

Assessing Vulnerabilities in Android Applications

by Greg Garnhart and Reid Nagurka

-
-
-
-
-
-
-

Are the requested permissions utilized?



Does the app interact with other apps behind the scenes? Can the app's permissions be abused in this way?



Does the app perform valid certificate checking?



Does the app perform valid hostname verification?



QUESTIONING OURSELVES...



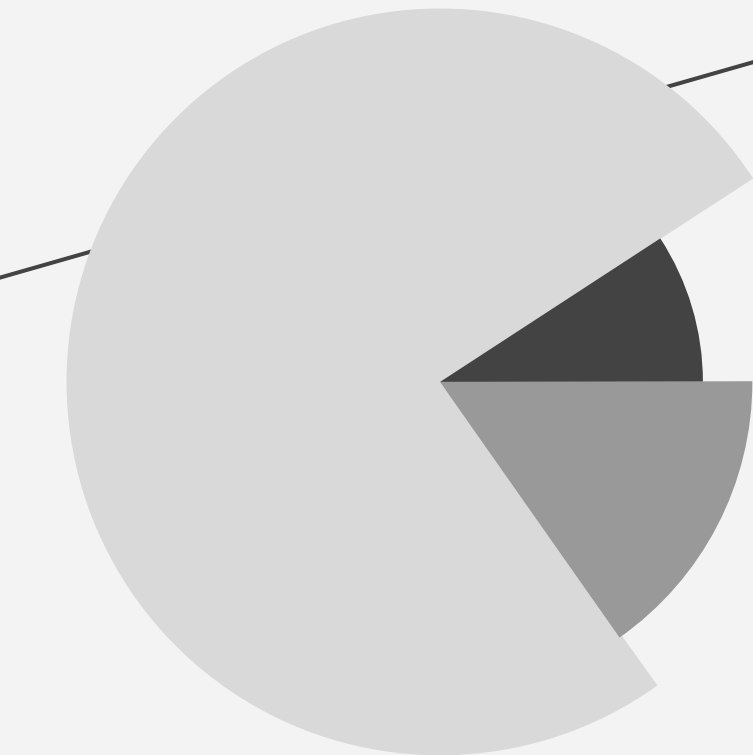
RQ1. Idle Hands are the Devil's Workshop

Permission Mapping Lite

- Goal: not to determine whether or not a permission is being used maliciously, but rather if a permission is being used at all.
- 80% of permissions requested will be utilized.
- Scan through requested permissions, then look for use in all files.

What about those results?

RQ1 RESULTS



Apps that used all requested permissions:
4



Apps that used at least 80% of requested
permissions: 7



Apps that used less than 80% of requested
permissions: 39



RQ2. HELL IS PAVED WITH GOOD INTENTIONS



Does the app interact with other apps behind the scenes?

Hypothesis: over 50% of apps
will not interact with other
apps.

Simplified methodology by looking
at intents

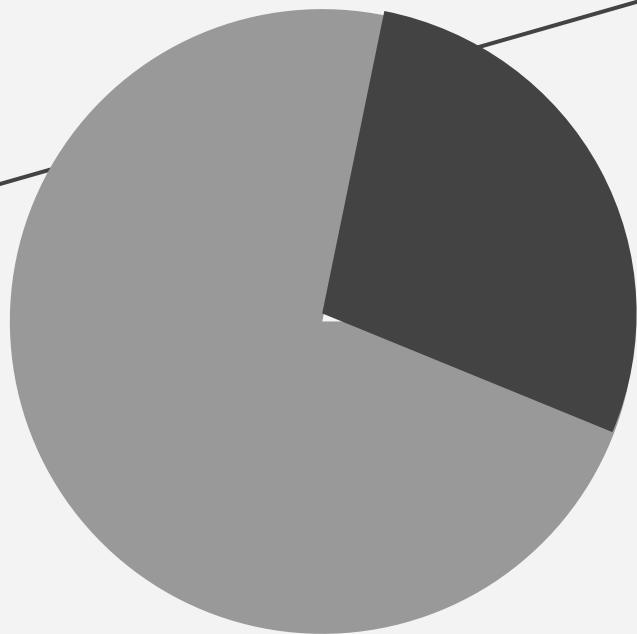
What Activities are passed to
Intents?

Are they within the file path of the
apk, or are they starting another
app?



What does this miss?

