DREBIN

November 2, 2016

In [1]:
```
import numpy as np
import os
from sklearn.decomposition import PCA
import glob
```

In [2]:
```
script_dir=os.getcwd()
rel_path_i='Input_data/DREBIN/feature_vectors/'
abs_path_i=os.path.join(script_dir,rel_path_i)
rel_path_d='Input_data/DREBIN/'
abs_path_d=os.path.join(script_dir,rel_path_d)
```

In [3]:
```
malicious_files=np.genfromtxt(abs_path_d+'sha256_family.csv',dtype=str,delimiter=',',skip_heade
```

In [4]:
```
np.shape(malicious_files)
```

Out[4]:
```
(5560, 2)
```

In [5]:
```
no_of_mal=5560
labels=np.zeros((129013))
```

In [6]:
```
labels[0]
```

Out[6]:
```
0.0
```

In [7]:
```
#file_list=glob.glob(abs_path_i+'/*')
file_list_2=np.genfromtxt('file_list.txt',dtype='S')
```

In [8]:
```
labels_2=np.zeros((129013))
```

In [11]:
```
mal_set=malicious_files[:,0]
feature_set=set()
eight_features=set()
all_data=[]
file_count=0
for file_path in file_list_2:
    words=file_path.split('/')
    if words[-1] in mal_set:
        labels_2[file_count]=1
#         print words[-1], file_count
    curr_array=np.genfromtxt(file_path,dtype=str,delimiter="   ",usecols=(0))
    if np.ndim(curr_array)==0:
        curr_array=curr_array.reshape(1)
    for item in curr_array:
        feature_set.add(item)
        parts=item.split('::')
        eight_features.add(parts[0])
    all_data.append(curr_array)
    file_count=file_count+1
```

```
/Users/arjunbhagoji/anaconda/lib/python2.7/site-packages/numpy/lib/npyio.py:1487: UserWarning: genfromt
  warnings.warn('genfromtxt: Empty input file: "%s"' % fname)
/Users/arjunbhagoji/anaconda/lib/python2.7/site-packages/numpy/lib/npyio.py:1487: UserWarning: genfromt
  warnings.warn('genfromtxt: Empty input file: "%s"' % fname)
/Users/arjunbhagoji/anaconda/lib/python2.7/site-packages/numpy/lib/npyio.py:1487: UserWarning: genfromt
  warnings.warn('genfromtxt: Empty input file: "%s"' % fname)
/Users/arjunbhagoji/anaconda/lib/python2.7/site-packages/numpy/lib/npyio.py:1487: UserWarning: genfromt
  warnings.warn('genfromtxt: Empty input file: "%s"' % fname)
/Users/arjunbhagoji/anaconda/lib/python2.7/site-packages/numpy/lib/npyio.py:1487: UserWarning: genfromt
  warnings.warn('genfromtxt: Empty input file: "%s"' % fname)
/Users/arjunbhagoji/anaconda/lib/python2.7/site-packages/numpy/lib/npyio.py:1487: UserWarning: genfromt
  warnings.warn('genfromtxt: Empty input file: "%s"' % fname)
/Users/arjunbhagoji/anaconda/lib/python2.7/site-packages/numpy/lib/npyio.py:1487: UserWarning: genfromt
  warnings.warn('genfromtxt: Empty input file: "%s"' % fname)
/Users/arjunbhagoji/anaconda/lib/python2.7/site-packages/numpy/lib/npyio.py:1487: UserWarning: genfromt
  warnings.warn('genfromtxt: Empty input file: "%s"' % fname)
/Users/arjunbhagoji/anaconda/lib/python2.7/site-packages/numpy/lib/npyio.py:1487: UserWarning: genfromt
  warnings.warn('genfromtxt: Empty input file: "%s"' % fname)
/Users/arjunbhagoji/anaconda/lib/python2.7/site-packages/numpy/lib/npyio.py:1487: UserWarning: genfromt
  warnings.warn('genfromtxt: Empty input file: "%s"' % fname)
/Users/arjunbhagoji/anaconda/lib/python2.7/site-packages/numpy/lib/npyio.py:1487: UserWarning: genfromt
  warnings.warn('genfromtxt: Empty input file: "%s"' % fname)
/Users/arjunbhagoji/anaconda/lib/python2.7/site-packages/numpy/lib/npyio.py:1487: UserWarning: genfromt
  warnings.warn('genfromtxt: Empty input file: "%s"' % fname)
/Users/arjunbhagoji/anaconda/lib/python2.7/site-packages/numpy/lib/npyio.py:1487: UserWarning: genfromt
  warnings.warn('genfromtxt: Empty input file: "%s"' % fname)
/Users/arjunbhagoji/anaconda/lib/python2.7/site-packages/numpy/lib/npyio.py:1487: UserWarning: genfromt
  warnings.warn('genfromtxt: Empty input file: "%s"' % fname)
/Users/arjunbhagoji/anaconda/lib/python2.7/site-packages/numpy/lib/npyio.py:1487: UserWarning: genfromt
  warnings.warn('genfromtxt: Empty input file: "%s"' % fname)
```

```
In [13]: labels_2[1]
```

```
Out[13]: 1.0
```

```
In [15]: eight_features
```

```
Out[15]: {'activity',
          'api_call',
          'call',
          'feature',
          'intent',
          'permission',
          'provider',
          'real_permission',
          'service_receiver',
          'url'}
```

```
In [14]: labels=np.genfromtxt('labels.txt')
```

```
In [16]: file_list=np.genfromtxt('file_list.txt',dtype='S')
```

```
In [18]: labels[1]
```

```
Out[18]: 1.0
```

```
In [19]: a=np.where(labels==1.0)
```

```
In [20]: a

Out[20]: (array([     1,     24,     26, ..., 128963, 128968, 129000]),)

In [21]: b=np.where(labels_2==1.0)

In [22]: b

Out[22]: (array([     1,     24,     26, ..., 128963, 128968, 129000]),)

In [23]: len(a[0])

Out[23]: 5560

In [24]: len(feature_set)

Out[24]: 545333

In [25]: no_of_features=len(feature_set)

