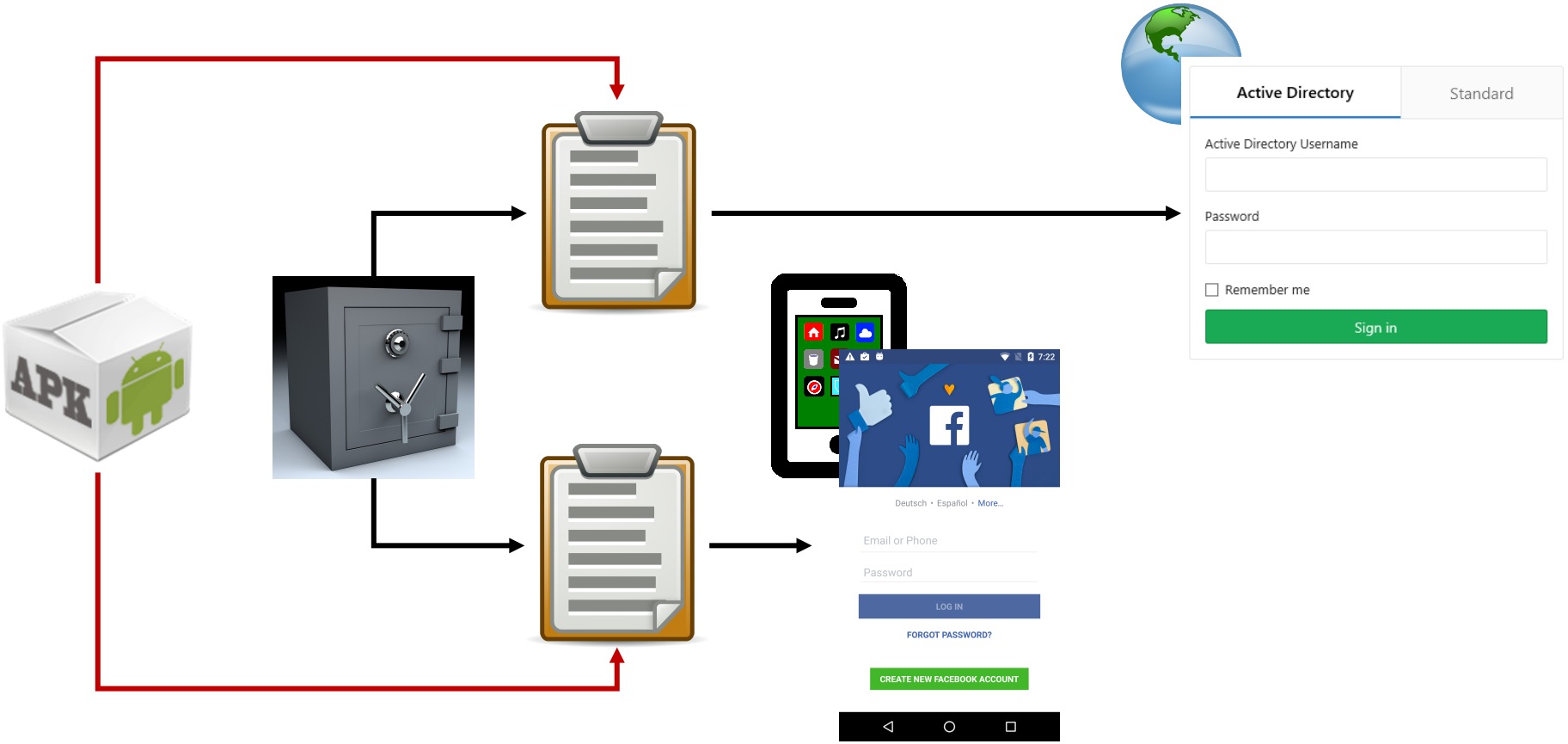
md5(„pincodeValue“) *

base64(encr(key, PIN))

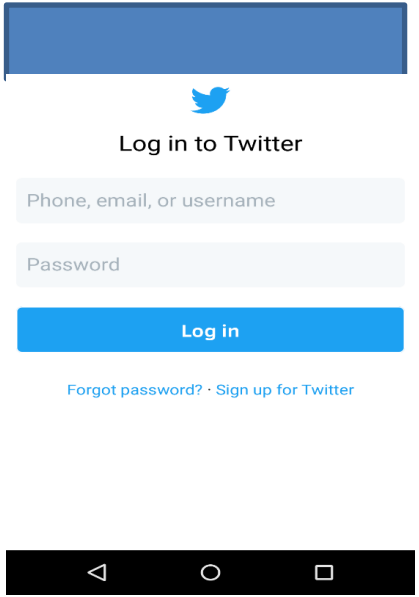
*obfuscated attribute values (for this example)

Data Exchange Problem

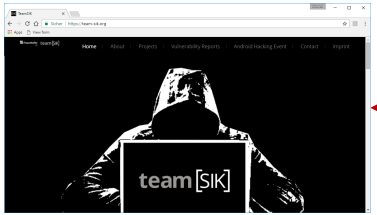

Active Directory
Standard
Active Directory Username
Password
Remember me
Sign in
7:22
Deutsch • Español • More...
Email or Phone
Password
LOG IN
FORGOT PASSWORD?
CREATE NEW FACEBOOK ACCOUNT


APK
Active Directory
Standard
Active Directory Username
Password
Remember me
Sign in
7:22
Deutsch • Español • More...
Email or Phone
Password
LOG IN
FORGOT PASSWORD?
CREATE NEW FACEBOOK ACCOUNT

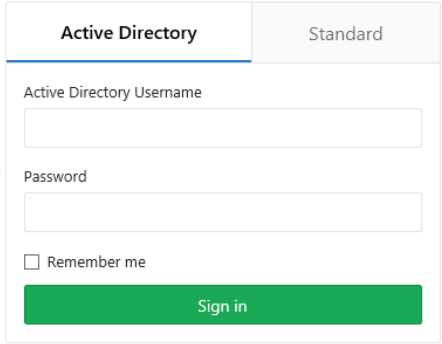
"An accessibility service is an application that provides user interface enhancements to assist users with disabilities, or who may temporarily be unable to fully interact with a device. For example, users who are driving, taking care of a young child or attending a very loud party might need additional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



