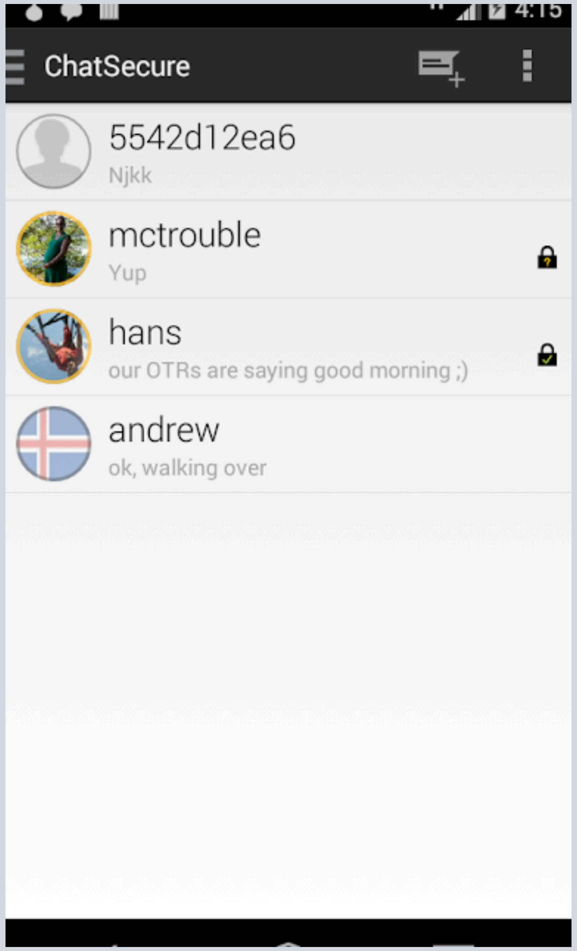
Lifting all boats: getting developers to improve app security

GUARDIAN PROJECT

https://guardianproject.info

modern design with privacy is possible

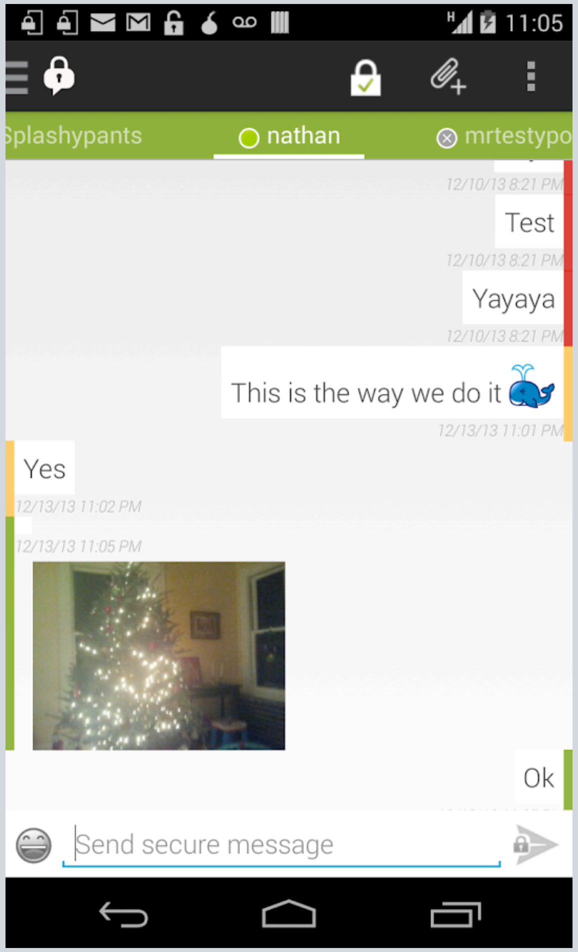


5542d12ea6
Njkk

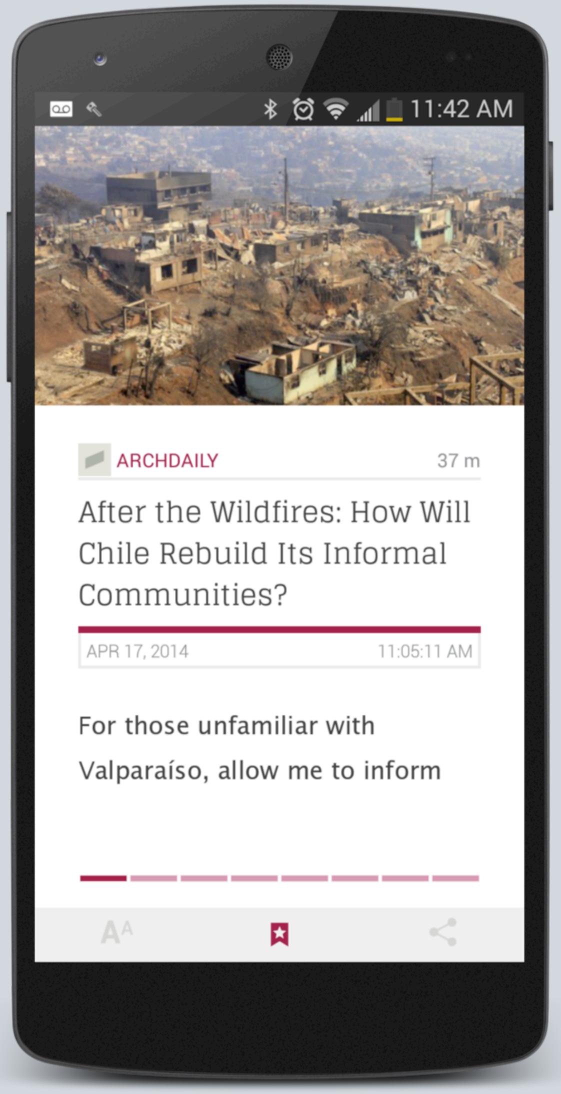
mctrouble
Yup

hans
our OTRs are saying good morning ;)

andrew
ok, walking over



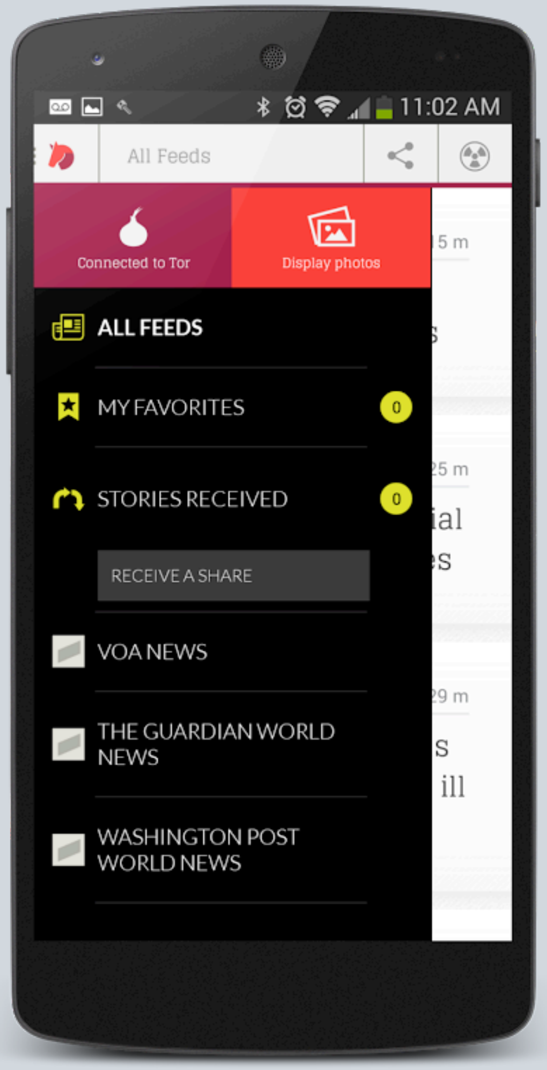
12/10/13 8:21 PM
Test
12/10/13 8:21 PM
Yayaya
12/10/13 8:21 PM
This is the way we do it
12/13/13 11:01 PM
Yes
12/13/13 11:02 PM
12/13/13 11:05 PM
Ok



After the Wildfires: How Will Chile Rebuild Its Informal Communities?

