김일성종합대학학보
(자연과학)
주체104(2015)년 제61권 제10호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 61 No. 10 JUCHE104(2015).

허위코드삽입에 의한 DEX화일보안의 한가지 방법

박철준, 최혁철

DEX(Dalvik Executable)는 최근에 지능형손전화기와 판형콤퓨터에서 널리 리용되는 Android응용프로그람의 실행화일이다. Android응용프로그람은 주로 Java로 작성되며 바이트코드로 구성되므로 Apktool과 같은 역공학도구들을 리용하여 그 원천코드를 쉽게 얻어낼수 있다. 이로부터 Android응용프로그람의 보안문제가 중요하게 제기된다.[1, 2] 론문에서는 코드혼란기술을 리용하여 DEX화일에 대한 자동해석을 방지하고 Android응용프로그람의 보안을 실현하는 한가지 방법에 대하여 제안한다.

1. Android역공학도구들과 코드혼란기술

모든 Android응용프로그람은 하나의 실행화일 즉 classes.dex를 가진다. DEX화일은 Java의 class화일에 기초하고있으며 여러개의 class화일들을 하나로 묶어 최량화한 구조를 가지고있다.[1]

여러가지 역공학도구들은 DEX화일의 구조를 해석하여 바이트렬을 Dalvik명령렬로 변환하며 Java원천코드 또는 중간코드를 생성한다.

대표적인 Android역공학도구들로는 Baksmali, Apktool, Dex2jar, IDA Pro, Virtuous Ten Studio들이 있다.

Baksmali는 바이트코드별로 해석하여 모든 명령을 알기 쉬운 문자렬형식으로 출력하며 본문우에서 수정이 가능하다. Smali를 리용하면 다시 DEX화일을 생성할수 있다.

Apktool은 apk화일을 전부 해석하고 다시 묶을수 있는 간단하면서도 편리한 도구이다. 내적으로는 baksmali/smali를 리용하여 DEX화일을 해석 및 생성한다.

Dex2jar는 DEX화일을 해석하여 Java원천코드를 생성하며 결과는 jar화일로 얻어진다. jar화일의 내용은 jd-gui를 비롯한 다른 Java역공학도구들에서 열람 및 편집할수 있다.

IDA Pro는 강력한 역아쎔블러로서 Dalvik바이트코드렬을 해석하며 그라프사용자대면을 비롯한 여러가지 편리한 기능들을 지원한다.

Virtuous Ten Studio는 baksmali/smali를 내장하고있으며 apk에 대한 해석과 건설을 통합적으로 진행할수 있는 개발환경을 제공한다.

역공학도구들의 동작과정은 어디까지나 프로그람적인 해석과정이므로 코드혼란기술을 리용하여 원천코드해석을 방지할수 있다.

코드혼란기술에는 구조적혼란, 조종흐름혼란, 자료혼란방법들이 있다.[1]

구조적혼란은 변수나 함수이름들을 교체함으로써 역공학의 결과로 얻어지는 코드를 실

행 및 리해불가능하게 하는 방법이며 자료혼란은 문자렬, 배렬 등의 자료들이나 변수의 위치 등을 변경하는 방법이다. 조종흐름혼란은 프로그람의 조종흐름을 복잡하게 만들어 역공학을 방지하는 기술이며 그중의 한가지가 허위코드삽입방법이다.

허위코드란 Dalvik명령렬로 정확히 해석할수 없거나 해석되는 경우에도 의미가 없는 명령렬을 이루는 바이트렬을 의미하며 허위코드삽입은 프로그람의 실행에 영향을 주지 않으면서 허위코드를 추가하는 방법이다.

선행연구 [1]에서는 여러가지 코드혼란기술들과 함께 함수들의 끝에 명령렬을 추가하는 허위코드삽입방법을 서술하였다. 그러나 이 방법은 특정한 역공학도구에 대해서만 효과적이고 현대적인 역공학도구들에 대해서는 적용할수 없다. 이로부터 론문에서는 보다 강도가 높은 한가지 허위코드삽입방법을 제안한다.

2. 허위코드삽입에 의한 DEX화일보안방법

우리는 허위코드삽입을 두가지 방법으로 진행하였다.