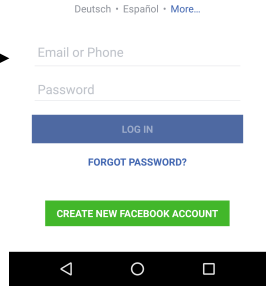
Source: https://developer.android.com

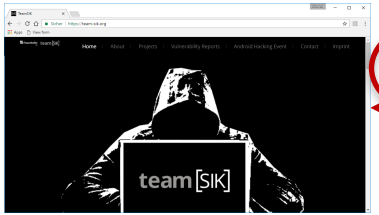

team [SIK]

APK


Active Directory
Standard
Active Directory Username
Password
Remember me
Sign in

7:22


Deutsch • Español • More...
Email or Phone
Password
LOG IN
FORGOT PASSWORD?
CREATE NEW FACEBOOK ACCOUNT



http://login.foo.com

Active Directory | Standard

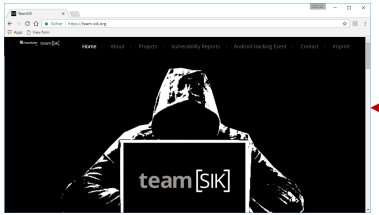
Active Directory Username

Password

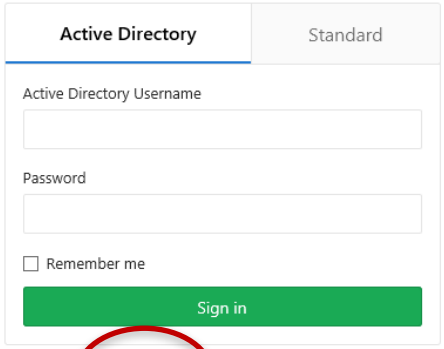
Remember me

Sign in

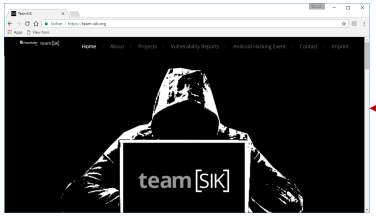
https://login.foo.com



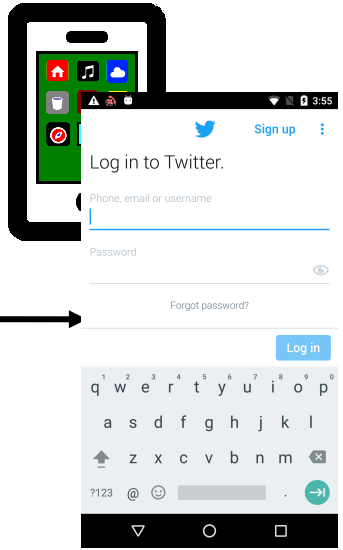
https://b.wordpress.com



https://a.wordpress.com

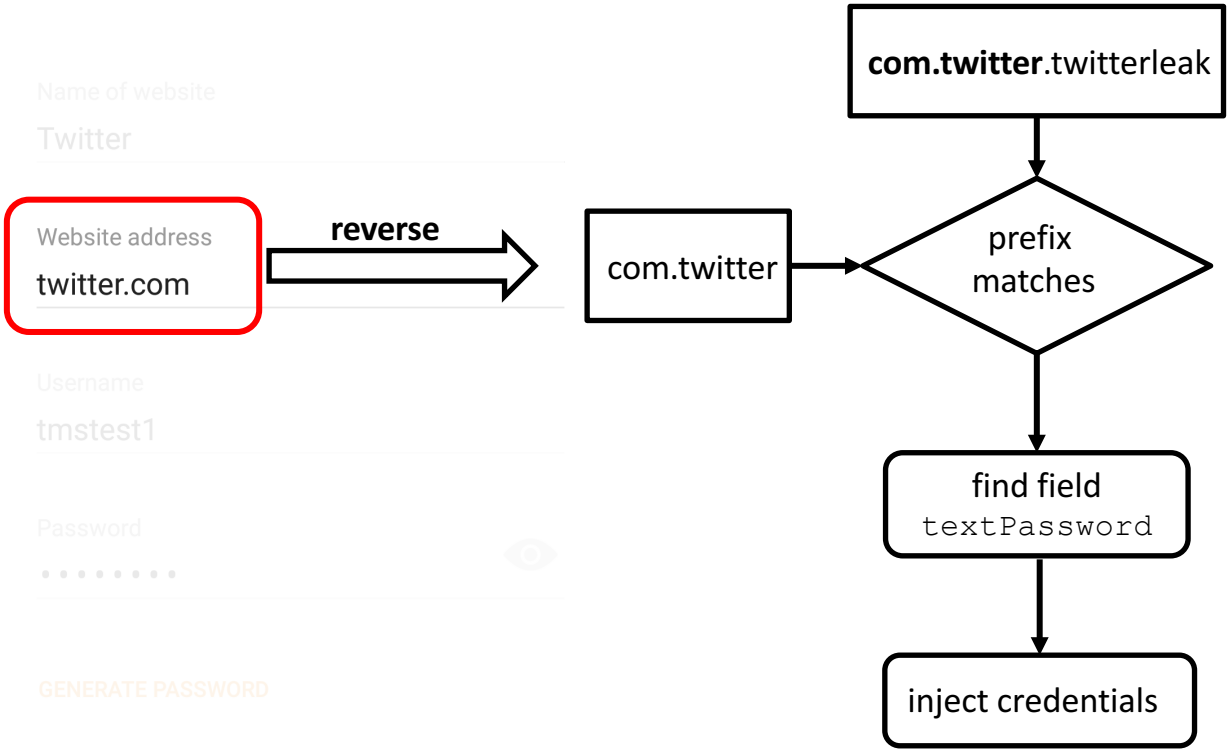


https://c.wordpress.com



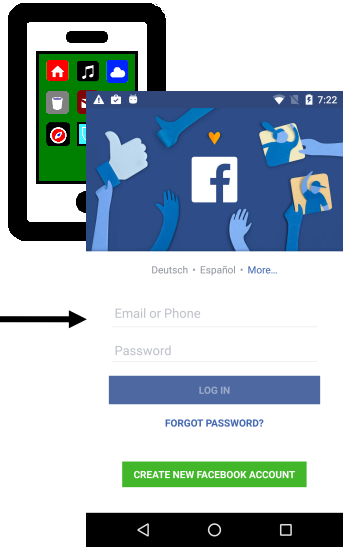
com.twitter

com.twitterleak

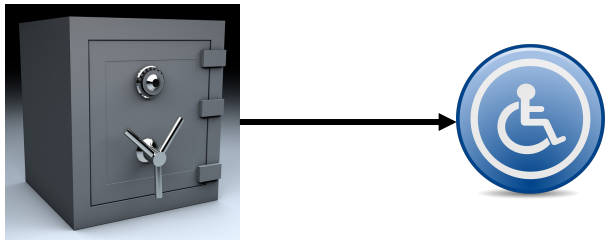

com.twitter.twitterleak
Website address
twitter.com
reverse
com.twitter
prefix
matches
find field
textPassword
inject credentials