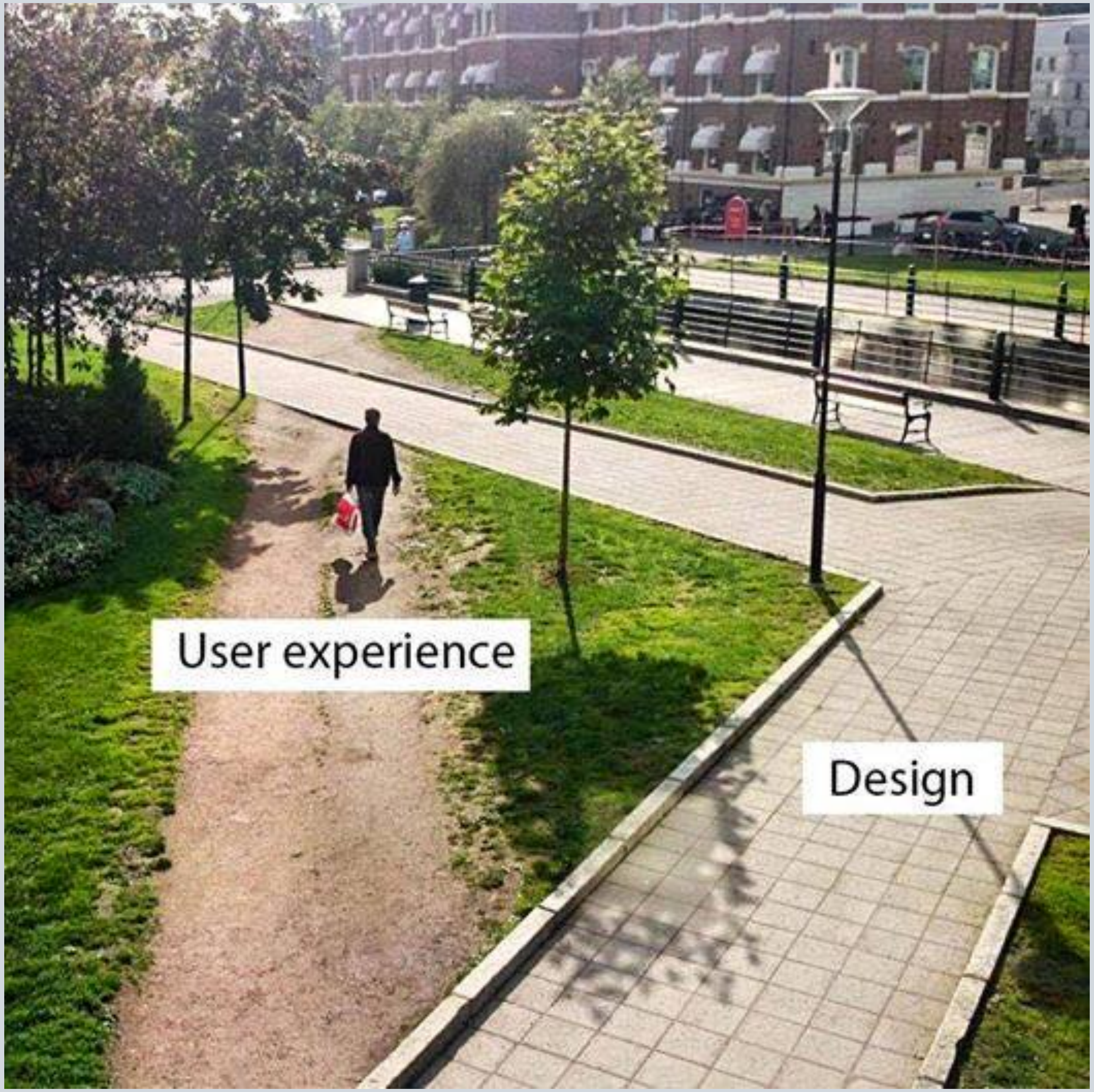
APR 17, 2014 11:05:11 AM

For those unfamiliar with Valparaíso, allow me to inform



we put privacy first

privacy through user experience



ACTIVISTS & CITIZEN JOURNALISTS

Tech savvy citizen journalists and activists in the street use Guardian apps to share updates, photos and videos without interception or monitoring by the authorities.

Reporters in the field can use Guardian apps to stay in touch with their safety networks, while safeguarding information on contacts, story notes and captured digital media, enabling a new, secure "reporter's notepad". In addition, high-resolution cameras of new Android hardware meet the quality standards for broadcast, print and online production.

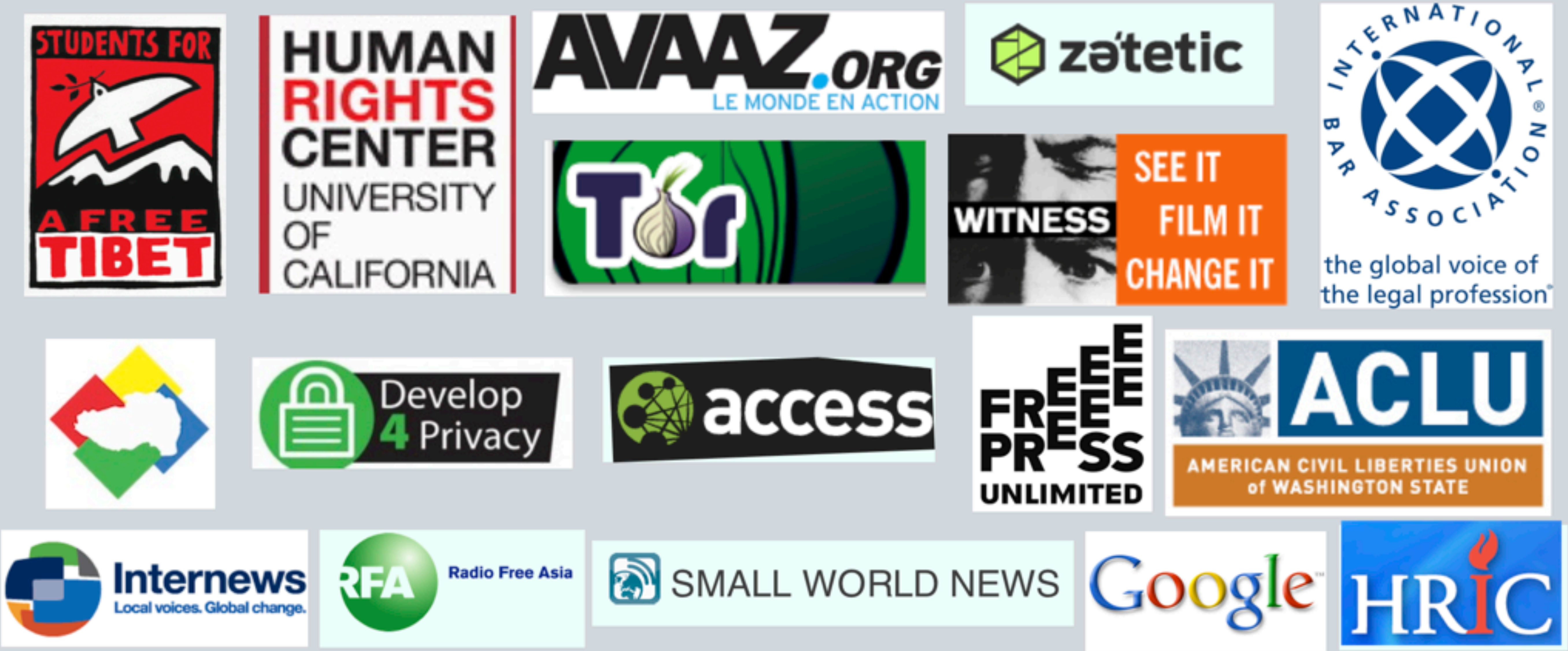
FRONTLINE REPORTERS

Business people travel all over the world, using foreign networks, bandwidth and systems. At any point, confidential information can be compromised. While some organizations implement solutions, these are often expensive, difficult to use, and not comprehensive