1) 허위분기삽입방법

진리값이 항상 거짓인 조건식을 리용하여 함수의 앞부분에 한쪽 분기만 실행되는 if 문을 삽입한다.

실례

Java코드	바이트렬(16진수)	Dalvik명령렬
int i = 1;	12 10	const/4 v0, 1
int j = 0;	12 01	const/4 v1. 0
if (i < j) {	35 10 06 00	if-ge v0, v1, label1
…	…	…
} else {	label1: …	…
… …	…	
} …	…	

실례에서 보는바와 같이 첫번째 분기에는 허위코드를, 두번째 분기에는 원래의 함수본체를 배치하는데 허위코드로는 불완전명령을 리용한다. 완전한 하나의 Dalvik명령은 연산코드와 그에 따르는 여러개의 자료바이트로 이루어진다. 여기서 하나 또는 그 이상의 자료바이트를 없애면 불완전한 명령으로 된다. 결과 순차적인 해석과정에 뒤에 놓이는 완전명령의 연산코드부분을 자료바이트로 해석하게 함으로써 진짜 함수본체에 대한 정확한 원천코드를 얻을수 없게 한다.

2) 련속이행문삽입방법

Dalvik바이트코드에는 여러개의 이행명령이 있다. 실례로 연산코드 0x2A는 뒤에 오는 4B변위주소에로 이행하는 goto명령이며 연산코드 0x28, 0x29는 각각 1e, 2B변위주소를 가진다.

함수의 앞부분에 뒤에로의 이행명령을 삽입하되 그것의 자료바이트의 뒤부분이 원래 함수본체의 첫 부분과 일치하도록 한다. 이행된 위치에서 다시 원래 함수본체의 첫 부분에로의 이행명령을 삽입한다. 결과 하나의 명령을 두가지 의미로 해석하는것은 불가능하므로 함수본체에 대해 정확히 해석할수 없게 한다.(그림)

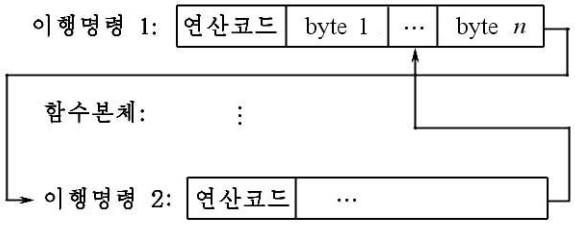

그림. 련속이행문삽입과정

3. 실험 및 결과분석

실험결과는 표와 같다.

표. 실험결과

방법	도구		
	Dex2jar	Baksmali	IDA Pro
선행방법[1]	해석실패	허위코드를 무시하고 해석	허위코드를 무시하고 해석
허위분기 삽입방법	해석실패	틀리게 해석	허위코드를 무시하고 해석
련속이행문 삽입방법	해석실패	틀리게 해석	틀리게 해석

표에서 보는바와 같이 제안한 방법에 대해 거의 모든 역공학도구들이 해석하지 못하거나 틀린 해석결과를 출력하였다. 이로부터 허위코드삽입에 의해 역공학도구들에 의한 DEX화일의 자동해석을 방지할수 있다는것을 확인하였다. 역공학도구들가운데서도 역번역기들보다 역아쎔블러가 코드혼란에 보다 강하며 제안된 방법을 Proguard를 비롯한 다른 코드혼란도구들과 결합하여 리용하면 보안강도를 보다 높일수 있다.

맺 는 말

코드혼란기술의 한가지 방법인 허위코드삽입에 의해 DEX화일에 대한 보안을 실현하는 방법을 제안하였다. 실험결과는 제안된 방법에 의해 역공학도구들에 의한 자동해석을 충분히 방지할수 있다는것을 보여주었다.

참 고 문 헌

[1] Godfrey Nolan; Decompiling Android, Apress, 1～296, 2012.

[2] William Enck et al.; http://www.enck.org.

주체104(2015)년 6월 5일 원고접수

A DEX File Protection Method by Pseudo-Code Injection

Pak Chol Jun, *Choe Hyok Chol*

We propose a DEX file protection method by pseudo-code injection, a kind of code confusion technique. Pseudo-code means byte array that can't be analyzed with DVM statements exactly and has no effect on original program's execution. Experimental results show that our method is effective to prevent automatic analysis by common reverse engineering tools.

Key words: confusion, Android