Demo Time

Residue Attacks

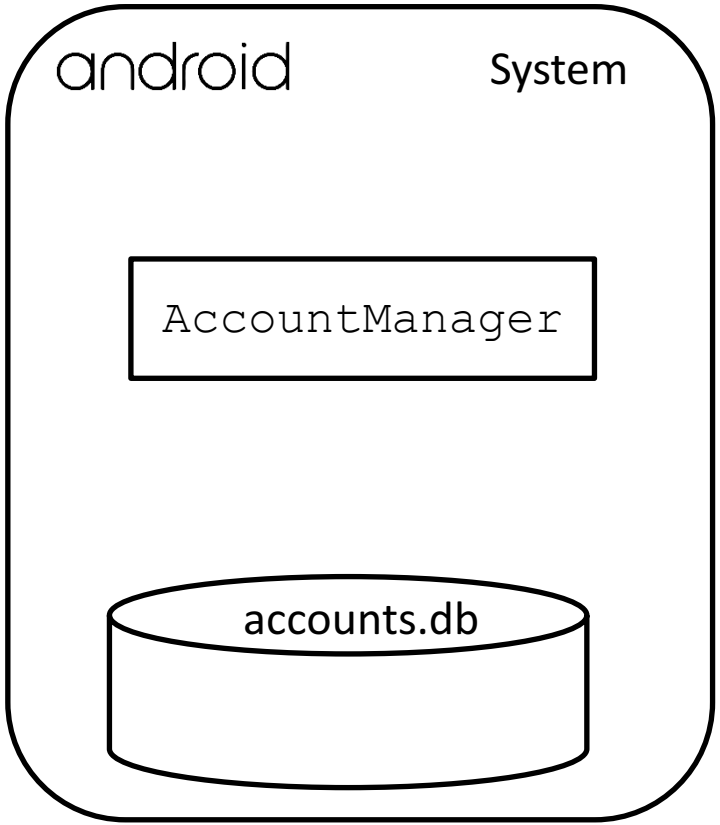


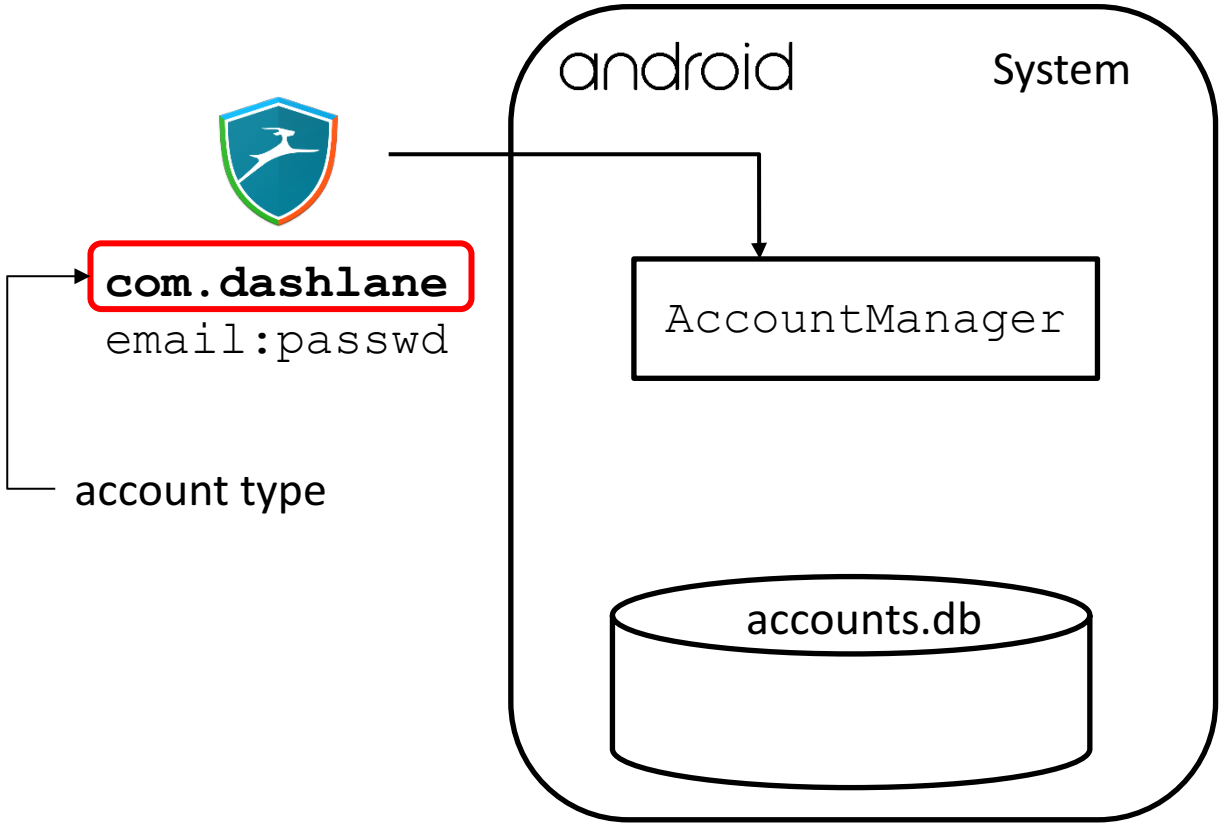
com.facebook