BUSINESS

HUMAN RIGHTS DEFENDERS

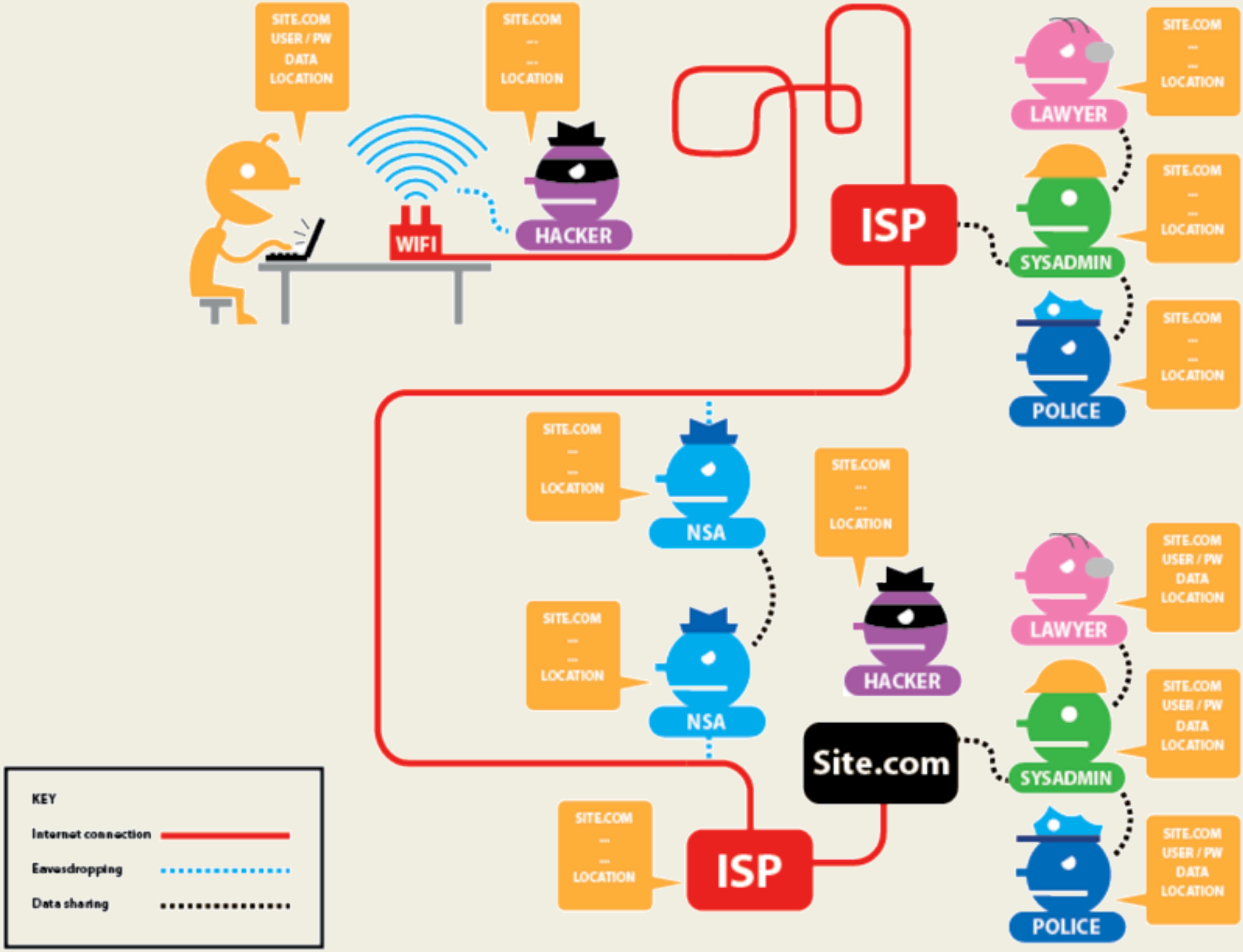
An undercover human rights researcher traveling through a remote region without mobile data service is able to use Guardian to document local conditions using secured video, audio and photo capture. Data is stored encrypted on the device, and if necessary, it can be safely and quickly erased.


STUDENTS FOR A FREE TIBET
HUMAN RIGHTS CENTER UNIVERSITY OF CALIFORNIA
AVAAZ.ORG LE MONDE EN ACTION
zətetic
INTERNATIONAL BAR ASSOCIATION
the global voice of the legal profession
Tor
WITNESS
SEE IT FILM IT CHANGE IT
Develop 4 Privacy
access
FREE PRESS UNLIMITED
ACLU
AMERICAN CIVIL LIBERTIES UNION of WASHINGTON STATE
Internews
Local voices. Global change.
RFA
Radio Free Asia
SMALL WORLD NEWS
Google
HRIC

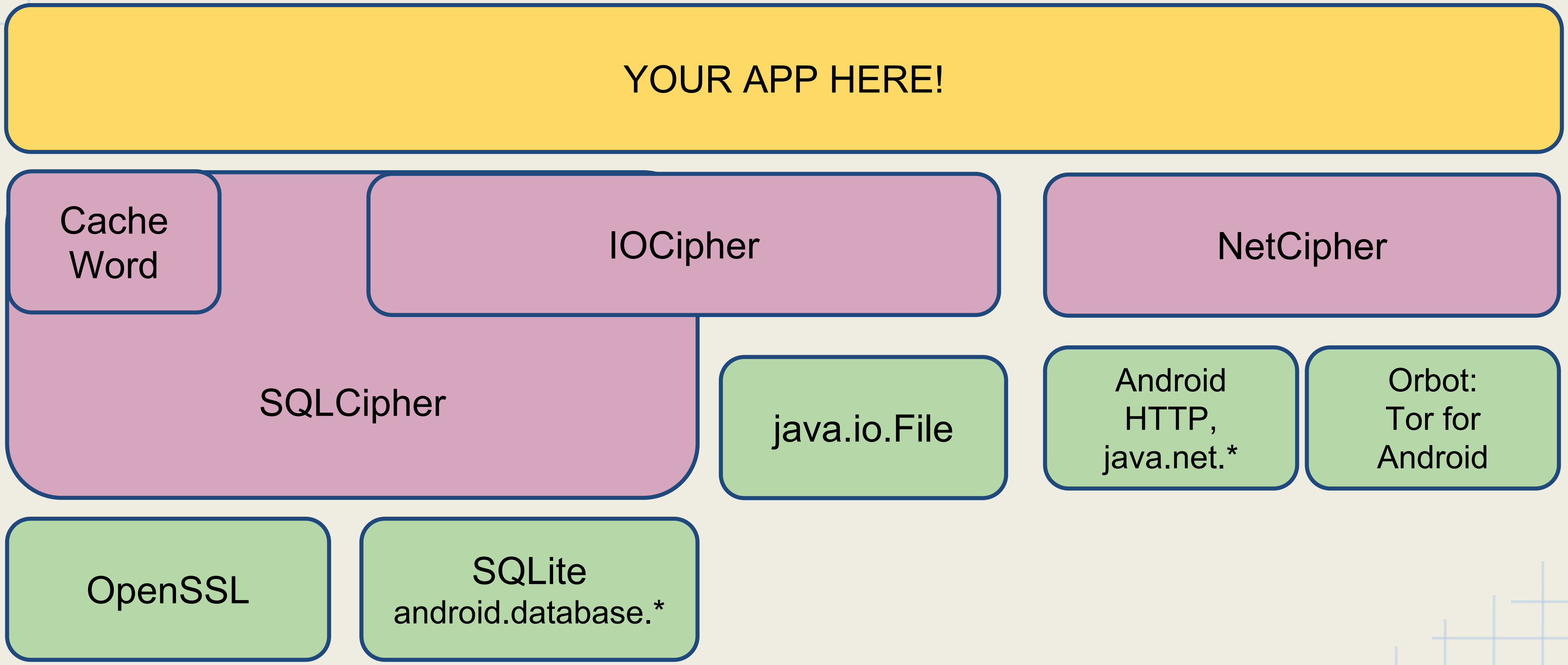
PARTNERSHIPS

We believe in protocols, not products / in partnerships, not proprietary fiefdoms / in building a community of collaborators, not a cacophony of criticism and unnecessary competition / in practical solutions to perilous problems.

there are many threats



CipherKit libraries



YOUR APP HERE!