In [26]: no_of_samples=len(all_data)

In [27]: feature_list=list(feature_set)

In [28]: feature_list[0]

Out[28]: 'activity::.ScanActivity1'

In [29]: no_of_features

Out[29]: 545333

In [30]: from scipy.sparse import coo_matrix
```

sample_row_list=[] feature_col_list=[] sample_count=0 for sample in all_data: print sample_count dims=np.ndim(sample) curr_features=set(sample) elif dims<2: sample=sample.reshape((1,2)) curr_features=set(sample[:,1]) curr_f_list=[i for i,item in enumerate(feature_list) if item in curr_features] feature_col_list.extend(curr_f_list) curr_s_list=[sample_count for item in curr_f_list] sample_row_list.extend(curr_s_list) for i in range(no_of_features): if feature_list[i] in curr_features: sample_row_list.append(sample_count) feature_col_list.append(i) sample_count=sample_count+1 np.savetxt('col_list.txt',feature_col_list,fmt='%0u') np.savetxt('row_list.txt',sample_row_list,fmt='%0u')

```
In [31]: row=np.genfromtxt('row_list.txt')
         col=np.genfromtxt('col_list.txt')

In [32]: len(row)

Out[32]: 6113087

In [33]: len(col)

Out[33]: 6113087

In [34]: data=np.ones((len(col)))

In [35]: data_matrix=coo_matrix((data,(row,col)),shape=(no_of_samples,no_of_features))

In [36]: data_matrix.shape

Out[36]: (129013, 545333)
```

```
In [37]: data_matrix_csc=data_matrix.tocsc()

In [38]: data_matrix_train=data_matrix_csc[0:60000,:]

In [39]: data_matrix_test=data_matrix_csc[60000:,:]

In [40]: labels_train=labels[0:60000]

In [41]: labels_test=labels[60000:]

In [42]: from sklearn import svm

In [43]: clf=svm.LinearSVC()
         clf.fit(data_matrix_train,labels_train)

Out[43]: LinearSVC(C=1.0, class_weight=None, dual=True, fit_intercept=True,
              intercept_scaling=1, loss='squared_hinge', max_iter=1000,
              multi_class='ovr', penalty='l2', random_state=None, tol=0.0001,
              verbose=0)

In [44]: clf.score(data_matrix_test,labels_test)

Out[44]: 0.99289988842681809

In [45]: len(np.where(labels_test==1.0)[0])

Out[45]: 2910

In [46]: len(np.where(labels_train==1.0)[0])

Out[46]: 2650

In [70]: for i in range(1):
             print np.linalg.norm(clf.coef_[i,:])

16.7304365089

In [71]: top_features=np.argsort(np.abs(clf.coef_[0,:]))[::-1][:100]

In [72]: top_features

Out[72]: array([473112, 119243, 229850,  17953, 234374, 114456, 282304, 182144,
                102237, 195002, 115600, 513051, 318827,  75705, 139163, 380311,
                457352, 388316, 257065,  76803, 358170, 544592,  28991, 432983,
                220836, 105308, 372185, 215830, 401532,  63148, 297934,  99672,
                327624, 245829,  27588, 222662, 313046, 149712, 120608, 529327,
                378995, 524339, 209403,  25128, 248694, 384699,   2603, 134113,
                445086, 152294, 119065, 105556, 316956, 526448, 130266,   7649,
                341010, 382180, 291933, 323170, 211067, 125065, 327380, 379232,
                 22903, 105955, 381442, 408629, 347452, 464969, 544747, 498032,
                392381,  45623,  53891, 208072, 255230, 127142, 119149, 438720,
                329660, 490592, 199094, 221494, 290788, 363330, 107103,  46487,
                283882, 412599, 143378, 154949, 386209, 164518, 377219, 446690,
                 56148,  60253, 521102, 219120])

In [73]: feature_array=np.array(feature_list)

In [74]: w=clf.coef_[0]
```

```
In [78]: actual_features=np.where(w!=0)[0]

In [54]: clf.decision_function(data_matrix_train[0,:])

Out[54]: array([-1.75225602])

In [55]: clf.decision_function(data_matrix_train[1,:])

Out[55]: array([ 0.97484011])

In [56]: test_mal_indices=np.where(labels_test==1.0)

In [57]: all_data_array=np.array(all_data)

In [58]: mal_test=all_data_array[test_mal_indices]

In [64]: mal_test[0:10]

Out[64]: array([ array(['feature::android.hardware.touchscreen', 'call::getSystemService'],
                dtype='|S37'),
                array(['feature::android.hardware.touchscreen',
                'url::http://support.twitter.com/forums/10711/entries/15364).',
                'url::https://userstream.twitter.com/2/',
                'url::http://twitter4j.org/configuration.html',
                'url::http://api.twitter.com/oauth/request_token',
                'call::printStackTrace',
                'permission::android.permission.ACCESS_COARSE_LOCATION',
                'activity::.Main', 'permission::android.permission.INTERNET',
                'url::search.twitter.com',
                'intent::android.intent.category.DEFAULT',
                'api_call::android/net/ConnectivityManager;->getActiveNetworkInfo',
                'real_permission::android.permission.ACCESS_FINE_LOCATION',
                'url::dev.twitter.com', 'url::http://twitter4j.org/',