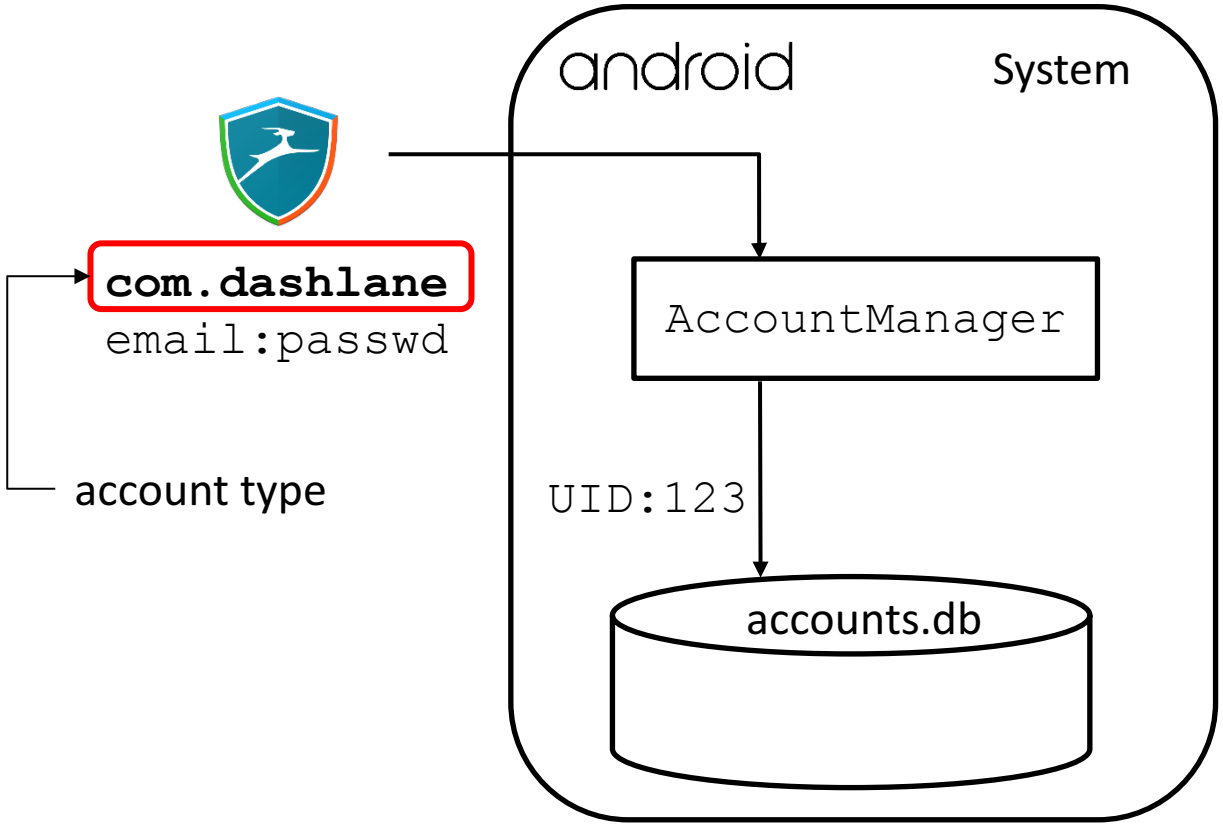


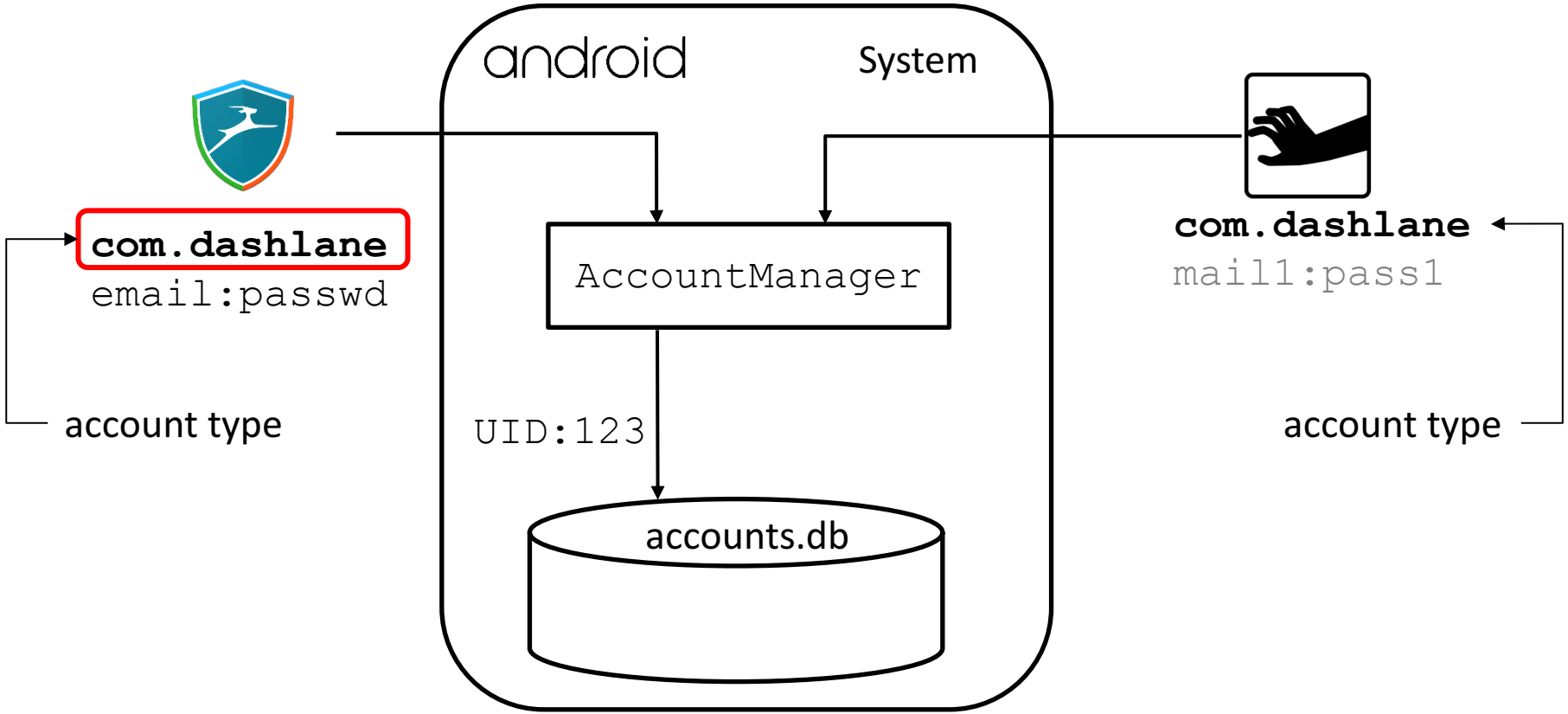
Deutsch · Español · More...
CREATE NEW FACEBOOK ACCOUNT

