CENSUS
IT Security Works

Side Channel Leaks in Mobile Applications

6th Infocom Mobile World Conference 2016

Ioannis Stais, IT Security Consultant
istais@census-labs.com

www.census-labs.com

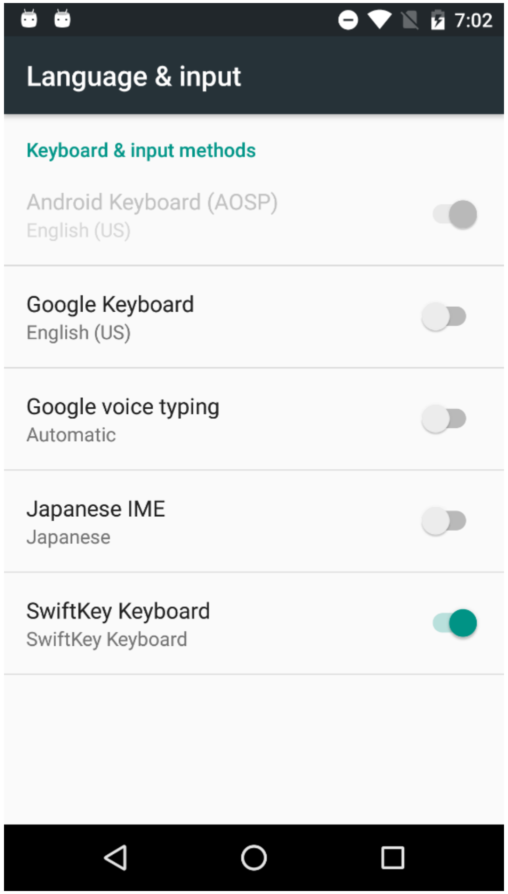
> INTRO

> SIDE CHANNEL LEAKS - WHAT? WHY?

- *Mobile App unintentionally exposes sensitive data through a side channel*
- Arises as a side effect from the underlying mobile platform
- Commonly related to features that enhance app performance & to poorly implemented functionalities
- Leads to significant impact:
  - *Violates User Privacy*
  - *Creates Legal, regulatory, and financial risks*
  - *Affects Corporate Reputation & Brand Image*

> COMMON SIDE CHANNEL LEAK VULNERABILITIES

> CUSTOM KEYBOARD



7:02

Language & input

Keyboard & input methods

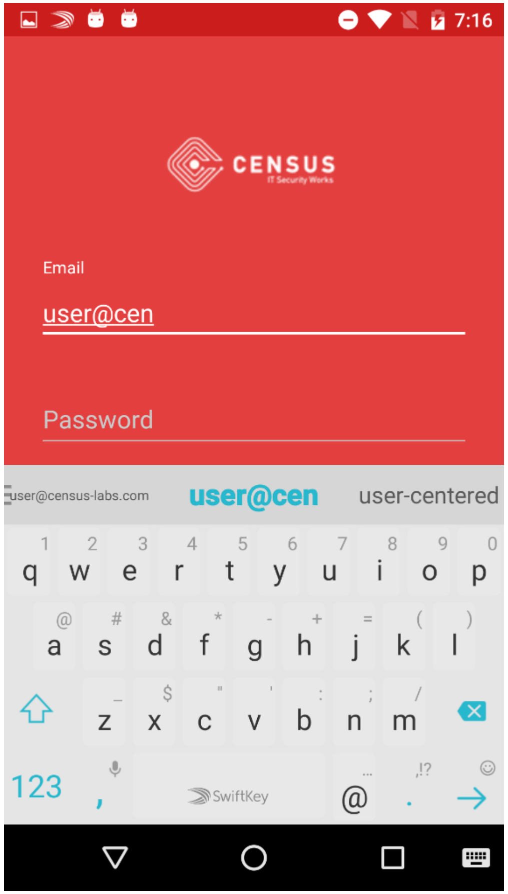
Android Keyboard (AOSP)
English (US)

Google Keyboard
English (US)