Cache Word

IOCipher

NetCipher

SQLCipher

java.io.File

Android HTTP, java.net.*

Orbot: Tor for Android

OpenSSL

SQLite android.database.*

SQLCipher for Android

https://github.com/sqlcipher/android-database-sqlcipher

```
~ sjlombardo$ hexdump -C sqlite.db
00000000 53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 |SQLite format 3.|
…
000003c0 65 74 32 74 32 03 43 52 45 41 54 45 20 54 41 42 |et2t2.CREATE TAB|
000003d0 4c 45 20 74 32 28 61 2c 62 29 24 01 06 17 11 11 |LE t2(a,b)$…..|
…
000007e0 20 74 68 65 20 73 68 6f 77 15 01 03 01 2f 01 6f | the show…./.o|
000007f0 6e 65 20 66 6f 72 20 74 68 65 20 6d 6f 6e 65 79 |ne for the money|

~ $ sqlite3 sqlcipher.db
sqlite> PRAGMA KEY=’test123’;
sqlite> CREATE TABLE t1(a,b);
sqlite> INSERT INTO t1(a,b) VALUES (‘one for the money’, ‘two for the show’);
sqlite> .quit

~ $ hexdump -C sqlite.db
00000000 84 d1 36 18 eb b5 82 90 c4 70 0d ee 43 cb 61 87 |.?6.?..?p.?C?a.|
00000010 91 42 3c cd 55 24 ab c6 c4 1d c6 67 b4 e3 96 bb |.B?..?|
00000bf0 8e 99 ee 28 23 43 ab a4 97 cd 63 42 8a 8e 7c c6 |..?(#C??.?cB..|?|

~ $ sqlite3 sqlcipher.db
sqlite> SELECT * FROM t1;
Error: file is encrypted or is not a database
```

SQLite vs. SQLCipher

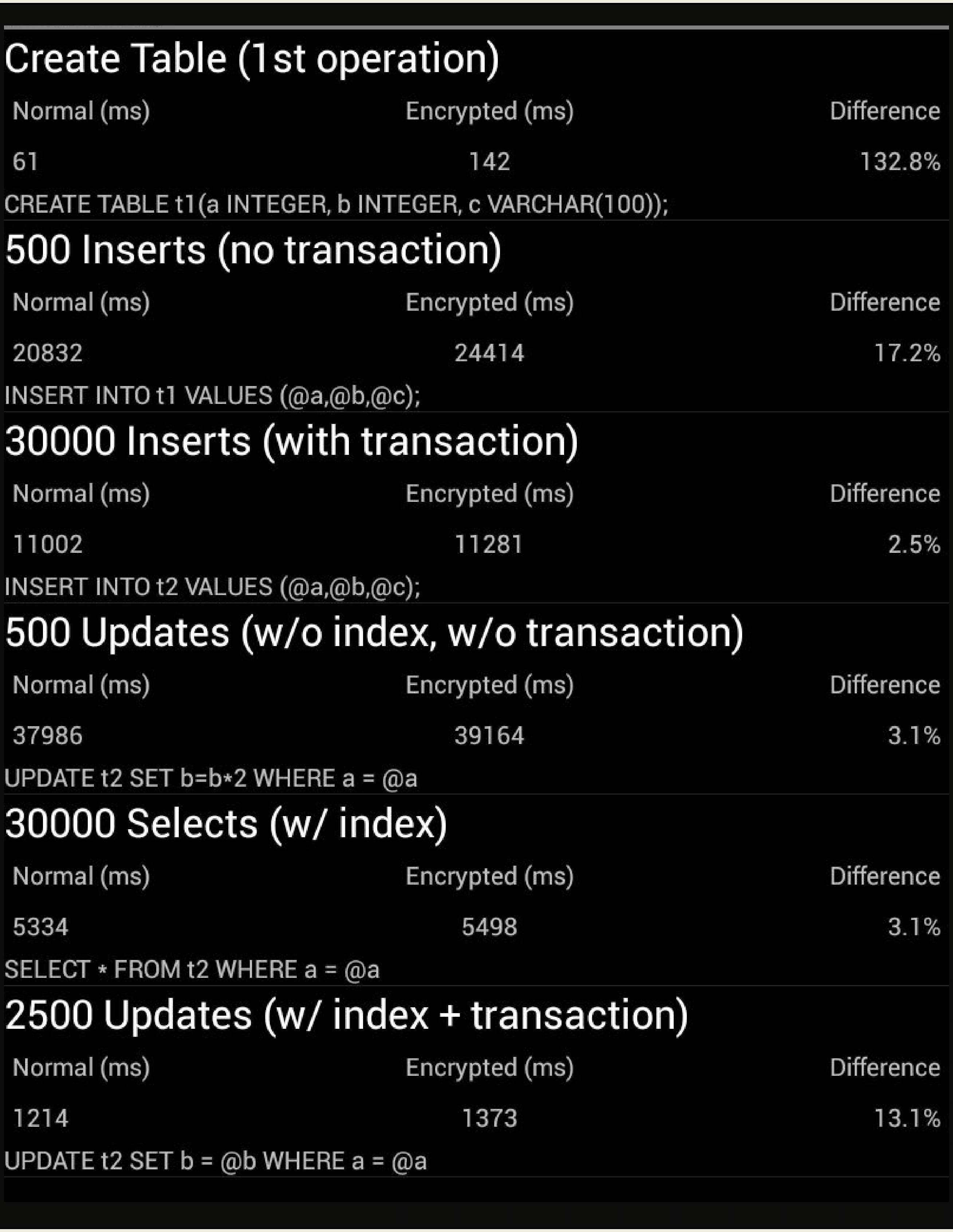
```
import net.sqlcipher.database.SQLiteDatabase;

SQLiteDatabase.loadLibs(this);

SQLiteDatabase db = eventsData.getWritableDatabase
(“mypassword”);
```

https://github.com/sqlcipher/android-database-sqlcipher

Performance



Create Table (1st operation)

Normal (ms)	Encrypted (ms)	Difference
61	142	132.8%

CREATE TABLE t1(a INTEGER, b INTEGER, c VARCHAR(100));

500 Inserts (no transaction)

Normal (ms)	Encrypted (ms)	Difference
20832	24414	17.2%

INSERT INTO t1 VALUES (@a,@b,@c);

30000 Inserts (with transaction)

Normal (ms)	Encrypted (ms)	Difference
11002	11281	2.5%

INSERT INTO t2 VALUES (@a,@b,@c);

500 Updates (w/o index, w/o transaction)

Normal (ms)	Encrypted (ms)	Difference
37986	39164	3.1%

UPDATE t2 SET b=b*2 WHERE a = @a

30000 Selects (w/ index)

Normal (ms)	Encrypted (ms)	Difference
5334	5498	3.1%

SELECT * FROM t2 WHERE a = @a

2500 Updates (w/ index + transaction)

Normal (ms)	Encrypted (ms)	Difference
1214	1373	13.1%

UPDATE t2 SET b = @b WHERE a = @a

https://github.com/sqlcipher/android-database-sqlcipher

NetCipher

https://github.com/guardianproject/netcipher

NetCipher

- add TLSv1.2 on older devices
- good TLS settings on all devices
- easy Tor support
- simplified proxy support
- used in Facebook Android app

https://github.com/guardianproject/netcipher

```
build.gradle:

 compile 'info.guardianproject.netcipher:netcipher:1.2.1'
```

Android URLConnection:

```
HttpsURLConnection connection =
  NetCipher.getHttpsURLConnection(“https://mysite.com”)
```

ch.boye Apache HttpClient:

```
StrongHttpsClient httpClient = new
   StrongHttpsClient(getApplicationContext());
```

more APIs!

- OkHTTP / Retrofit
  `'info.guardianproject.netcipher:netcipher-okhttp3:2.0.0-alpha1'`
- Google Volley
- `'info.guardianproject.netcipher:netcipher-volley:2.0.0-alpha1'`
- Apache HttpClient for Android
  `'info.guardianproject.netcipher:netcipher-httpclient:2.0.0-alpha1'`

https://github.com/guardianproject/netcipher

more proxying!

new proxies:

