Technische Universität München

# Repackaged Malware Detection in Android
**Bachelor Thesis**

Supervisors: Prof. Dr. Alexander Pretschner, Alei Salem
Email: pretschn, salem @ in.tum.de
Phone: +49 89 289 – 17, 340
Starting date: Immediately

Fakultät für Informatik
Lehrstuhl 22
Software Engineering
Prof. Dr. Alexander Pretschner

Boltzmannstraße 3 85748
Garching bei München

Tel: +49 89 289 17885,
+49 89 289 17314

Web: http://www22.in.tum.de

## Context
Repackaging is one of the techniques recently adopted by Android malware authors. In essence, malware authors download legitimate applications (hereafter apps) from the Android marketplaces e.g. *Google Play Store*, implant their malicious segments within the apps, and re-upload them to the marketplaces under different names. Consequently, repackaging facilitates spreading malware instances leveraging the trust users have in application distribution platforms.

In order to evade detection, repackaged malware authors have designed instances to maintain the dormancy of the implanted malicious behavior until the realization of pre-defined trigger conditions. Failure to trigger such dormant behaviors provides any employed detection mechanisms with unsufficient information about the app, effectively preventing them from properly classifying the app as malicious. In other words, a decent stimulation technique is a pre-requisite to successful detection of repackaged malware.

Thus, several efforts have been made to devise stimulation techniques of repackaged malware; one of which yielded a tool named *GroddDroid*. In essence, GroddDroid examines an app's code, identifies potentionally malicious code segments, and forces them to execute by altering the conditional statements that govern their execution [1]. The creators of GroddDroid have tested its performance on a limited number of APKs with decent success, in terms of (dormant) malicious behaviors the tool managed to disclose and execute. Nevertheless, despite such promising results, the sophistication of Android apps raises questions of whether the tool can force the execution of malicious segments within repackaged malware without crashing the app itself.

## Goal
In this thesis, we are going to investigate the applicability of GroddDroid to the problem of stimulation, analysis, and detection of Android repackaged malware. We are going to use the tool as a stimulation mechanism that provides our detection algorithms with representations of an Android app's behavior. The detection module will also provide GroddDroid–through a feedback loop–with information so as to guide stimulation towards better detection results.

To evaluate our approach, we will use the *Drebin* dataset, the majority of which comprises repackaged malware. Using Drebin, we will investigate (a) whether GroddDroid manages to force the execution of dormant malicious behaviors within repackaged malware without crashing the app, and (b) whether the approach it adopts helps detect Android repackaged malware i.e. yields good detection accuracy rates.

Technische Universität München

### Work-plan

1. Get acquainted to GroddDroid:
   a. Setup the framework.
   b. Study its inputs/outputs.
   c. Research method(s) to alter/control its behavior.
2. Automate the execution of GroddDroid against dataset of APKs.
3. Connect the outputs of GroddDroid to machine learning algorithms for detection.
4. Implement a feedback loop to GroddDroid to enhance its stimulation.
5. Evaluate GroddDroid against the Drebin dataset.
6. Writing of the final thesis containing:
   a. Description of the problem and motivation.
   b. State of the art survey of repackaged malware detection in Android.
   c. Rationale for using the selected techniques.
   d. Implementation description.
   e. Evaluation.
   f. Conclusion and further work.

Fakultät für Informatik
Lehrstuhl 22
Software Engineering
Prof. Dr. Alexander Pretschner

Boltzmannstraße 3 85748
Garching bei München

Tel: +49 89 289 17885,
+49 89 289 17314

Web: http://www22.in.tum.de

### Deliverables

- A virtual machine containing the implemented framework.
- The thesis document in accordance with the TUM guidelines.

### References

[1] Adrien Abraham, Radoniaina Andriatsimandefitra, Adrien Brunelat, Jean-François Lalande, and Valérie Viet Triem Tong. GroddDroid: a Gorilla for Triggering Malicious Behaviors. In *10th International Conference on Malicious and Unwanted Software*, Fajardo, Puerto Rico, 2015. IEEE Computer Society.