Google voice typing
Automatic

Japanese IME
Japanese

SwiftKey Keyboard
SwiftKey Keyboard



7:16

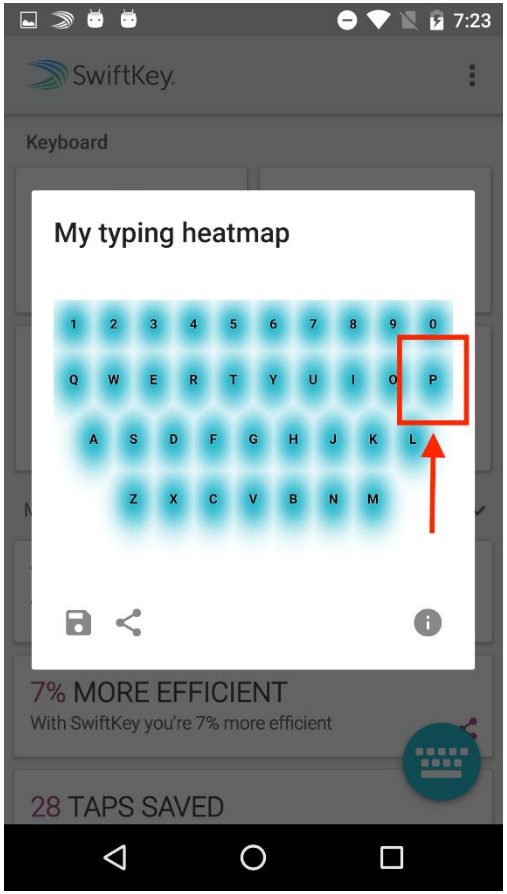
CENSUS
IT Security Works

Email

user@cen

Password

user@census-labs.com | user@cen | user-centered



7:23

SwiftKey

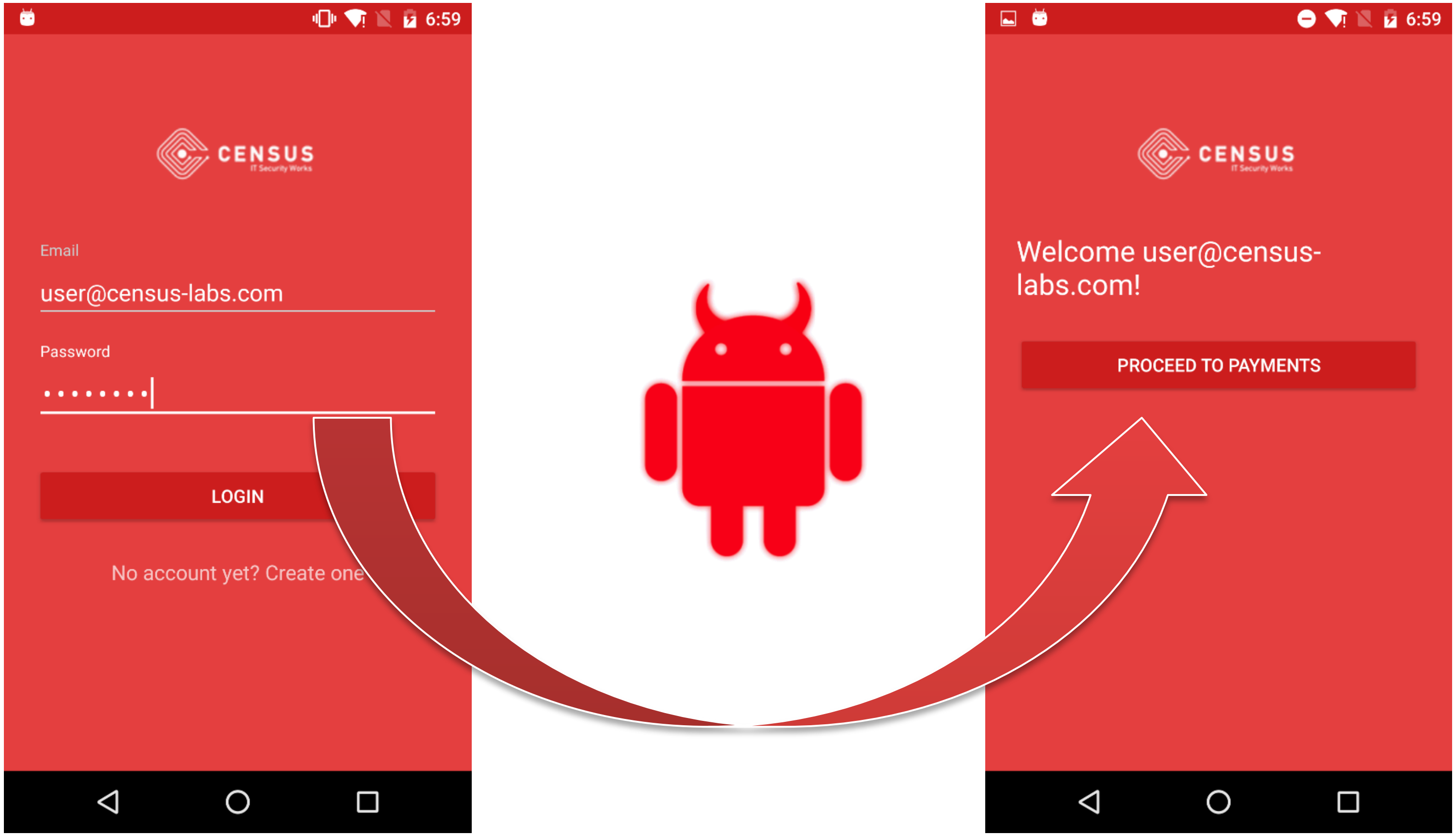
Keyboard

My typing heatmap

