GRACE HOPPER CELEBRATION

/ ANITA B.ORG

Emerging Attacks on Mobile Applications

Agenda

- Introduction
- Importance of Mobile Security
- Demonstration of Android Exploits
- Key Take Away

Disclaimer

- The vulnerabilities discussed in this presentation are not specific to Android platform and they apply to other mobile platforms such as IOS, Windows, Blackberry, etc.

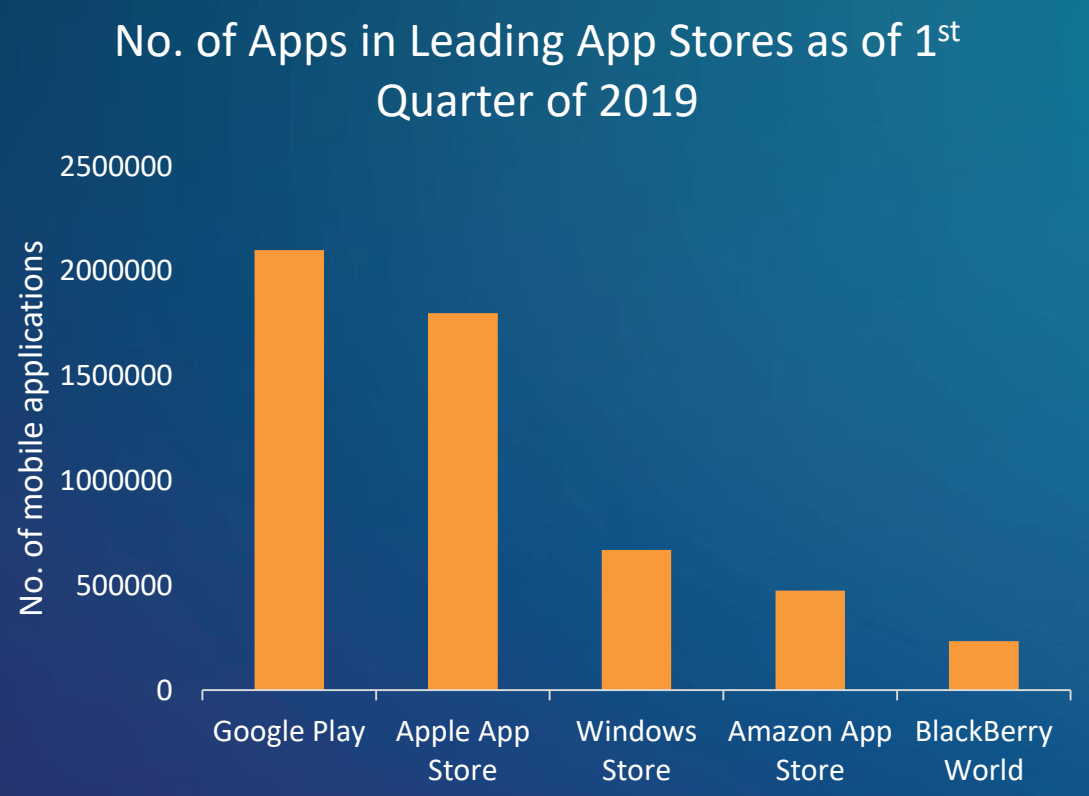
Anusha Daka

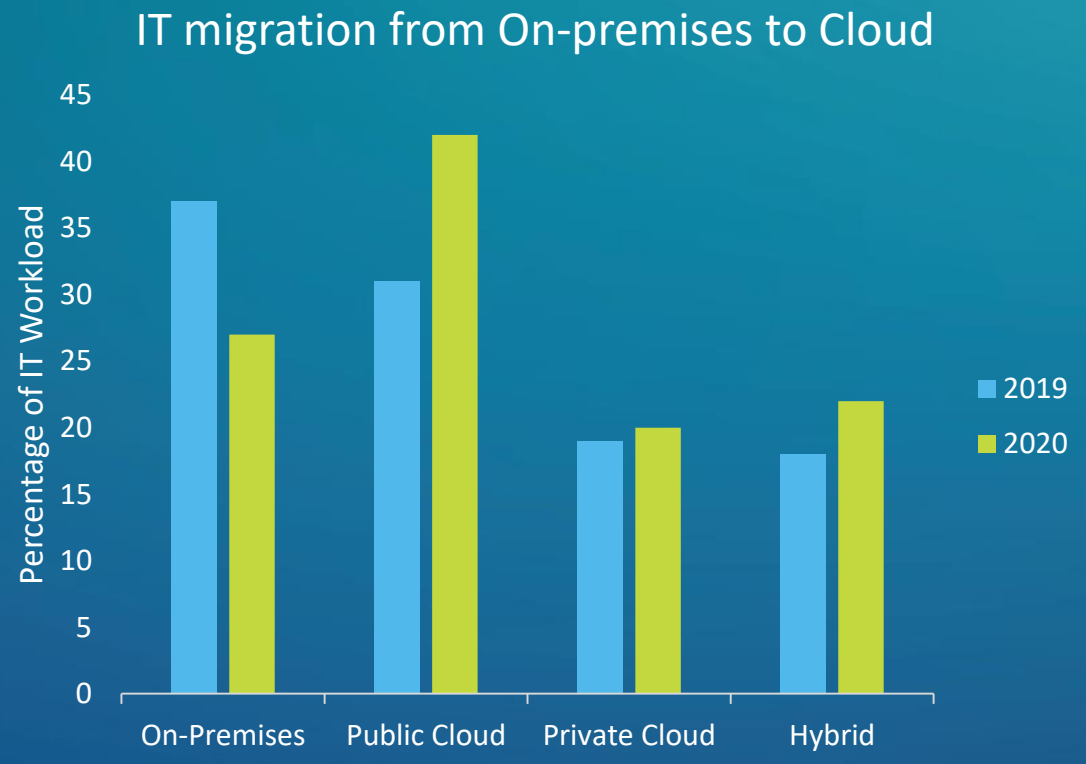
- Product Security Engineer at HP Inc., Palo Alto, CA
- A white-hat hacker and a security researcher.
- Asia Regional champions in Global Cyberlympics-2018 representing HP Inc.
- Ethical hacking and red teaming across various web, product, cloud and mobile technologies
- Love dancing, playing volley ball, and travelling.

