Mobile Top 10 2014-M2 Insecure Data Storage

by

Anant Shrivastava

About Me

- Anant Shrivastava
- http://anantshri.info
- Independent Information Security Consultant
- Interest Areas : Web, Mobile, Linux
- Project Lead
  - Android Tamer
    - Live ISO environment for Android Security. Used by multiple professionals and trainers across the globe.
  - CodeVigilant
    - A initiative to find flaws in opensource softwares. Holds 160+ responsibly disclosed web vulnerabilities at this point in time.

Agenda

- Understand Insecure Data Storage
- Effects on overall Security
- Examples of Insecure Data Storage
- How to Find Insecure Data Storage
- How to prevent it

Understand mobile Storage

- Android
  - /data/data/<app>
    - Application specific data section, only application has access. Root has access to this partition also
  - /sdcard/
    - External memory generally FAT32 hence no ACL applies. Data can be read by all applications and externally read by card reader.
- IOS
  - <Application_Home>/Documents/ : Accessible only to app and root user.
  - No Sdcard for iOS devices

Insecure Data Storage

- It occurs when development teams assume that users or malware will not have access to a mobile device's filesystem.
- And sensitive information such as PII(Personally Identifiable Information) is stored in the data-stores on the device in insecure format.
- Insecure format
  - Plain text
  - Reversable trivial encoding (double ROT-13 or ROT-n, base64/32/128 etc)

Effect of Insecure Data Storage

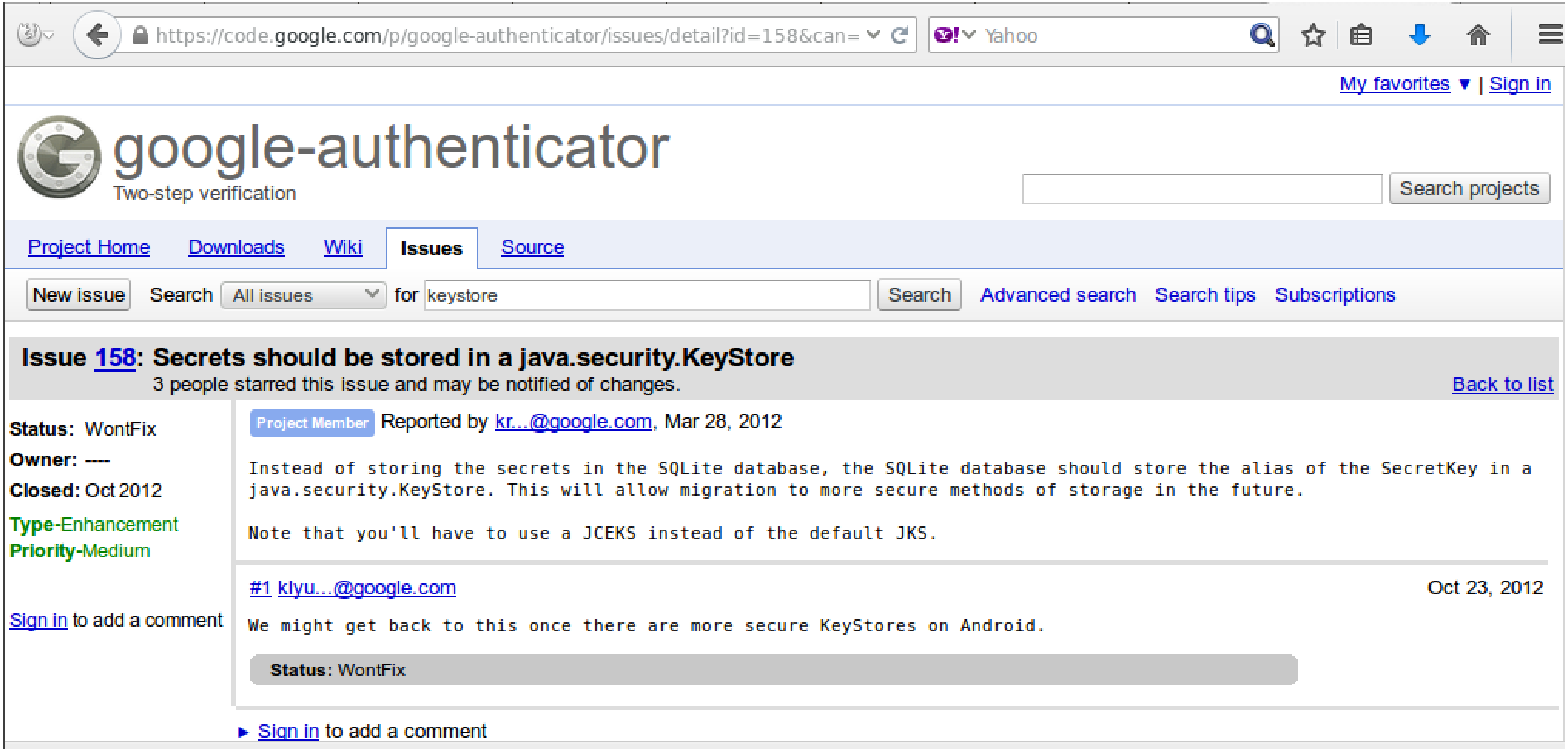
- This could lead to
  - Identity Theft
  - Fraud
  - Reputation Damage
  - External Policy Violation (PCI)
  - or Material Loss.

