

스마트 플랫폼 커널 악성코드 시연

Android 플랫폼 커널 기반 악성코드 시연 및 대응 방안


2011. 06. 20.

(주)아이넷캡
연구소장 유동훈
x82@inetcop.org

Dong-hoon You – Xpl017Elz (x82)

- INetCop Security Research institute Director
- <http://x82.inetcop.org>
- Chonnam national university graduate school of Information Security
- Field of research
 - * analyzing web application vulnerability
 - * analyzing system application vulnerability
 - * analyzing system kernel, library vulnerability
 - * analyzing application exploit source code vulnerability
 - * developing Proof-of-concept exploit code
- Regularly published security advisory report and POC exploits since 2002
- Supervised SNOsoft's security advisory





National Infrastructure Protection Center

CyberNotes

www.nipc.gov

CyberNotes - 2003

CyberNotes

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

CyberNotes seeks to provide computer security professionals with a summary of security-related topics and issues and does not provide exhaustive details regarding any issue. CyberNotes does provide references to the respective sources used in compilation of the report in order to allow follow up on the part of the security professional.

MILWORM				
Author:		XPL017ELZ		
Homepage:		http://x82.inetcop.org		
DATE	DESCRIPTION	EXPLOITS/POC CODE	STATUS	AUTHOR
2007-07-08	Apache Tomcat Connector (mod_jk) Remote Exploit (Cross-Shell)	25256	R	Xpl017Elz
2007-05-14	mshtmlcomctl R.R.1 (GET Request) Remote Root Exploit (Cross-Shell)	6797	R	Xpl017Elz
2007-05-02	Spawning R533 group's Input() Remote Overflow Exploit (Cross-Shell)	7619	R	Xpl017Elz
2007-04-28	Remote GDI+ Remote L33t Remote Buffer Overflow Exploit (Cross-Shell)	6783	R	Xpl017Elz
2007-04-28	Local Machine Group R533 Remote Format String Exploit (Cross-Shell)	7149	R	Xpl017Elz
2007-04-18	Root R533 Local L33t Local Local Overflow Exploit (Cross-Shell)	11787	R	Xpl017Elz
2005-04-11	gdi L33t (GDI+ Local Overflow) Remote Format String Exploit	2873	R	Xpl017Elz
2003-08-11	Use Pspid 2.0.2 Remote Root Exploit (Advanced version)	12203	R	Xpl017Elz
2003-08-03	Use Pspid 2.0.2 off by one Remote Root Exploit	7794	R	Xpl017Elz
2003-03-22	Worm L33t Remote Root Heap Overflow Exploit	5478	R	Xpl017Elz
2003-04-29	Groupware R533 Remote Local Root Exploit	5922	R	Xpl017Elz
DATE	DESCRIPTION	EXPLOITS/POC CODE	STATUS	AUTHOR
2007-04-18	Advanced exploitation to cross-shell (Remote Code Execution)	12000	R	Xpl017Elz



packet storm

packet storm

about network search assessment defense education papers magazines infrastructure links

Archive Search Results for: Xpl017Elz

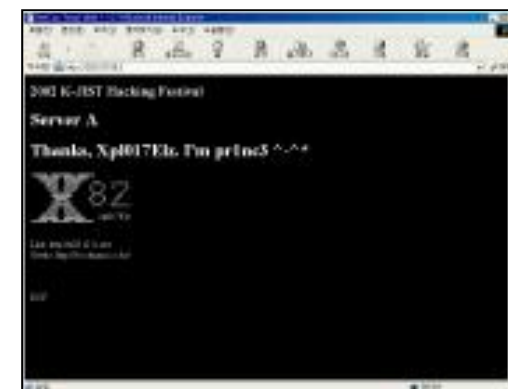
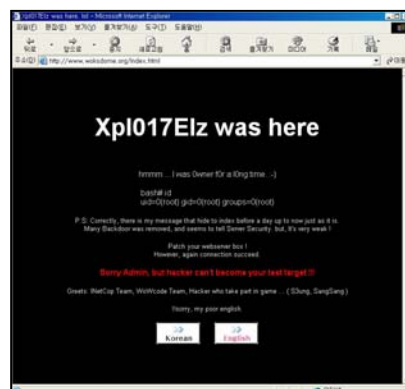
Search Results: 1 - 15