Prathibha Muraleedhara

- Product Security Engineer at HP Inc., Fort Collins
- HP’s internal mobile security research and develops custom signatures for emerging mobile threats.
- Passionate researcher, speaker, and enjoys spending time educating people on security exploits and remediation.
- Love hiking, camping and travelling.

Mobile First / Cloud First Strategy





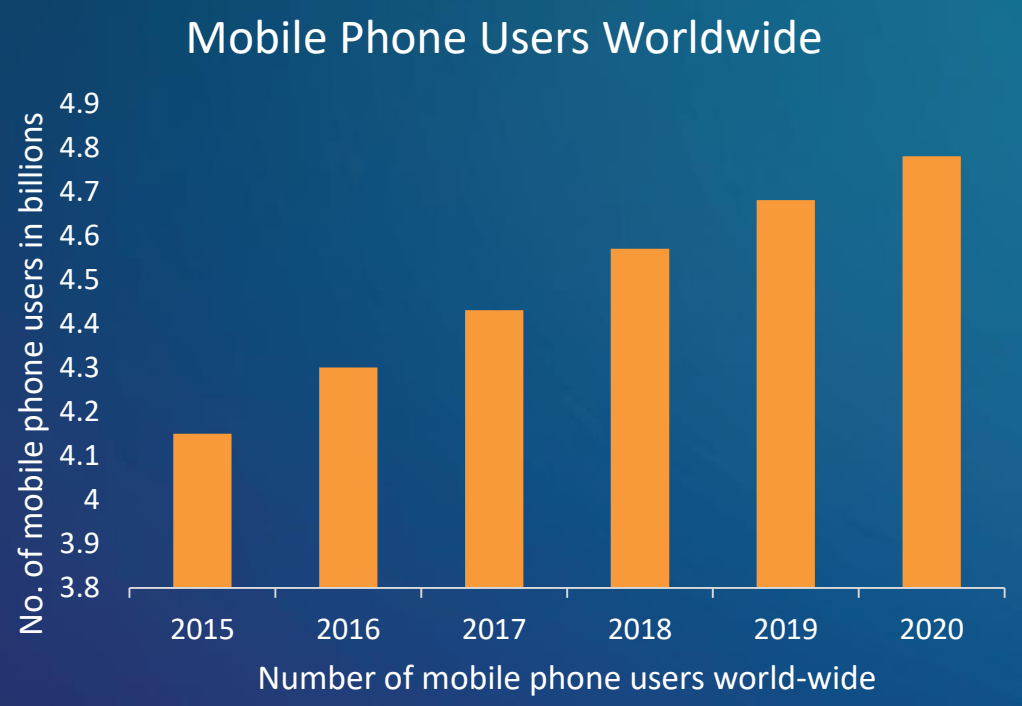
- Enterprises have increased service delivery using mobile platforms
- Mobile apps available to users are rapidly increasing

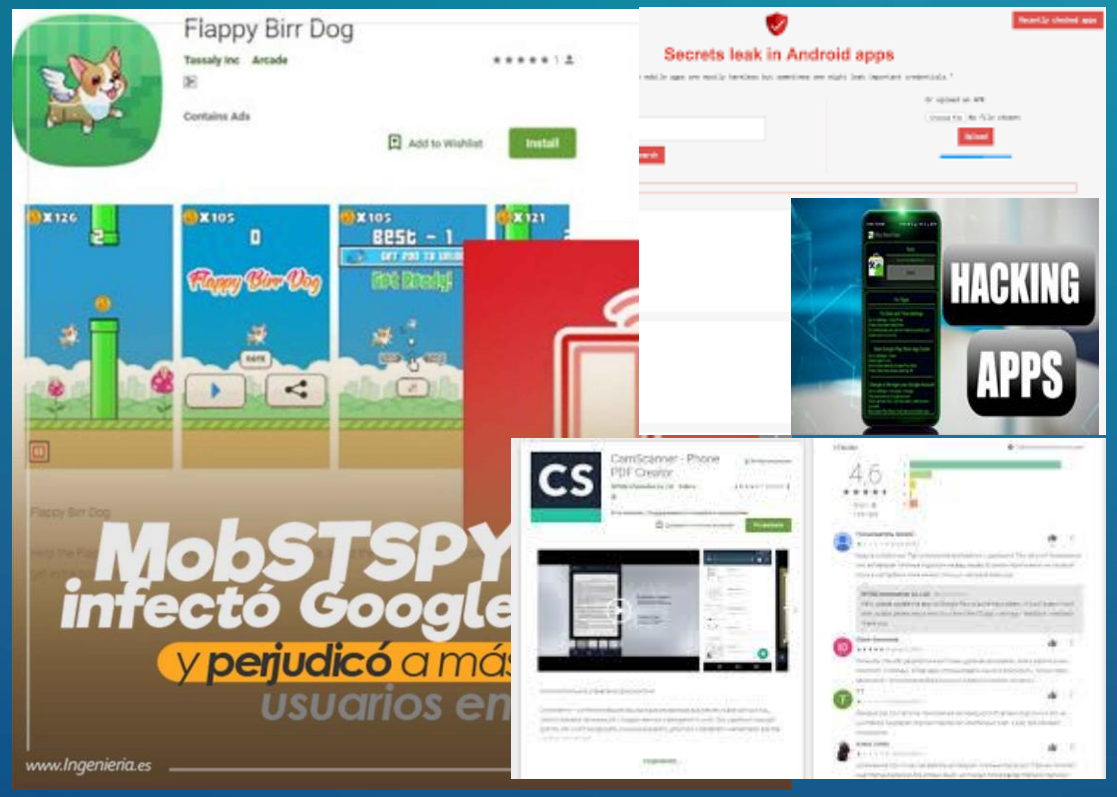
- Enterprises are shifting On-premises IT environment to Cloud
- Cloud solutions provide enterprises with flexibility, faster service delivery, scalability, use of emerging technologies AI and IoT, etc.