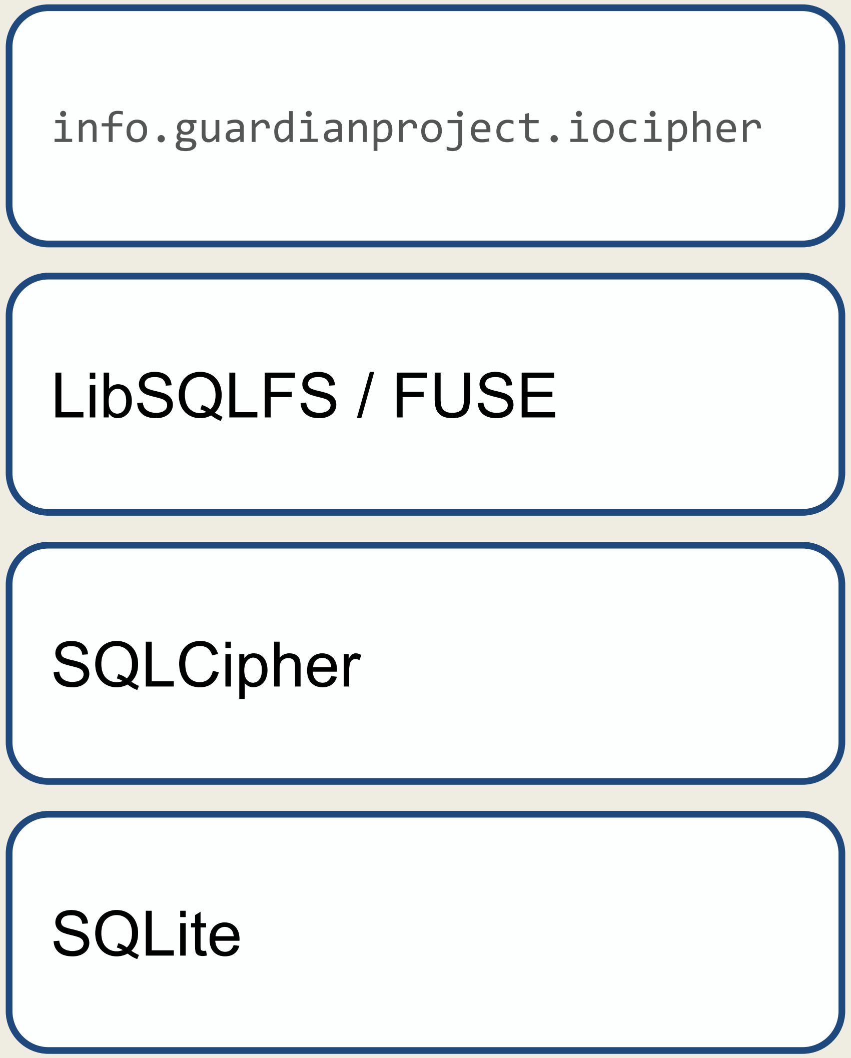
- Lantern
- Psiphon
- Meek and Tor Pluggable Transports

https://github.com/guardianproject/netcipher

IOCipher

https://github.com/guardianproject/iocipher

IOCipher: The Stack



`info.guardianproject.iocipher`

Java/JNI wrapper API

LibSQLFS / FUSE

Virtual Filesystem that maps to SQL schema / structured database

SQLCipher

Encryption layer for SQLite

SQLite

Base storage mechanism

https://github.com/guardianproject/iocipher

```java
import info.guardianproject.iocipher.File;
import info.guardianproject.iocipher.FileOutputStream;
import info.guardianproject.iocipher.VirtualFileSystem;

File dbFile = getDir("vfs", MODE_PRIVATE).getAbsolutePath() + "/myfiles.db";
vfs = new VirtualFileSystem(dbFile);


// TODO don't use a hard-coded password! prompt for the password
vfs.mount("my fake password");

File file = new File(dirPath);
File[] files = file.listFiles();
```

https://github.com/guardianproject/IOCipherExample

Adding IOCipher to App

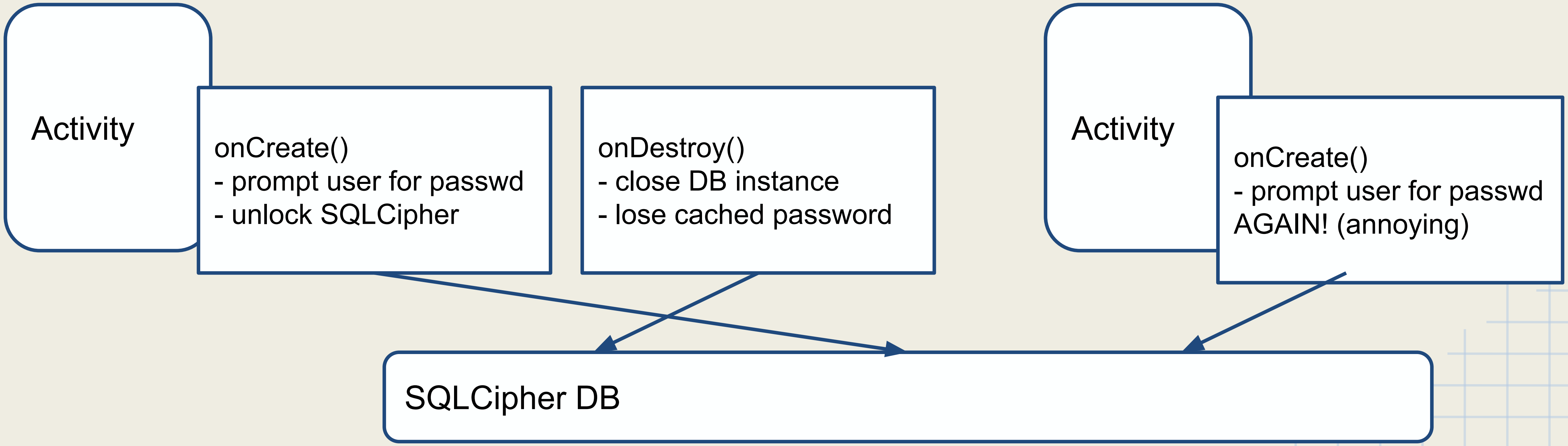
- manage the password
- connect to your encrypted disk’s file using new VirtualFileSystem(dbFile)
- mount it with a password using VirtualFileSystem.mount(password)
- replace the relevant java.io import statements withinfo.guardianproject.iocipher, e.g.:
    - import info.guardianproject.iocipher.File;
    - import info.guardianproject.iocipher.FileOutputStream;
    - import info.guardianproject.iocipher.FileReader;
    - import info.guardianproject.iocipher.IOCipherFileChannel;
    - import info.guardianproject.iocipher.VirtualFileSystem;
    - import java.io.FileNotFoundException;
    - import java.io.IOException;
    - import java.io.InputStream;
    - import java.nio.channels.Channels;
    - import java.nio.channels.ReadableByteChannel;

https://github.com/guardianproject/iocipher

CacheWord

https://github.com/guardianproject/cacheword

The problem with app passwords



Activity

onCreate()
- prompt user for passwd
- unlock SQLCipher

onDestroy()
- close DB instance
- lose cached password

Activity

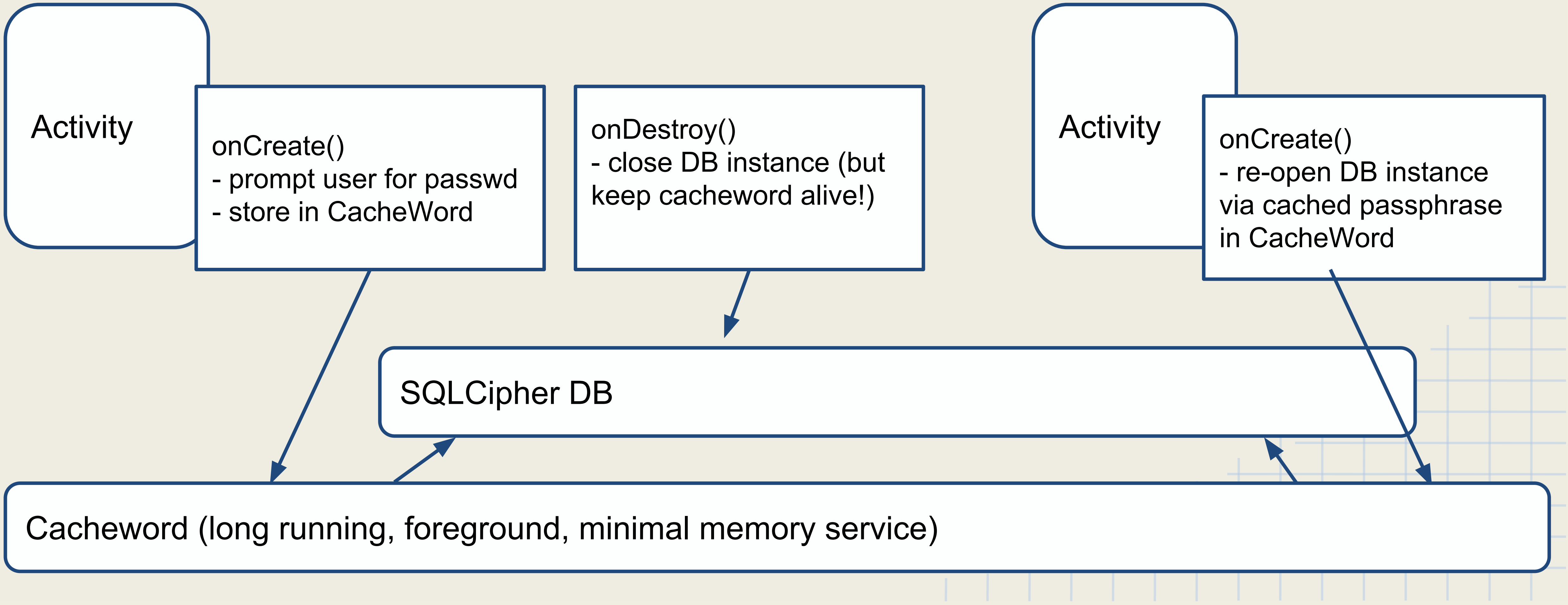
onCreate()
- prompt user for passwd
AGAIN! (annoying)