File Name	Description	Author	Homepage	MSVC Checksum
LightHTTP.dll	Packet Storm Security Advisory #2002-0422-001 - A directory browser vulnerability has been found in Tiny HTTP 1.0. Basic exploitation is documented.	Xpl017Elz	http://packetstormsecurity.com/~xpl017elz/	43123a4d3b4a74309a2950a6c
LightHTTP.dll	Packet Storm Security Advisory #2002-0422-002 - A buffer overflow in Light HTTP version 1.0 allows for remote attackers to grab a shell or perform related activities as the webserver user.	Xpl017Elz	http://packetstormsecurity.com/~xpl017elz/	25683c1201420f4a6d2950f3a3a6
LightHTTP.dll	Packet Storm Security Advisory #2002-0422-003 - Light HTTP, a utility that can be used to add basic web server capabilities to an application or embedded device, is vulnerable to a buffer overflow which allows remote attackers to gain root access to the system.	Xpl017Elz	http://packetstormsecurity.com/~xpl017elz/	320a4a4a12477b4a6d2950f3a3a6
LightHTTP.dll				

Dong-hoon You - Xpl017Elz (x82)

- Winning a prize career

- * King of Fighters 2001 International Hacking Competition prize
- * Chongin college Hacking Contest 2001 prize
- * \$100K WOKSDOME (KDWorks) Global Hacking Competition 2002 prize
- * KHF2002 KJIST SeeCure-CSRL Hacking Festival prize
- * Hackerschool 2nd Hacking Festival 2002 prize
- * DaeDuk college Hacking Championships 2002 prize
- * Kimcheon science college Hacking Contest 2003 prize
- * UDCSC Hacking Festival 2005 prize
- * Defcon CTF 2007 Prequal SOF Team
- * Defcon CTF 2008 Prequal WOWHACKER Team
- * Defcon CTF 2009 Prequal WOWHACKER Team



Dong-hoon You – Xpl017Elz (x82)

– Teaching Career

- * High Level security lecture to a government institute with Samsung SDS
- * Special Level security lecture to a government institute
- * High Level security lecture to Software developers with Samsung SDS
- * Lecture on annual Security Seminar for a government institute
- * lectures on Security-Proof seminar
- * Major speaker of POC 2006 conference
- * Major speaker of PADOCON 2007 conference
- * Major speaker of ISEC 2008 conference
- * Major speaker of POC 2008 conference



삼성SDS



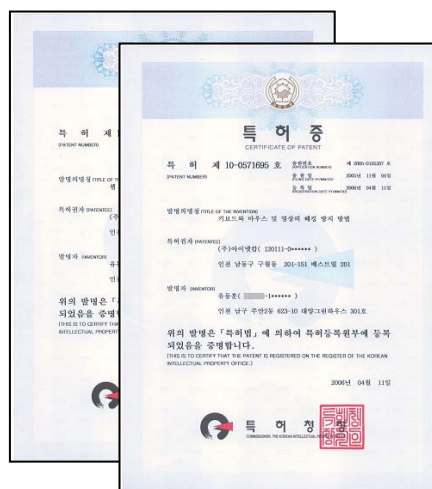
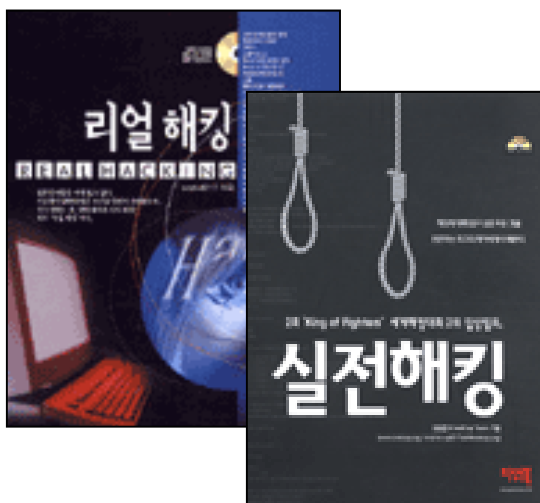
SECURITYPROOF



Dong-hoon You – Xpl017Elz (x82)

– Patterns, writings and other articles

- * Published 'REAL HACKING'
- * Published 'REAL HACKING2'
- * Small buffer format string attack (bugtraq)
- * Patterned 'Hacking Prevention Method On Keyboard, Mouse And Images'
- * Patterned 'Web User's Physical Location Tracing System And Method'
- * Web 2.0 CSRF exploitation (web-board case study)
- * New Ways to Attack Applications of Operating System Under Execshield
- * Advanced exploitation in exec-shield (Fedora Core case study)
- * New Local & Remote Exploit to Get Over Exec-shield Protection