#GHC19

https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

Why Mobile Applications Security?





https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/

#GHC19

Attack Surface for Mobile Applications

CLIENT-SIDE

- Data Exposure to Other Apps
- Private Data Collection
- Platform Vulnerabilities
- Malware
- Buffer Overflow
- Etc.

NETWORK

- Rogue Access Point
- Weak/No Encryption Wi-Fi
- Insecure SSL implementation,
- Etc.

SERVER SIDE

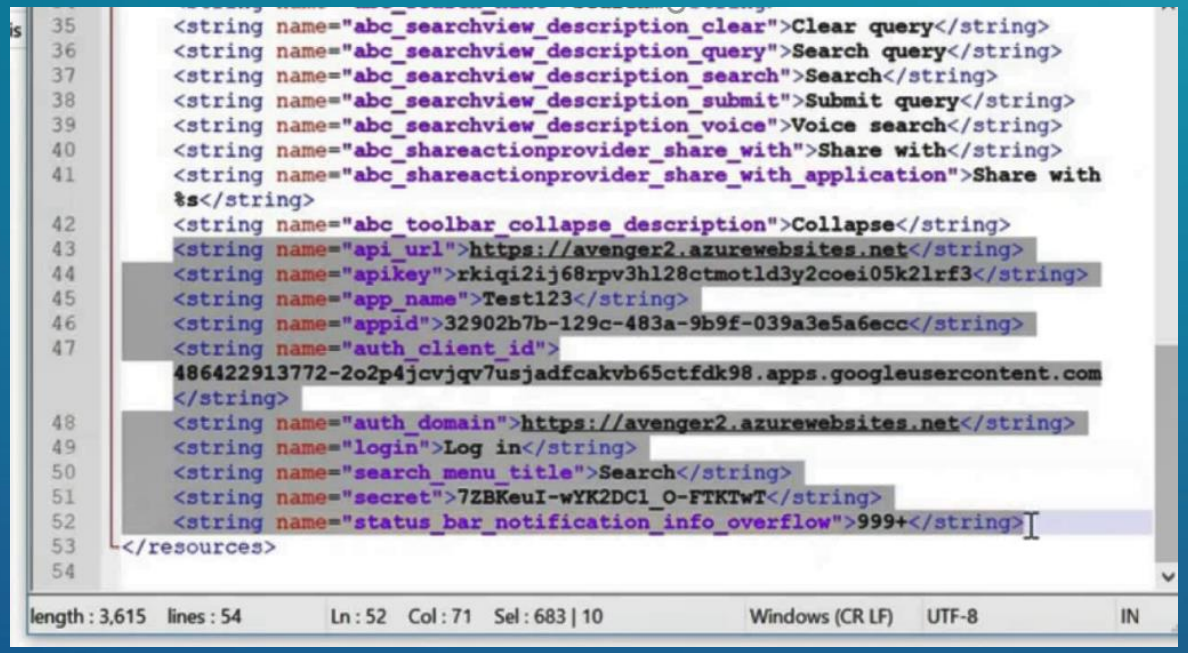
- Webserver Security Vulnerabilities
- Improper Database Configuration
- Insecure Handling of Data at Rest
- Etc.

Most Common Android Exploits

Insecure Data Storage

- Disclosure of sensitive information such as backend credentials, client id, client secret, api keys, config details etc. through client-side code

- Mobile applications can be reverse engineered to obtain hardcoded data present in the client-side code



```
35    <string name="abc_searchview_description_clear">Clear query</string>
36    <string name="abc_searchview_description_query">Search query</string>
37    <string name="abc_searchview_description_search">Search</string>
38    <string name="abc_searchview_description_submit">Submit query</string>
39    <string name="abc_searchview_description_voice">Voice search</string>
40    <string name="abc_shareactionprovider_share_with">Share with</string>
41    <string name="abc_shareactionprovider_share_with_application">Share with
      %s</string>
42    <string name="abc_toolbar_collapse_description">Collapse</string>
43    <string name="api_url">https://avenger2.azurewebsites.net</string>
44    <string name="apikey">rkiqi2ij68rpv3hl28ctmotld3y2coei05k2lrf3</string>
45    <string name="app_name">Test123</string>
46    <string name="appid">32902b7b-129c-483a-9b9f-039a3e5a6ecc</string>
47    <string name="auth_client_id">
      486422913772-2o2p4jcvjqv7usjadfcakvb65ctfdk98.apps.googleusercontent.com
      </string>
48    <string name="auth_domain">https://avenger2.azurewebsites.net</string>
49    <string name="login">Log in</string>
50    <string name="search_menu_title">Search</string>
51    <string name="secret">7ZBKeuI-wYK2DC1_O-FTKTwT</string>
52    <string name="status_bar_notification_info_overflow">999+</string>
53  </resources>
54
length : 3,615   lines : 54   Ln : 52   Col : 71   Sel : 683 | 10   Windows (CR LF)   UTF-8   IN
```