7% MORE EFFICIENT
With SwiftKey you're 7% more efficient

28 TAPS SAVED

> LEAKING ACTIVITY COMPONENTS



6:59

CENSUS IT Security Works

Email

user@census-labs.com

Password

•••••••••

LOGIN

No account yet? Create one

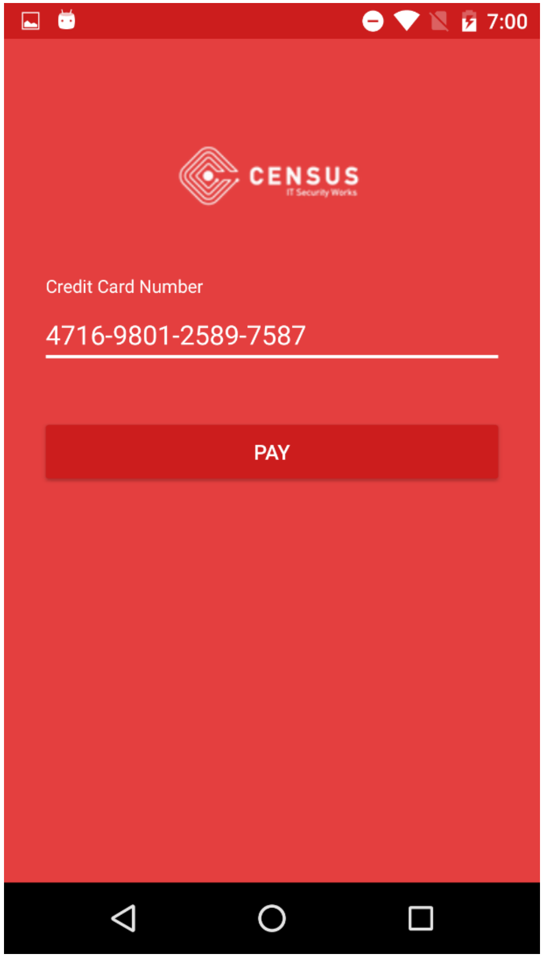
6:59

CENSUS IT Security Works

Welcome user@census-labs.com!