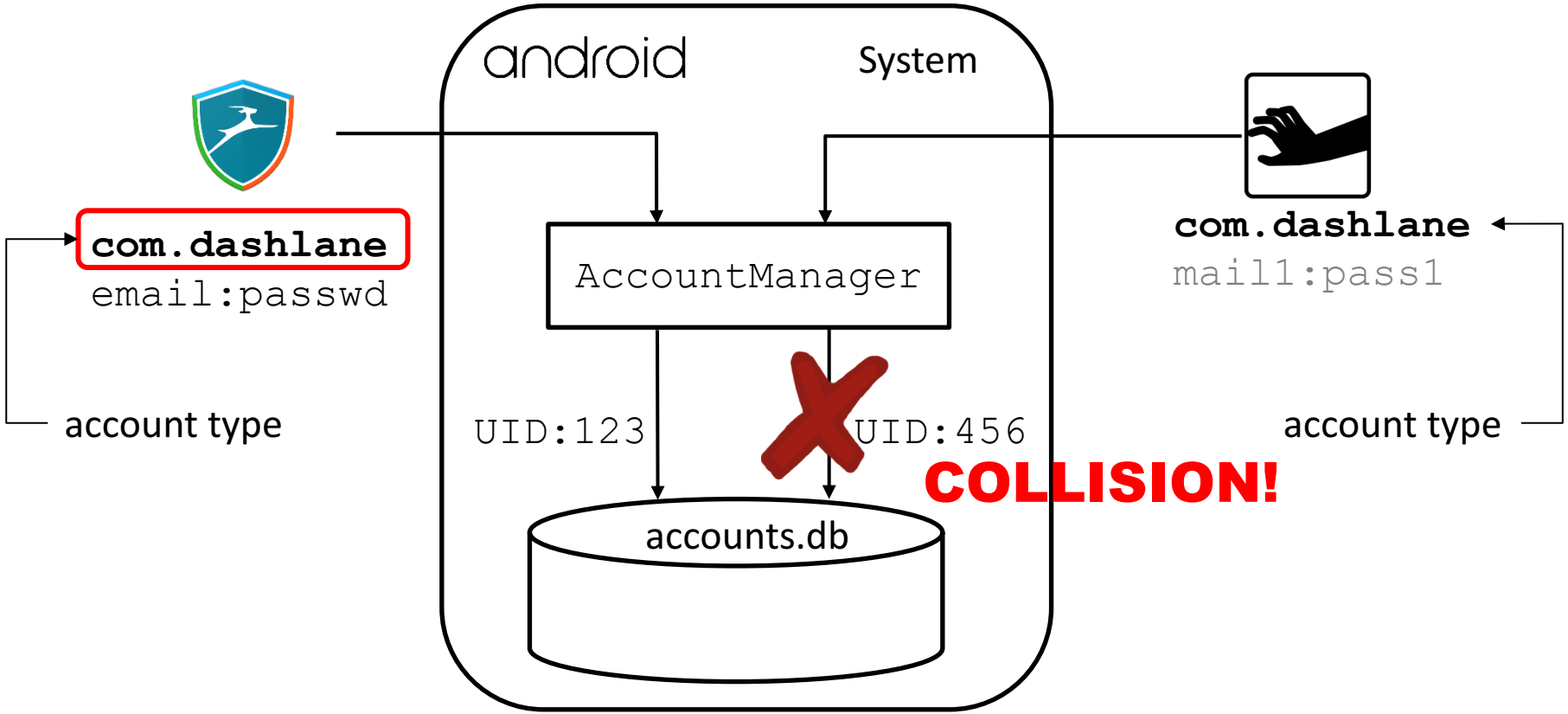
com.facebook

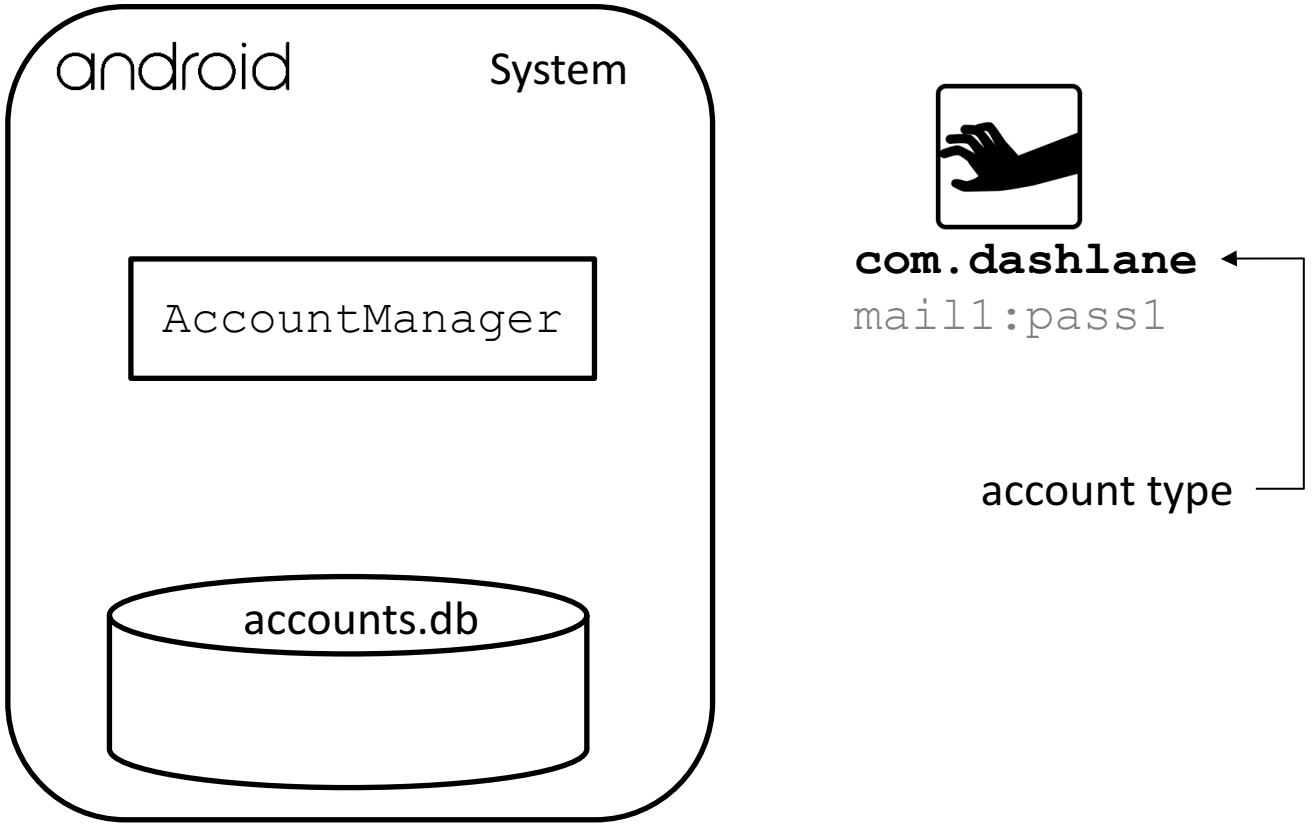

android
System
AccountManager
accounts.db

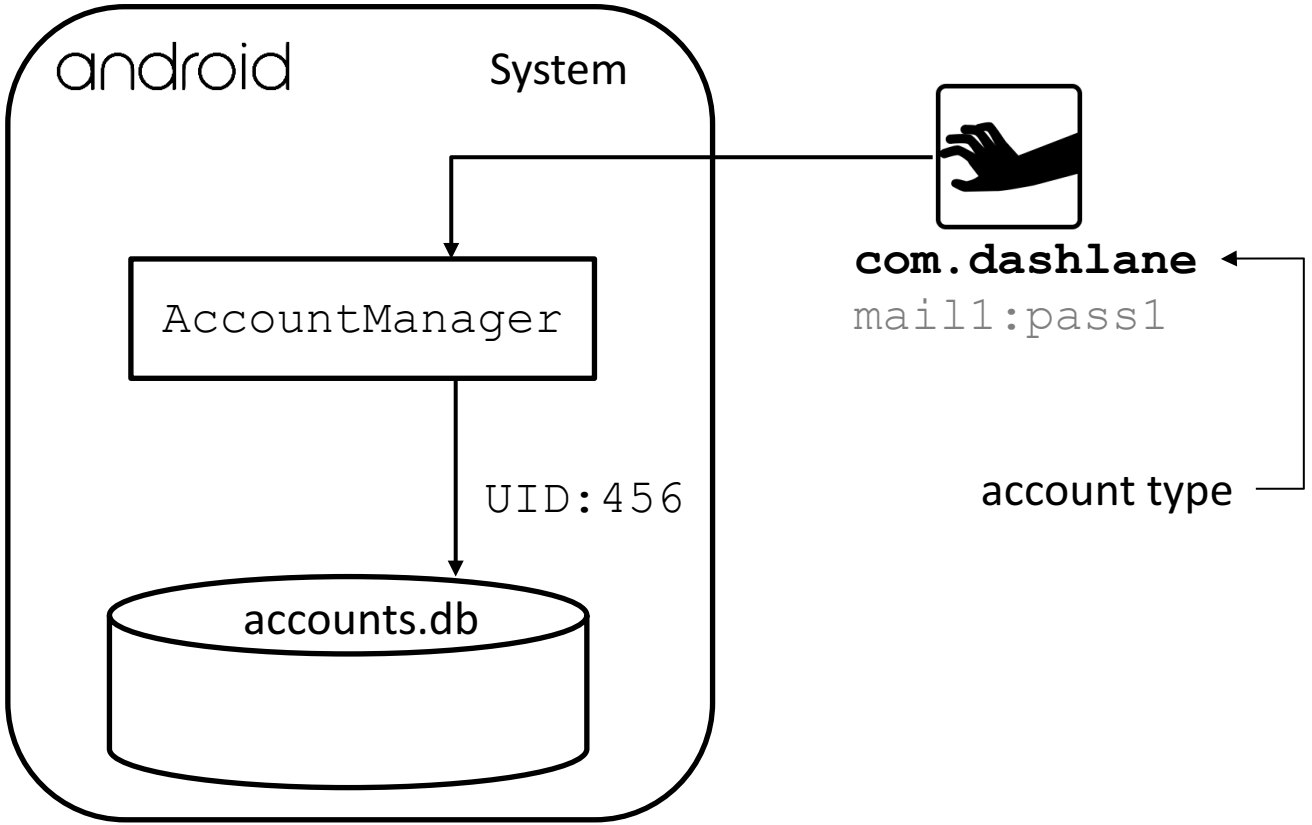

android
System
com.dashlane
email:passwd
account type
AccountManager
accounts.db


android
System
com.dashlane
email:passwd
account type
AccountManager
UID:123
accounts.db


android
System
com.dashlane
email:passwd