RQ2 RESULTS



Total number of apps with outside Activity calls: 17



Apps with no outside Activity Calls: 33



RQ3. CERTIFIABLY EVIL

Expect 10% of apps to perform certificate checking incorrectly

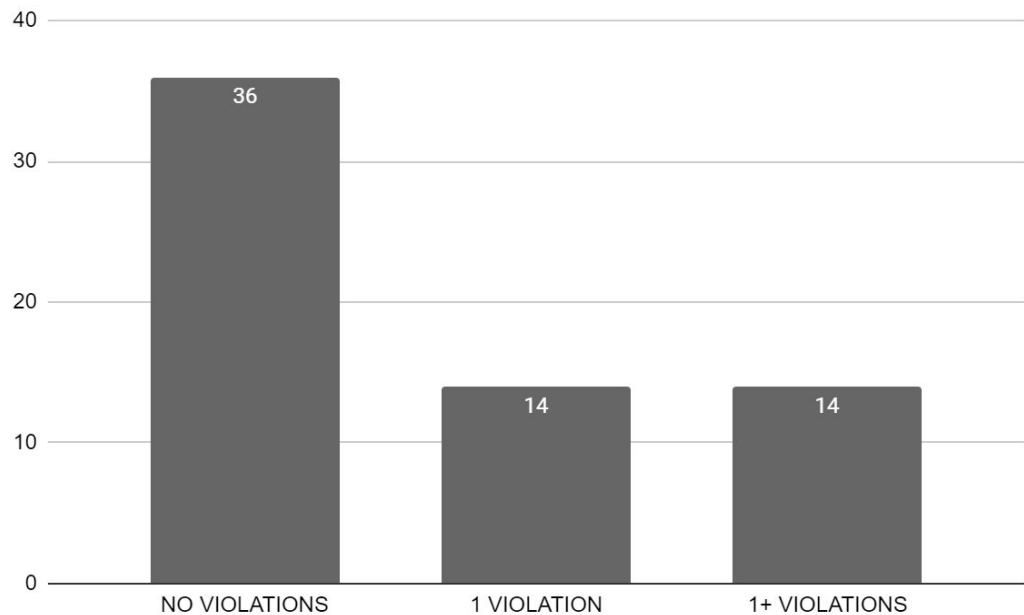
Looking to discover Man-in-the-Middle attacks

Three point scale:

- Standard certificate validation is used (no override)
- Overrides certificate validation, but no vulnerabilities
- Bad certificate validation: either completely absent or not implemented correctly and thus there are vulnerabilities



RQ3. SCALES OF (IN) JUSTICE



36 apps did not override the certificate TrustManager

14 apps overrode

All 14 apps with vulnerabilities committed multiple implementation violations.

RQ4. HOSTS OF ERROR

Also expect 10% of apps to have a hostname verification vulnerability

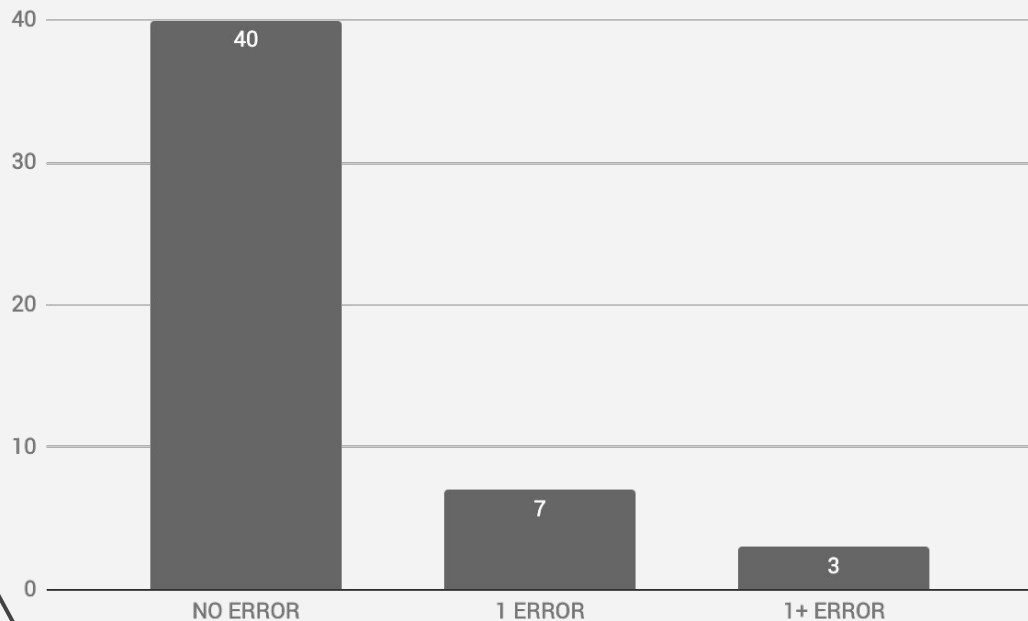
Very similar to our Certificate Check

Three point scale:

- Standard hostname verification is used (no override)
- Overrides hostname verification, but no vulnerabilities
- Bad hostname verification: either completely absent or not implemented correctly and thus leave room for vulnerabilities



RQ4. (HOST)AGES



40 apps showed no sign of misused hostnames.

