Vision Statement

A growing number of Android malware detection systems are based on Machine Learning (ML) methods. However, ML methods are often vulnerable to evasion attacks, in which an adversary manipulates malicious instances, so they are classified as benign.

Any android application is compressed as an apk file that has several layers;

- META-INF – The folder contains the manifest information and other metadata about the java package carried by the jar file.
- lib - The directory containing the compiled code that is platform-dependent(the directory is split into more directories)
- res - The directory containing resources not compiled into resources.arsc
- assets - A directory containing applications assets, which can be retrieved by AssetManager.
- **AndroidManifest** - An additional Android manifest file, describing the name, version, access rights, referenced library files for the application.
- **classes.dex** - The classes compiled in the dex file format understandable by the Dalvik virtual machine and by the Android Runtime
- resources.arsc - A file containing precompiled resources, such as binary XML for example.

our scope is on the manifest (include apps package name, components, permissions, hardware requirements) and classes.dex(compiled .dex classes of the app).
Our project goal is to find the weakness in malware detection systems and specifically "Sec-SVM" – a Derbin based static analysis system for Android applications.

Static analysis: collect as many features as possible from the application code and manifest. These features are organized into string groups and embedded in a common vector space that allows DREBIN to detect combinations and feature patterns that indicate malicious software automatically using machine learning techniques.

Sec-SVM: renews the weights on the first Static-analysis malware detection system which helps to derive computationally efficient training algorithms with (potentially strong) convergence guarantees.

Also, we like to build our attacks that will deal with Derbin based system – "Sec-SVM".
Milestones:
· Vision statement – end of Nov. 2020
· Poster Description – middle of June. 2021
· Final presentation day – end of Jul. 2021
· Book Project – at the beginning of Aug. 2021