                'url::http://api.twitter.com/oauth/access_token',
                'url::sitestream.twitter.com', 'call::getPackageInfo',
                'url::http://schemas.android.com/apk/lib/com.google.ads',
                'call::HttpPost',
                'url::http://dev.twitter.com/pages/rate-limiting).\\nReturned',
                'url::http://dev.twitter.com/pages/auth)',
                'api_call::android/app/Activity;->startActivity',
                'url::http://www.gstatic.com/afma/sdk-core-v40.js\\',
                'url::http://www.google.co.jp/search?q%3D', 'url::www.twitter.com',
                'feature::android.hardware.location', 'url::http://a.admob.com/f0?',
                'url::http://twitter4j.org/en/twitter4j-', 'activity::.Auth',
                'call::getSystemService', 'url::http://www.twitter.com/',
                'url::http://stream.twitter.com/1/',
                'url::http://api.twitter.com/oauth/authenticate',
                'url::http://api.twitter.com/oauth/authorize',
                'url::http://hashtags.org/', 'call::Obfuscation(Base64)',
                'real_permission::android.permission.ACCESS_NETWORK_STATE',
                'url::twitter4j.org', 'url::http://api.twitter.com/1/',
                'url::stream.twitter.com', 'url::userstream.twitter.com',
                'url::support.twitter.com',
                'intent::android.intent.category.BROWSABLE', 'url::a.admob.com',
                'url::http://search.twitter.com/',
                'intent::android.intent.action.VIEW', 'url::api.twitter.com',
```

```
 'url::http://sitestream.twitter.com/2b/',
 'api_call::android/webkit/WebView', 'url::www.google.co.jp',
 'intent::android.intent.action.MAIN', 'url::hashtags.org',
 'call::Cipher(AES/CBC/PKCS5Padding)',
 'api_call::android/location/LocationManager;->getBestProvider',
 'real_permission::android.permission.INTERNET',
 'feature::android.hardware.location.network',
 'url::www.gstatic.com',
 'url::http://dev.twitter.com/pages/support)',
 'intent::android.intent.category.LAUNCHER',
 'permission::android.permission.ACCESS_NETWORK_STATE',
 'url::schemas.android.com'],
dtype='|S64'),
 array(['feature::android.hardware.touchscreen',
 'url::http://kawa.gnu.org/unknown-namespace/', 'url::www.w3.org',
 'url::http://www.gnu.org/software/kawa/',
 'url::schemas.xmlsoap.org', 'url::twitter.com',
 'api_call::android/media/MediaPlayer;->start',
 'api_call::java/net/ServerSocket',
 'real_permission::android.permission.CHANGE_COMPONENT_ENABLED_STATE',
 'url::www.gnu.org', 'call::Read/Write External Storage',
 'url::http://schemas.xmlsoap.org/soap/envelope/\\',
 'real_permission::android.permission.ACCESS_FINE_LOCATION',
 'real_permission::android.permission.WAKE_LOCK',
 'url::http://kawa.gnu.org/unit', 'url::yusuke.homeip.net',
 'real_permission::android.permission.READ_CONTACTS',
 'call::getPackageInfo', 'url::http://www.w3.org/2000/xmlns/',
 'real_permission::android.permission.INTERNET', 'call::HttpPost',
 'url::http://status.twitter.com/.',
 'url::http://yusuke.homeip.net/twitter4j/',
 'api_call::android/content/ContentResolver;->query',
 'url::http://www.w3.org/1999/xhtml',
 'real_permission::android.permission.READ_LOGS',
 'api_call::android/os/Vibrator;->cancel',
 'url::http://www.cs.caltech.edu/',
 'url::http://yusuke.homeip.net/twitter4j/en/twitter4j-',
 'url::http://appinvgameserver.appspot.com', 'call::printStackTrace',
 'url::http://status.twitter.com/',
 'call::Execution of external commands',
 'real_permission::android.permission.VIBRATE',
 'url::www.cs.caltech.edu', 'url::http://www.facebook.com',
 'url::www.twitter.com\\', 'api_call::java/lang/Runtime;->exec',
 'call::getSystemService', 'url::appinvgameserver.appspot.com',
 'url::status.twitter.com',
 'url::http://appinvtinywebdb.appspot.com/',
 'call::Obfuscation(Base64)',
 'api_call::android/media/MediaRecorder;->setAudioSource',
 'real_permission::android.permission.SEND_SMS',
 'url::http://appinvtinywebdb.appspot.com',
 'real_permission::android.permission.RECORD_AUDIO',
 'url::stream.twitter.com',
 'api_call::android/telephony/gsm/SmsManager;->sendTextMessage',
 'url::appinvtinywebdb.appspot.com',
 'api_call::android/location/LocationManager;->getBestProvider',
```

```
 'api_call::android/app/Activity;->startActivity',
 'url::http://twitter.com/oauth_clients/new',
 'url::www.facebook.com', 'call::sendSMS',
 'intent::android.intent.action.MAIN',
 'url::http://www.w3.org/XML/1998/namespace',
 'url::https://stream.twitter.com/', 'activity::.Screen1',
 'url::http://developer.android.com/guide/appendix/media-formats.html\\',
 'url::kawa.gnu.org', 'url::androvote.appspot.com',
 'intent::android.intent.category.LAUNCHER',
 'url::developer.android.com', 'url::http://www.twitter.com\\',