SQLCipher DB

(Activity, Service and even App lifespan is unpredictable)

https://github.com/guardianproject/cacheword

CacheWord Solution



Activity

onCreate()
- prompt user for passwd
- store in CacheWord

onDestroy()
- close DB instance (but keep cacheword alive!)

Activity

onCreate()
- re-open DB instance via cached passphrase in CacheWord

SQLCipher DB

Cacheword (long running, foreground, minimal memory service)

https://github.com/guardianproject/cacheword

```
public class CacheWordSampleActivity extends Activity implements      ICacheWordSubscriber {
...
        mCacheWord = new CacheWordActivityHandler(this);

@Override
    public void onCacheWordLocked() {}

    @Override
    public void onCacheWordOpened() {
               // fetch the encryption key from CacheWordService
        SecretKey key = ((PassphraseSecrets) mCacheWord.getCachedSecrets()).getSecretKey();
    }

    @Override
       public void onCacheWordUninitialized() {
               mCacheWord.setCachedSecrets(PassphraseSecrets.initializeSecrets(
                       CacheWordSampleActivity.this, “my secret passphrase”));
           }
```

https://github.com/guardianproject/cacheword/tree/master/sample

do not use device IDs as passwords!

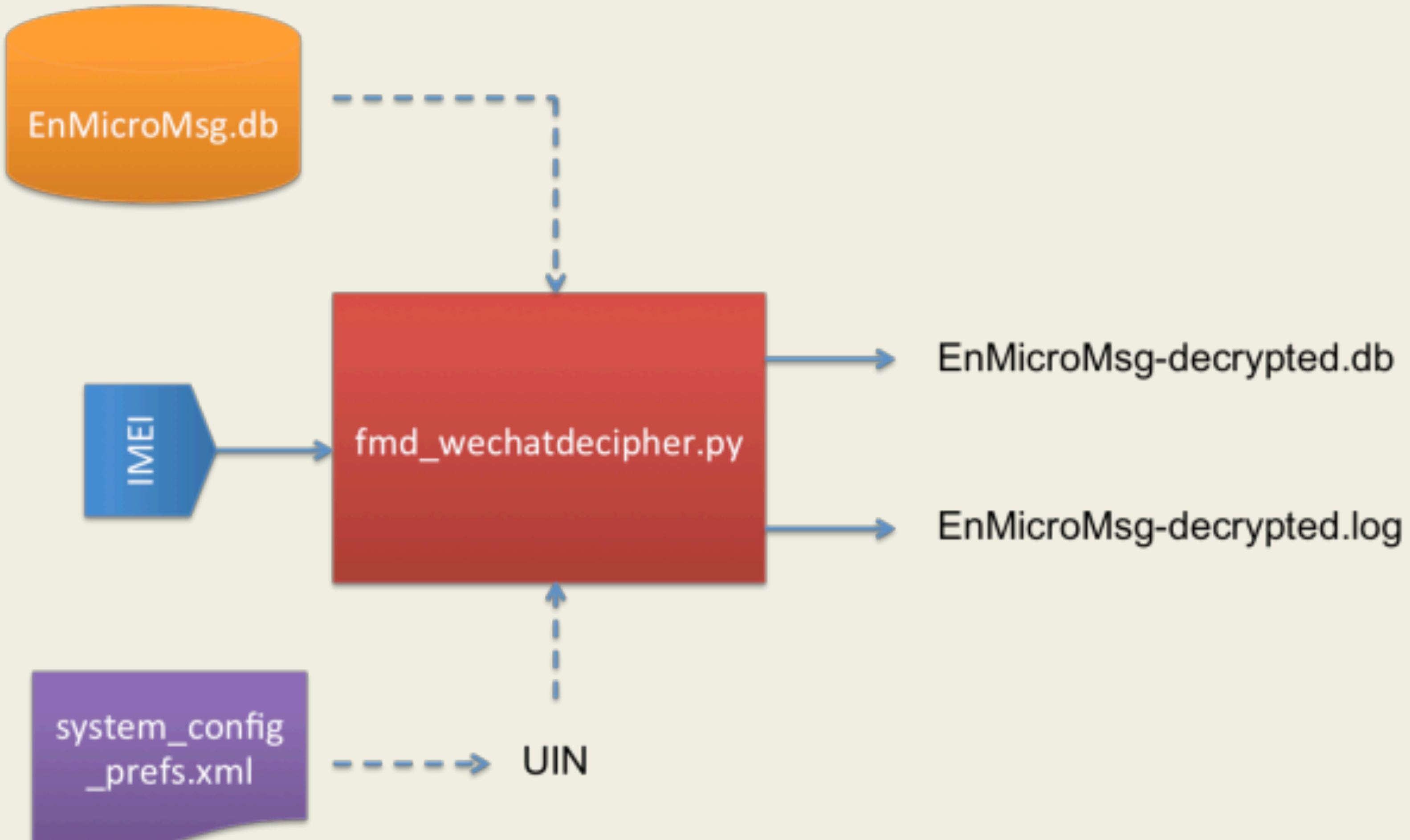
KEY = MD5(IMEI + UIN)[0:7]

