**First Assignment**

רוני הראל – 209208024 , גל בריימוק – 315695981

name of the paper:

**Android Malware Detection, Static Analysis, Secure Machine Learning, Computer Security** (secSVM Classifier)

video of running the classifier:

<https://youtu.be/xBO1srxUPQM>

The type of classifier that you analyze:

static/dynamic/behavioral

git link (Fork):

<https://github.com/CodesParadox/AndroidATT>

We upload the result to the git. You can see the Json file 'mal\_train\_drebin\_apps.json' which contain the permissions,

And the log file 'static.log'.

feature set that the paper uses:

1. Permissions

"app\_permissions::android\_permission\_RECEIVE\_BOOT\_COMPLETED":1,"app\_permissions::android\_permission\_INTERNET":1,

"app\_permissions::android\_permission\_READ\_PHONE\_STATE":1,

"app\_permissions::android\_permission\_SEND\_SMS":1

,"app\_permissions::android\_permission\_RECEIVE\_SMS":1,

"app\_permissions::android\_permission\_CHANGE\_CONFIGURATION":1,"api\_permissions::android\_permission\_SEND\_SMS":1,

"api\_permissions::android\_permission\_READ\_PHONE\_STATE":1

,"api\_permissions::android\_permission\_VIBRATE":1

api\_permissions::android\_permission\_INTERNET  
"app\_permissions::android\_permission\_READ\_PHONE\_STATE":1,

"app\_permissions::android\_permission\_INTERNET":1,

"app\_permissions::android\_permission\_ACCESS\_NETWORK\_STATE":1

,"app\_permissions::android\_permission\_ACCESS\_WIFI\_STATE":1

,"app\_permissions::android\_permission\_WRITE\_EXTERNAL\_STORAGE":1,"app\_permissions::android\_permission\_RECEIVE\_BOOT\_COMPLETED":1,"app\_permissions::com\_android\_launcher\_permission\_UNINSTALL\_SHORTCUT":1,

"app\_permissions::com\_android\_launcher\_permission\_INSTALL\_SHORTCUT":1,

"api\_permissions::android\_permission\_INTERNET":1,"api\_permissions::android\_permission\_READ\_CONTACTS":1

,"api\_permissions::android\_permission\_ACCESS\_FINE\_LOCATION":1,

"api\_permissions::android\_permission\_ACCESS\_NETWORK\_STATE":1,

"api\_permissions::android\_permission\_READ\_PHONE\_STATE":1,

"api\_permissions::android\_permission\_VIBRATE":1

,"api\_permissions::android\_permission\_WAKE\_LOCK":1,

"api\_permissions::android\_permission\_ACCESS\_WIFI\_STATE":1,

API calls  
api\_calls::android\/webkit\/WebView":1,"api\_calls::java\/net\/HttpURLConnection":1,"api\_calls::java\/net\/HttpURLConnection;->connect":1,"api\_calls::java\/net\/URL;->openConnection":1,"api\_calls::android\/content\/Context;>startActivit

Activities  
activities::b'\_GirlGame'":1,"activities::b'net\_youmi\_android\_AdActivity'":1,

"activities::b'net\_youmi\_android\_spotad\_AdActivity'":1,

"activities::b'cn\_domob\_android\_ads\_DomobActivity'":1,

"activities::b'??????'":1,

"activities::b'com\_google\_ads\_AdActivity'":1

,"activities::b'ifw\_uMUab\_MyActivity'":1,

"activities::b'ifw\_uMUab\_ApopMain'":1,

"activities::b'ifw\_uMUab\_bSSHuSpsd16'":1,

"activities::b'ifw\_uMUab\_bSSHuSpsd8'":1,

"activities::b'ifw\_uMUab\_bSSHuSpsd9'":1,

"activities::b'ifw\_uMUab\_bSSHuSpsd2'":1

,"activities::b'ifw\_uMUab\_bSSHuSpsd10'":1,

"s\_and\_r::b'ifw\_uMUab\_bSSHuSpsd11'":1,

"s\_and\_r::b'ifw\_uMUab\_bSSHuSpsd12'":1,

interesting\_calls

interesting\_calls::getPackageInfo":1,

"interesting\_calls::Read\/Write External Storage":1,

"interesting\_calls::HttpPost":1,

"interesting\_calls::getSystemService":1,

"interesting\_calls::getSubscriberId":1,

"interesting\_calls::getDeviceId":1,

"interesting\_calls::getCellLocation":1,"interesting\_calls::Obfuscation(Base64)":1,

"interesting\_calls::printStackTrace":1,

"interesting\_calls::Cipher(DESede)":1, "interesting\_calls::Cipher(thisBlockSize)":1,"interesting\_calls::getNetwor

kCountryIso":1