Demo Time

Demo's

- Approtect
- Google Authenticator

Example - 1



Issue 158: Secrets should be stored in a java.security.KeyStore

3 people starred this issue and may be notified of changes.

Back to list

Status: WontFix

Owner: ----

Closed: Oct 2012

Type-Enhancement

Priority-Medium

Sign in to add a comment

Project Member Reported by kr...@google.com, Mar 28, 2012

```
Instead of storing the secrets in the SQLite database, the SQLite database should store the alias of the SecretKey in a
java.security.KeyStore. This will allow migration to more secure methods of storage in the future.

Note that you'll have to use a JCEKS instead of the default JKS.
```

#1 klyu...@google.com Oct 23, 2012

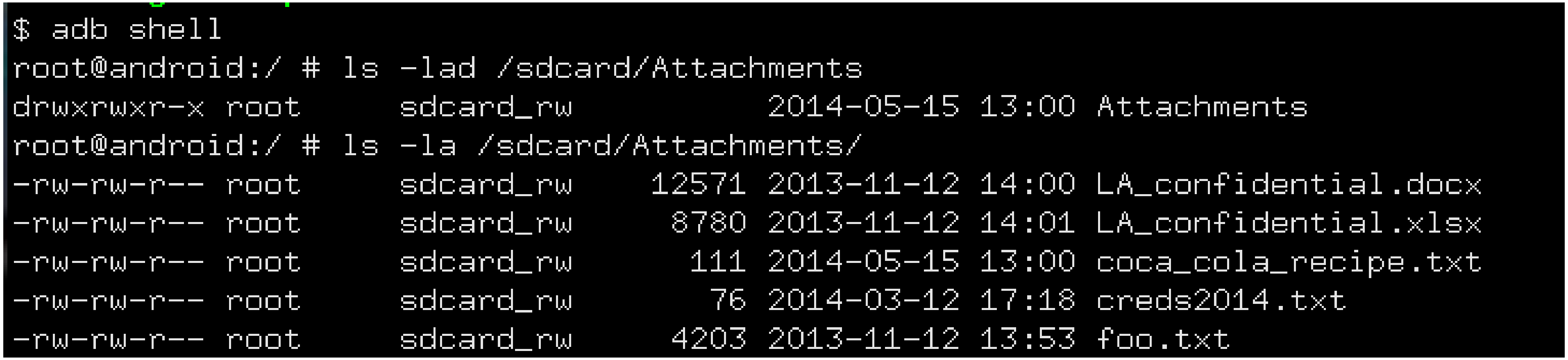
```
We might get back to this once there are more secure KeyStores on Android.
```

Status: WontFix

▸ Sign in to add a comment

Ref: https://code.google.com/p/google-authenticator/issues/detail?id=158&can=1&q=keystore

