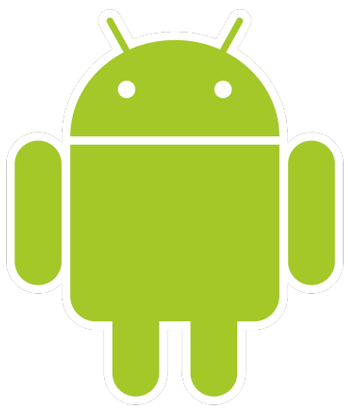
Android Security & Exploitation



Aditya Gupta (@adi1391)

Founder, Attify (http://attify.com)

adi@attify.com

Certifications : http://securitytube-training.com
Pentester Academy : http://PentesterAcademy.com

DEX

What is a dex

- Dalvik Executable
- Runs in the Dalvik Virtual Machine
- Structure : /aosp/dalvik/libdex/DexFile.h
- Dx and dexdump tool

```
struct DexFile {
    /* directly-mapped "opt" header */
    const DexOptHeader* pOptHeader;

    /* pointers to directly-mapped structs and arrays in base DEX */
    const DexHeader*    pHeader;
    const DexStringId*  pStringIds;
    const DexTypeId*    pTypeIds;
    const DexFieldId*   pFieldIds;
    const DexMethodId*  pMethodIds;
    const DexProtoId*   pProtoIds;
    const DexClassDef*  pClassDefs;
    const DexLink*      pLinkData;

    /*
     * These are mapped out of the "auxillary" section, and may not be
     * included in the file.
     */
    const DexClassLookup* pClassLookup;
    const void*         pRegisterMapPool;       // RegisterMapClassPool

    /* points to start of DEX file data */
    const u1*           baseAddr;

    /* track memory overhead for auxillary structures */
    int                 overhead;

    /* additional app-specific data structures associated with the DEX */
    //void*               auxData;
};
```

What is a dex

- Dalvik Executable
- Runs in the Dalvik Virtual Machine
- Structure : /aosp/dalvik/libdex/DexFile.h
- Dx and dexdump tool

Dex file heder

- Magic Number for dex files : 64 65 78 0a 30 33 35 00 or dex\n035

- Hexdump –C classes.dex | less

- Dx and Dexdump

```
struct DexHeader {
    u1  magic[8];           /* includes version number */
    u4  checksum;           /* adler32 checksum */
    u1  signature[kSHA1DigestLen]; /* SHA-1 hash */
    u4  fileSize;           /* length of entire file */
    u4  headerSize;         /* offset to start of next section */
    u4  endianTag;
    u4  linkSize;
    u4  linkOff;
    u4  mapOff;
    u4  stringIdsSize;
    u4  stringIdsOff;
    u4  typeIdsSize;
    u4  typeIdsOff;
    u4  protoIdsSize;
    u4  protoIdsOff;
    u4  fieldIdsSize;
    u4  fieldIdsOff;
    u4  methodIdsSize;
    u4  methodIdsOff;
    u4  classDefsSize;
    u4  classDefsOff;
    u4  dataSize;
    u4  dataOff;
```

Dexdump

```
mobisec@hacking:~/Downloads/Apps$ dexdump
dexdump: no file specified
Copyright (C) 2007 The Android Open Source Project

dexdump: [-c] [-d] [-f] [-h] [-i] [-l layout] [-m] [-t tempfile] dexfile...

-c : verify checksum and exit
-d : disassemble code sections
-f : display summary information from file header
-h : display file header details
-i : ignore checksum failures
-l : output layout, either 'plain' or 'xml'
-m : dump register maps (and nothing else)
-t : temp file name (defaults to /sdcard/dex-temp-*)
```

010 Editor

- Great tool to analyze dex files
- Available for Linux, OSX and Windows
- Download and install it from http://www.sweetscape.com/010editor/
- Download the dex template from https://github.com/strazzere/010Editor-stuff/

010 with dex template

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	0123456789ABCDEF
0000h:	64	65	78	0A	30	33	35	00	47	44	39	10	E7	B4	C3	2A	dex.035.GD9.ç´Ã*
0010h:	66	CB	70	E7	8A	9C	84	CB	A2	D4	6D	16	5B	F5	FC	C6	fËpçŠœ„Ë¢Ôm.[õüÆ
0020h:	50	FF	23	00	70	00	00	00	78	56	34	12	00	00	00	00	Pÿ#.p...xV4.....
0030h:	00	00	00	00	80	FE	23	00	D9	55	00	00	70	00	00	00	....€þ#.ÙU..p...
0040h:	92	0A	00	00	D4	57	01	00	62	0E	00	00	1C	82	01	00	'...ÔW..b....,..
0050h:	CA	37	00	00	B4	2E	02	00	C2	3D	00	00	04	ED	03	00	Ê7..´...Â=...í..
0060h:	90	07	00	00	14	DB	05	00	3C	32	1D	00	14	CD	06	00	.....Û..<2...Í..

Template Results - DEXTemplate.bt

Name	Value	Start	Size	Color	
struct string_id_item string_id[12382]	fb://event/{#%s}/wall/inner	C1E8h	4h	Fg: Bg:	String ID
struct string_id_item string_id[12383]	fb://events	C1ECh	4h	Fg: Bg:	String ID
struct string_id_item string_id[12384]	fb://faceweb/f?href={%s}	C1F0h	4h	Fg: Bg:	String ID
struct string_id_item string_id[12385]	fb://feed	C1F4h	4h	Fg: Bg:	String ID
struct string_id_item string_id[12386]	fb://feed/{#user_id}	C1F8h	4h	Fg: Bg:	String ID
struct string_id_item string_id[12387]	fb://friends	C1FCh	4h	Fg: Bg:	String ID
struct string_id_item string_id[12388]	fb://group/	C200h	4h	Fg: Bg:	String ID
struct string_id_item string_id[12389]	fb://group/{#%s}	C204h	4h	Fg: Bg:	String ID
struct string_id_item string_id[12390]	fb://group/{#%s}/wall/inner	C208h	4h	Fg: Bg:	String ID
struct string_id_item string_id[12391]	fb://groups	C20Ch	4h	Fg: Bg:	String ID
struct string_id_item string_id[12392]	fb://messaging	C210h	4h	Fg: Bg:	String ID
struct string_id_item string_id[12393]	fb://messaging/compose/	C214h	4h	Fg: Bg:	String ID
struct string_id_item string_id[12394]	fb://messaging/compose/{#%s}	C218h	4h	Fg: Bg:	String ID
struct string_id_item string_id[12395]	fb://messaging/{#user_id}	C21Ch	4h	Fg: Bg:	String ID
struct string_id_item string_id[12396]	fb://notes	C220h	4h	Fg: Bg:	String ID
struct string_id_item string_id[12397]	fb://notifications	C224h	4h	Fg: Bg:	String ID
struct string_id_item string_id[12398]	fb://online	C228h	4h	Fg: Bg:	String ID

DalvikVM

- Dalvik Virtual Machine
- Runs dex files
- javac HelloWorld.java
- dx --dex --ouptut=classes.dex Test.java
- Dalvikvm –cp classes.dex classname

DalvikVM

```
class HelloWorld{
        public static void main(String[] arg){
        System.out.println("Hello World");
        }
}
```