Bypassing Android Password Manager Apps Without Root

Stephan Huber, Siegfried Rasthofer, Steven Arzt

Fraunhofer SIT

Fraunhofer SIT

team [SIK]

Stephan

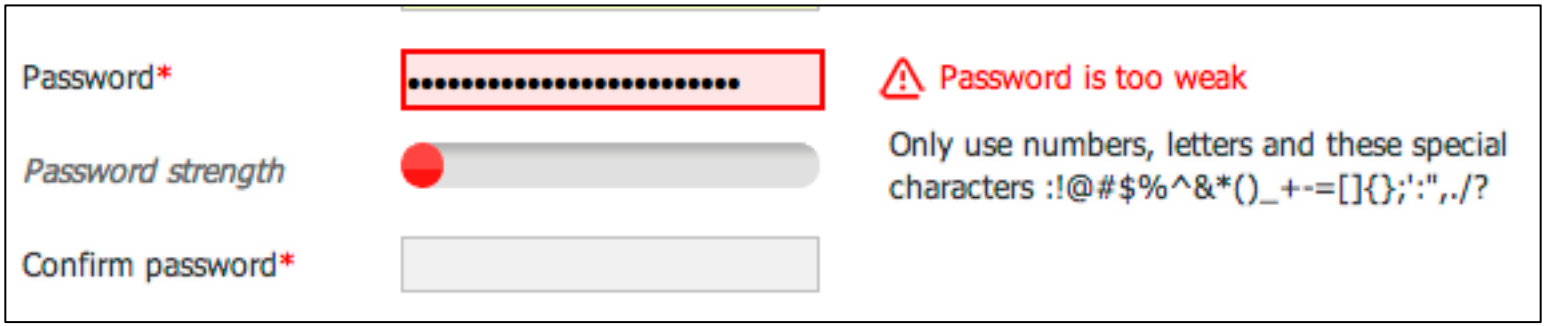
- Mobile Security Researcher at Fraunhofer SIT
- Enjoys teaching students in Android (app) hacking
- Twitter: @teamsik

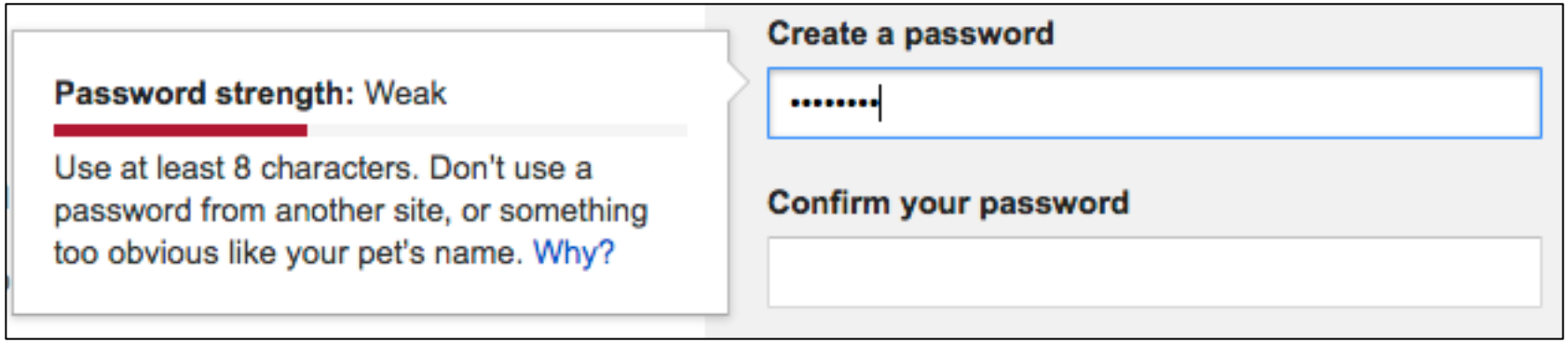
Siegfried

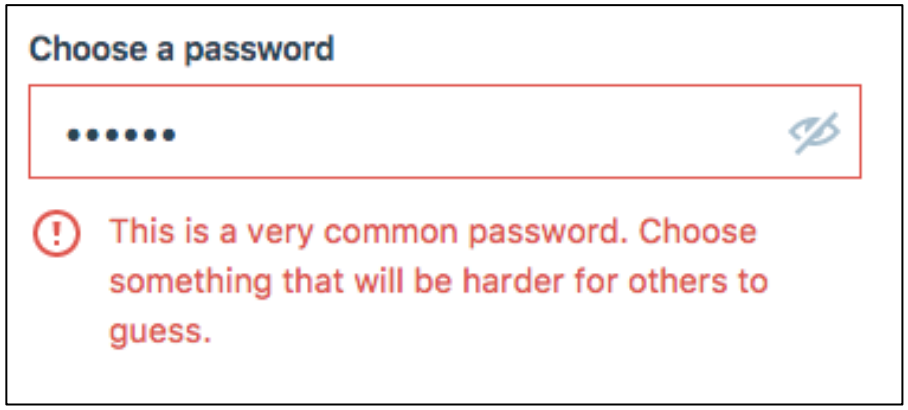
- Head of Secure Software Engineering at Fraunhofer SIT
- Founder of CodeInspect
- Web: www.rasthofer.info
- Twitter: @teamsik

Acknowledgements

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


Password*
Password is too weak
Password strength
Only use numbers, letters and these special characters :!@#$%^&*()_+-=[]{};':",./?
Confirm password*


Password strength: Weak
Use at least 8 characters. Don't use a password from another site, or something too obvious like your pet's name. Why?
Create a password
Confirm your password


Choose a password
This is a very common password. Choose something that will be harder for others to guess.

Wish

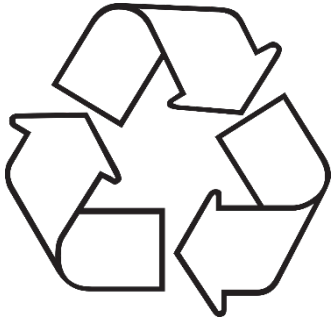
aim=e1Ioci	Ohyoh>wae0	kei7Gae$si	bei3coo<Li	ooB,iu9AhN	Phei0IeHa'	uhu;j5ohTi
Phi,Phu3di	Moo0ooz"oh	we(u,t0Zas	quucoo<d2I	Pae?gh<ie3	loh;Bah4ei	Wa[el~oh9i
ooh!ee7Aik	AX1aeSh>ai	eGah+K5iuM	yae$V4leex	ohjiu_Hei6	fee'Cho5Oo	jahK3Ad+ai
oH)eewaec0	KiG&ee4ahy	ujohj%ie1J	wae,Gei6mu	uSh=i2ahng	ainai]Le2i	Ieb~o5fohF
ohN\ah1gae	Dooch\ei7i	ich]a're1U	aiToh5cee=	eiZ2thaip;	ni"W3oom?i	oi(Sh7vie)
gu}i8Tohco	il@ah@ve9U	cie"tae8Eo	Au&S3aigae	eir0ieHo)c	ohch/ah6Ii	Bie*t9xie"
ukieTh6fu[	ie*vieZai9	ohwu(v0eeY	ua&ghi7aeR	em?ohG?oi3	phu$L^ah4p	ieX&i2shei
aiZie%l7Oo	ood8Pe<emo	faiGh[ie0i	OPho9sie>n	phie9Ib(ie	beiMei[r7a	Nagh(aid0U
AhTee:tah5	oY"a5pheib	ohthe1Na.e	eria9Ahn>u	eid8Ohso!o	Uv4ia6Gu`o	Aeli1li$i&
Toth^ai8ph	Euso6eu$ja	vie8Ieh?ai	leec4aeZ/o	Eele+ph2na	yai=b!a5Oo	Wefoh&m4oh
Vo-oX9ka0v	ei9eenuN<a	Eit}ae4ohF	heRie.J6Bo	OoZ-ue9mai	zait8coo]N	yoh9Oopoh$
xoh%C:ahk6	Zi]opu4eiB	eGh>ih2oPh	noo7Ish'ie	Uaz6she|Zu	oo0aiP*ee2	coh=Puo1Ve
roo9Kee-th	ra@c3Ce7sh	mabi6Malo[	auw1Eu\kie	eiVoo,Kuu5	aiW\oo5phu	Oos_abir7U

Your New Password: X3#RsT[7UE2d&S^r

Remember your password: XBOX 3 # ROPE skype TOKYO [7 USA EGG 2 drip & SKYPE ^ rope