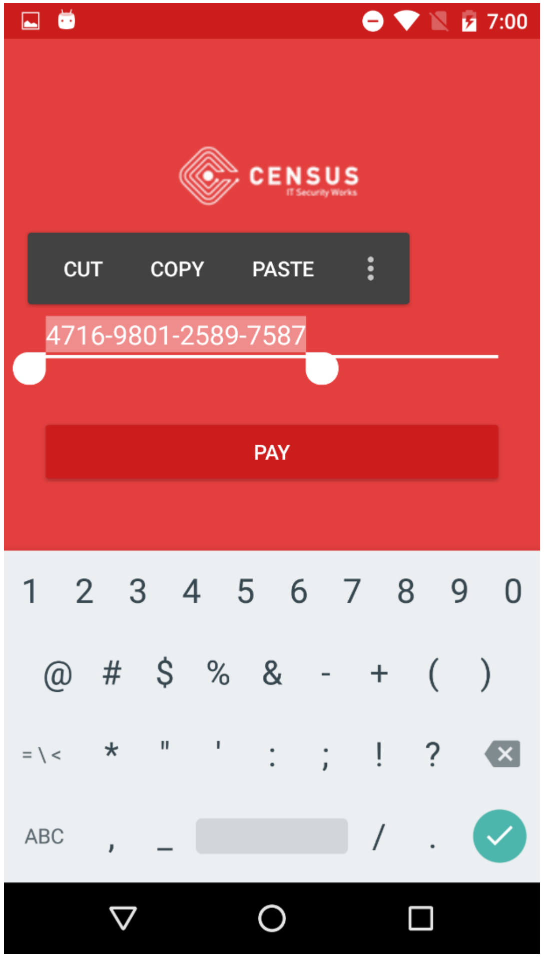
PROCEED TO PAYMENTS

> PASTEBOARD LEAKS



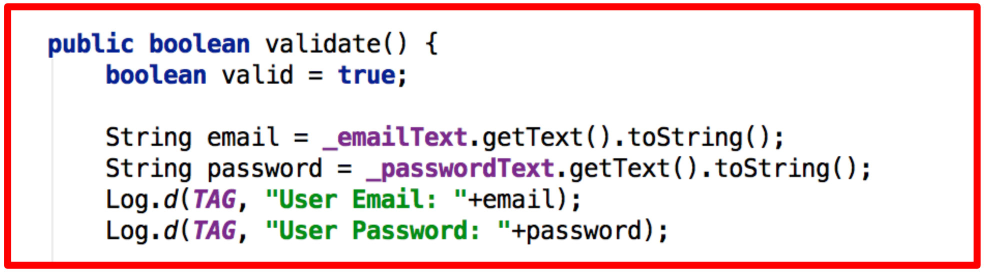
Credit Card Number

4716-9801-2589-7587

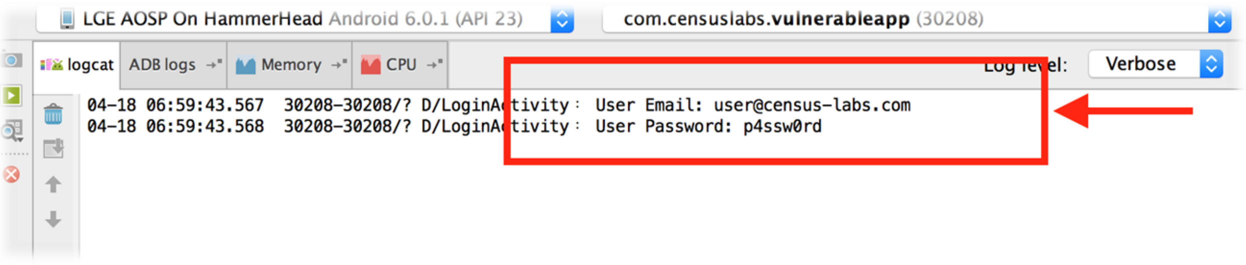


4716-9801-2589-7587

> DEBUG LOG LEAKS

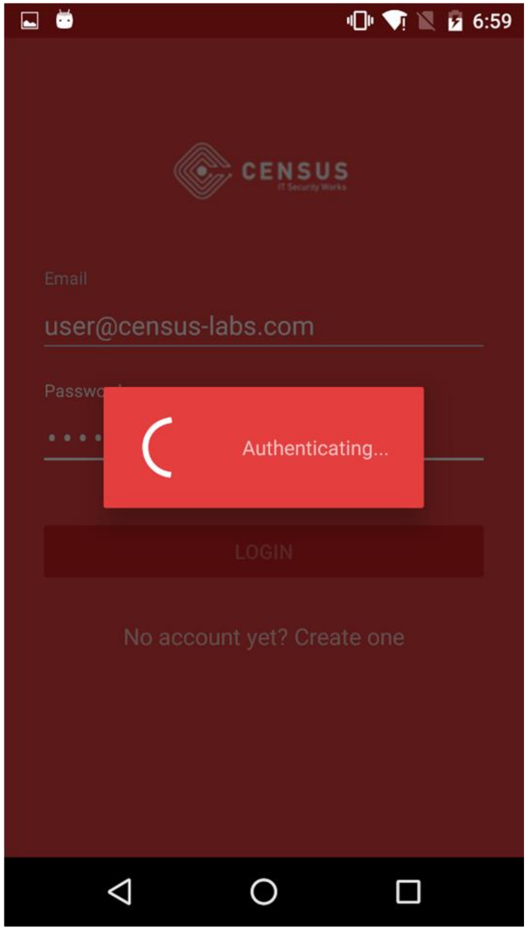


```
public boolean validate() {
    boolean valid = true;

    String email = _emailText.getText().toString();
    String password = _passwordText.getText().toString();