Tools Used:

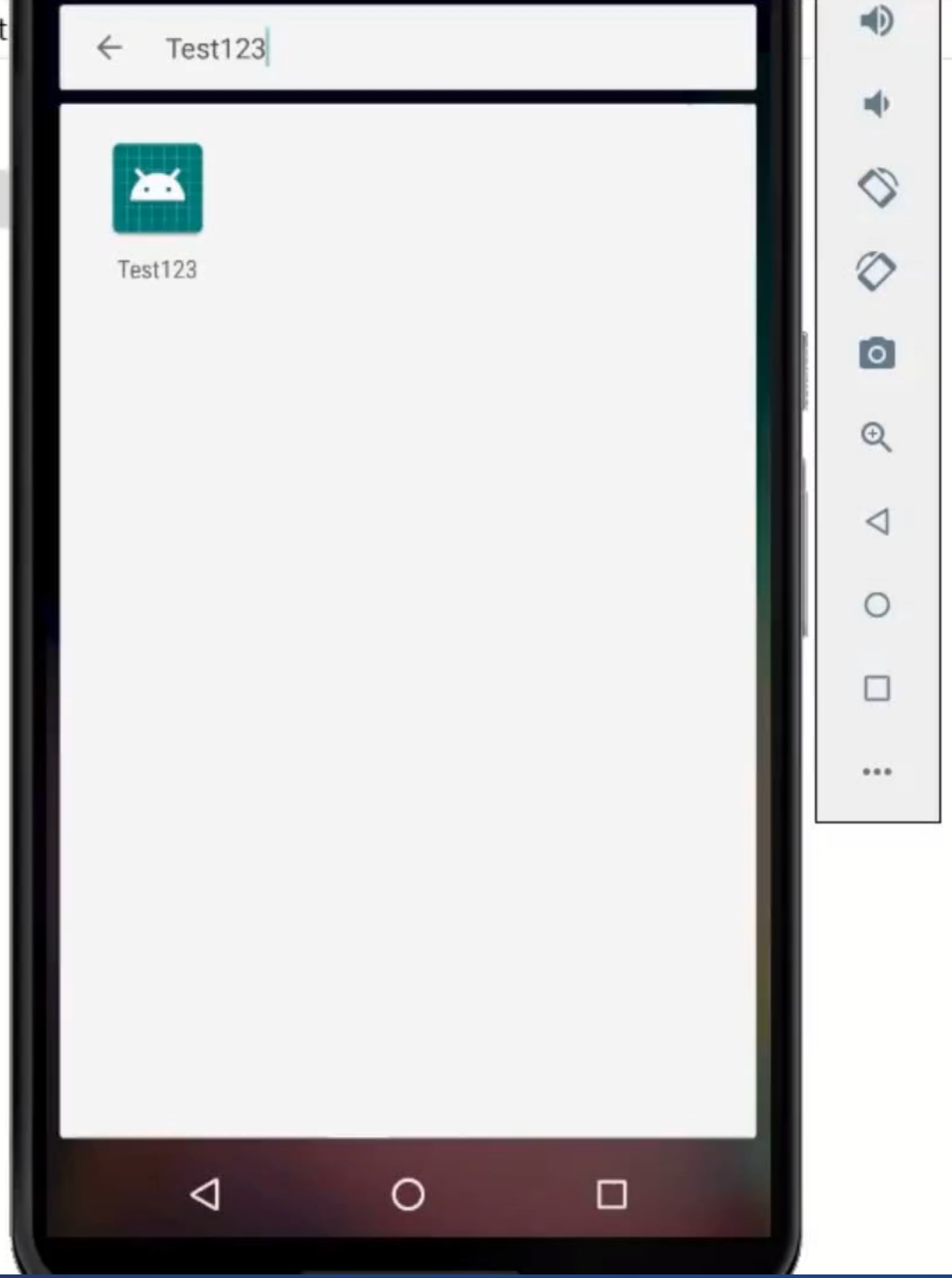
- APK Tool
- Dex2Jar
- JD JUI

his PC > PC COE (C:) > Users > daka > Document

Name

Tools

Test123.apk



Insecure Data Storage

✓ ***Recommendations:***

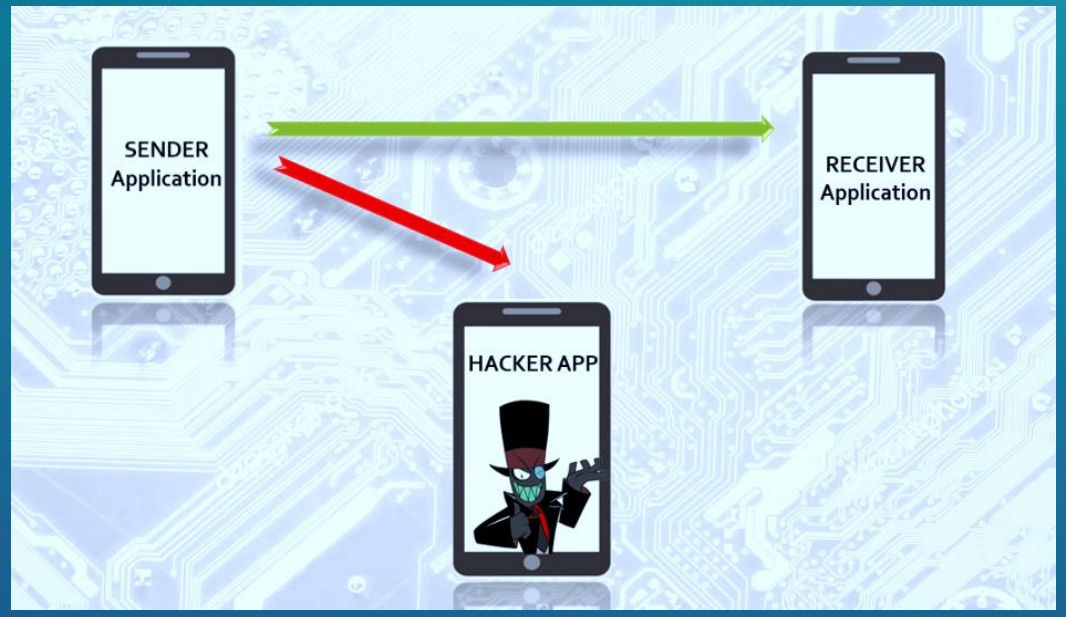
- Do not store sensitive application data on the device. Never hardcode the keys and secrets in the application code

- Make use of Android Keystore and IOS Keychain to secrets such as PINs, encryptions keys, api keys, etc.

Insecure Usage of Intents

- Intent is a messaging object which is used to request an action from another app component.

- The security of co-existing and inter-communicating applications is becoming even more challenging and the underlying security threats are not well understood leading to unauthorized data exposure between the mobile apps that co-exist on a given device



File Edit View Navigate Code Analyze Refactor Build Run Tools VCS Window Help

Sender3 > app > src > main > res > layout > activity_main.xml

app

Android

- app
  - manifests
  - java
    - com.sender2.muraleed.sender
      - MainActivity
    - com.sender2.muraleed.sender (androidTest)
    - com.sender2.muraleed.sender (test)
  - generatedJava
  - res
- Gradle Scripts

activity_main.xml | MainActivity.java

```
19
20      <EditText
21          android:id="@+id/commentEditText"
22          android:layout_width="wrap_content"
23          android:layout_height="wrap_content"
24          android:layout_marginStart="99dp"
25          android:layout_marginTop="306dp"
26          android:layout_marginEnd="99dp"
27          android:layout_marginBottom="381dp"
28          android:autofillHints=""
29          android:ems="10"
30          android:inputType="textPersonName"
31          android:text=""
32          app:layout_constraintBottom_toBottomOf="parent"