Dong-hoon You - Xpl017Elz (x82)






- Media news articles

2002년 12월 17일: [ZDNET] CNET, ZDNET UK TechRepublic 취약점 관련 기사
2003년 06월 10일: [ZDNET] ZDNET JP에 POC로 개발된 kernel rootkit 소개
2006년 03월 14일: [보안뉴스] 제로보드, 보안 취약점 패치 권고
2006년 05월 19일: [전자신문] 아이넷캡, 키보드 마우스 영상해킹 방지방법 특허 획득
2006년 05월 19일: [INews24] 아이넷캡, '키보드, 마우스 영상 해킹 방지' 특허 획득
2006년 08월 02일: [전자신문] 아이넷캡, '인스펙터' 개발
2006년 08월 07일: [전자신문] 악성맷글, 서버 공격 꼼짝 마
2006년 11월 17일: [보안뉴스] 취약점 공개장소 없어...해외에만 발표
2006년 11월 17일: [WIRED] Polite Hackers Kick It in Korea
2008년 09월 03일: [보안뉴스] [TV] 아시아 최대 규모 정보보안 컨퍼런스, ISEC 2008
2008년 11월 14일: [보안뉴스] [POC] x82, 업그레이드된 리눅스 공격방법 선보여

Dangerous flaw in Lib CGI

Tags: CGI Library, Security Focus, BugTraq, Security

John McCormick
Published: 17 Dec 2002 12:14 GMT

 Email  Trackback  Clip Link  Print  Post a comment

A serious vulnerability has been found in the CGI C library LibCGI (libcgi.h), which is used widely by Unix and Linux programmers. Some serious security concerns have also recently been raised about C compilers themselves.

Symantec reported that "improper bounds checking" is the cause of a LibCGI vulnerability, and that the flaw could allow an attacker to gain Web server process privileges to a system. The original report was posted to BugTraq and a Russian Web site, both of which describe the problem as a "remote frame pointer overwrite vulnerability." The latter report carries a detailed, if somewhat cryptic explanation of the problem (English is obviously a second language for the writer), which the author says is located in line 76 of Include/libcgi.h:

```
76  buffer[y]=pt[x]; //
```

エンタープライズ:特集 2003/06/10 15:23:00 更新

rootkitによるハッキングとその防御
第5回 kernel rootkitの概要 (3/4)

トロイの木馬としてのローダブルカーネルモジュール

では実際に、サンプルとしてトロイの木馬のローダブルカーネルモジュールである「LKMDx82」をロードして、これまで紹介してきたような検出ツールを単純に利用した場合にトロイによる改ざんを発見できるか確認してみよう。

ここで紹介しているLKMDx82は、ユーザー権限の引き上げ(rootアクセス)、ディレクトリ、ファイル、プロセス、接続元IPアドレスの隠蔽、そしてトロイの木馬自身の隠蔽(lsmodコマンドでリスト表示されない)が可能になっている。今回取り上げているトロイの木馬は、前述したLKMDのサンプルと同じように、「mkldir」や「cd」といった、ごく普通に利用するコマンドを介して実行できるようになっている。今回のテストはRedhat Linux 7.1上で行った。

■LKMDのロード

侵入したと仮定したシステムで、LKMDのトロイの木馬をロードする。LKMDは実行中のカーネルにロードされ、カーネルの一部となり動作する。今回利用しているトロイの木馬はロードされた時点から、lsmodコマンドではリスト表示されない。このため、lsmodコマンドでは検知することができない。

WIRED SUBSCRIBE >> SECTIONS >> BLOGS >> REVIEWS >> VIDEO >> Sign In RSS Fe

SCIENCE : DISCOVERIES

Polite Hackers Kick It in Korea

Quinn Norton 11.17.06



SEOUL, South Korea -- The first international hacker conference held in this most wired of nations would never be confused with its Western forebears. Instead of jeans and T-shirts with clever slogans, attendees wore button-down shirts and pleated slacks while listening quietly and attentively to speakers dressed in suits. There were few jokes, no interruptions and not a drinking game in sight.

But in terms of content, the two-day Power of Community conference that opened here Thursday follows squarely in the tradition of events like Defcon and Hope in the United States, featuring everything from a civil liberties stump speech from free-software guru Richard Stallman to live demonstrations of taking over a remote voice-over-internet-protocol session and remote exploits against Fedora Core.