7 apps had 1 error.

3 apps had over one error. The biggest offender was **3**.




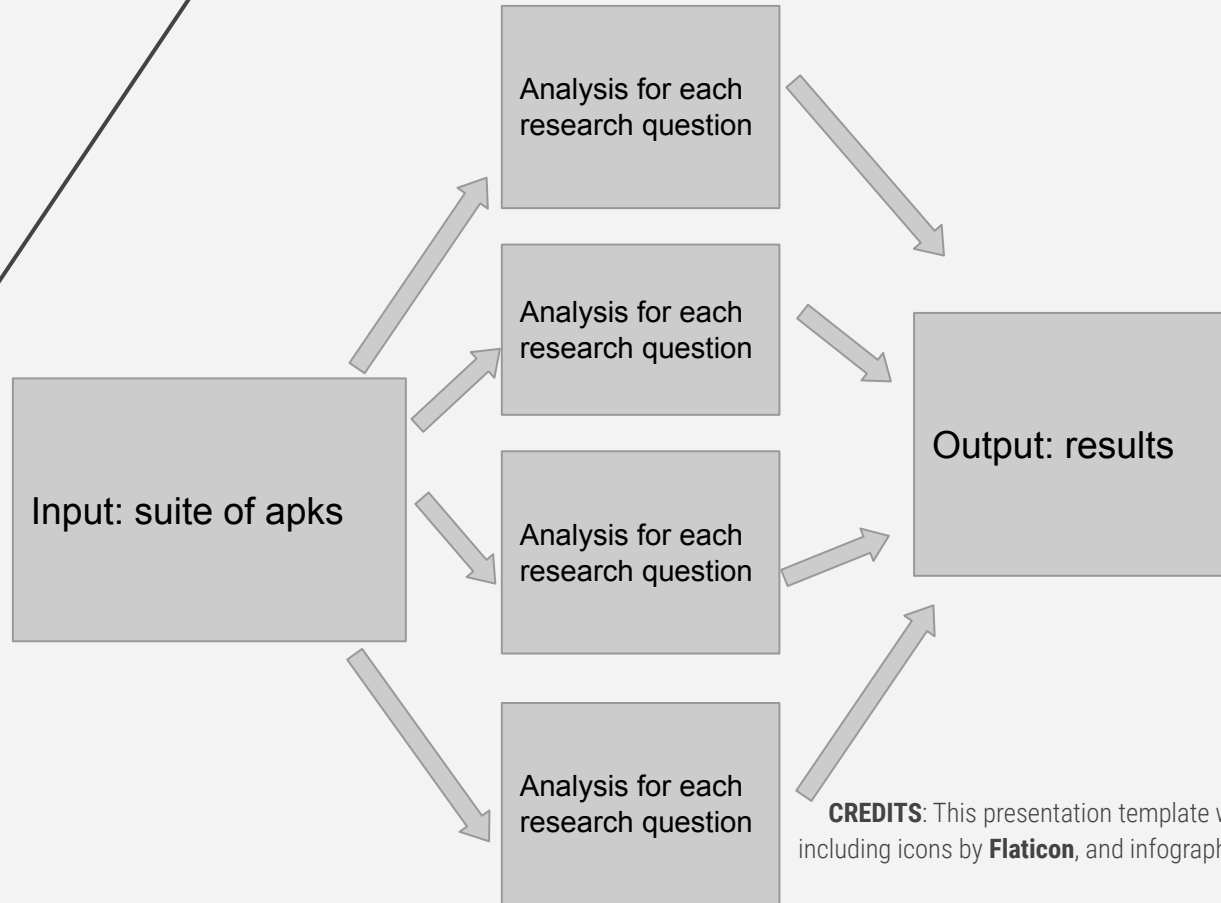
THANKS!

Can we answer any questions?

CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**

Please keep this slide for attribution





CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, and infographics & images by **Freepik**