33          app:layout_constraintEnd_toEndOf="parent"
34          app:layout_constraintStart_toStartOf="parent"
35          app:layout_constraintTop_toTopOf="parent" />
36
37      <Button
38          android:id="@+id/sendButton"
39          android:layout_width="wrap_content"
40          android:layout_height="wrap_content"
41          android:layout_marginStart="167dp"
42          android:layout_marginTop="448dp"
43          android:layout_marginEnd="156dp"
44          android:layout_marginBottom="235dp"
45          android:text="Send Secret to Receiver"
46          app:layout_constraintBottom_toBottomOf="parent"
47          app:layout_constraintEnd_toEndOf="parent"
48          app:layout_constraintStart_toStartOf="parent"
49          app:layout_constraintTop_toTopOf="parent" />
50
51  </android.support.constraint.ConstraintLayout>
```

android.support.constraint.ConstraintLayout > TextView

Design | Text

Build: Build Output | Sync

Build: completed successfully at 6/10/2019 6:33 PM — 2 s 168 ms

Run build C:\Users\muraleed\AndroidStudioProjects\Sender3 — 1 s 976 ms

TODO | Terminal | Build | 6: Logcat | Profiler | 4: Run | Event Log

Gradle build finished in 2 s 177 ms (today 6:33 PM)

9:14 CRLF UTF-8 4 spaces

Insecure Usage of Intents

✓ ***Recommendations:***

- Explicitly set android:exported = ‘false’ in Android Manifest file.
- Use only explicit intents where you explicitly define the exact components that needs to be called by the Android System.
- Add custom signature permissions so that it can be used by applications that are signed with the same key.

Insecure Data Backup

- Insecure data backup configuration of the application leading to exposure of sensitive application and user data

- Android:allowBackup="true" can be exploited by the attackers to steal sensitive data