목차

- Smart Phone Malware
 - Android 커널 악성코드 배경
 - Android 커널 악성코드 시연
 - Android 커널 악성코드 대응
 - 결론



Smart Phone Malware

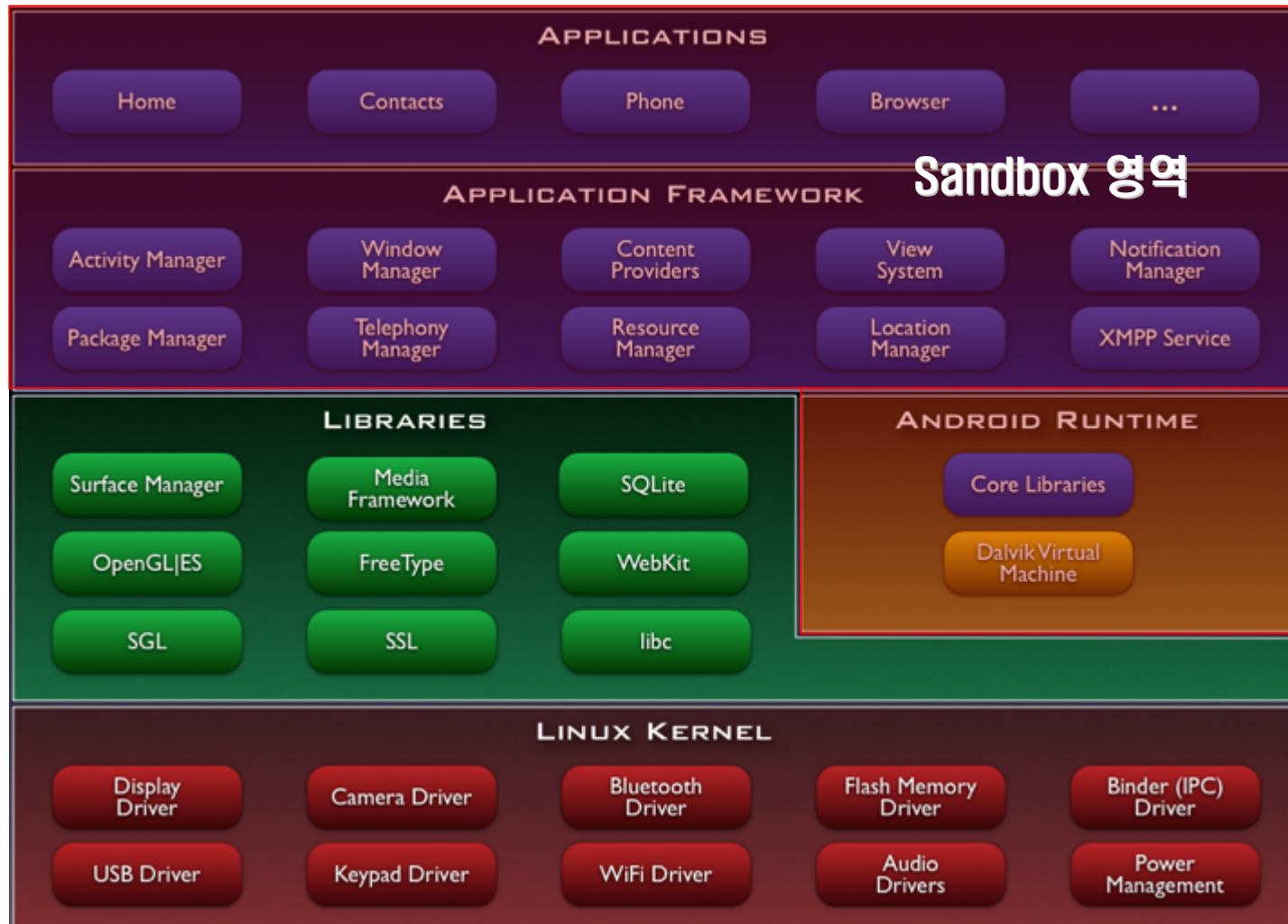
Android 커널 악성코드 배경



The purpose of Sandbox

The ideal operating of a sandbox

Android 플랫폼 sandbox 구성

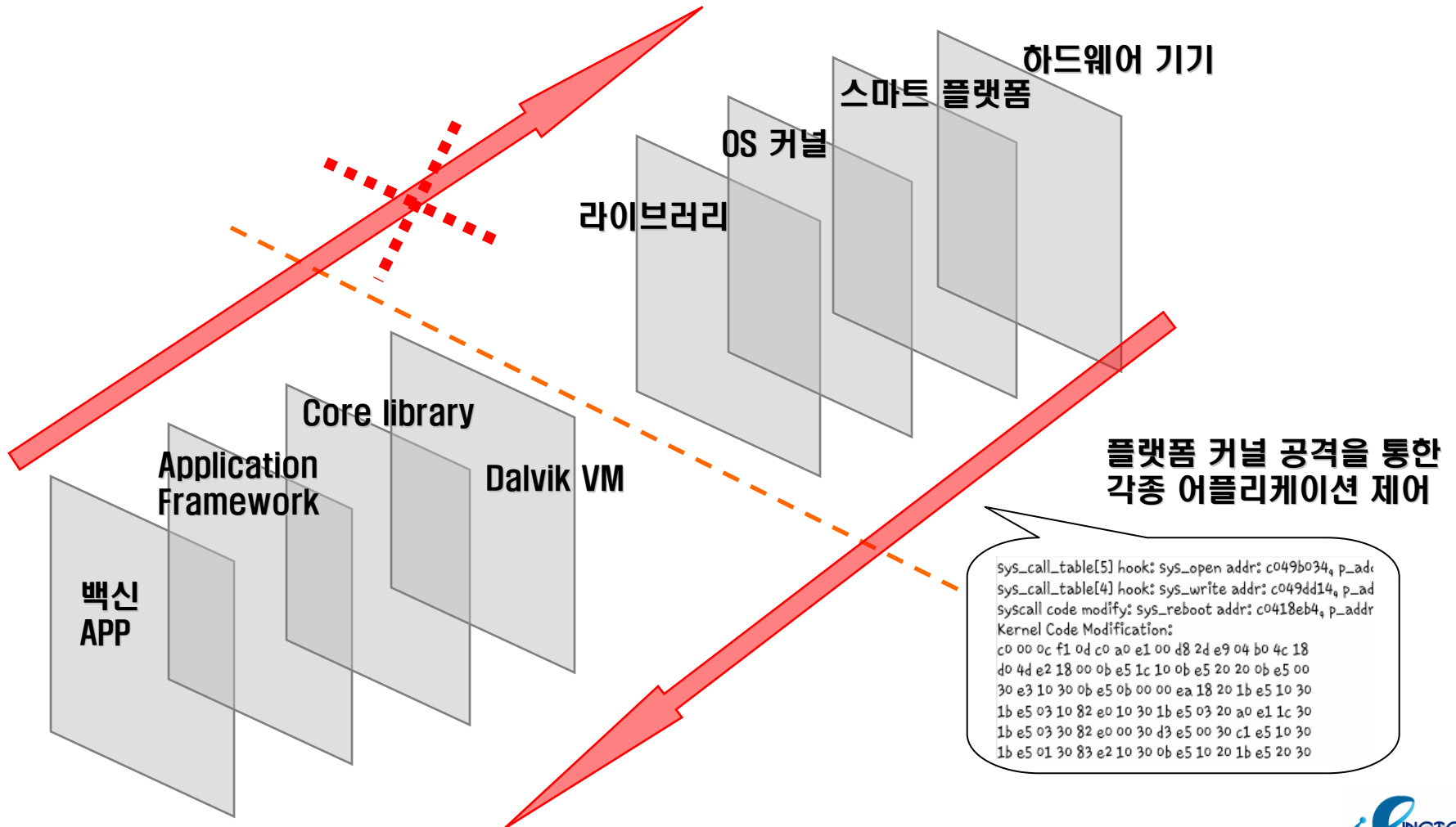




Reality of sandbox security

However, the reality is a battlefield

Android 플랫폼 sandbox 보안 기술의 문제점



- **Android 플랫폼 sandbox 내의 악성코드로 인한 보안 위협**
 - app으로 실행되는 각종 Backdoor, Trojan S/W 등의 악성코드 등장
 - 악의적인 요금 과금, 정보 탈취, 위치 추적, 영상/음성 도청 악성코드 등장
 - 기기 파괴, 대량 스팸 문자(SMS) 및 메일 발송, DDoS 봇넷 공격 시도
 - app 보안성 검증, 백신 제품으로 대응 가능