    Log.d(TAG, "User Email: "+email);
    Log.d(TAG, "User Password: "+password);
```

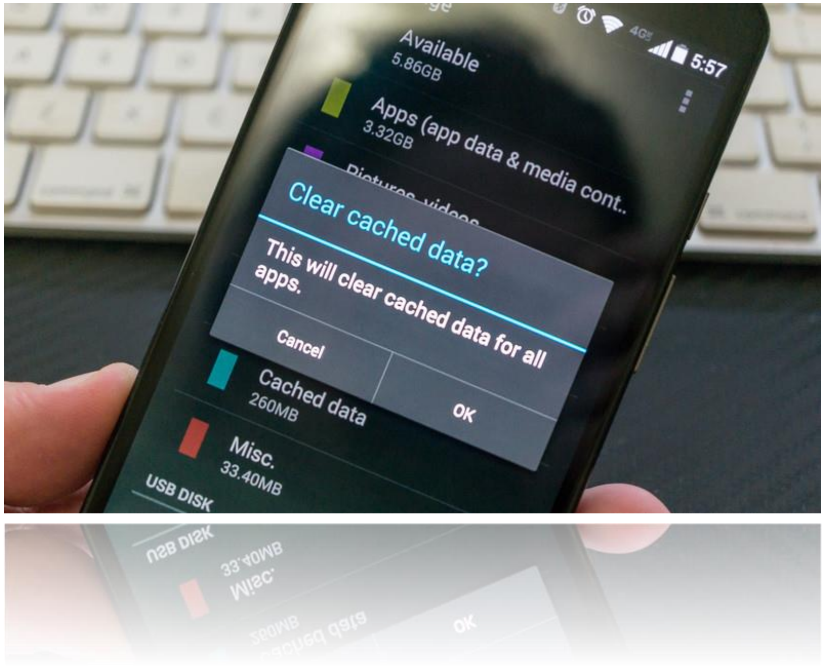


LGE AOSP On HammerHead Android 6.0.1 (API 23)
com.censuslabs.vulnerableapp (30208)
logcat
ADB logs
Memory
CPU
Log level:
Verbose

```
04-18 06:59:43.567  30208-30208/? D/LoginActivity: User Email: user@census-labs.com
04-18 06:59:43.568  30208-30208/? D/LoginActivity: User Password: p4ssw0rd
```