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest android:versionCode="1" android:versionName="1.0" package="com.android.insecurebankv2" platformBuildVersionCode="22" platfo
onName="5.1.1-1819727"
  xmlns:android="http://schemas.android.com/apk/res/android">
    <uses-sdk android:minSdkVersion="15" android:targetSdkVersion="22" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.SEND_SMS" />
    <uses-permission android:name="android.permission.USE_CREDENTIALS" />
    <uses-permission android:name="android.permission.GET_ACCOUNTS" />
    <uses-permission android:name="android.permission.READ_PROFILE" />
    <uses-permission android:name="android.permission.READ_CONTACTS" />
    <android:uses-permission android:name="android.permission.READ_PHONE_STATE" />
    <android:uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" android:maxSdkVersion="18" />
    <android:uses-permission android:name="android.permission.READ_CALL_LOG" />
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
    <uses-feature android:glEsVersion="0x00020000" android:required="true" />
    <application android:theme="@android:style/Theme.Holo.Light.DarkActionBar" android:label="@string/app_name" android:icon="@mipmap/
r" android:debuggable="true" android:allowBackup="true">
        <activity android:label="@string/app_name" android:name="com.android.insecurebankv2.LoginActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
        <activity android:label="@string/title_activity_file_pref" android:name="com.android.insecurebankv2.FilePrefActivity" android:
nputMode="adjustNothing|stateVisible" />
        <activity android:label="@string/title_activity_do_login" android:name="com.android.insecurebankv2.DoLogin" />
        <activity android:label="@string/title_activity_post_login" android:name="com.android.insecurebankv2.PostLogin" android:export
>
        <activity android:label="@string/title_activity_wrong_login" android:name="com.android.insecurebankv2.WrongLogin" />
        <activity android:label="@string/title_activity_do_transfer" android:name="com.android.insecurebankv2.DoTransfer" android:expo
/>
        <activity android:label="@string/title_activity_view_statement" android:name="com.android.insecurebankv2.ViewStatement" andro
```

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest android:versionCode="1" android:versionName="1.0" package="com.android.insecurebankv2" platformBuildVersionCode="22" platformBuildVersi
onName="5.1.1-1819727"
  xmlns:android="http://schemas.android.com/apk/res/android">
    <uses-sdk android:minSdkVersion="15" android:targetSdkVersion="22" />
    <uses-permission android:name="android.permission.INTERNET" />
    <uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
    <uses-permission android:name="android.permission.SEND_SMS" />
    <uses-permission android:name="android.permission.USE_CREDENTIALS" />
    <uses-permission android:name="android.permission.GET_ACCOUNTS" />
    <uses-permission android:name="android.permission.READ_PROFILE" />
    <uses-permission android:name="android.permission.READ_CONTACTS" />
    <android:uses-permission android:name="android.permission.READ_PHONE_STATE" />
    <android:uses-permission android:name="android.permission.READ_EXTERNAL_STORAGE" android:maxSdkVersion="18" />
    <android:uses-permission android:name="android.permission.READ_CALL_LOG" />
    <uses-permission android:name="android.permission.ACCESS_NETWORK_STATE" />
    <uses-permission android:name="android.permission.ACCESS_COARSE_LOCATION" />
    <uses-feature android:glEsVersion="0x00020000" android:required="true" />
    <application android:theme="@android:style/Theme.Holo.Light.DarkActionBar" android:label="@string/app_name" android:icon="@mipmap/ic_launche
r" android:debuggable="true" android:allowBackup="true">
        <activity android:label="@string/app_name" android:name="com.android.insecurebankv2.LoginActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />
                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
        <activity android:label="@string/title_activity_file_pref" android:name="com.android.insecurebankv2.FilePrefActivity" android:windowSoftI
nputMode="adjustNothing|stateVisible" />
        <activity android:label="@string/title_activity_do_login" android:name="com.android.insecurebankv2.DoLogin" />
        <activity android:label="@string/title_activity_post_login" android:name="com.android.insecurebankv2.PostLogin" android:exported="true" /
>
        <activity android:label="@string/title_activity_wrong_login" android:name="com.android.insecurebankv2.WrongLogin" />
        <activity android:label="@string/title_activity_do_transfer" android:name="com.android.insecurebankv2.DoTransfer" android:exported="true"
/>
        <activity android:label="@string/title_activity_view_statement" android:name="com.android.insecurebankv2.ViewStatement" android:exported=
"true" />
        <provider android:name="com.android.InsecureBankv2.TrackUserContentProvider" android:exported="true" android:authorities="com.android.ins
ecurebankv2.TrackUserContentProvider" />
        <receiver android:name="com.android.Insecurebankv2.MyBroadCastReceiver" android:exported="true">
            <intent-filter>
```

Insecure Data Backup

✓ ***Recommendations:***

- Do not allow back-up for any application sensitive data at client side.

- Explicitly set android: allowBackup= ‘false’ in Android Manifest file.