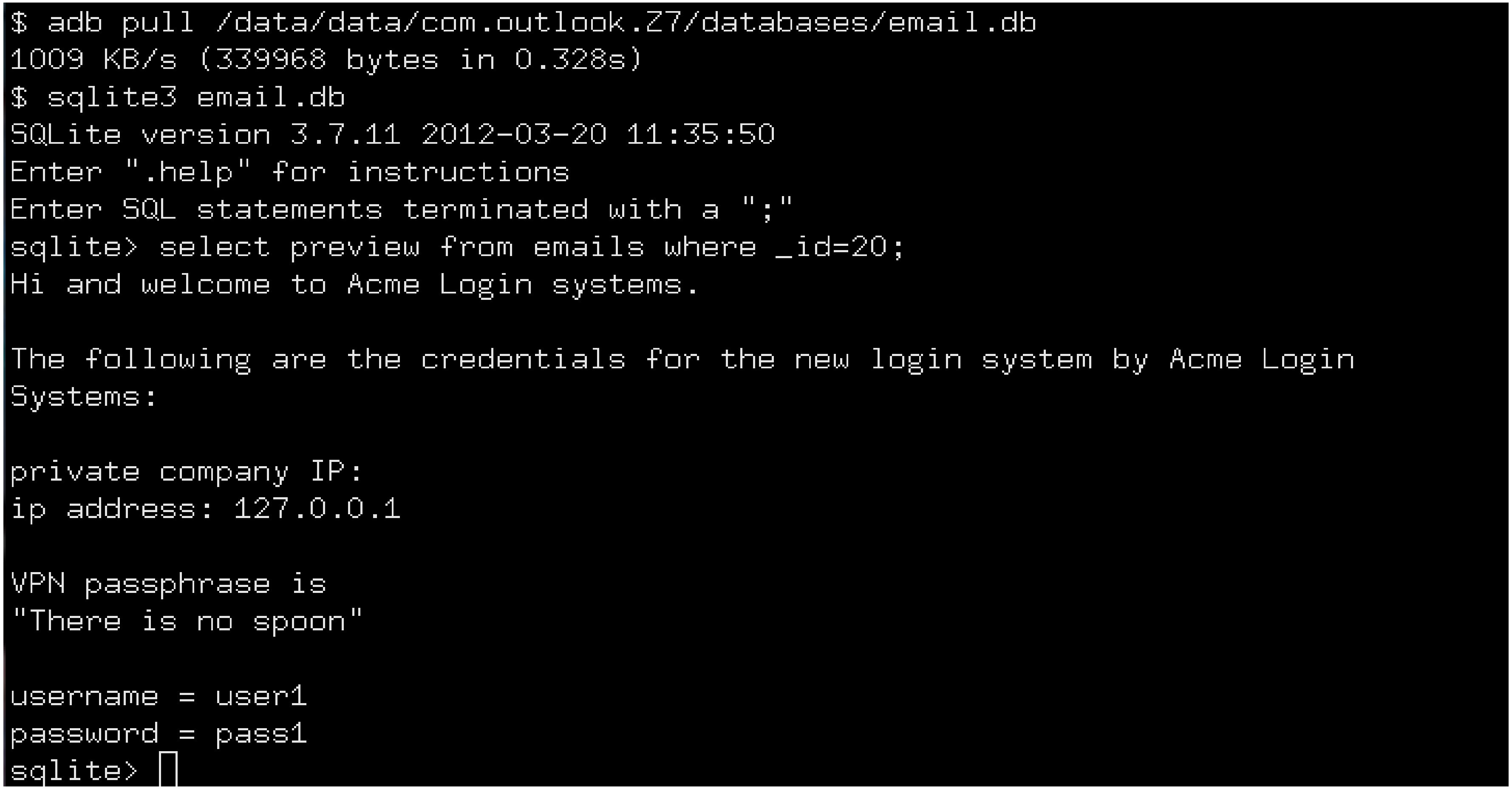
Outlook



```
$ adb shell
root@android:/ # ls -lad /sdcard/Attachments
drwxrwxr-x root     sdcard_rw          2014-05-15 13:00 Attachments
root@android:/ # ls -la /sdcard/Attachments/
-rw-rw-r-- root     sdcard_rw    12571 2013-11-12 14:00 LA_confidential.docx
-rw-rw-r-- root     sdcard_rw     8780 2013-11-12 14:01 LA_confidential.xlsx
-rw-rw-r-- root     sdcard_rw      111 2014-05-15 13:00 coca_cola_recipe.txt
-rw-rw-r-- root     sdcard_rw       76 2014-03-12 17:18 creds2014.txt
-rw-rw-r-- root     sdcard_rw     4203 2013-11-12 13:53 foo.txt
```

Ref: http://blog.includesecurity.com/2014/05/mobile-app-data-privacy-outlook-example.html

Outlook



```
$ adb pull /data/data/com.outlook.Z7/databases/email.db
1009 KB/s (339968 bytes in 0.328s)
$ sqlite3 email.db
SQLite version 3.7.11 2012-03-20 11:35:50
Enter ".help" for instructions
Enter SQL statements terminated with a ";"
sqlite> select preview from emails where _id=20;
Hi and welcome to Acme Login systems.

The following are the credentials for the new login system by Acme Login
Systems:

private company IP:
ip address: 127.0.0.1

VPN passphrase is
"There is no spoon"

username = user1
password = pass1
sqlite> 
```

How to find

- Data storage in mobile is generally in following formats
  - XML
  - Plist
  - SQLite
  - Plain text config files
  - Log Files
  - Cookies in webview

How to Find?

Android Apps

- Install the app
- Configure and run it for some time
- Extract the /data/data/<app_name>
- Also before installing and after installing application observe change in /sdcard also
- Identify files and content

Mitigation

- don’t store data unless absolutely necessary
- Never store credentials on the phone file system
- Force the user to authenticate using a standard web or API login scheme (over HTTPS) to the application upon each opening and ensure session timeouts are set at the bare minimum to meet the user experience requirements.
- For databases consider using SQLcipher for Sqlite data encryption
- Be aware that all data/entities using NSManagedObects will be stored in an unencrypted database file.

Mitigation

- Ensure any shared preferences properties are NOT MODE_WORLD_READABLE unless explicitly required for information sharing between apps.
- Ensure SDCARD storage is not used for PII or sensitive information of any sorts
- Avoid using NSUserDefaults to store senstitve pieces of information
- Apple or android keychains can be used but once jailbroken or rooted it can be easily read.

References

- www.owasp.org/index.php/Mobile_Top_10_2014-M2
- h30499.www3.hp.com/t5/Fortify-Application-Security/Exploring-The-OWASP-Mobile-Top-10-M1-Insecure-Data-Storage/ba-p/5904609#.VAEKztYvC00
- developer.android.com/training/articles/security-tips.html
- www.owasp.org/index.php/IOS_Developer_Cheat_Sheet

Questions

AND OVER THERE WE HAVE THE LABYRINTH GUARDS. ONE ALWAYS LIES, ONE ALWAYS TELLS THE TRUTH, AND ONE STABS PEOPLE WHO ASK TRICKY QUESTIONS.