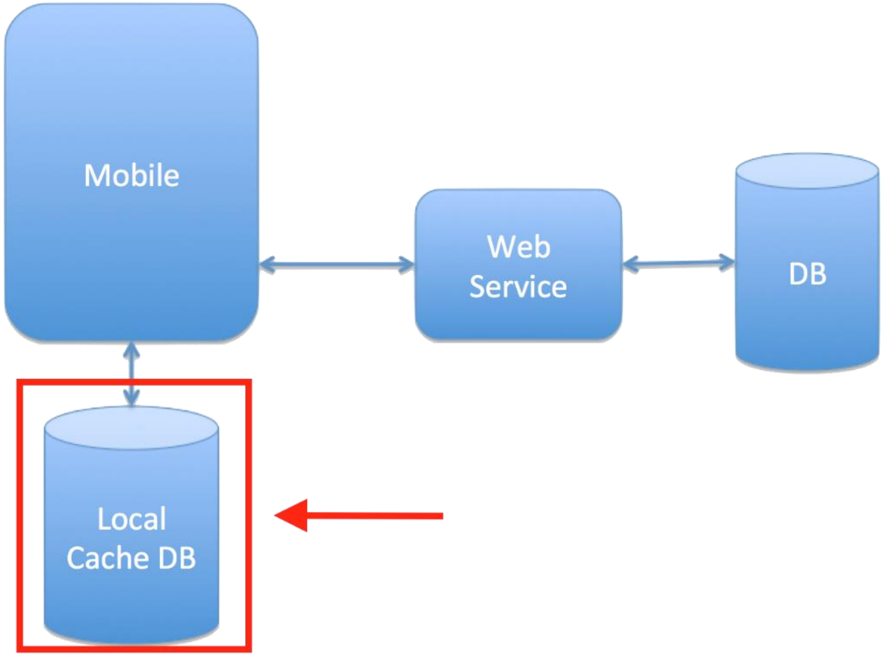


> URL CACHING & WEBVIEW OBJECTS

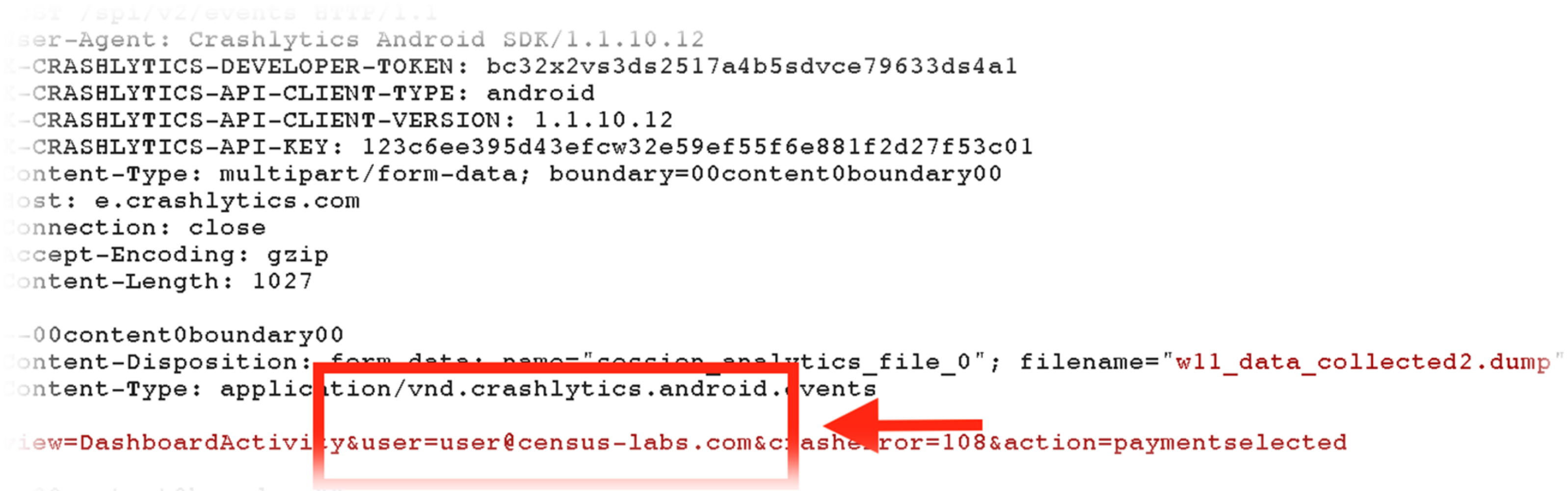


Clear cached data?