Insecure Android Permissions

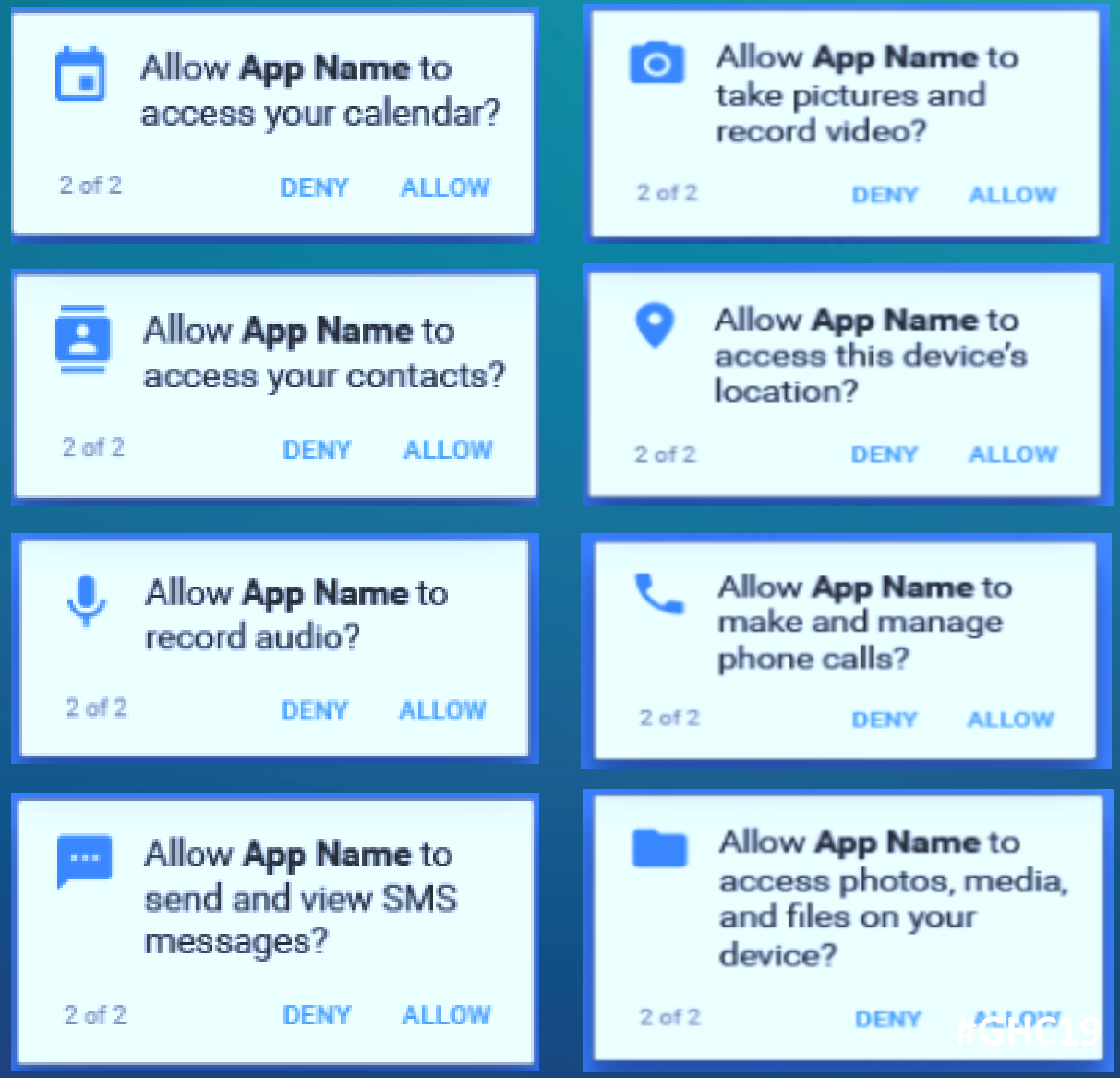
- Applications request wide range of permissions that if granted without reviewing, can compromise the device, its resources and the data stored on it.

- Unnecessary applications permissions may affect brand reputation of the publishing organization

✓ ***Recommendations:***

- Verify and remove permissions that are not required from the AndroidManifest file

- Provide justification for permissions requested in the application description



Insecure Authentication and Authorization

- Unauthorized access to the application data through user impersonation using binary attacks or request manipulation