Reality

Note



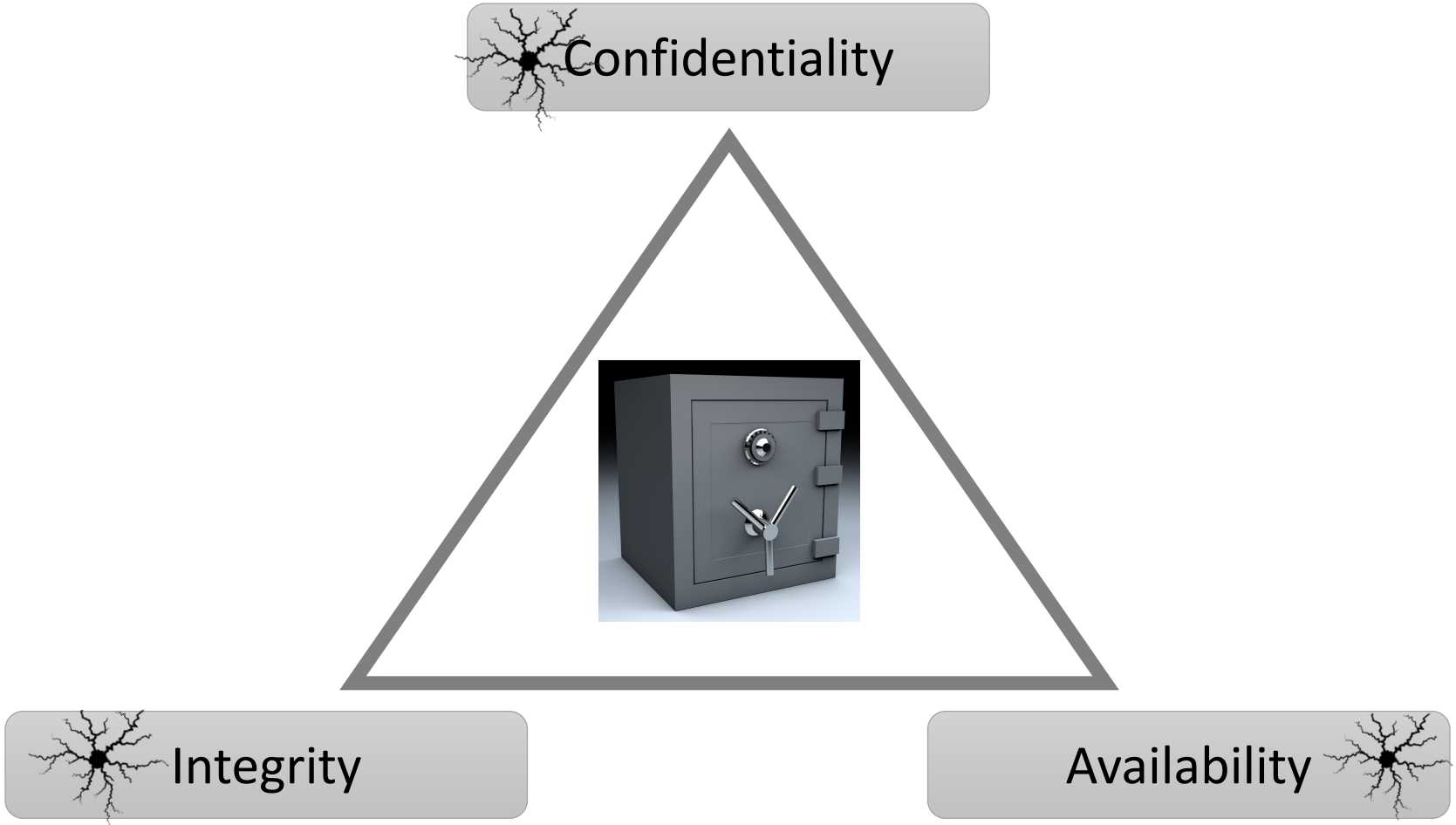
Password-Recycling

Browser
Password-Manager

Password-Manager

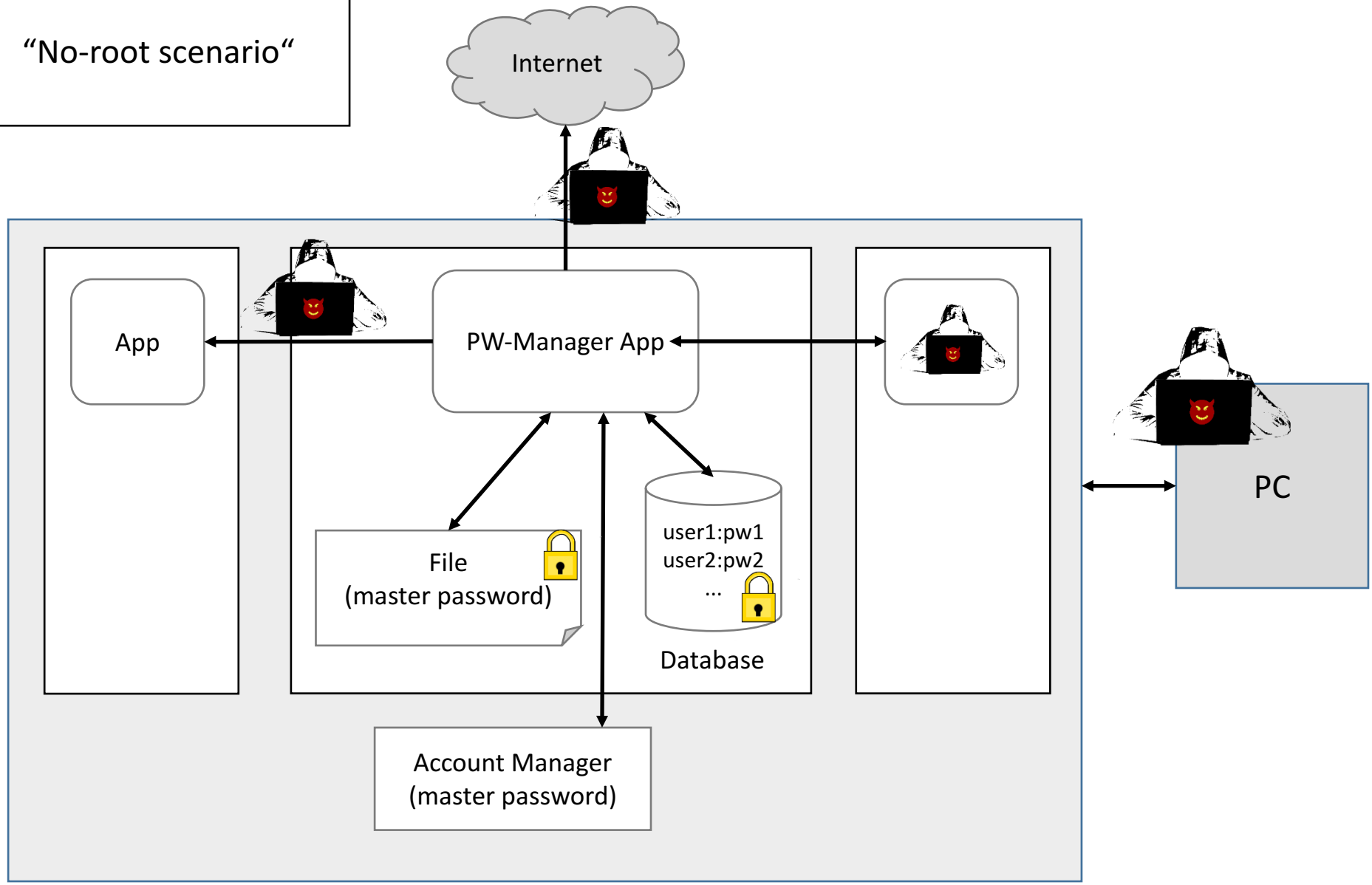
App	GooglePlay Downloads
Keeper	10 – 50 m
Keepsafe	10 – 50 m
1Password	1 – 5 m
Dashlane	1 – 5 m
Lastpass	1 – 5 m
Avast	0.5 – 1 m
MyPasswords	0.5 – 1 m
F-Secure	100 – 500 k
PasswordManger	50 – 100 k

Security Requirements



- Premium features for free
- Resetting master password with ease
- Breaking C.I.A
  - Lost device scenario
  - Mitm attacks
  - Via third party app

“No-root scenario“



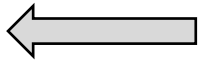
Premium upgrade for free !

Get Pro for Free

```
public abstract class BasePreferenceActivity extends AppCompatPreferenceActivity {

    protected static boolean a = false;

    protected void onCreate(Bundle bundle) {
        boolean z = false;
        super.onCreate(bundle);
        …
        if (getIntent().getIntExtra("com.xy.mo.apps.pwmgr.EXTRA_SUFCXNUQVRF", 0) == 2) {
            z = true;
        }
        a = z;
    }
```



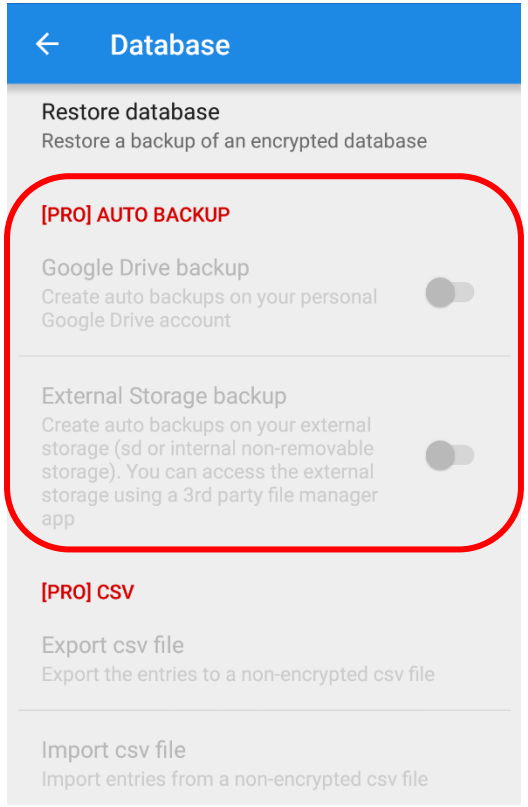
Premium Flag

check `Intent` value

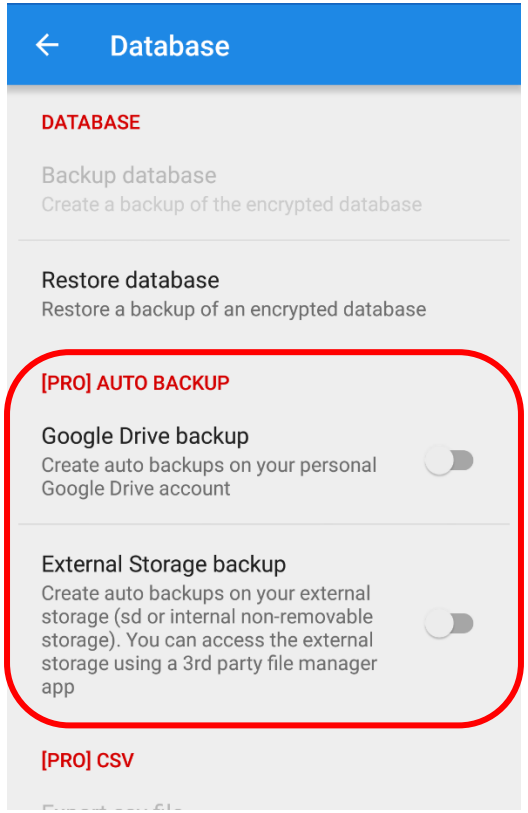
```
adb shell am start -n
com.xy.mo.apps.pwmgr/.settings.DatabaseSettings --ei
com.xy.mo.apps.pwmgr.EXTRA_SUFCXNUQVRF 2
```