 'url::http://androvote.appspot.com',
 'url::http://schemas.xmlsoap.org/soap/encoding/\\',
 'api_call::android/content/pm/PackageManager;->setComponentEnabledSetting',
 'url::http://stream.twitter.com/'],
dtype='|S72'),
 array(['feature::android.hardware.touchscreen',
 'url::http://kawa.gnu.org/unknown-namespace/', 'url::www.w3.org',
 'url::http://www.gnu.org/software/kawa/',
 'url::schemas.xmlsoap.org', 'url::twitter.com',
 'real_permission::android.permission.USE_CREDENTIALS',
 'api_call::android/media/MediaPlayer;->start',
 'api_call::java/net/ServerSocket',
 'permission::android.permission.RECEIVE_SMS',
 'permission::android.permission.INTERNET', 'url::www.gnu.org',
 'real_permission::android.permission.GET_ACCOUNTS',
 'url::http://schemas.xmlsoap.org/soap/envelope/\\',
 'real_permission::android.permission.ACCESS_FINE_LOCATION',
 'real_permission::android.permission.WAKE_LOCK',
 'url::http://kawa.gnu.org/unit', 'url::yusuke.homeip.net',
 'real_permission::android.permission.READ_CONTACTS',
 'call::getPackageInfo', 'url::http://www.w3.org/2000/xmlns/',
 'real_permission::android.permission.INTERNET', 'call::HttpPost',
 'url::http://status.twitter.com/.',
 'url::http://yusuke.homeip.net/twitter4j/',
 'api_call::android/content/ContentResolver;->query',
 'url::http://www.w3.org/1999/xhtml',
 'permission::android.permission.WRITE_EXTERNAL_STORAGE',
 'api_call::android/app/Activity;->startActivity',
 'url::http://www.cs.caltech.edu/',
 'url::http://yusuke.homeip.net/twitter4j/en/twitter4j-',
 'url::www.google.com', 'url::http://appinvgameserver.appspot.com',
 'call::printStackTrace', 'url::http://status.twitter.com/',
 'api_call::java/lang/Runtime;->exec',
 'api_call::android/accounts/AccountManager;->getAccounts',
 'call::Execution of external commands',
 'real_permission::android.permission.VIBRATE',
 'url::www.cs.caltech.edu', 'url::http://www.facebook.com',
 'url::www.twitter.com\\', 'call::Obfuscation(Base64)',
 'call::getSystemService', 'url::appinvgameserver.appspot.com',
 'url::status.twitter.com',
 'url::http://appinvtinywebdb.appspot.com/',
 'permission::android.permission.SEND_SMS',
 'api_call::android/media/MediaRecorder;->setAudioSource',
 'real_permission::android.permission.SEND_SMS',
```

```
 'url::http://appinvtinywebdb.appspot.com',
 'real_permission::android.permission.RECORD_AUDIO',
 'feature::android.hardware.telephony',
 'api_call::android/telephony/gsm/SmsManager;->sendTextMessage',
 'url::appinvtinywebdb.appspot.com',
 'api_call::android/accounts/AccountManager;->invalidateAuthToken',
 'url::http://www.google.com/fusiontables/api/query',
 'call::sendSMS', 'call::Read/Write External Storage',
 'url::http://twitter.com/oauth_clients/new',
 'url::www.facebook.com',
 'real_permission::android.permission.MANAGE_ACCOUNTS',
 'real_permission::android.permission.READ_LOGS',
 'intent::android.intent.action.MAIN',
 'url::http://www.w3.org/XML/1998/namespace',
 'api_call::android/os/Vibrator;->cancel',
 'url::https://stream.twitter.com/', 'url::stream.twitter.com',
 'activity::.Screen1',
 'url::http://developer.android.com/guide/appendix/media-formats.html\\',
 'url::kawa.gnu.org',
 'api_call::android/location/LocationManager;->getBestProvider',
 'url::androvote.appspot.com',
 'intent::android.intent.category.LAUNCHER',
 'url::developer.android.com', 'url::http://www.twitter.com\\',
 'real_permission::android.permission.CHANGE_COMPONENT_ENABLED_STATE',
 'url::http://androvote.appspot.com',
 'url::http://schemas.xmlsoap.org/soap/encoding/\\',
 'api_call::android/content/pm/PackageManager;->setComponentEnabledSetting',
 'url::http://stream.twitter.com/',
 'api_call::android/accounts/AccountManager;->getAuthToken'],
dtype='|S72'),
 array(['feature::android.hardware.touchscreen',
 'url::http://schemas.android.com/apk/res/',
 'api_call::java/net/HttpURLConnection', 'url::r.admob.com',
 'permission::android.permission.INTERNET',
 'url::http://r.admob.com/ad_source.php', 'activity::.galletita',
 'real_permission::android.permission.ACCESS_FINE_LOCATION',
 'call::getPackageInfo',
 'real_permission::android.permission.INTERNET',
 'url::http://mm.admob.com/static/android/i18n/20100709',
 'url::http://mm.admob.com/static/android/canvas.html',
 'url::http://api.admob.com/v1/pubcode/android_sdk_emulator_notice',
 'api_call::android/content/Context;->startActivity',
 'permission::android.permission.ACCESS_COARSE_LOCATION',
 'feature::android.hardware.location', 'url::http://a.admob.com/f0?',
 'real_permission::android.permission.VIBRATE',
 'call::getSystemService', 'permission::android.permission.VIBRATE',
 'api_call::android/os/Vibrator;->vibrate', 'url::mm.admob.com',
 'url::api.admob.com', 'url::a.admob.com',
 'intent::android.intent.action.MAIN',
