DRD18. Do not use the default behavior in a cryptographic library if it does not use recommended practices

(THIS CODING RULE OR GUIDELINE IS UNDER CONSTRUCTION)

Default behaviors of cryptographic libraries used in Android systems often do not use recommended practices. For example, the predominant Android Java security provider API defaults to using an insecure AES encryption method: ECB block cipher mode for AES encryption (see DRD17-J). Extensive app testing by [Egele 2013] has shown that the following 6 rules are often not followed, resulting in 88% of apps with cryptographic APIs on Google Play making at least one mistake.

Six common cryptography rules they tested:

1. Do not use ECB mode for encryption.
2. Do not use a non-random IV for CBC encryption.
3. Do not use constant encryption keys.
4. Do not use constant salts for PBE.
5. Do not use fewer than 1,000 iterations for PBE.
6. Do not use static seeds to seed `SecureRandom(·)`.

Noncompliant Code Example

This noncompliant code example shows an application that ..., and hence not secure.

```
```

Compliant Solution

In this compliant solution ...

```
```

Risk Assessment

If an insecure encryption method is used, then the encryption does not assure privacy, integrity, and authentication of the data.

Rule	Severity	Likelihood	Remediation Cost	Priority	Level
DRD18-J	High	Likely	Medium	P18	L1

Automated Detection

Automatic detection of ...

Related Guidelines

CERT Android-Only Secure Coding Rules and Guidelines	DRD17-J. Do not use the Android cryptographic security provider encryption default for AES

Bibliography

Egele 2013	An Empirical Study of Cryptographic Misuse in Android Applications
Android Developers	Android Developers: Security with HTTPS and SSL (accessed 6/25/2014)