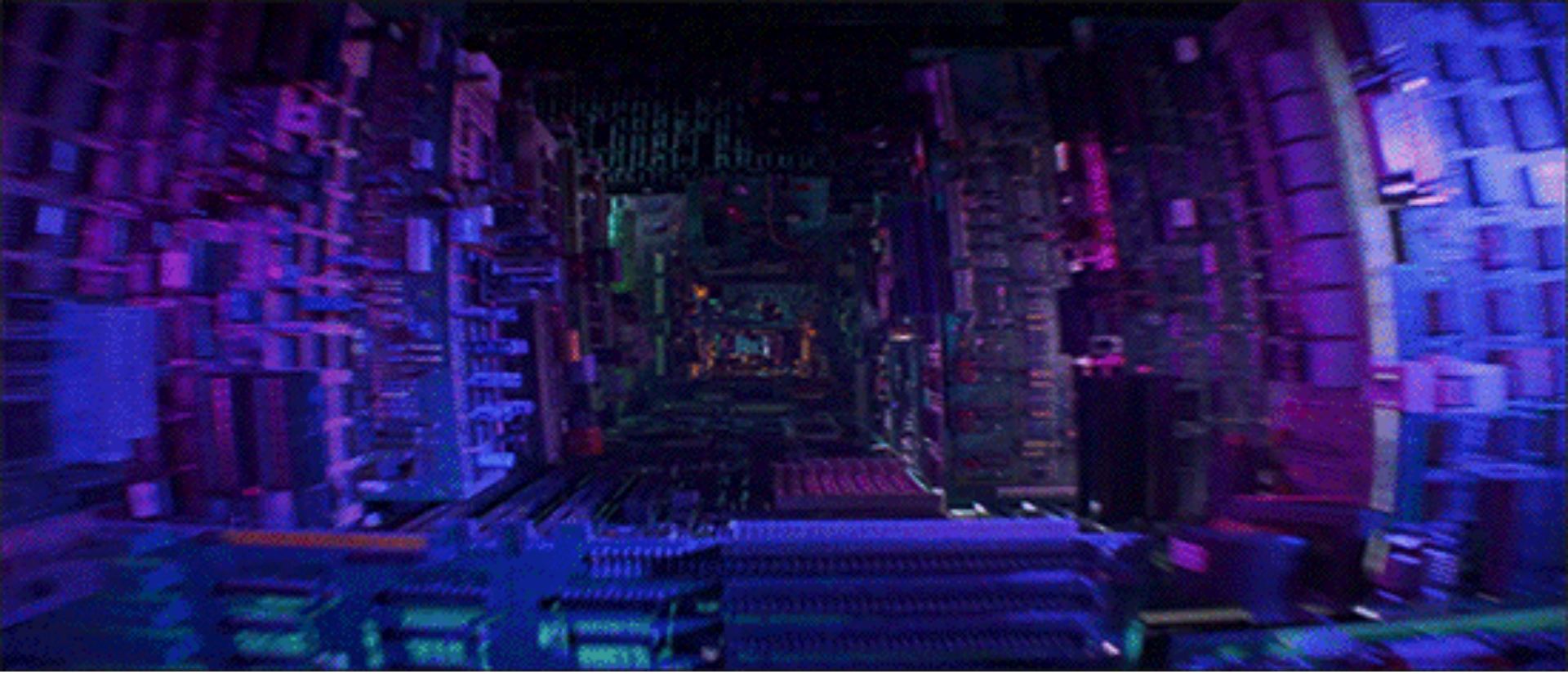
Before and After Intent

Before Intent:



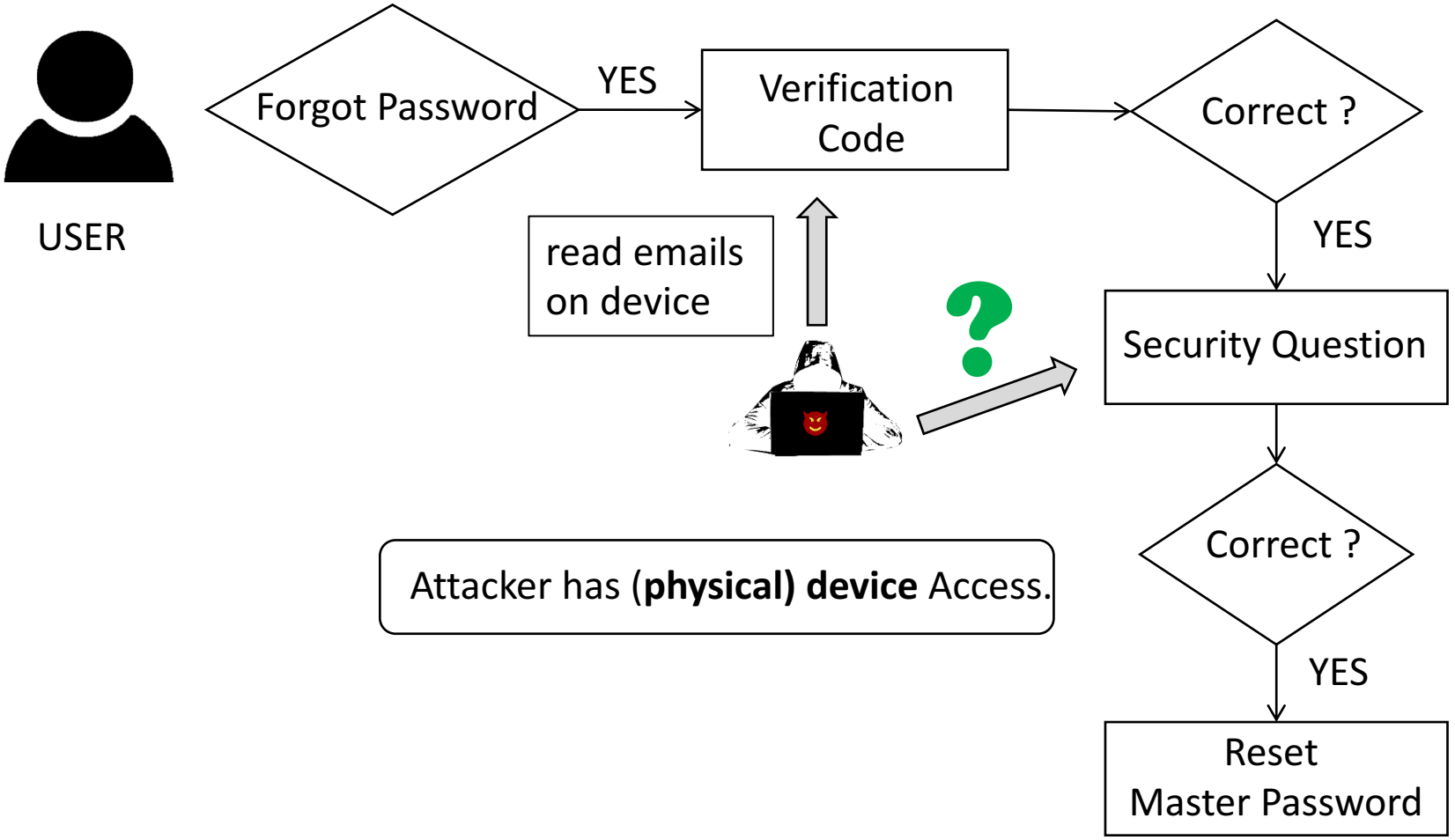
After Intent:





Logic Flaw

Logic Design Flaw



Logic Design Flaw

- Manifest:

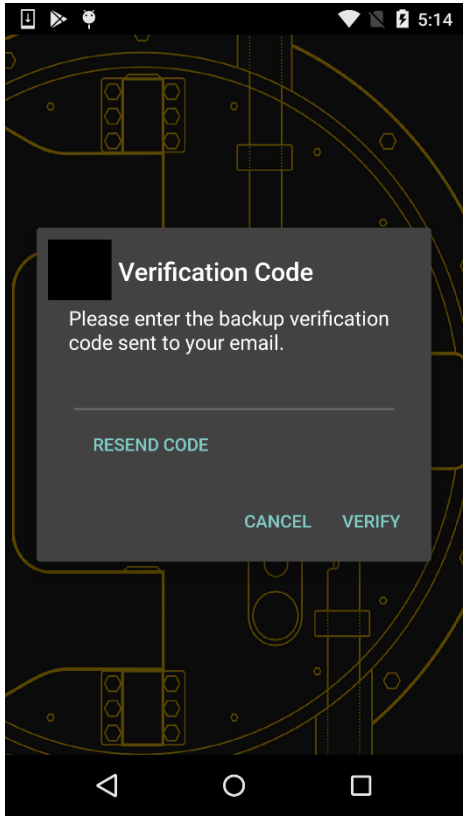
```
<activity android:theme="@*android:style/Theme.NoDisplay"
  android:label="@afk/app_name"
  android:name="com.xyz.android_apps.noname.DeepLinkActivity">
  <intent-filter>
     <action android:name="android.intent.action.VIEW" />
     <category android:name="android.intent.category.DEFAULT" />
     <category android:name="android.intent.category.BROWSABLE" />
     <data android:scheme="https" android:host="xyz.com" android:pathPattern="/.*st.*" />
  </intent-filter>
</activity>
```

- Start Activity:

```
adb shell am start -n com.xyz.android_apps.noname/.DeepLinkActivity
```