 'api_call::android/location/LocationManager;->getBestProvider',
 'feature::android.hardware.screen.portrait',
 'feature::android.hardware.location.network',
 'intent::android.intent.category.LAUNCHER',
 'url::schemas.android.com'],
```

```
dtype='|S64'),
 array(['call::getDeviceId',
 'permission::android.permission.ACCESS_MOCK_LOCATION',
 'url::http://www3.adhubs.net/mob4app/travelapp/bars',
 'api_call::android/net/ConnectivityManager;->getActiveNetworkInfo',
 'real_permission::android.permission.ACCESS_FINE_LOCATION',
 'url::elanoffice.dyndns.org', 'call::HttpPost',
 'api_call::android/hardware/Camera;->open',
 'api_call::android/net/wifi/WifiManager;->getConnectionInfo',
 'call::getSystemService',
 'url::http://www3.adhubs.net/mob4app/travelapp/details/getmyfavourite',
 'url::www.adhubs.net',
 'url::http://www3.adhubs.net/mob4app/travelapp/public//flag_images/',
 'url::http://www3.adhubs.net/mob4app/travelapp/hotels/hoteldetail',
 'url::http://api.appcelerator.net/p/v1/geo?',
 'url::http://www3.adhubs.net/mob4app/travelapp/favorite',
 'url::http://elanoffice.dyndns.org:85/MobWebApps/travelapp/search_detail.php',
 'api_call::android/os/Vibrator;->vibrate',
 'permission::android.permission.INTERNET',
 'activity::org.appcelerator.titanium.TiModalActivity',
 'real_permission::android.permission.READ_CONTACTS',
 'url::http://www3.adhubs.net/mob4app/travelapp/nearme',
 'url::http://www3.adhubs.net/mob4app/travelapp/weather',
 'url::api.appcelerator.net',
 'feature::android.hardware.location.gps',
 'url::http://www.adhubs.net/ads?SiteId%3D',
 'url::http://www.adhubs.net/cronjob.php?device&bulk_data%3D[',
 'url::http://www3.adhubs.net/mob4app/travelapp/nightlife/details',
 'activity::Travel Guide - SE - Stockholm',
 'url::http://www3.adhubs.net/mob4app/travelapp/bars/bardetail',
 'url::http://www3.adhubs.net/mob4app/travelapp/City',
 'url::http://www3.adhubs.net/mob4app/travelapp/index/latlongfromappid',
 'url::http://www.adhubs.net/apps/timeinterval.php?flag%3Dtitaniumapp',
 'api_call::android/content/Context;->sendBroadcast',
 'real_permission::android.permission.READ_PHONE_STATE',
 'url::http://www3.adhubs.net/mob4app/travelapp/',
 'url::http://www.w3.org/XML/1998/namespace',
 'feature::android.hardware.location.network',
 'intent::android.intent.category.LAUNCHER',
 'url::http://maps.google.com/maps/geo?q%3D',
 'permission::android.permission.ACCESS_FINE_LOCATION',
 'api_call::java/net/HttpURLConnection',
 'api_call::android/telephony/TelephonyManager;->getDeviceId',
 'call::Read/Write External Storage',
 'url::https://api.appcelerator.net/p/v2/mobile-track',
 'real_permission::android.permission.CAMERA',
 'url::http://www3.adhubs.net/mob4app/travelapp/travel',
 'url::http://www3.adhubs.net/mob4app/travelapp/travel/traveldetails',
 'call::setWifiEnabled',
 'url::http://www3.adhubs.net/mob4app/travelapp/shopping/index',
 'real_permission::android.permission.CHANGE_WIFI_STATE',
 'url::http://www3.adhubs.net/mob4app/travelapp/public/check_payment.php',
 'url::http://www3.adhubs.net/mob4app/travelapp/details/gethelpline',
 'feature::android.hardware.wifi',
```

```
 'permission::android.permission.WRITE_EXTERNAL_STORAGE',
 'permission::android.permission.ACCESS_NETWORK_STATE',
 'url::www3.adhubs.net',
 'url::http://www3.adhubs.net/mob4app/travelapp/events/eventdetail',
 'url::maps.google.com',
 'url::http://www3.adhubs.net/mob4app/travelapp/public/flag_images/',
 'service_receiver::org.appcelerator.titanium.analytics.TiAnalyticsService',
 'feature::android.hardware.touchscreen',
 'activity::.TravelGuideSeStockholmActivity',
 'call::printStackTrace',
 'permission::android.permission.READ_PHONE_STATE',
 'url::http://www3.adhubs.net/mob4app/travelapp/shopping/details',
 'url::http://www3.adhubs.net/mob4app/travelapp/nightlife/index',
 'real_permission::android.permission.ACCESS_WIFI_STATE',
 'url::http://www.w3.org/2000/xmlns/',
 'url::http://www3.adhubs.net/mob4app/travelapp/hotels',
 'real_permission::android.permission.WAKE_LOCK',
 'activity::ti.modules.titanium.media.TiVideoActivity',
 'url::http://elanoffice.dyndns.org:85/MobWebApps/travelapp/favorite_detail.php',
 'permission::android.permission.ACCESS_WIFI_STATE',
 'api_call::android/media/MediaPlayer;->start',
 'permission::android.permission.ACCESS_COARSE_LOCATION',
 'feature::android.hardware.location',
 'real_permission::android.permission.VIBRATE',
 'url::http://www3.adhubs.net/mob4app/travelapp/City/citydetail',
 'api_call::android/content/ContentResolver;->query',
 'call::Obfuscation(Base64)',
 'real_permission::android.permission.ACCESS_NETWORK_STATE',
 'url::http://www3.adhubs.net/mob4app/travelapp/events',
 'url::http://www3.adhubs.net/mob4app/travelapp/public/payment.php?app_dev_id%3D',
