DRD22. Do not cache sensitive information

(THIS CODING RULE OR GUIDELINE IS UNDER CONSTRUCTION)

This rule was developed in part by Beriwan Salamat Ravandi at the October 20-22, 2017 OurCS Workshop (http://www.cs.cmu.edu/ourcs/register.html). For more information about this statement, see the About the OurCS Workshop page.

Information that is cached may become accessible to other applications, and certainly becomes accessible if the device is found or stolen by a third party.

viaForensics [viaForensics 2014] warns of four situations where caching information may lead to sensitive data being leaked:

1. Caching web application data may result in URL histories, HTTP headers, HTML form inputs, cookies and other web-based data being revealed, see 2. Avoid caching app data.
2. Words entered by a user via the keyboard are stored in the Android user dictionary for future auto-correction. The user dictionary is available to any app without requiring any permission and this could lead to sensitive data being leaked, see 15. Be aware of the keyboard cache.
3. Apps may cache camera images which remain available after the app has finished, see 29. Android: avoid storing cached camera images.
4. Application screens are retained in memory enabling transaction histories to be viewed by anyone with access to the device who can directly launch the transaction view activity, see: 30. Android: Avoid GUI objects caching.

Furthermore, [Android Security] section Using WebView says:

> *If your application accesses sensitive data with a `WebView`, you may want to use the `clearCache()` method to delete any files stored locally. Server-side headers like `no-cache` can also be used to indicate that an application should not cache particular content.*

[This rule may require four or five NCCE/CS pairs.]

Noncompliant Code Example

This noncompliant code example shows an application that caches sensitive information.

```
TBD
```

Another application could access the cache, thereby revealing the sensitive information.

Compliant Solution

In this compliant solution the sensitive information is not cached.

```
TBD
```

Risk Assessment

Caching sensitive information may result in the information becoming accessible.

Rule	Severity	Likelihood	Remediation Cost	Priority	Level
DRD22-J	Medium	Probable	High	P4	L3

Automated Detection

It is not possible to automatically detect all situations when sensitive information may be cached.

Bibliography

[viaForensics 2014]	2. Avoid caching app data 15. Be aware of the keyboard cache 29. Android: avoid storing cached camera images 30. Android: Avoid GUI objects caching
[Android Security]	Using WebView
[Android API 2013]	`clearCache()` method