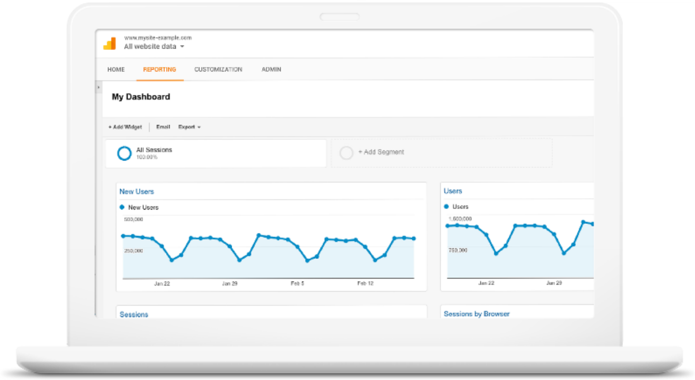
This will clear cached data for all apps.



> ANALYTICS DATA LEAKS

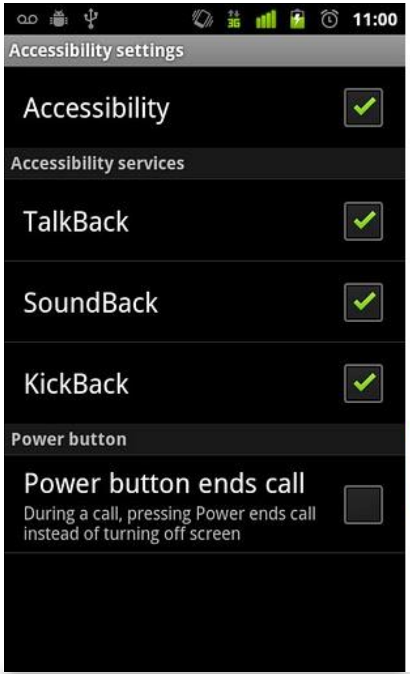


```
POST /spi/v2/events HTTP/1.1
User-Agent: Crashlytics Android SDK/1.1.10.12
X-CRASHLYTICS-DEVELOPER-TOKEN: bc32x2vs3ds2517a4b5sdvce79633ds4a1
X-CRASHLYTICS-API-CLIENT-TYPE: android
X-CRASHLYTICS-API-CLIENT-VERSION: 1.1.10.12
X-CRASHLYTICS-API-KEY: 123c6ee395d43efcw32e59ef55f6e881f2d27f53c01
Content-Type: multipart/form-data; boundary=00content0boundary00
Host: e.crashlytics.com
Connection: close
Accept-Encoding: gzip
Content-Length: 1027

--00content0boundary00
Content-Disposition: form-data; name="session_analytics_file_0"; filename="w11_data_collected2.dump"
Content-Type: application/vnd.crashlytics.android.events

view=DashboardActivity&user=user@census-labs.com&crasherror=108&action=paymentselected

--00content0boundary00--
```



CENSUS S.A.
www.census-labs.com

> EXPLOITING ACCESSIBILITY



11:00

Accessibility settings

Accessibility ☑

Accessibility services

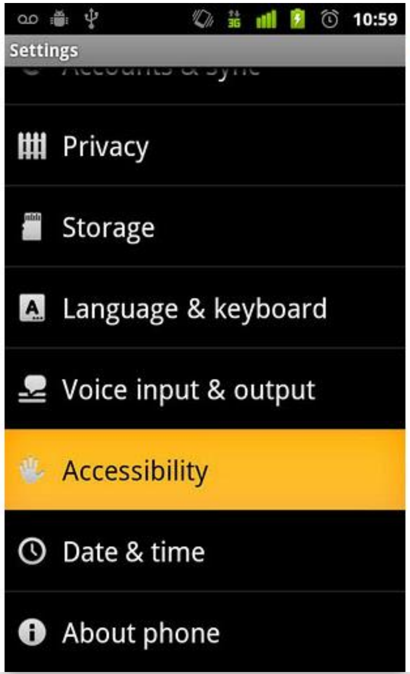
TalkBack ☑

SoundBack ☑

KickBack ☑

Power button

Power button ends call ☐
During a call, pressing Power ends call instead of turning off screen