 'intent::android.intent.action.MAIN', 'url::www.w3.org',
 'api_call::android/net/wifi/WifiManager;->setWifiEnabled',
 'api_call::android/location/LocationManager;->getBestProvider',
 'real_permission::android.permission.INTERNET',
 'url::http://www3.adhubs.net/mob4app/travelapp/search',
 'url::http://www3.adhubs.net/mob4app/travelapp/mob4/terms'],
dtype='|S78'),
 array(['activity::.QucikUninstaller',
 'feature::android.hardware.touchscreen',
 'permission::android.permission.ACCESS_FINE_LOCATION',
 'url::http://schemas.android.com/apk/res/',
 'activity::.network.NetStatusInfo',
 'permission::android.permission.READ_LOGS', 'url::ditu.google.cn',
 'permission::android.permission.READ_PHONE_STATE',
 'api_call::android/net/ConnectivityManager;->getActiveNetworkInfo',
 'api_call::android/app/ActivityManager;->restartPackage',
 'service_receiver::.AutoStartReceiver',
 'call::Read/Write External Storage',
 'service_receiver::.network.NetService',
 'real_permission::android.permission.ACCESS_FINE_LOCATION',
 'api_call::java/net/HttpURLConnection',
 'url::http://www.umeng.com/app_logs', 'url::www.umeng.com',
 'call::getPackageInfo',
 'intent::android.intent.action.BOOT_COMPLETED',
```

```
 'real_permission::android.permission.ACCESS_WIFI_STATE',
 'permission::android.permission.GET_TASKS',
 'feature::android.hardware.location.gps',
 'real_permission::android.permission.READ_PHONE_STATE',
 'url::http://www.umeng.com/api/check_app_update', 'call::HttpPost',
 'call::printStackTrace',
 'api_call::android/telephony/TelephonyManager;->getDeviceId',
 'url::http://gw.youmi.net/cacapp',
 'feature::android.hardware.location',
 'url::http://gw.youmi.net/reqad',
 'api_call::android/net/wifi/WifiManager;->getConnectionInfo',
 'url::http://static.youmi.net/files/pic/480.png',
 'service_receiver::.CPUService', 'call::getSystemService',
 'url::http://static.youmi.net/files/pic/320.png',
 'api_call::android/app/ActivityManager;->getRecentTasks',
 'permission::android.permission.PACKAGE_USAGE_STATS',
 'api_call::java/lang/Runtime;->exec',
 'real_permission::android.permission.ACCESS_NETWORK_STATE',
 'service_receiver::.TaskMgrService', 'call::getDeviceId',
 'permission::android.permission.INTERNET',
 'real_permission::android.permission.VIBRATE', 'url::gw.youmi.net',
 'api_call::android/content/Context;->startService',
 'call::getSubscriberId',
 'real_permission::android.permission.GET_TASKS',
 'url::http://ditu.google.cn/staticmap?center%3D',
 'permission::android.permission.ACCESS_NETWORK_STATE',
 'url::http://gw.youmi.net/clkad', 'url::static.youmi.net',
 'url::http://gw.youmi.net/prsad',
 'call::Execution of external commands',
 'url::http://static.youmi.net/files/pic/240.png',
 'real_permission::android.permission.READ_LOGS',
 'api_call::android/app/NotificationManager;->notify',
 'intent::android.intent.action.MAIN',
 'permission::android.permission.WRITE_EXTERNAL_STORAGE',
 'permission::android.permission.RECEIVE_BOOT_COMPLETED',
 'activity::.TaskManager',
 'real_permission::android.permission.INTERNET',
 'real_permission::android.permission.RESTART_PACKAGES',
 'api_call::android/location/LocationManager;->getLastKnownLocation',
 'intent::android.intent.category.LAUNCHER',
 'url::http://static.youmi.net/files/pic/176.png',
 'permission::android.permission.RESTART_PACKAGES',
 'url::http://gw.youmi.net/effad', 'activity::.LaunchView',
 'url::schemas.android.com'],
dtype='|S65'),
 array(['feature::android.hardware.touchscreen',
 'permission::android.permission.ACCESS_FINE_LOCATION',
 'api_call::org/apache/http/impl/client/DefaultHttpClient',
 'service_receiver::.SnakeService',
 'real_permission::android.permission.ACCESS_FINE_LOCATION',
 'service_receiver::.BootDetector',
 'intent::android.intent.action.BOOT_COMPLETED', 'call::HttpPost',
 'real_permission::android.permission.WAKE_LOCK',
 'feature::android.hardware.location.gps',
```

```
 'url::http://routecentral.maxicom.net/gpspoints/addPoint',
 'permission::android.permission.ACCESS_COARSE_LOCATION',
 'feature::android.hardware.location', 'call::getSystemService',
 'api_call::android/os/PowerManager$WakeLock;->acquire',
 'api_call::android/location/LocationManager;->requestLocationUpdates',
 'permission::android.permission.INTERNET',
 'url::http://routecentral.maxicom.net/gpspoints/getTime',
 'api_call::android/content/Context;->startService',
 'permission::android.permission.WAKE_LOCK',
 'intent::android.intent.action.MAIN',
 'real_permission::android.permission.INTERNET',
 'feature::android.hardware.location.network',
 'url::http://routecentral.maxicom.net/sms/controller',
 'url::routecentral.maxicom.net',
 'permission::android.permission.RECEIVE_BOOT_COMPLETED',
 'intent::android.intent.category.INFO'],
dtype='|S67'),
