

**Uniwersytet Warszawski**  
Wydział Matematyki, Informatyki i Mechaniki

**Marcel Kołodziejczyk**

Nr albumu: 219533

# **Luki w bezpieczeństwie systemu operacyjnego Android**

**Praca magisterska  
na kierunku INFORMATYKA**

Praca wykonana pod kierunkiem  
**dra Marcina Peczarskiego**  
Instytut Informatyki

Czerwiec 2013

## **Oświadczenie kierującego pracą**

Potwierdzam, że niniejsza praca została przygotowana pod moim kierunkiem i kwalifikuje się do przedstawienia jej w postępowaniu o nadanie tytułu zawodowego.

Data

Podpis kierującego pracą

## **Oświadczenie autora (autorów) pracy**

Świadom odpowiedzialności prawnej oświadczam, że niniejsza praca dyplomowa została napisana przeze mnie samodzielnie i nie zawiera treści uzyskanych w sposób niezgodny z obowiązującymi przepisami.

Oświadczam również, że przedstawiona praca nie była wcześniej przedmiotem procedur związanych z uzyskaniem tytułu zawodowego w wyższej uczelni.

Oświadczam ponadto, że niniejsza wersja pracy jest identyczna z załączoną wersją elektroniczną.

Data

Podpis autora (autorów) pracy

## **Streszczenie**

krótkie streszczenie pracy

## **Słowa kluczowe**

android, arm, atak, bezpieczeństwo, przepełnienie bufora, metasploit, exploit, shellcode

## **Dziedzina pracy (kody wg programu Socrates-Erasmus)**

11.3 Informatyka

## **Klasyfikacja tematyczna**

D. Software  
D.4. Operating Systems  
D.4.6. Security and Privacy Protection

## **Tytuł pracy w języku angielskim**

Vulnerabilities in Android operating system



# Spis treści

<b>1. Omówienie problemu . . . . .</b>	<b>7</b>
<b>2. Podsumowanie . . . . .</b>	<b>9</b>
<b>Bibliografia . . . . .</b>	<b>11</b>

## Todo list

Sprawdzić klasyfikację ACM . . . . .	5
--------------------------------------	---



# Wprowadzenie

Jakiś przydługi niewiele mówiący opis.

Sprawdzić  
klasy-  
fikację  
ACM



## Rozdział 1

# Omówienie problemu



## **Rozdział 2**

### **Podsumowanie**



# Bibliografia

- [1] Anthony Desnos, Geoffroy Gueguen *Android: From Reversing to Decompilation*, Black Hat, Abu Dhabi, 2011
- [2] S. Höbarth, R. Mayrhofer, *A framework for on-device privilege escalation exploit execution on android*, IWSSI/SPMU 2011: 3rd International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use, colocated with Pervasive 2011, czerwiec 2011. dostępne na <http://www.medien.ifi.lmu.de/iwssi2011/>
- [3] Gaurav Kumar, Aditya Gupta, *A Short Guide on ARM Exploitation*, <http://www.exploit-db.com/wp-content/themes/exploit/docs/24493.pdf>
- [4] Yves Younan, Pieter Philippaerts, *Alphanumeric RISC ARM shellcode*, Phrack, 66, czerwiec 2009
- [5] Joshua Hulse, *Buffer Overflows: Anatomy of an Exploit*, <http://packetstormsecurity.com/files/108549/Buffer-Overflows-Anatomy-Of-An-Exploit.html>
- [6] Emanuele Acri, *Exploiting Arm Linux Systems*, <http://packetstormsecurity.com/files/98376/Exploiting-ARM-Linux-Systems.html>
- [7] Collin Mulliner, Charlie Miller, *Fuzzing the Phone in your Phone*, Black Hat USA, 2009
- [8] Jonathan Salwan, *How to Create a Shellcode on ARM Architecture*, <http://www.exploit-db.com/papers/15652/>
- [9] Dustin „Itruid” Trammel, *Metasploit Framework Telephony*, Black Hat USA, 2009
- [10] Itzhak Avraham, *Non-Executable Stack ARM Exploitation*, Black Hat DC, 2011
- [11] jip@soldierx.com, *Stack Smashing On A Modern Linux System*, <http://www.soldierx.com/tutorials/Stack-Smashing-Modern-Linux-System>
- [12] Metasploit framework, <http://www.metasploit.com>
- [13] Android project, <http://developer.android.com>
- [14] The WebKit Open Source Project, <http://www.webkit.org>