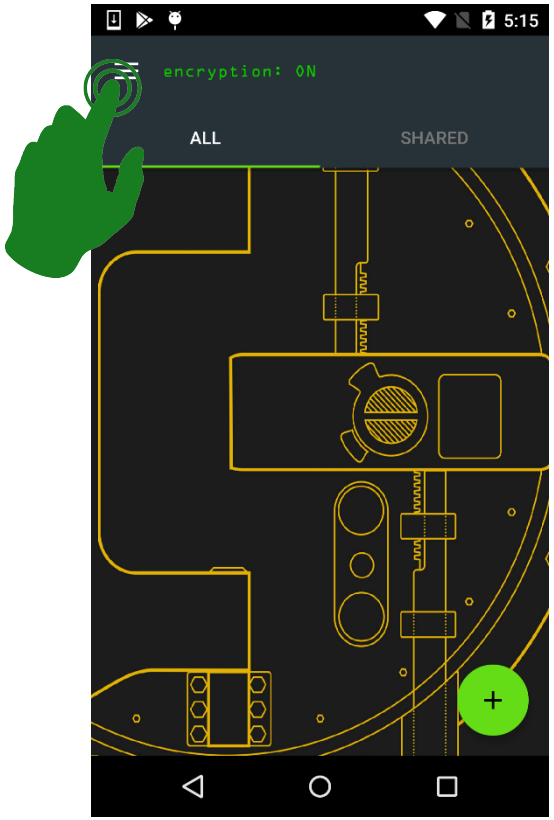
Logic Design Flaw

- “Forget Password“ function



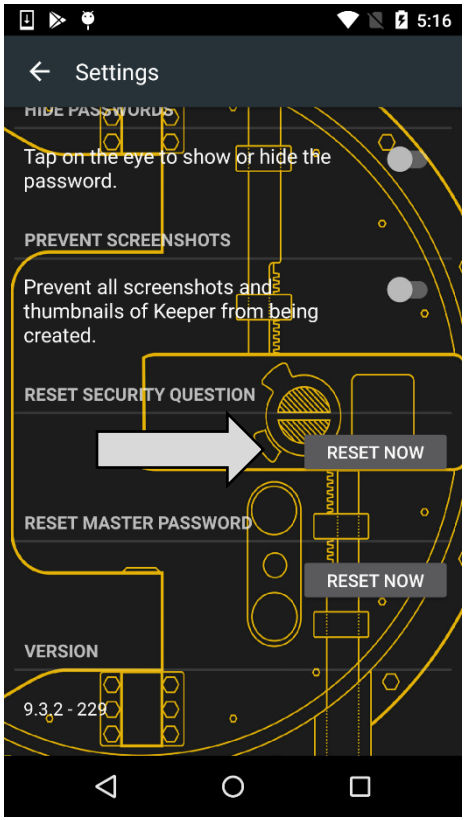
Logic Design Flaw

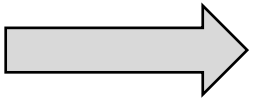
- Fire intent, start `DeepLinkActivity`

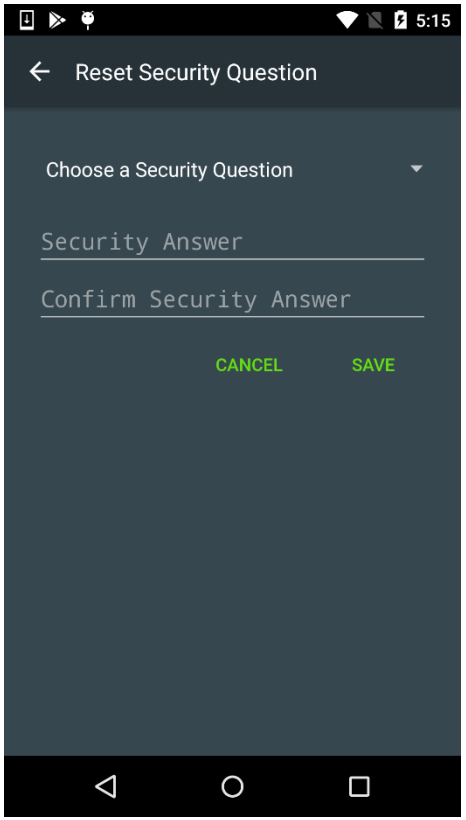


Logic Design Flaw

- Settings -> “RESET SECURITY QUESTION“







Attacker Flow

ATTACKER

Forgot Password

YES

Verification Code

Start Settings

get code from emails on device

Change Security Question

Enter Verification Code
Answer Sec. Question

Reset Master Password

Attacker has (**physical) device** Access

Side Effects

- Change security question **without authentication**
- **Insert new data** into the database -> **synchronization** (no code ☹)
- Turn of **auto destroy** function -> brute forcing

Get Master Secret

Master Secret

1

Extraction process

- ADB-backup
- **Mitm attack**
- **Browser file access**
- **Residue attack**

2

Decryption process

- Plaintext
- **Custom crypto**
- **Hardcoded symmetric keys**
- **Custom obfuscation**

Master Secret

1

Extraction process

- ADB-backup
- **Mitm attack**
- **Browser file access**
- **Residue attack**

2

Decryption process

- Plaintext
- **Custom crypto**
- **Hardcoded symmetric keys**
- **Custom obfuscation**

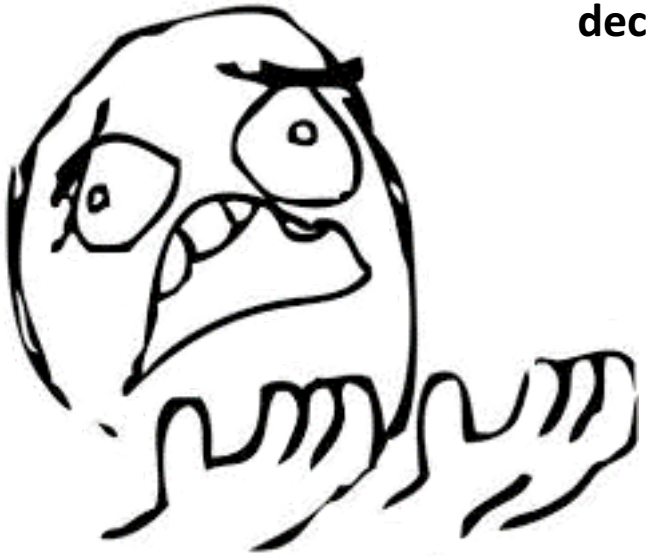
User Authentication

Authentication Process

seed = time[ms]

key = random(seed)

enc_data = **AES**(**key**, auth_data)

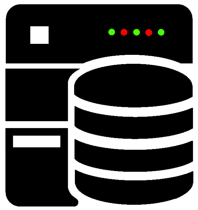


dec_data = AES(key, auth_data)

key = random(seed)

seed = time[ms]

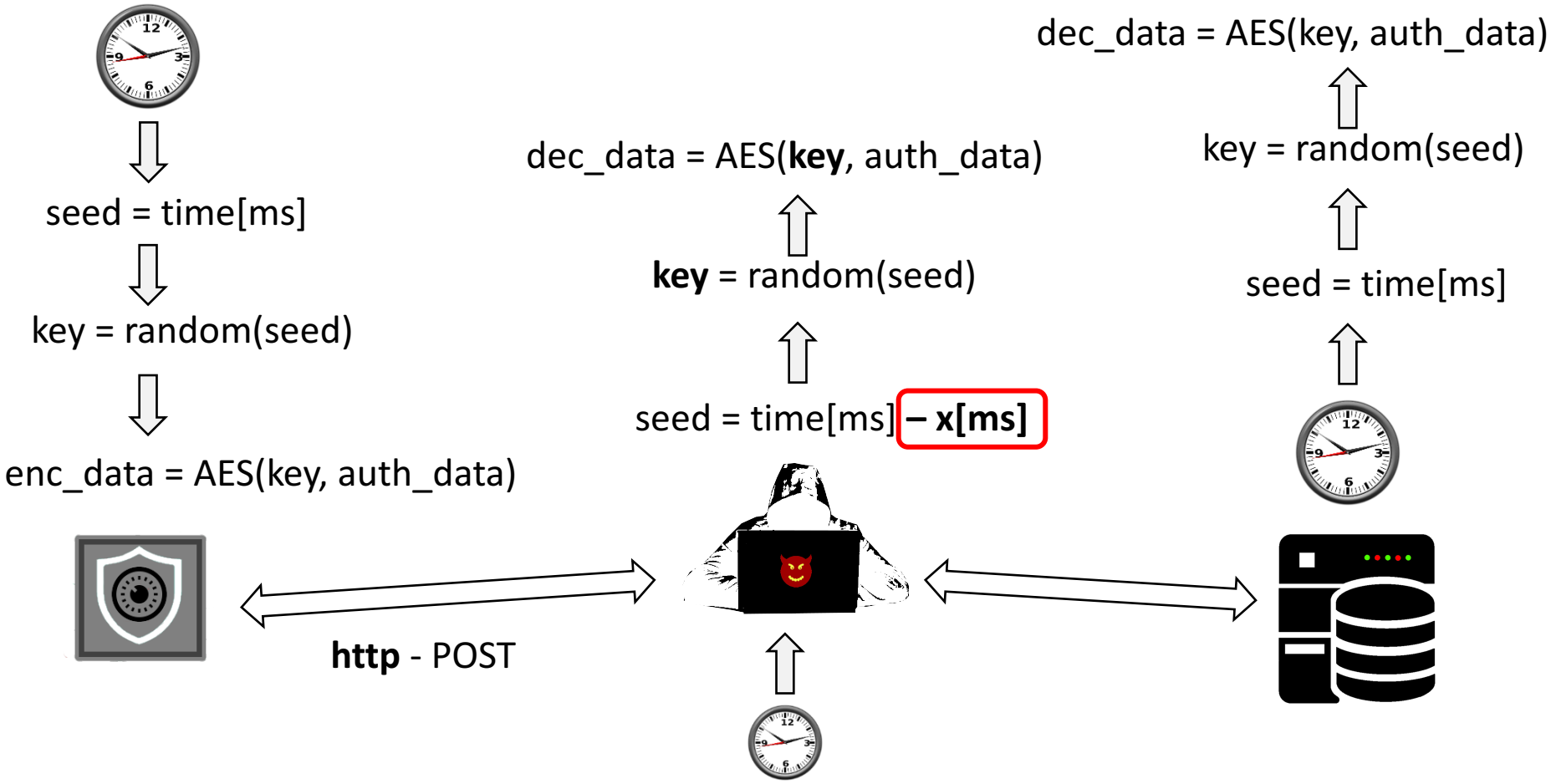
http – POST - request



Header:

Body: enc_data ← **encrypted payload**

Authentication Process



Best Practices: Secure Communication

- Android, correct ssl*

```
URL url = new URL("https://example.org");
URLConnection urlConnection = url.openConnection();
InputStream in = urlConnection.getInputStream();
…
```

- Stronger, SSL (Pinning)
  - Android 7 supports pinning (security configuration file)
  - Use library with pinning support, e.g. `OkHttp` library (take care of version)

*https://developer.android.com/training/articles/security-ssl.html

Master Secret

1

Extraction process

- ADB-backup
- **Mitm attack**
- **Browser file access**
- **Residue attack**

2

Decryption process

- Plaintext
- **Custom crypto**
- **Hardcoded symmetric keys**
- **Custom obfuscation**