IMEI: 357725678854269
UIN: -1881034049

IMEI + UIN = 357725678854269-1881034049

MD5(IMEI + UIN) = **4bc36a0**3296a8b4fc63e5bb8e74db2a2

KEY = **4bc36a0**



EnMicroMsg.db

IMEI

fmd_wechatdecipher.py

EnMicroMsg-decrypted.db

EnMicroMsg-decrypted.log

system_config_prefs.xml

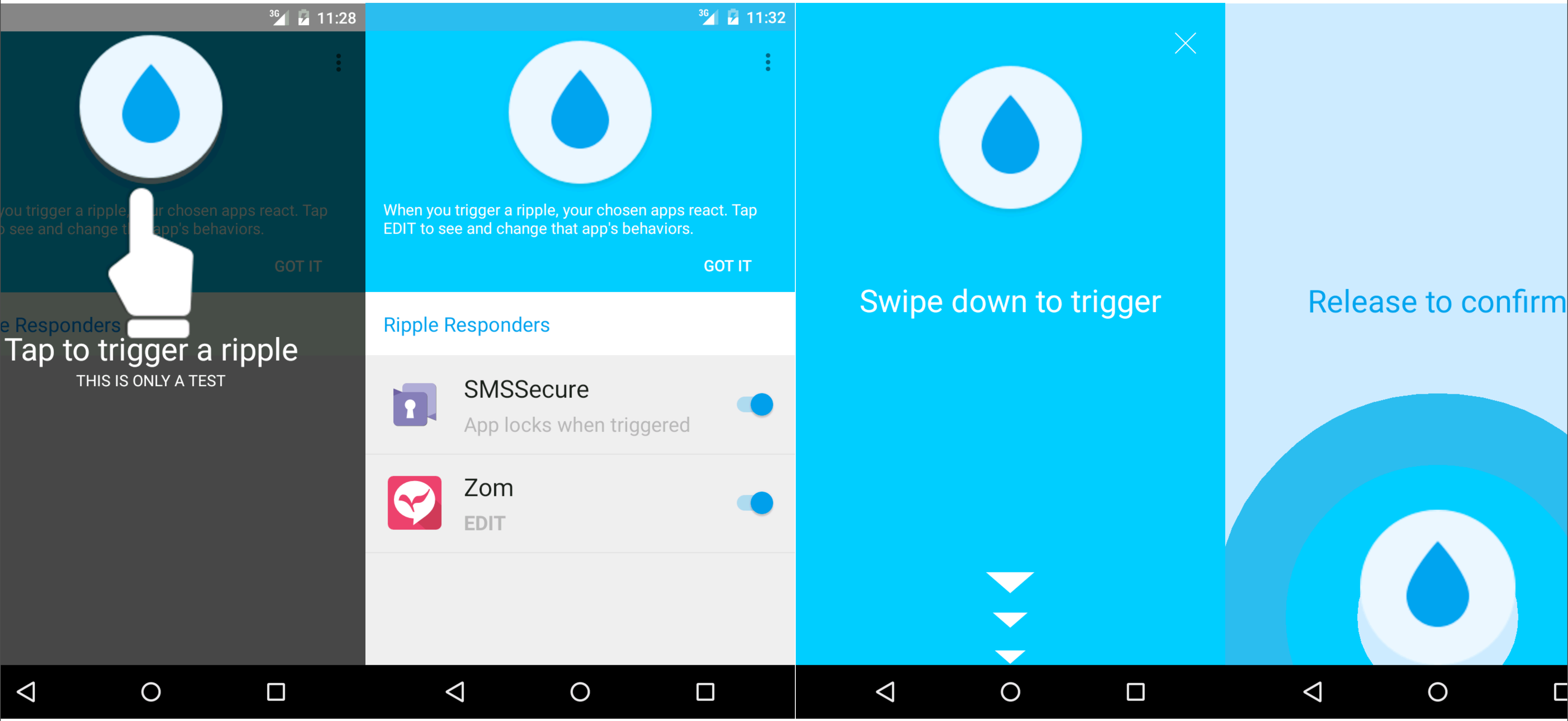
UIN

https://articles.forensicfocus.com/2014/10/01/decrypt-wechat-enmicromsgdb-database/

PanicKit

https://github.com/guardianproject/panickit

PanicKit



Tap to trigger a ripple

THIS IS ONLY A TEST

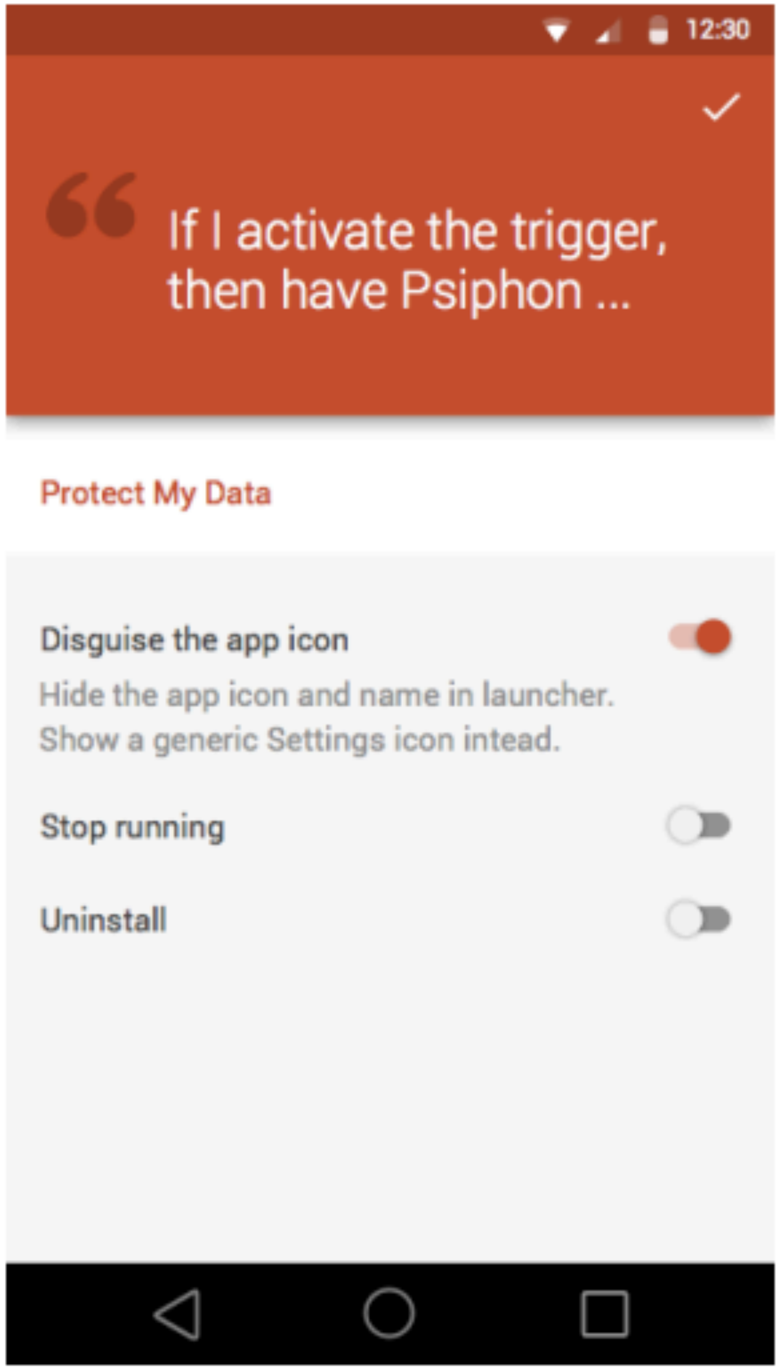
When you trigger a ripple, your chosen apps react. Tap EDIT to see and change that app's behaviors.

Swipe down to trigger

Release to confirm

https://github.com/guardianproject/panickit

02 Responders



12:30

“ If I activate the trigger, then have Psiphon ...

Protect My Data

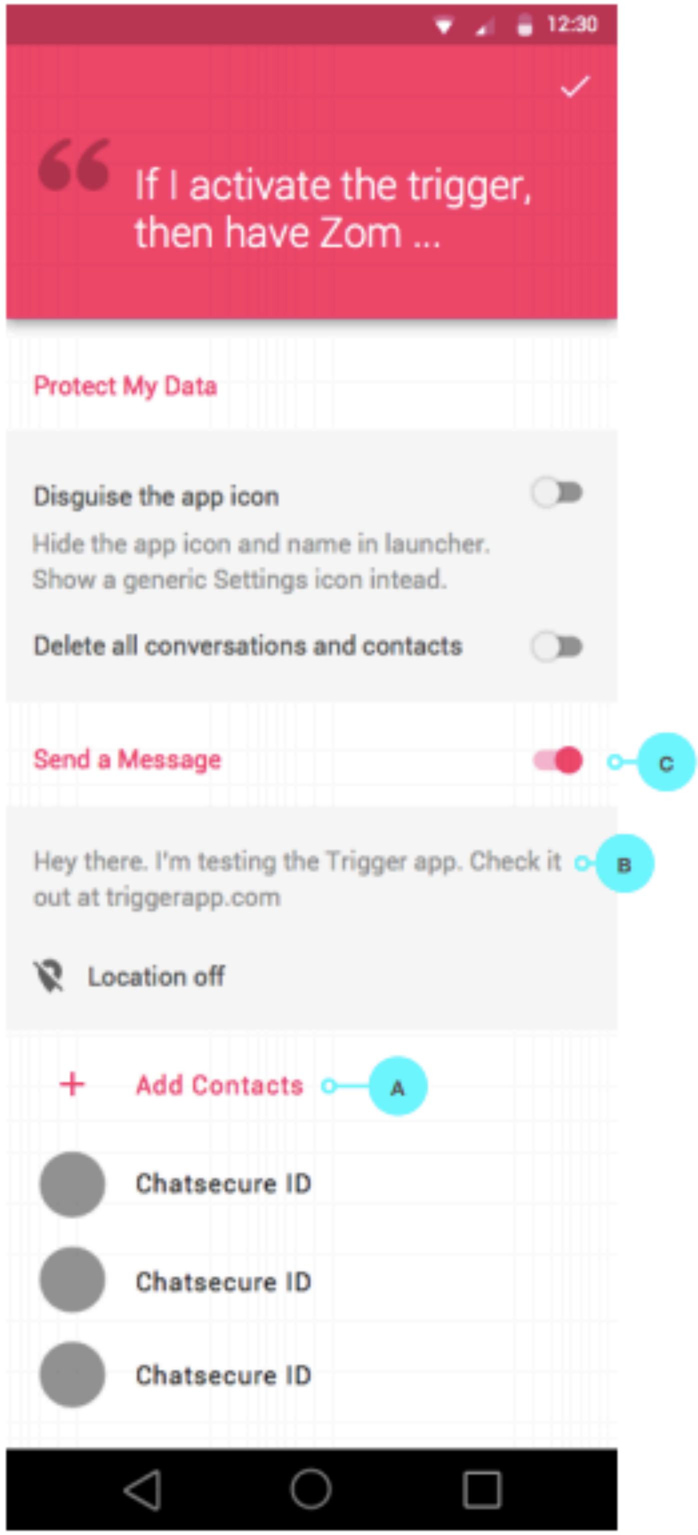
Disguise the app icon

Hide the app icon and name in launcher. Show a generic Settings icon intead.