AccountManager
com.dashlane
mail1:pass1
account type
UID:123
account type
accounts.db


android
System
com.dashlane
email:passwd
account type
AccountManager
UID:123
UID:456
accounts.db
COLLISION!
com.dashlane
mail1:pass1
account type


android
System
AccountManager
accounts.db
com.dashlane
mail1:pass1
account type


android
System
AccountManager
UID:456
accounts.db
com.dashlane
mail1:pass1
account type

Reading from AccountManager

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

DEMO TIME
memegenerator.net

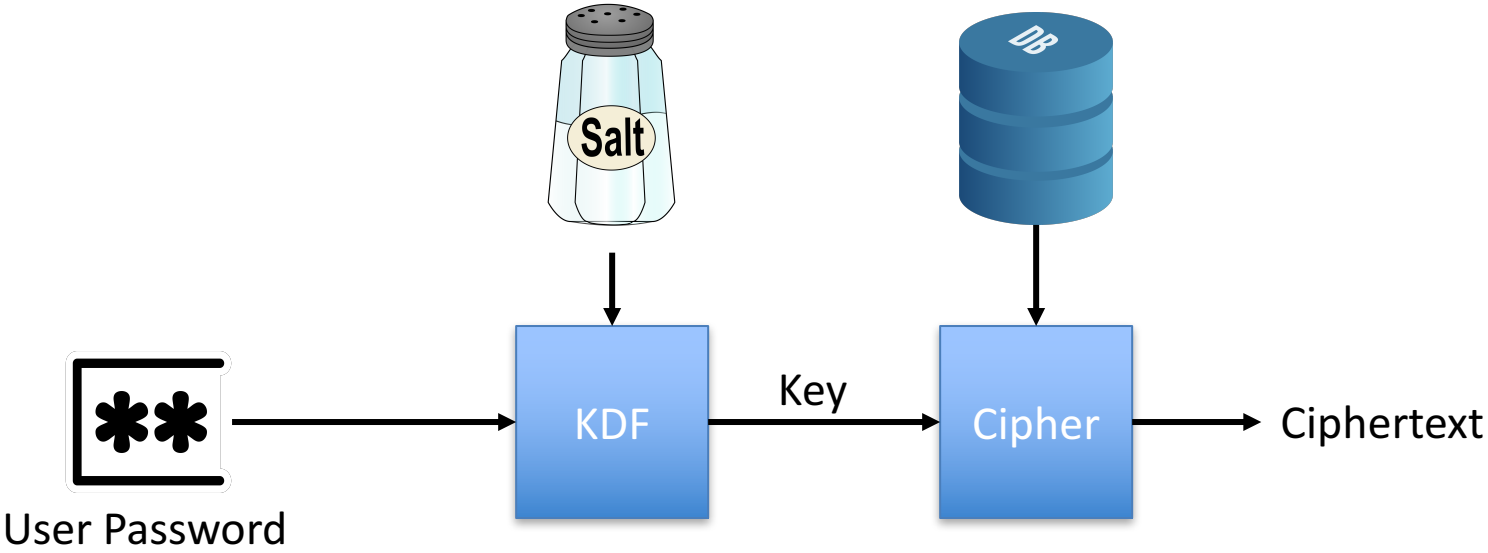
*“With this in mind, you **shouldn't pass the user's actual password** to `AccountManager.addAccountExplicitly()`. Instead, you should store a cryptographically **secure token** that would be of limited use to an attacker.*