10:59

Settings

Accounts & sync

Privacy

Storage

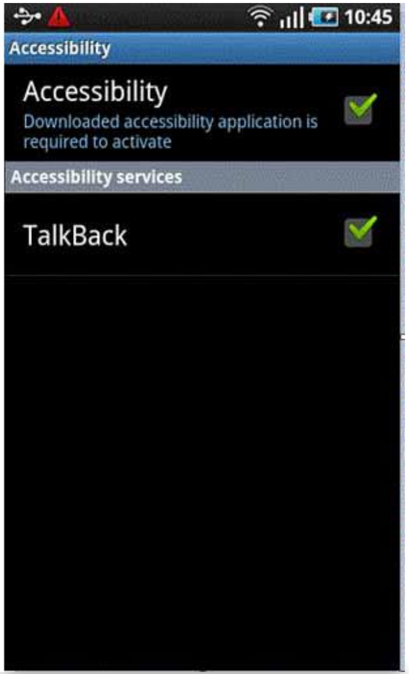
Language & keyboard

Voice input & output

Accessibility

Date & time

About phone



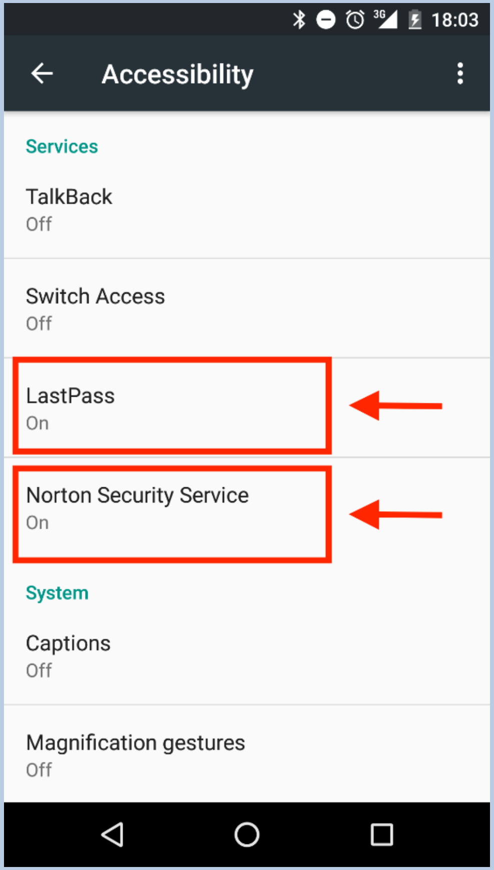
10:45

Accessibility

Accessibility ☑
Downloaded accessibility application is required to activate

Accessibility services

TalkBack ☑



18:03

Accessibility

Services

TalkBack
Off

Switch Access
Off

LastPass
On

Norton Security Service
On

System

Captions
Off

Magnification gestures
Off

> CONCLUSIONS

> CONCLUSIONS

- Risk Mitigation
  - Practice Privacy By Design: Be proactive
  - Perform Security Assessments
  - Communicate Openly & Effectively
  - Make Your Privacy Policy Easily Accessible
  - Empower users: Provide Choices & Controls
  - Enforce Accountability

> CONCLUSIONS

- Limit Data Collection & Retention
  - Don’t access or collect user data
  - Shorten the life cycle of sensitive data
  - Establish a data retention policy
  - Delete user data promptly following the deletion of an account
- Mobile App internal processes may need to be examined, and re-engineered

Thank you!

CENSUS

IT Security Works