Critique on
WILLIAM ENCK, MACHIGAR ONGTANG, AND PATRICK MCDANIEL. 2009. "Understanding Android Security"

Astha Sharma
asharma6@uno.edu

SUMMARY

The paper presented here deals with the useability, scope and associated vulnerability in using Android Applications - that executes on Java middleware and underlying Linux system. Since Android is the most extensively used OS, it gives its users an opportunity to perform almost every digital activity. And with this opportunity are associated threats that are somehow addressed in this research paper. The paper also discusses about the architecture of an ideal android application and mentions about the major system components, related activity, services, database and others. The authors here, have also discussed about the two security enforcement mechanisms based on system level and ICC level. It also discusses about the security reinforcement techniques based on Public vs Private components, implicitly open components, broadcast intent permission, service hooks, content permission levels, content provider permission and protected API.

STRENGTHS

1. Since every application in Android has its own user permission for access and restriction, the potential damage is limited.
2. Making the components private keeps them protected and less prone to vulnerability.
3. Since Android applications run on underlying Linux system (most secure OS), the security measures is considered good enough.

WEAKNESSES

1. It is easy to inject malicious code in Android because methods are defined separately and doesn't start within a main method. This is majorly because every method called has a different intent.
2. It cannot guarantee if the information is flawed.
3. Users are restricted to set all the components as private.
4. There are chances that the user information is leaked when the app is updated.