FIU | Applied Research Center

Malware Forensics on Mobile Devices for DOE-EM Applications

Andrew De La Rosa
Applied Research Center, Florida International University

Introduction

- Malware attacks are deployed in order to achieve one of the following goals:
  1. To disrupt system functionality.
  2. To gather sensitive information.
  3. To gain access to private data.
- The top areas that become primary targets for malware to attack are:
  1. Availability
  2. Integrity
  3. Confidentiality
- Malware forensics is a particular field where the execution and methods of a malware are studied.

Purpose

- Malware activity has increased on unprotected mobile devices.
- Establishing an accurate and ethical approach is critical when assessing security issues.
- Knowing the method of execution leads to fewer security risks and prevention of future attacks.
- Our intentions are not to create a new wave of malware attacks, but to study them and point to possible vulnerabilities that can occur.

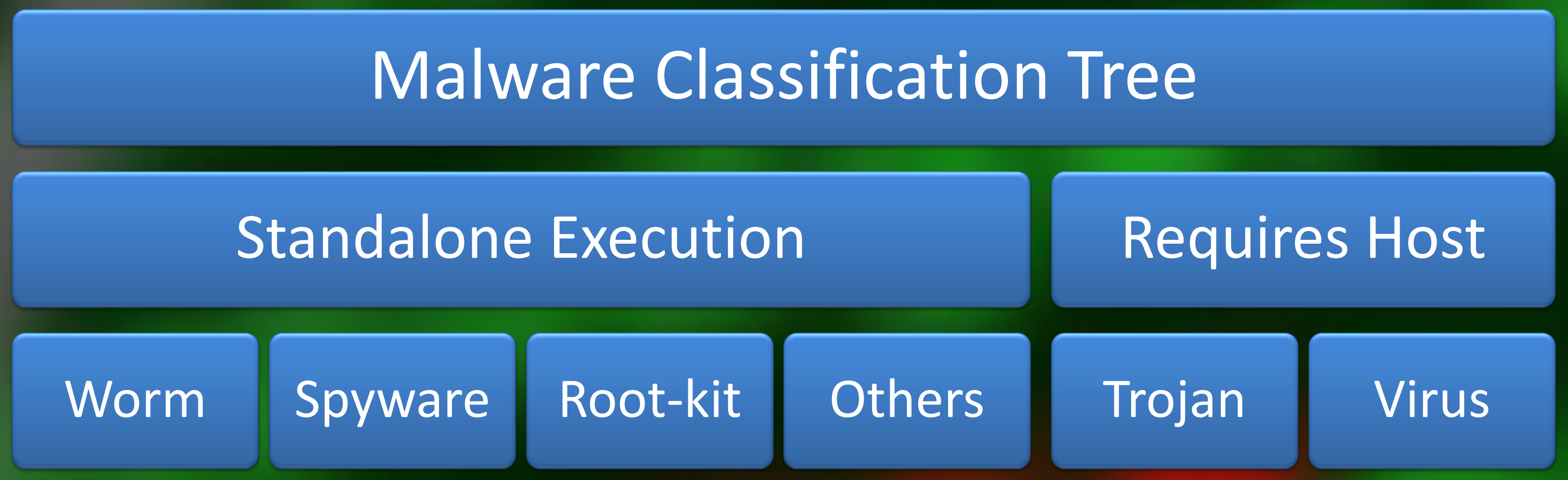
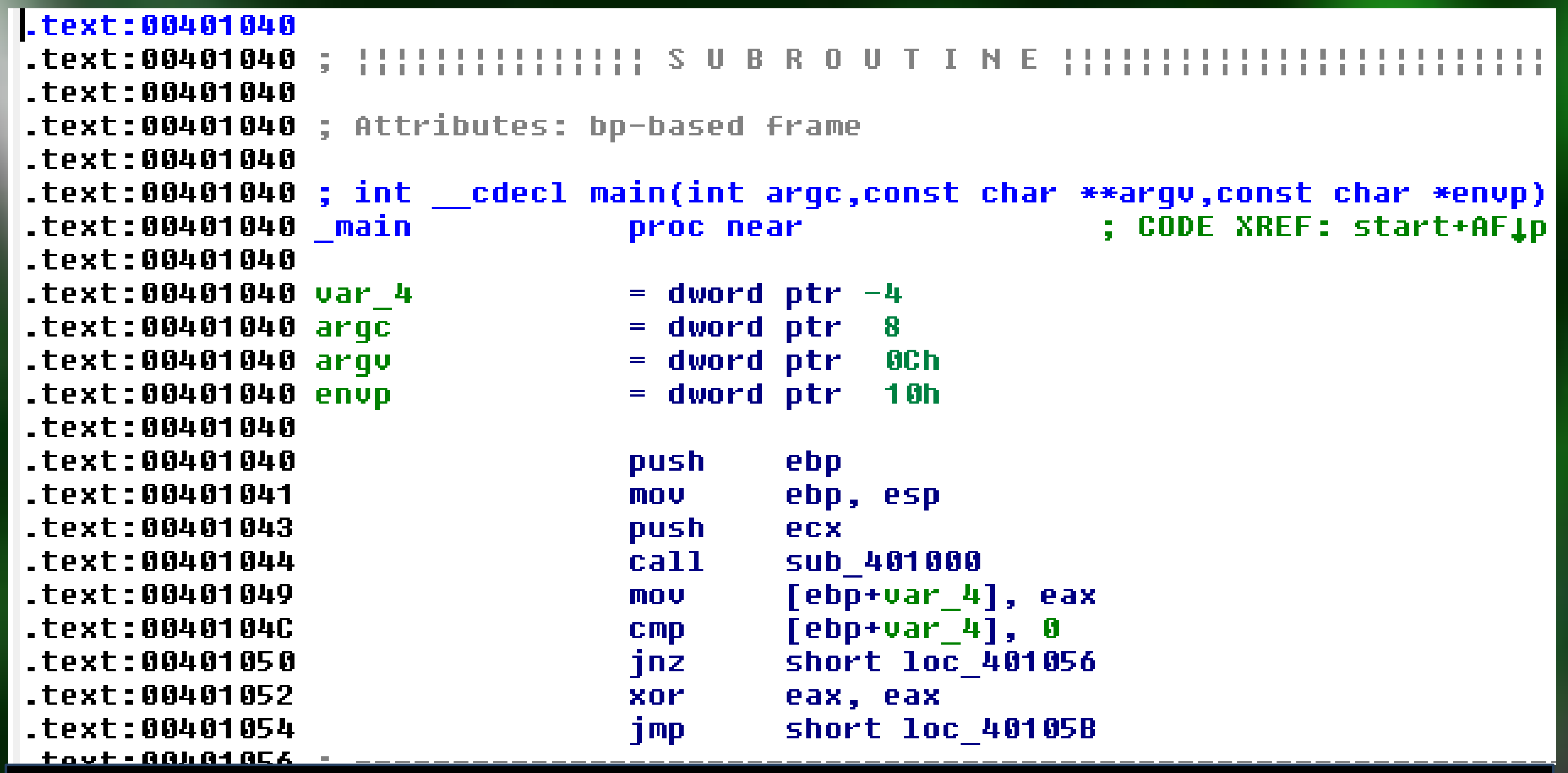