11:20
file:///data/data/package.name/shared_prefs/passwd_pref.xml
This XML file does not appear to have any style information associated with it. The document tree is shown below.
<map>
<string name="uid">104984802</string>
<string name="showlaunchalert">1</string>
<string name="dofastdecryption">1</string>
<string name="loginpw">!CRpsShT82h9bfkoPprrtHA==|EbI41MyZXyI3XT1Yne4EoA==</string>
<string name="allowofflinelocal">1</string>
base64(encr(key, PASS))
This XML file does not appear to have any style information associated with it. The document tree is shown below.
<map>
<boolean name="9e907907d6f425ba97f7203533ea1204" value="true"/>
<string name="edbbbc9eb6fe5b240cf4d8a084d9ef0a">PLAYSTORE</string>
<boolean name="9e7dbf400f05775f556fd2b442cdc557" value="true"/>
md5(“ pinCodeValue“)
<int name="2f489516ce7edc99ef89d88ce9f3ffa1" value="0"/>
<boolean name="bcffca8558d146de09ad1b1a1cc0e9fc" value="true"/>
<long name="credentials_timestamp" value="1474018940377"/>
<string name="2e5d8aa3dfa8ef34ca5131d20f9dad51">
+F4dkegeBO2WMP8jheQkkSzfw237ztAZL6ne9RYV5jNLVOMz9xgSCLtvI/TVW/3NgrDOge4c8qsJhRSfpHNhWQvjwKbp8vJQYd5AwhVCt(
</string>
<long name="3164a9674a6ff29071c3d43f0d8caaed" value="1474018411304"/>
<string name="d2d8e0ab85be1ce1b690efac17be5b16">
NBDBu6bclc+n+TKCbzLzpjZqoerErdRxUK/8JqMV7C1LVOMzD/j32tWdQdr36iWL4yuR4SVAWb/6t3Hq2OjCrit5AQA=
</string>

Master Secret

1

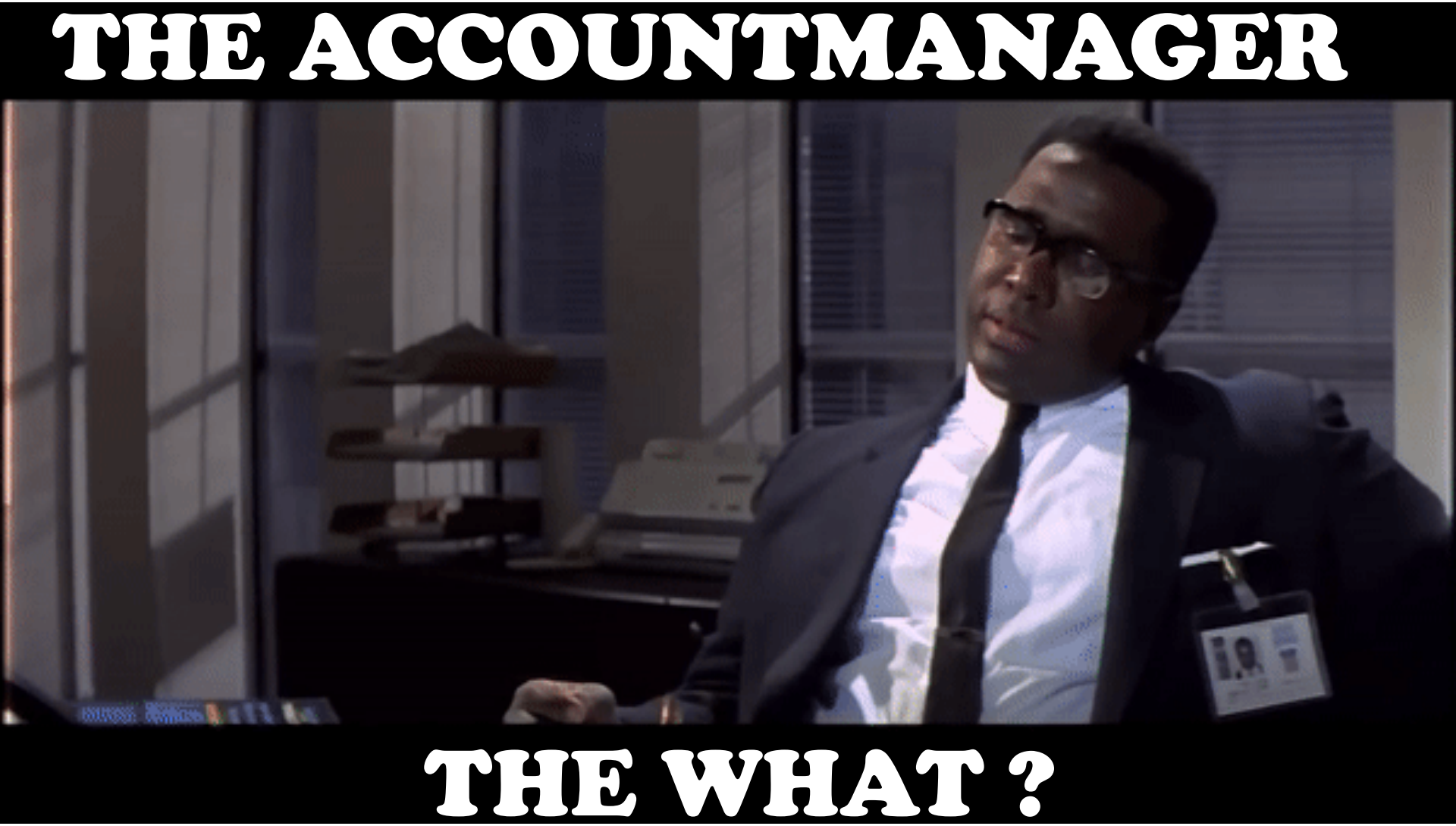
Extraction process

- ADB-backup
- **Mitm attack**
- **Browser file access**
- **Residue attack**

2

Decryption process

- Plaintext
- **Custom crypto**
- **Hardcoded symmetric keys**
- **Custom obfuscation**


THE ACCOUNTMANAGER
THE WHAT ?

Android `AccountManger`

- „This class provides access to a centralized registry for the user‘s online accounts …“
- SQLITE Database for storing tokens or temp. Credentials
- API provides access for Application

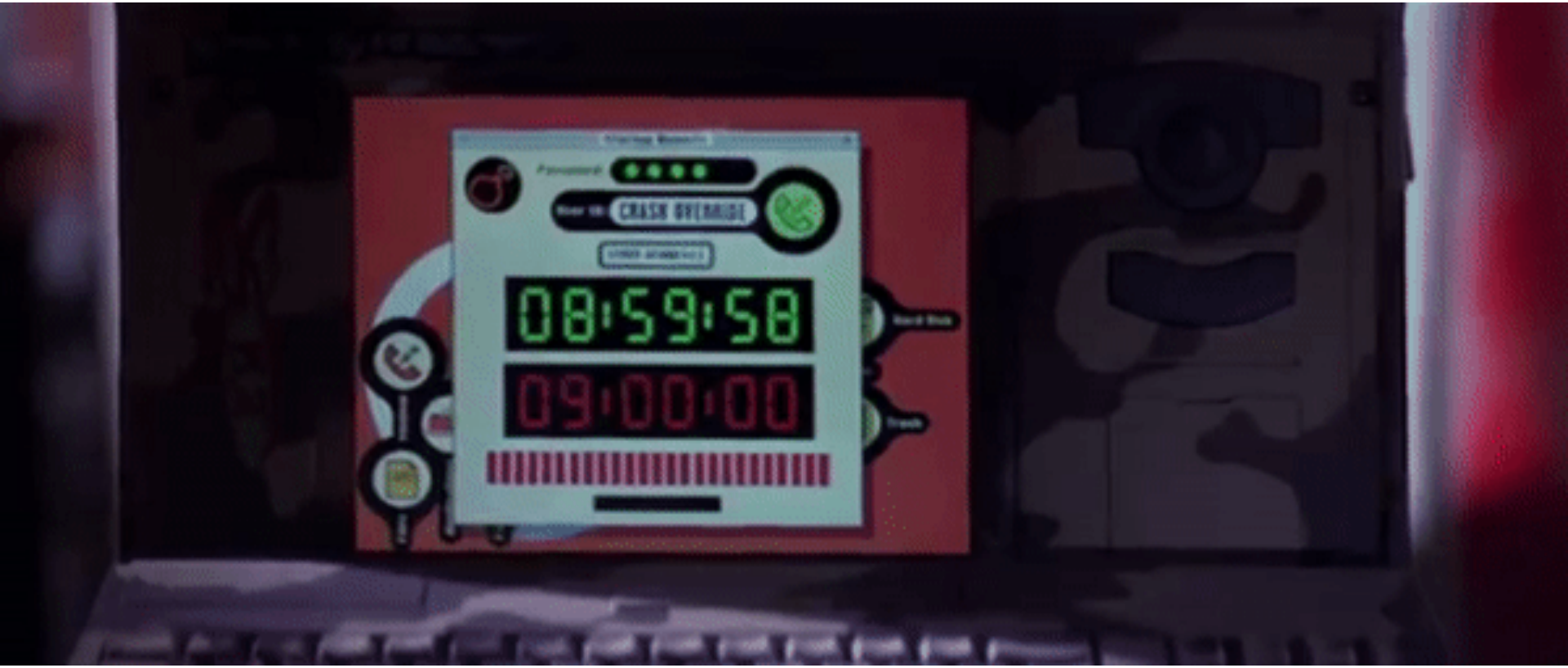
```
/data/system/users/0 # ls -l accounts.db
-rw-rw---- system   system     241664 2017-04-03 10:58 accounts.db
```

*"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)

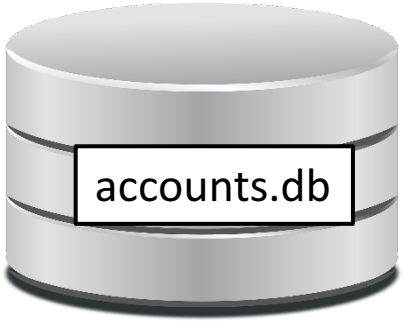
`https://developer.android.com/training/id-auth/custom_auth.html`



DEMO TIME !