 array(['feature::android.hardware.touchscreen',
 'api_call::android/net/ConnectivityManager;->getActiveNetworkInfo',
 'intent::android.intent.action.MAIN', 'call::printStackTrace',
 'permission::android.permission.ACCESS_NETWORK_STATE',
 'activity::.BrowserFullScreen',
 'real_permission::android.permission.ACCESS_NETWORK_STATE',
 'permission::android.permission.INTERNET',
 'api_call::android/location/LocationManager;->getBestProvider',
 'feature::android.hardware.screen.portrait',
 'activity::Open Black Belt',
 'real_permission::android.permission.ACCESS_FINE_LOCATION',
 'intent::android.intent.category.LAUNCHER',
 'api_call::android/webkit/WebView',
 'permission::android.webkit.permission.PLUGIN',
 'real_permission::android.permission.INTERNET',
 'call::getSystemService'],
dtype='|S64'),
 array(['feature::android.hardware.touchscreen',
 'permission::android.permission.ACCESS_FINE_LOCATION',
 'permission::android.permission.ACCESS_LOCATION',
 'permission::android.permission.ACCESS_COARSE_LOCATION',
 'activity::.MostWanted', 'permission::android.permission.INTERNET',
 'real_permission::android.permission.ACCESS_FINE_LOCATION',
 'real_permission::android.permission.INTERNET',
 'feature::android.hardware.location.gps',
 'feature::android.hardware.camera.autofocus',
 'permission::android.permission.ACCESS_LOCATION_EXTRA_COMMANDS',
 'feature::android.hardware.location',
 'permission::android.permission.CAMERA', 'call::getSystemService',
 'url::mobileweb.cdc.nicusa.com',
 'url::http://mobileweb.cdc.nicusa.com/most_wanted_web?lat%3D',
 'url::http://mobileweb.cdc.nicusa.com/most_wanted_web',
 'url::http://mobileweb.cdc.nicusa.com/most_wanted_web?do:getButtons&lat%3D',
 'api_call::android/webkit/WebView',
 'intent::android.intent.action.MAIN',
 'url::http://mobileweb.cdc.nicusa.com/most_wanted_web?do:',
 'permission::android.permission.CONTROL_LOCATION_UPDATES',
```

```
               'feature::android.hardware.screen.portrait',
               'feature::android.hardware.location.network',
               'api_call::android/location/LocationManager;->getLastKnownLocation',
               'intent::android.intent.category.LAUNCHER',
               'permission::android.permission.ACCESS_GPS',
               'feature::android.hardware.camera'],
              dtype='|S73')], dtype=object)

In [63]: clf.decision_function(data_matrix_test[6,:])

Out[63]: array([ 0.18315719])

In [62]: test_mal_indices

Out[62]: (array([    6,    49,   102, ..., 68963, 68968, 69000]),)

In [69]: w[10]

Out[69]: 0.0

In [82]: allowed_features=set()
         temp_list=['feature','intent','permission','provider','service_receiver','intent','activity']
         for item in temp_list:
             allowed_features.add(item)

In [85]: attack_features=[]
         for item in actual_features:
             curr_feature=feature_list[item]
             parts=curr_feature.split('::')
             if parts[0] in allowed_features:
                 attack_features.append(item)

In [88]: feature_array[attack_features]

Out[88]: array(['service_receiver::com.apostek.slotmachinevalentine.XtifyBlocker',
                'service_receiver::.widget.AbstractWidgetProvider$AutoSyncToogleService',
                'service_receiver::com.p1.chompsms.appwidget.WidgetEventReceiver',
                ..., 'activity::.activity.NetCounterPreferences',
                'service_receiver::.service.QxinService',
                'activity::.activities.HomeActivity'],
               dtype='|S111')

In [134]: min(w[attack_features])

Out[134]: -1.1888253811561742

In [135]: np.sort(w[attack_features])[:100]

Out[135]: array([-1.18882538, -1.07381339, -1.04866996, -1.02846373, -0.8991482 ,
                 -0.86741942, -0.85307315, -0.84553601, -0.73646666, -0.73269753,
                 -0.71895318, -0.69874506, -0.67029038, -0.6398326 , -0.63661839,
                 -0.63622917, -0.62462156, -0.61432749, -0.61098185, -0.61098185,
                 -0.60853578, -0.60263804, -0.59999444, -0.59577714, -0.59355441,
                 -0.58462396, -0.58125283, -0.58002643, -0.58002643, -0.52980562,
                 -0.52405398, -0.52397081, -0.51953891, -0.51953891, -0.51779576,
                 -0.50254254, -0.49045217, -0.49045217, -0.48249609, -0.48249609,
                 -0.47136588, -0.46522655, -0.46207933, -0.4571313 , -0.4571313 ,
```

```
                -0.45363964, -0.45114858, -0.45027648, -0.44891498, -0.44516729,
                -0.44406171, -0.43827888, -0.43637017, -0.4345185 , -0.42920235,
                -0.42920235, -0.42920235, -0.42920235, -0.42351867, -0.42351867,
                -0.41812063, -0.41757353, -0.41559495, -0.41433679, -0.41408622,
                -0.41408483, -0.40943818, -0.4054886 , -0.40310802, -0.39844098,