Stop running

Uninstall

PSIPHON CONFIG



12:30

“ If I activate the trigger, then have Zom ...

Protect My Data

Disguise the app icon

Hide the app icon and name in launcher. Show a generic Settings icon intead.

Delete all conversations and contacts

Send a Message

Hey there. I'm testing the Trigger app. Check it out at triggerapp.com

Location off

+ Add Contacts

Chatsecure ID

Chatsecure ID

Chatsecure ID

ZOM CONFIG

Defaults

The default panic action of a responder is a non-destructive action such as locking the app or disguising the app icon. This default response is set by the creators of the responder app.

User Actions

A. Tap to choose contacts. Go to **03 ZOM CONFIG: CHOOSE CONTACTS**

B. Tap to edit the message. Go to **03 ZOM CONFIG: EDIT MESSAGE**.

C. Toggle to enable or disable this action. If enabled the default action within this section would be selected (ex: Disguise app icon). The default action would change based on the most recently selected action by the user.

Add a note about the OR cases

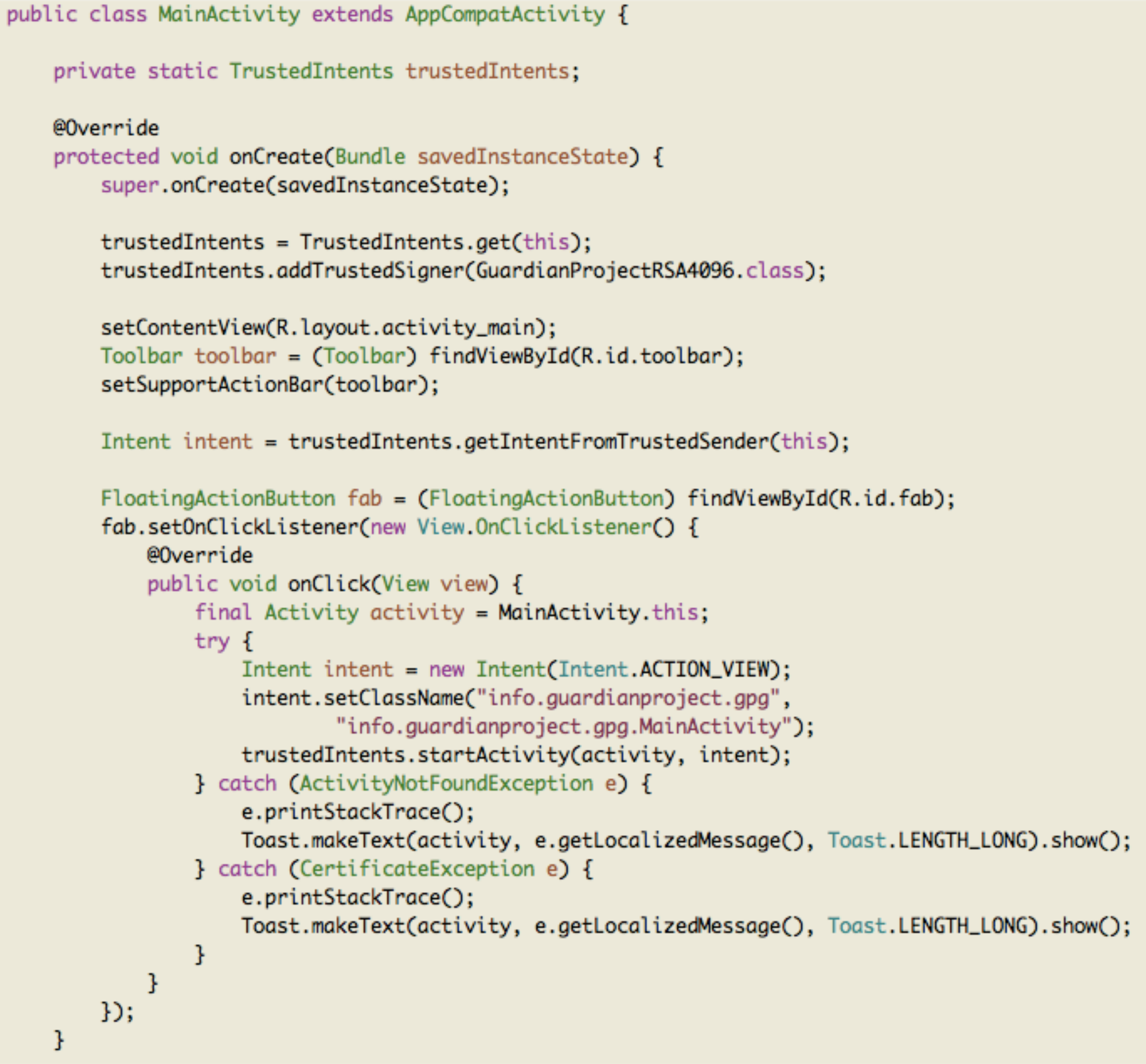
TrustedIntents

https://github.com/guardianproject/trustedintents

is it really you?

- am I directing users to the real Orbot?
- did this file come from the real Google Drive?
- was this Intent from one of our own apps?

`https://github.com/guardianproject/trustedintents`



```
public class MainActivity extends AppCompatActivity {

    private static TrustedIntents trustedIntents;

    @Override
    protected void onCreate(Bundle savedInstanceState) {
        super.onCreate(savedInstanceState);

        trustedIntents = TrustedIntents.get(this);
        trustedIntents.addTrustedSigner(GuardianProjectRSA4096.class);

        setContentView(R.layout.activity_main);
        Toolbar toolbar = (Toolbar) findViewById(R.id.toolbar);
        setSupportActionBar(toolbar);

        Intent intent = trustedIntents.getIntentFromTrustedSender(this);

        FloatingActionButton fab = (FloatingActionButton) findViewById(R.id.fab);
        fab.setOnClickListener(new View.OnClickListener() {
            @Override
            public void onClick(View view) {
                final Activity activity = MainActivity.this;
                try {
                    Intent intent = new Intent(Intent.ACTION_VIEW);
                    intent.setClassName("info.guardianproject.gpg",
                            "info.guardianproject.gpg.MainActivity");
                    trustedIntents.startActivity(activity, intent);
                } catch (ActivityNotFoundException e) {
                    e.printStackTrace();
                    Toast.makeText(activity, e.getLocalizedMessage(), Toast.LENGTH_LONG).show();
                } catch (CertificateException e) {
                    e.printStackTrace();
                    Toast.makeText(activity, e.getLocalizedMessage(), Toast.LENGTH_LONG).show();
                }
            }
        });
    }
```

https://github.com/guardianproject/trustedintents

reproducible builds!

XCodeGhost

- malware version of XCode inserted library
- 10s of millions of users received affected apps
- reproducible builds would have prevented this
- more info at https://reproducible-builds.org

F-Droid

an community run Android app store that distributes verified Free Software

fdroidserver tools

- makes reproducible builds trivial
- drozer scans for vulnerabilities
- libscout scans for old libs
- full, automated, secure build environment
- flexible automated signatures

https://github.com/guardianproject

Lifting all boats: getting developers to improve app security

Hans-Christoph Steiner
Guardian Project
hans@guardianproject.info

The Guardian Project

https://guardianproject.info

Secure Your Mobile Life
Apps & Tools You Can Trust

The Guardian Project creates easy-to-use open source apps, mobile OS security enhancements, and customized mobile devices for people around the world to help them communicate more freely, and protect themselves from intrusion and monitoring.