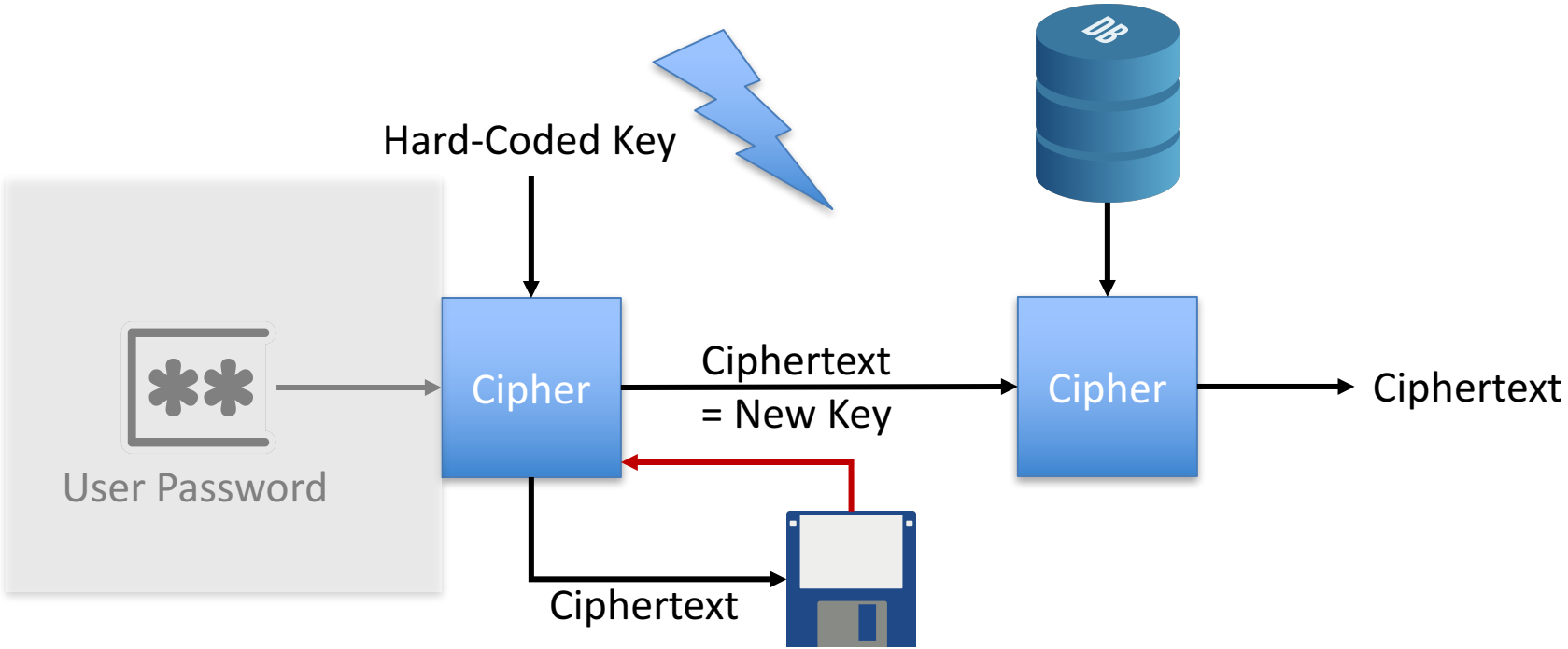
If your user credentials are protecting something valuable, you should carefully consider doing something similar.”

Quote google developer (AccountManager)

`https://developer.android.com/training/id-auth/custom_auth.html`

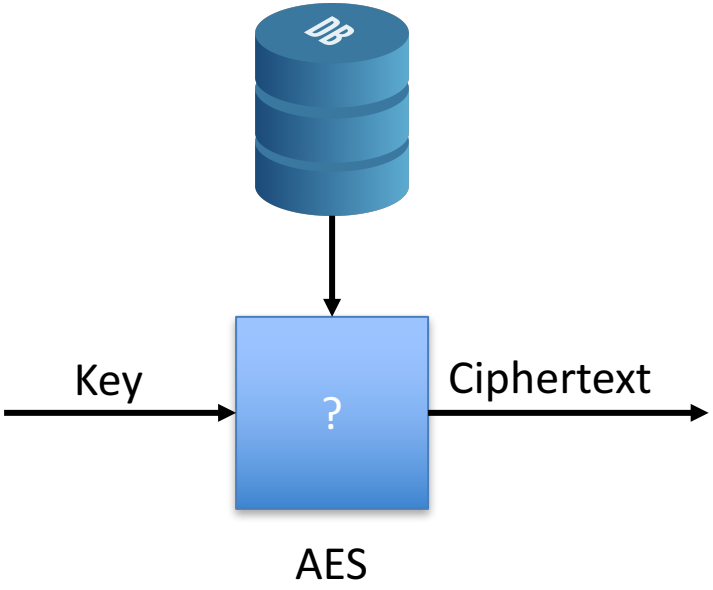
Improper Crypto

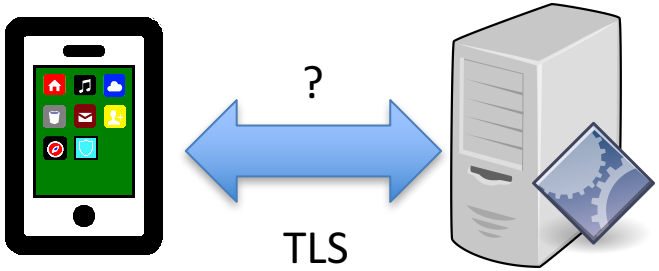

Salt
DB
**
KDF
Key
Cipher
Ciphertext
User Password


Hard-Coded Key
DB
**
User Password
Cipher
Ciphertext
= New Key
Cipher
Ciphertext
Ciphertext

```
public abstract class LPCommon {
//first part of the key
protected static String aA = "ldT52Fjsnjdn4390";
//second part of the key
protected static String aB = "89y23489h989fFFF";
```

AES-Key: ldT52Fjsnjdn439089y23489h989fFFF





Never do your own crypto. Ever.

Kerckhoffs's principle:

"A cryptosystem should be secure even if everything about the system, except the key, is public knowledge." *

*JOURNAL DES SCIENCES MILITAIRES. Janvier 1883. LA CRYPTOGRAPHIE MILITAIRE.

	Keeper	Lastp	1Pass	MyPass	Avast	F-Sec	Keeps.	PwMgr	MyPass	Dash
Master/PIN	X	X		X		X	X	X	X	X
Hardcoded Key		X		X					X	X
Sandbox Bypass		X	X	X					X	X
Side channel		X	X	X	X					X
Subdomain		X	X		X	X		X		X
Data leakage		X	X							X
Partial encryption			X							
Broken sync.					X					

www.sit4.me/pw-manager

Convenience functions weaken or destroy security

- Save password
- PIN
- Autofill
- SSO
- …

Summary:

- Use **secure storage** for **passwords** and **keys**
- Use proper crypto (**no own** algorithms)
- **NEVER** USE **HARDCODED** KEYS !!
- **Validate receivers** of sensitive information
- Use **TLS** for securing **communications**