                -0.39570337, -0.39570337, -0.39570337, -0.39422076, -0.39422076,
                -0.39422076, -0.39177844, -0.39033092, -0.38985297, -0.38815814,
                -0.38815814, -0.38761487, -0.38704022, -0.38527821, -0.38504566,
                -0.38468577, -0.38468577, -0.38468577, -0.38288574, -0.3813808 ,
                -0.37783455, -0.37748268, -0.37748268, -0.37448264, -0.37448264,
                -0.37172569, -0.36885485, -0.36807448, -0.36752685, -0.36752685])

In [136]: w_index=np.argsort(w[attack_features])[:100]

In [137]: attack_features_array=np.array(attack_features)

In [138]: top_attack_f=attack_features_array[w_index]

In [139]: top_attack_f[0]

Out[139]: 115600

In [140]: feature_list[115600]

Out[140]: 'service_receiver::com.YRHNew.BootReceiver'

In [141]: test_mal_indices=np.array(test_mal_indices).reshape((1,-1))

In [142]: test_mal_indices.shape

Out[142]: (1, 2910)

In [143]: test_mal_indices.reshape((2910))

Out[143]: array([    6,    49,   102, ..., 68963, 68968, 69000])

In [176]: count_wrong=0.0
          count_tot=0.0
          count_adv=0.0
          base_wrong=0.0
          for index in test_mal_indices:
              mal_test_sample=data_matrix_test[index,:]
              mal_test_sample[:,top_attack_f[0]]=1.0
              if clf.predict(data_matrix_test[index,:])[0]!=1.0:
                  base_wrong=base_wrong+1
              if clf.predict(mal_test_sample)[0]!=1.0:
                  count_wrong=count_wrong+1
              if clf.predict(mal_test_sample)[0]!=clf.predict(data_matrix_test[index,:])[0]:
                  count_adv=count_adv+1
              count_tot=count_tot+1
          print count_wrong/count_tot*100, count_adv/count_tot*100, base_wrong/count_tot

100.0 100.0 0.0

In [168]: mal_test_sample

Out[168]: <69013x545333 sparse matrix of type '<type 'numpy.float64'>'
                  with 3289471 stored elements in Compressed Sparse Column format>
```

```
In [169]: mal_test_sample[:,top_attack_f[0]]=1.0

In [170]: mal_test_sample

Out[170]: <69013x545333 sparse matrix of type '<type 'numpy.float64'>'
                with 3358484 stored elements in Compressed Sparse Column format>

In [173]: clf.predict(mal_test_sample[0,:])[0]

Out[173]: 0.0

In [148]: clf.decision_function(mal_test_sample)

Out[148]: array([-1.00566819])

In [130]: clf.decision_function(data_matrix_test[,:])

Out[130]: array([-2.69279674])

In [132]: labels_test[0]

Out[132]: 0.0

In [152]: from sklearn.decomposition import PCA
          from sklearn.decomposition import TruncatedSVD

In [153]: svd=TruncatedSVD(n_components=1000)
          svd.fit(data_matrix_train)

Out[153]: TruncatedSVD(algorithm='randomized', n_components=1000, n_iter=5,
                random_state=None, tol=0.0)

In [154]: X_train_rd=svd.transform(data_matrix_train)

In [156]: X_train_rd.shape

Out[156]: (60000, 1000)

In [157]: clf_svd=svm.LinearSVC()
          clf_svd.fit(X_train_rd,labels_train)

Out[157]: LinearSVC(C=1.0, class_weight=None, dual=True, fit_intercept=True,
               intercept_scaling=1, loss='squared_hinge', max_iter=1000,
               multi_class='ovr', penalty='l2', random_state=None, tol=0.0001,
               verbose=0)

In [159]: clf_svd.score(X_train_rd,labels_train)

Out[159]: 0.99129999999999996

In [161]: clf_svd.predict(X_train_rd[0,:])

/Users/arjunbhagoji/anaconda/lib/python2.7/site-packages/sklearn/utils/validation.py:386: DeprecationWa
  DeprecationWarning)

Out[161]: array([ 0.])

In [162]: X_test_rd=svd.transform(data_matrix_test)

In [163]: clf_svd.score(X_test_rd,labels_test)
```

```
Out[163]: 0.98929187254575224

In [164]: mal_rd=svd.transform(mal_test_sample)

In [165]: clf_svd.predict(mal_rd)

Out[165]: array([ 1.])

In [166]: clf.predict(mal_test_sample)

Out[166]: array([ 0.])

In [179]: count_wrong=0.0
          count_tot=0.0
          count_adv=0.0
          base_wrong=0.0
          for index in test_mal_indices:
              mal_test_sample=data_matrix_test[index,:]
              mal_test_sample[:,top_attack_f[0]]=1.0
              mal_rd=svd.transform(mal_test_sample)
              if clf_svd.predict(X_test_rd[index,:])[0]!=1.0:
                  base_wrong=base_wrong+1
              if clf_svd.predict(mal_rd)[0]!=1.0:
                  count_wrong=count_wrong+1
              if clf_svd.predict(mal_rd)[0]!=clf_svd.predict(X_test_rd[index,:])[0]:
                  count_adv=count_adv+1
              count_tot=count_tot+1
          print count_wrong/count_tot*100, count_adv/count_tot*100, base_wrong/count_tot

0.0 0.0 0.0

In [181]: from sklearn.externals import joblib

In [ ]: joblib.dump(svd,"DREBIN_svd.pkl")
        joblib.dump(clf_svd,"DREBIN_SVM_dr.pkl")
        joblib.dump(clf_svd,"DREBIN_SVM.pkl")

In [ ]:
```