AccountManager

ID	email	type	token

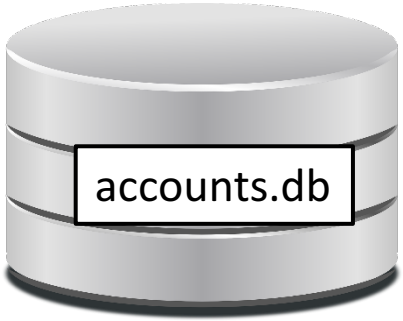


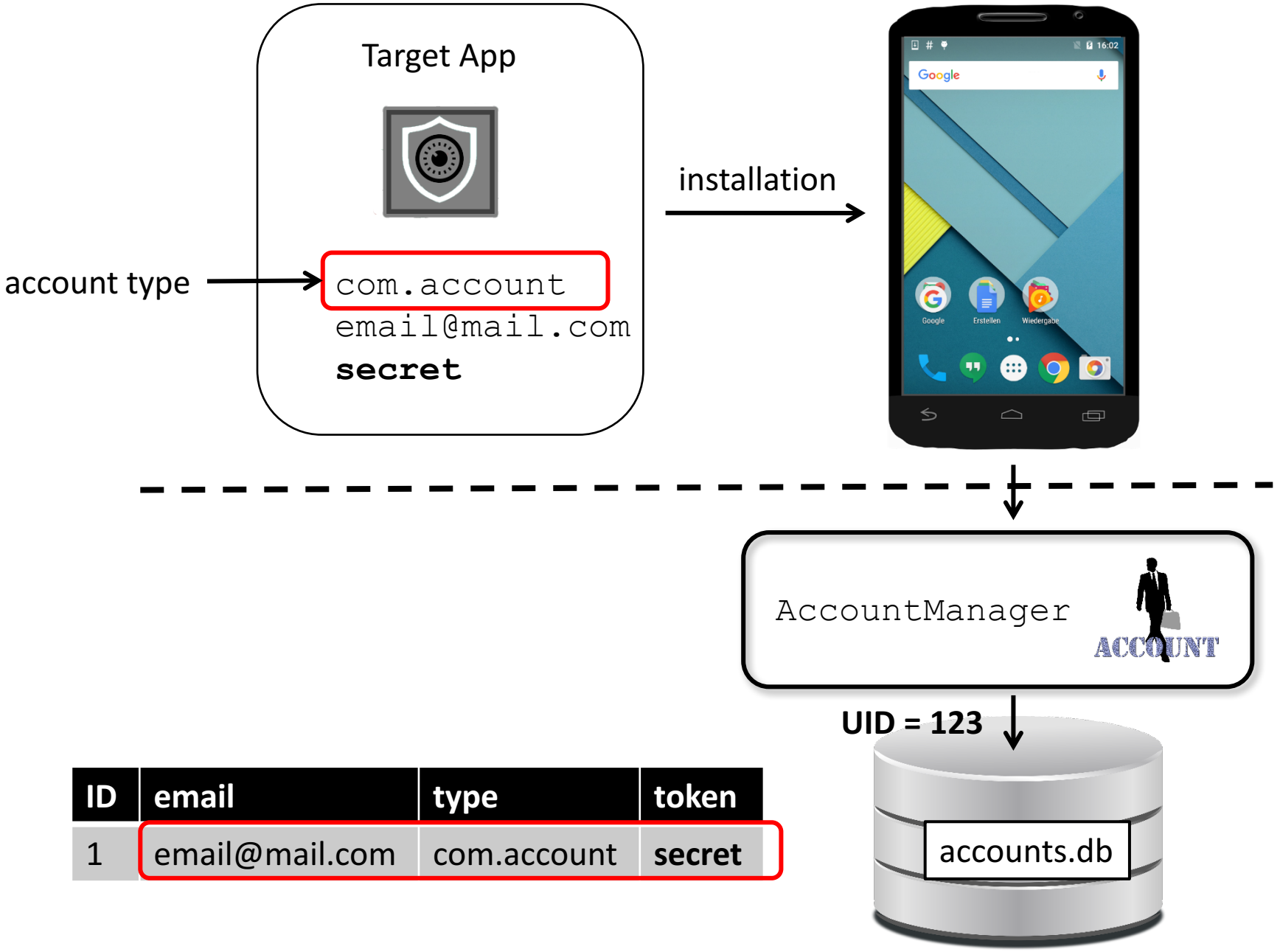
Target App

account type → com.account
email@mail.com
secret

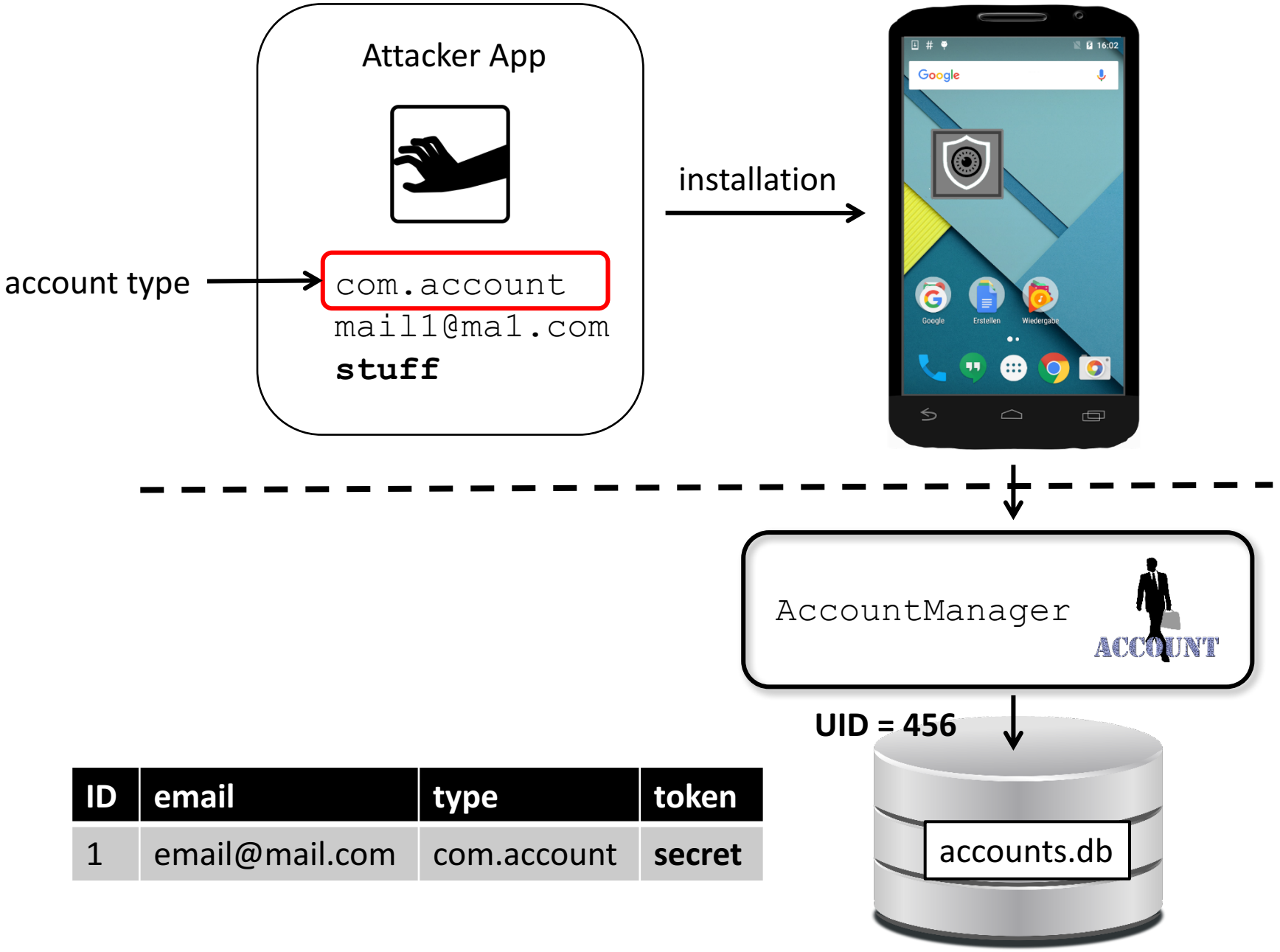
AccountManager

ID	email	type	token

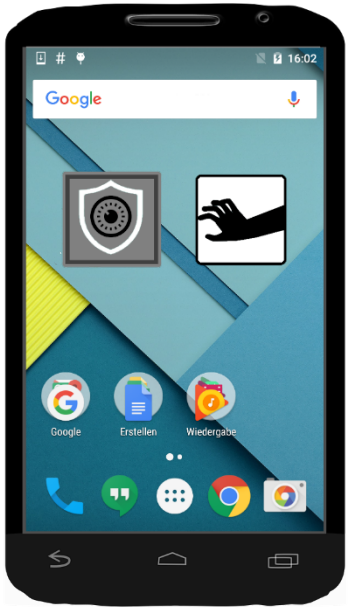




ID	email	type	token
1	email@mail.com	com.account	**secret**

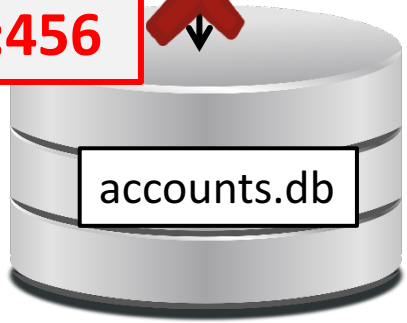


ID	email	type	token
1	email@mail.com	com.account	**secret**

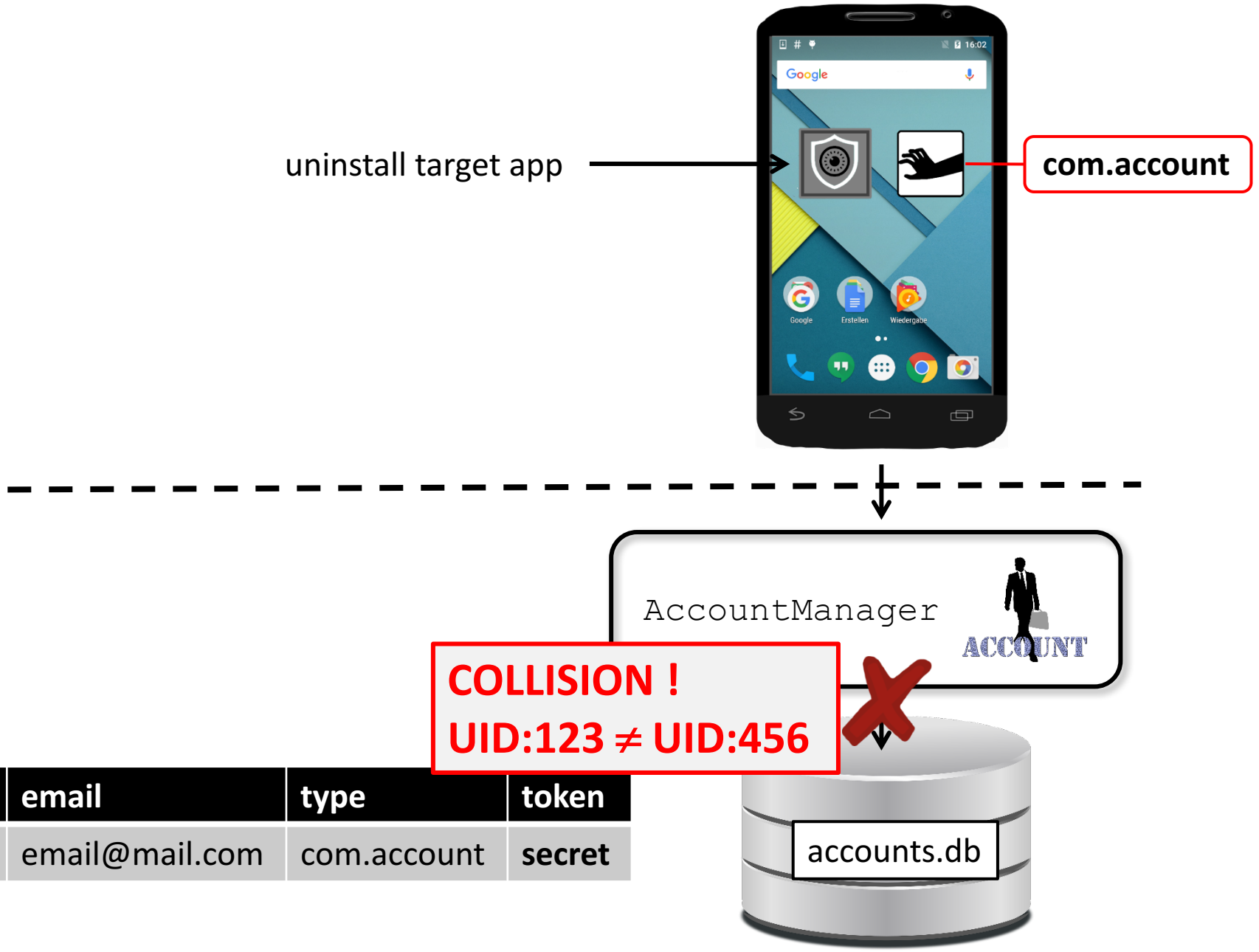


AccountManager

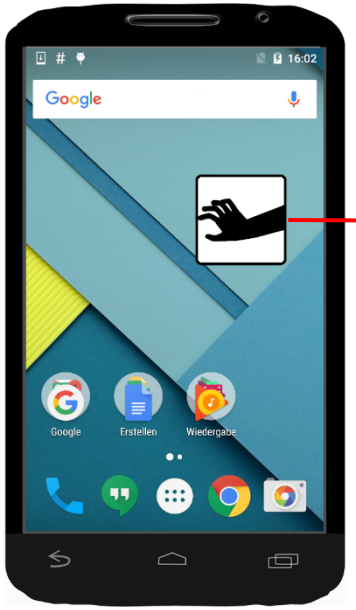
COLLISION !
UID:123 ≠ UID:456



ID	email	type	token
1	email@mail.com	com.account	**secret**



ID	email	type	token
1	email@mail.com	com.account	**secret**

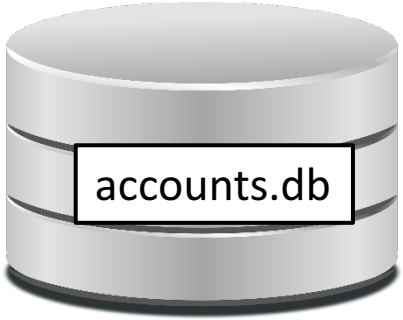


com.account