Figure 1: General Classification of Malware

Figure 2: Emulation of Android Nexus 4, using Genymotion, an Android Emulator



```
.text:00401040
.text:00401040 ; ¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦ S U B R O U T I N E ¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦¦
.text:00401040
.text:00401040 ; Attributes: bp-based frame
.text:00401040
.text:00401040 ; int __cdecl main(int argc,const char **argv,const char *envp)
.text:00401040 _main           proc near               ; CODE XREF: start+AF↓p
.text:00401040
.text:00401040 var_4           = dword ptr -4
.text:00401040 argc            = dword ptr  8
.text:00401040 argv            = dword ptr  0Ch
.text:00401040 envp            = dword ptr  10h
.text:00401040
.text:00401040                 push    ebp
.text:00401041                 mov     ebp, esp
.text:00401043                 push    ecx
.text:00401044                 call    sub_401000
.text:00401049                 mov     [ebp+var_4], eax
.text:0040104C                 cmp     [ebp+var_4], 0
.text:00401050                 jnz     short loc_401056
.text:00401052                 xor     eax, eax
.text:00401054                 jmp     short loc_40105B
.text:00401056 ; ---------------------------------------------------------------
```

Figure 3: Entrance Point of Virus (Hacking port 8225, TCP)

Methodology & Results

- To create a workflow for desktop computers, the following benchmarks are used: Using an isolated environment, tracing the host processes, using dynamic analysis to isolate the malware and destroy it.
  - The isolated environment will prevent any malignant code from activating and risking the rest of the computers in the vicinity and/or network.
  - Tracing the host processes will allow us to read the host and user processes, giving us valuable information on the activities of the device.
  - Using dynamic analysis will allow us to manipulate the malware in a number of ways, such as using a debugger to try and change it.
- We used a virus and a Trojan to infiltrate a desktop computer for the following reasons:
  A. The virus will inject itself to force data to connect using a port.
  B. The Trojan will unlock and grant access to an unauthorized port.

Conclusion and Future Work

- With the desktop workflow in place as a systematic approach for mobile applications, we will investigate how to apply the same methods to the mobile devices.
- We are currently looking into different ways to develop ‘friendly’ malware to launch on the Android.
- We will then try to use malignant Windows malware to infect an Android, and using the workflow try to come to the same conclusion as with the Android and Desktop, separately.

Acknowledgements: DOE-FIU Science & Technology Workforce Development Program, Dr. Leonel Lagos and Dr. Himanshu Upadhyay.