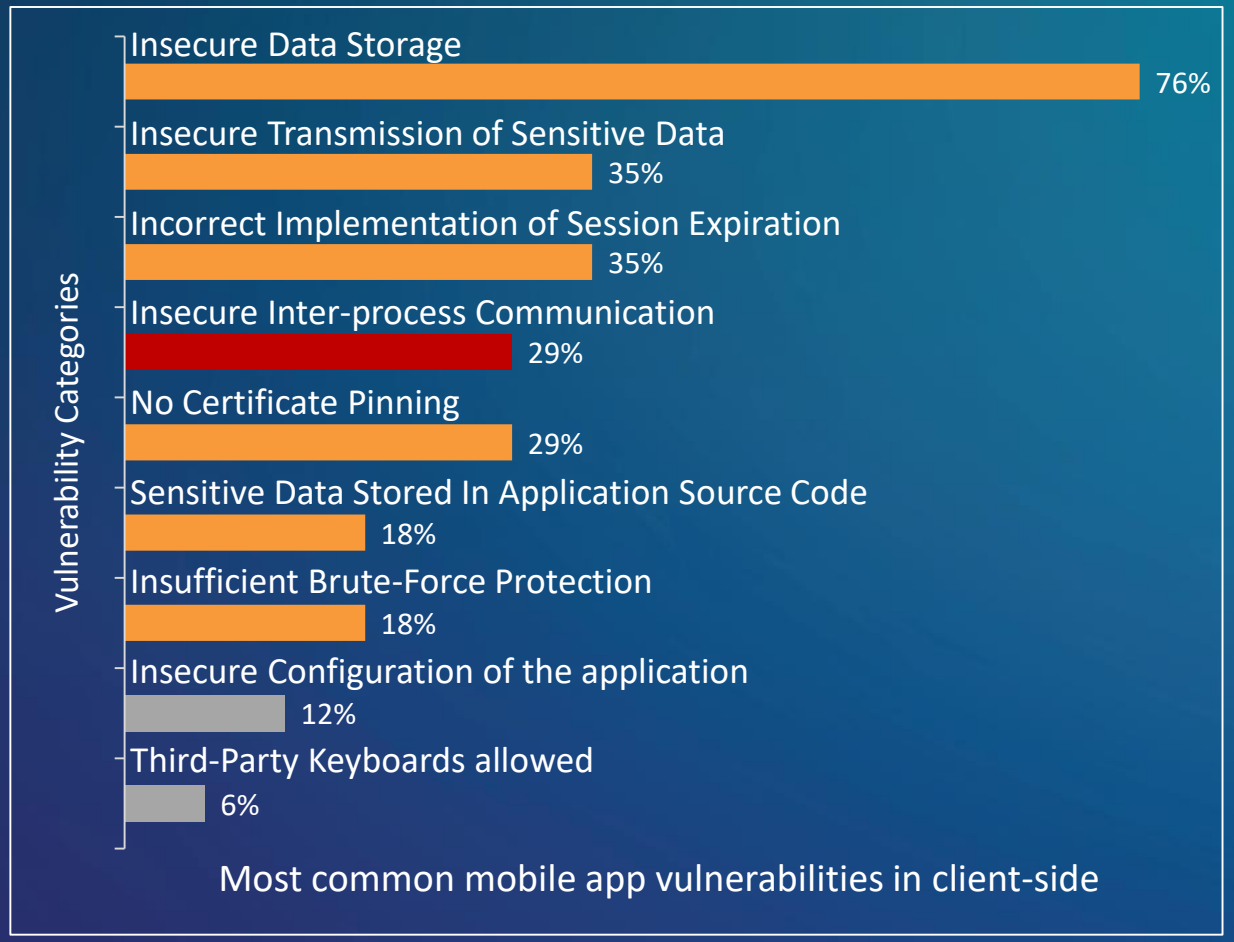
✓ ***Recommendations:***

- Implement server side controls to perform authorization checks

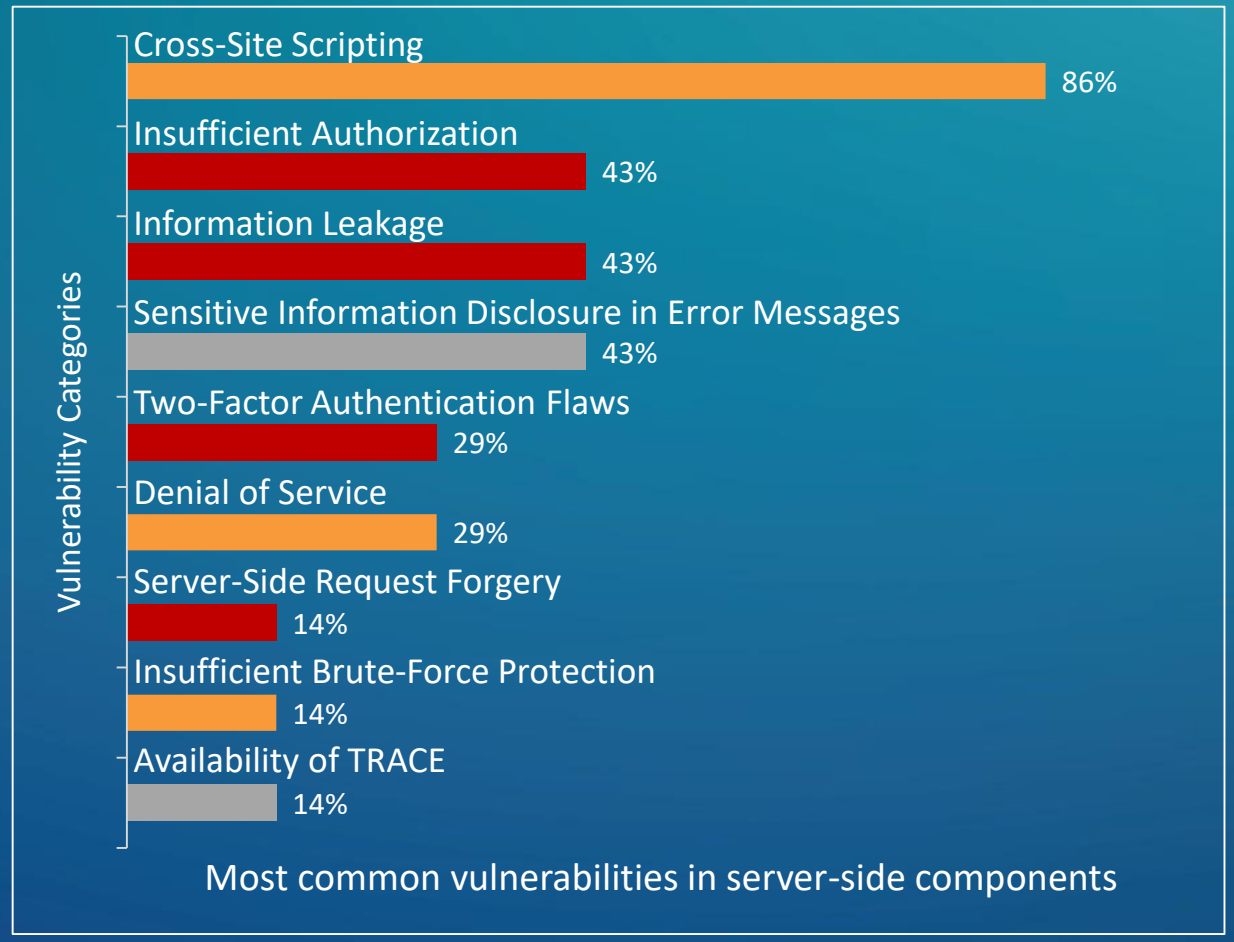
- Applications should verify and implement integrity requirements for auth tokens through signature validation to prevent unauthorized access.

Take Away

Vulnerability Categories



Most common mobile app vulnerabilities in client-side



Most common vulnerabilities in server-side components

Take Away

PEOPLE

- ✓ Update your OS and apps
- ✓ Do not connect your device to untrusted Wi-Fi .
- ✓ Do not download apps from untrusted source.
- ✓ Do not root or jailbreak a device.
- ✓ Set strong password and PIN

TECHNOLOGY

- ✓ Implement strong SSL
- ✓ Prevent screen capture via 3rd party applications
- ✓ Implement Safety APIs.
- ✓ Use certificate pinning.
- ✓ Implement strong authentication and authorization mechanism

PROCESS

- ✓ Conduct mobile security awareness and trainings to developers regularly
- ✓ Perform mobile application security penetration testing before releasing to AppStore
- ✓ Perform vulnerability scans periodically, at least half-yearly

Please remember to complete the session survey in the mobile app.

THANK YOU

GRACE HOPPER CELEBRATION

ANITA B.ORG

#GHC19