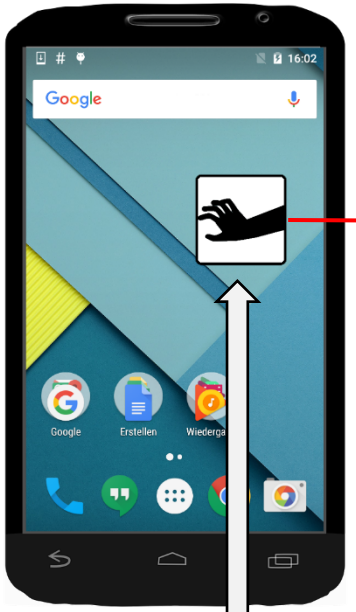
AccountManager

Not removed,
there is an app with matching account type

ID	email	type	token
1	email@mail.com	com.account	**secret**



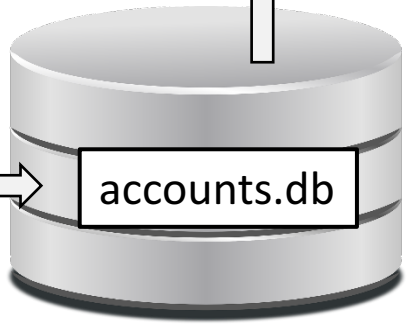
Attacker app can now access the secret !



com.account

AccountManager

ID	email	type	token
1	email@mail.com	com.account	**secret**



Master Secret

1

Extraction process

- ADB-backup
- **Mitm attack**
- **Browser file access**
- **Residue attack**

2

Decryption process

- Plaintext
- **Custom crypto**
- **Hardcoded symmetric keys**
- **Custom obfuscation**

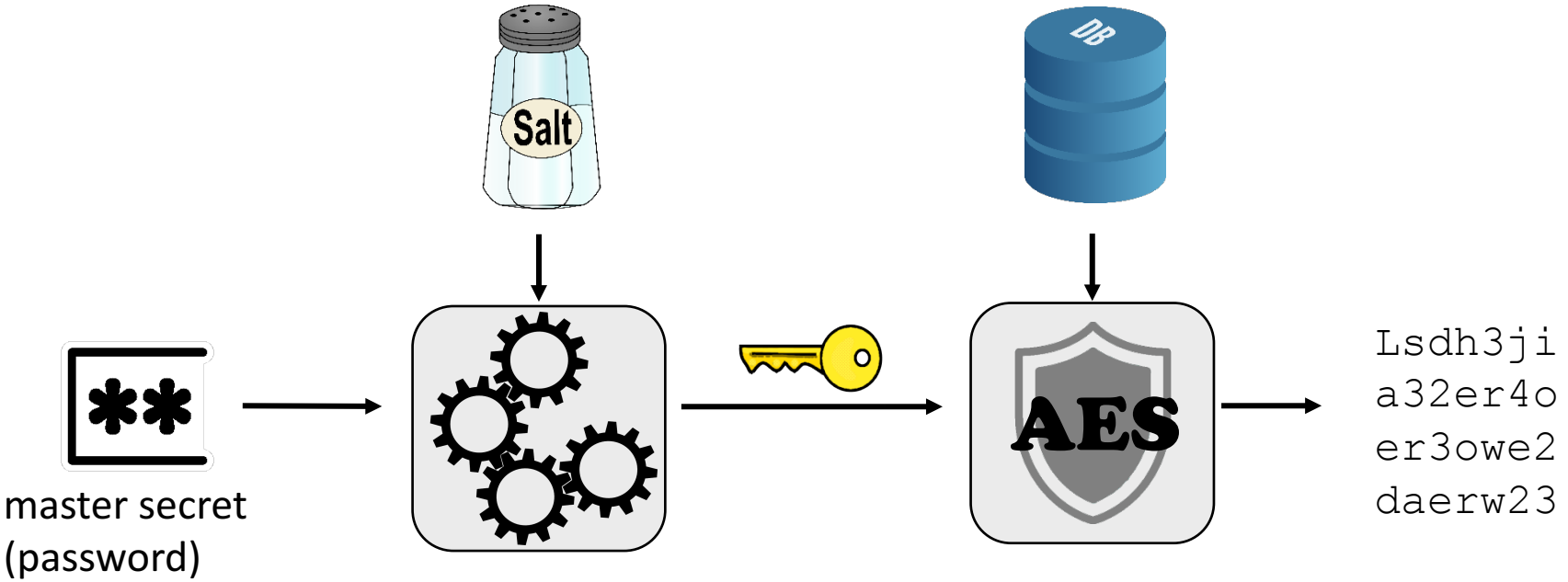
Crypto – Do it right

Kerckhoffs's principle

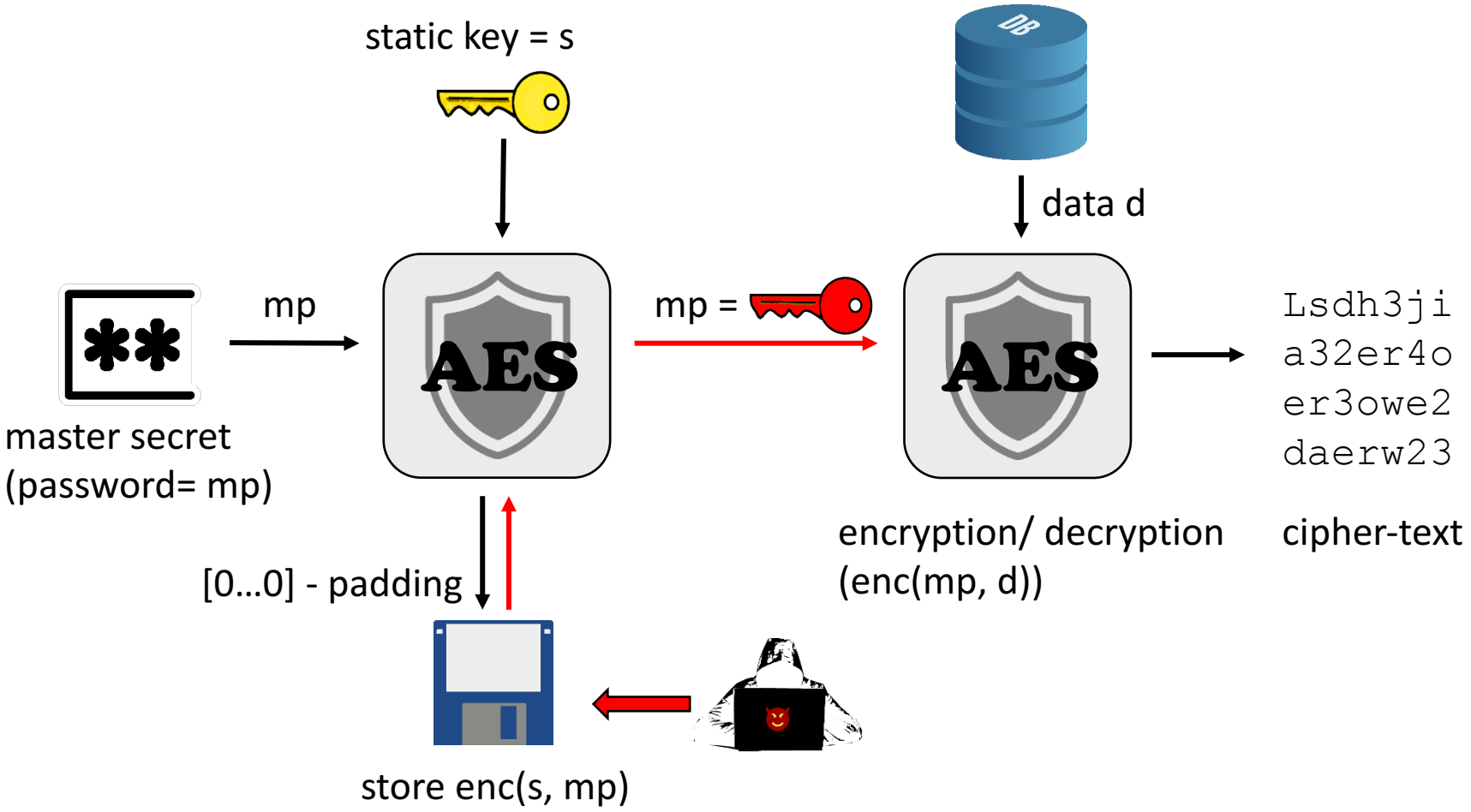
“A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.” *

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

Correct encryption



Bad Crypto


static key = s
DB
data d
mp
AES
mp =
AES
Lsdh3ji
a32er4o
er3owe2
daerw23
master secret
(password= mp)
encryption/ decryption
(enc(mp, d))
cipher-text
[0…0] - padding
store enc(s, mp)

Hard-coded keys

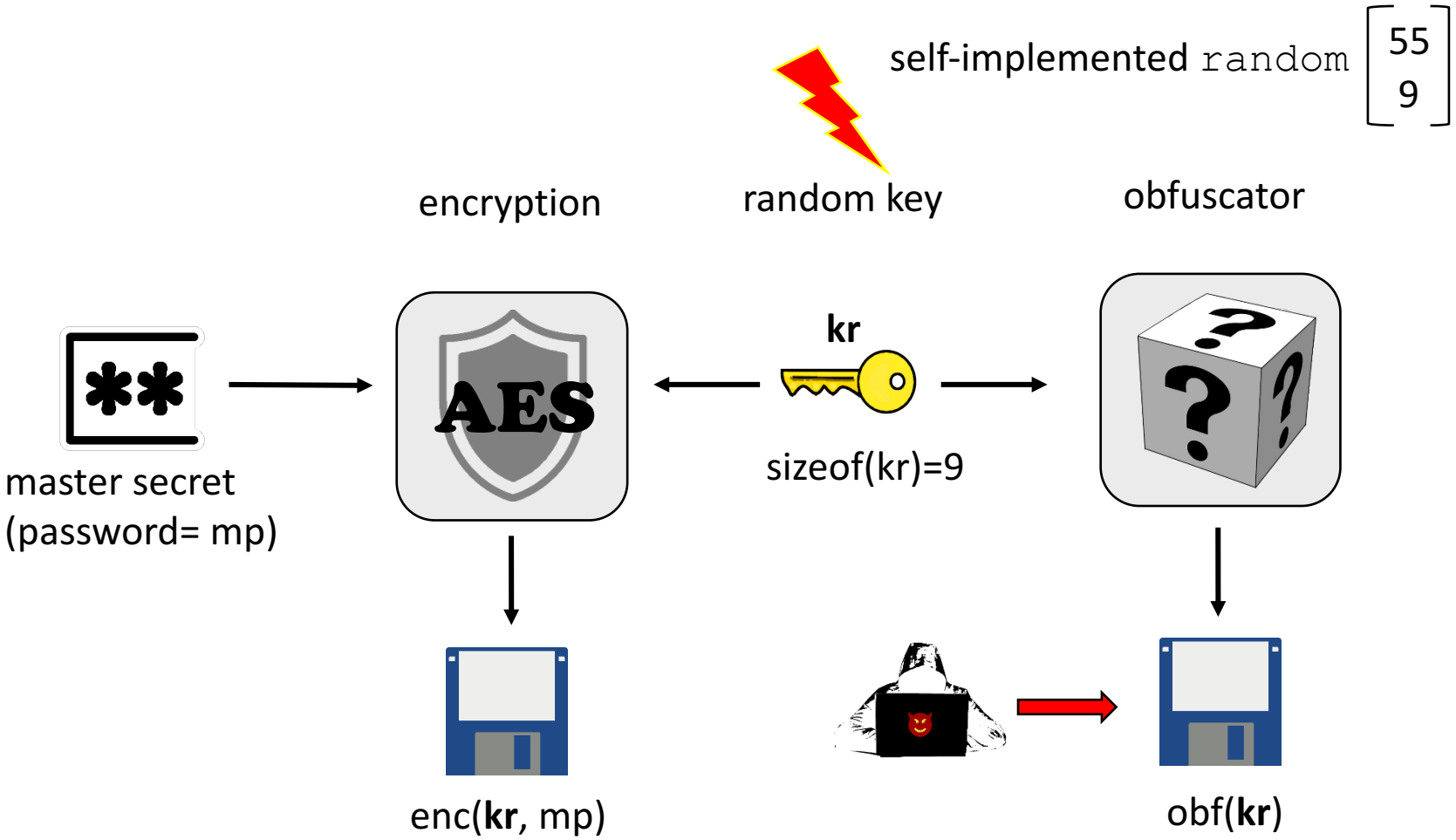
```
String = staticinvoke f.b("ydPCPFnpqfPuuBYPzhfGXD38gtUPN2yj",
$String);
```

AES-Key = ydPCPFnpqfPuuBYPzhfGXD38gtUPN2yj

```
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 = ldT52Fjsnjdn4390 89y23489h989fFFF;

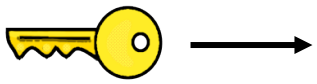
Broken Key Obfuscation



Broken Key Obfuscation

Random encryption key

kr



sizeof(kr)=9

obf(**kr**)

Obfuscated key

Abc2Abc2Abc2

sizeof(obf(kr))=12

obf(kr) parts	kr parts
Abc	kr[0] + kr[1]
2	kr[2]
Abc	kr[3] + kr[4]
2	kr[5]
Abc	kr[6] + kr[7]
2	kr[8]

Scheme:

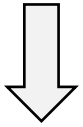
kr[0] + kr[1] = kr[3] + kr[4] =
kr [6] + kr[7]

and:
kr[2] = kr[5] = kr[8]

Broken Key Obfuscation

obf(kr) parts	kr parts
Abc	kr[0] + kr[1]
2	kr[2]
Abc	kr[3] + kr[4]
2	kr[5]
Abc	kr[6] + kr[7]
2	kr[8]

„Bruteforcing“



obf(kr) parts	Key kr[n] + kr[n+1]
ISF	!!
ISN	!#
QUF	AA
…	…
Abc	**kl**
…	…
enp	zz

- simple „rainbow“ tables
- 3 character mapping
- 1 character mapping

kr = **kl**$**kl**$**kl**$ ⟸ obf(kr)=Abc2Abc2Abc2

Recommendations (1/2)

- Use Android **`KeyStore`**
- Key derivation (e.g. **PBKDF2 (API), Conceal (Open Source, bcrypt, …**)
- No **static keys**
- Use **AES/CBC** or **AES/GCM**

Recommendations (2/2)

- Disable **backup flag** (apps support backend synchronization -> implicit backup)

- If there is a master pass storage function, **do not** store it in **plaintext**

- **Do not** store the **master pass** in the **local app folder**, this is not a protected area

	Keeper	Lastp	1Pass	MyPass	Avast	F-Sec	Keeps.	PwMgr	Mirsoft	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

THIS IS THE END
MY FRIEND

aim=e1Ioci	Ohyoh>wae0	kei7Gae$si	bei3coo<Li	ooB,iu9AhN	Phei0IeHa'	uhu;j5ohTi
Phi,Phu3di	Moo0ooz"oh	we(u,t0Zas	quucoo<d2I	Pae?gh<ie3	loh;Bah4ei	Wa[el~oh9i
ooh!ee7Aik	AX1aeSh>ai	eGah+K5iuM	yae$V4leex	ohjiu_Hei6	fee'Cho5Oo	jahK3Ad+ai
oH)eewaec0	KiG&ee4ahy	ujohj%ie1J	wae,Gei6mu	uSh=i2ahng	ainai]Le2i	Ieb~o5fohF
ohN\ah1gae	Dooch\ei7i	ich]a're1U	aiToh5cee=	eiZ2thaip;	ni"W3oom?i	oi(Sh7vie)
gu}i8Tohco	il@ah@ve9U	cie"tae8Eo	Au&S3aigae	eir0ieHo)c	ohch/ah6Ii	Bie*t9xie"
ukieTh6fu[	ie*vieZai9	ohwu(v0eeY	ua&ghi7aeR	em?ohG?oi3	phu$L^ah4p	ieX&i2shei
aiZie%l7Oo	ood8Pe<emo	faiGh[ie0i	OPho9sie>n	phie9Ib(ie	beiMei[r7a	Nagh(aid0U
AhTee:tah5	oY"a5pheib	ohthe1Na.e	eria9Ahn>u	eid8Ohso!o	Uv4ia6Gu`o	Aeli1li$i&
Toth^ai8ph	Euso6eu$ja	vie8Ieh?ai	leec4aeZ/o	Eele+ph2na	yai=b!a5Oo	Wefoh&m4oh
Vo-oX9ka0v	ei9eenuN<a	Eit}ae4ohF	heRie.J6Bo	OoZ-ue9mai	zait8coo]N	yoh9Oopoh$
xoh%C:ahk6	Zi]opu4eiB	eGh>ih2oPh	noo7Ish'ie	Uaz6she|Zu	oo0aiP*ee2	coh=Puo1Ve
roo9Kee-th	ra@c3Ce7sh	mabi6Malo[	auw1Eu\kie	eiVoo,Kuu5	aiW\oo5phu	Oos_abir7U

Password-Manager

- Premium features for free
- Resetting master password with ease
- Breaking C.I.A
  - Lost device scenario
  - Mitm attacks
  - Via third party app

	Keeper	Lastp	1Pass	MyPass	Avast	F-Sec	Keeps.	PwMgr	Mirsoft	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

team [SIK]

Stephan Huber
Email: stephan.huber@sit.fraunhofer.de

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

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