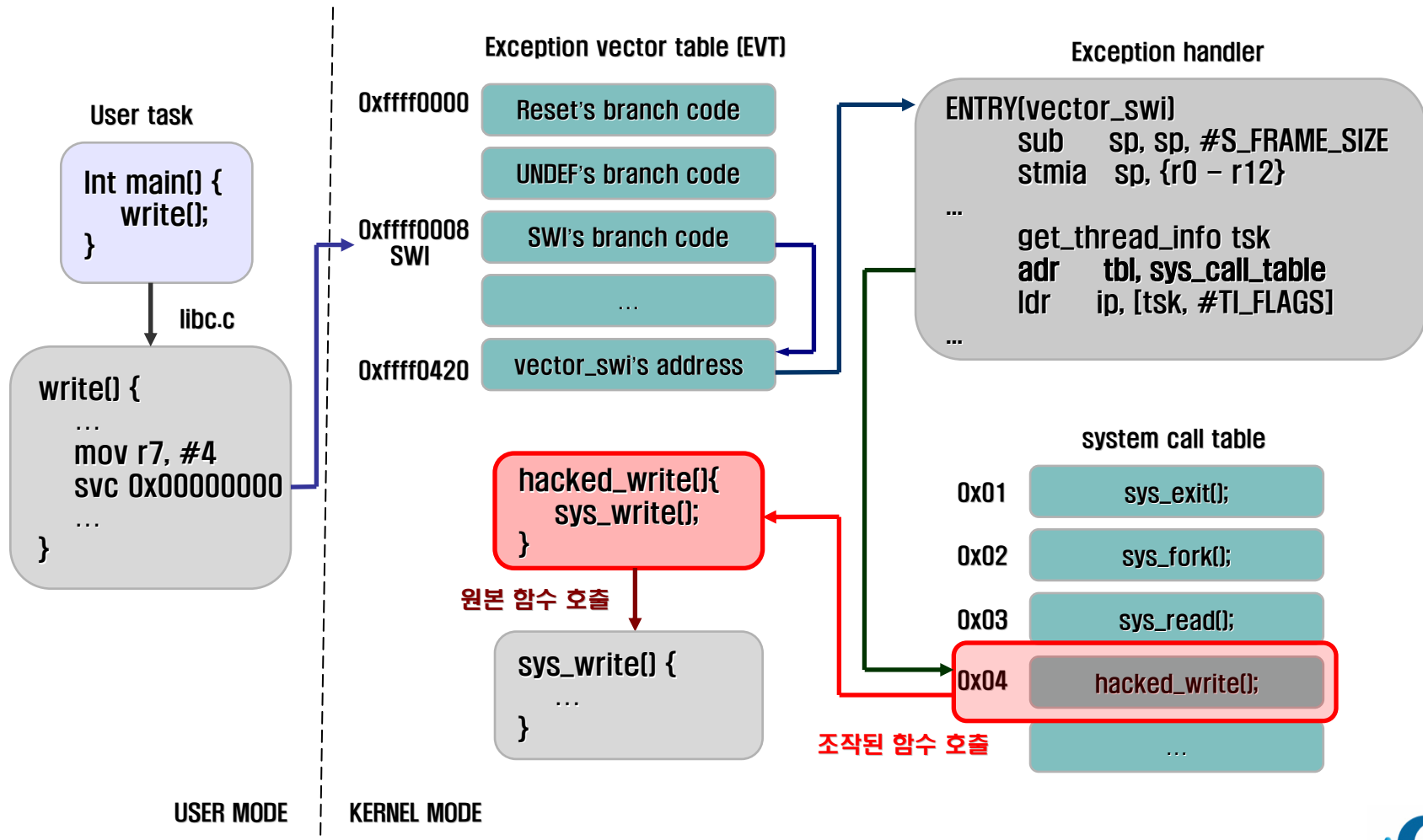
- **Android 플랫폼 sandbox 밖의 취약점으로 인한 보안 위협**
 - 2010년, Android 3rd party 어플리케이션, 웹 브라우저 원격 공격 코드 등장
 - 2009년 8월, 플랫폼에 탑재된 커널 결함을 통한 로컬 루팅 공격 코드 등장
 - 2010년 6월, LKM 형태의 Android 커널 기반 Rootkit 등장 (Defcon 18)
 - 보안 업데이트 적용이 어려운 근본적인 문제점 존재

* 참조: <http://www.exploit-db.com>

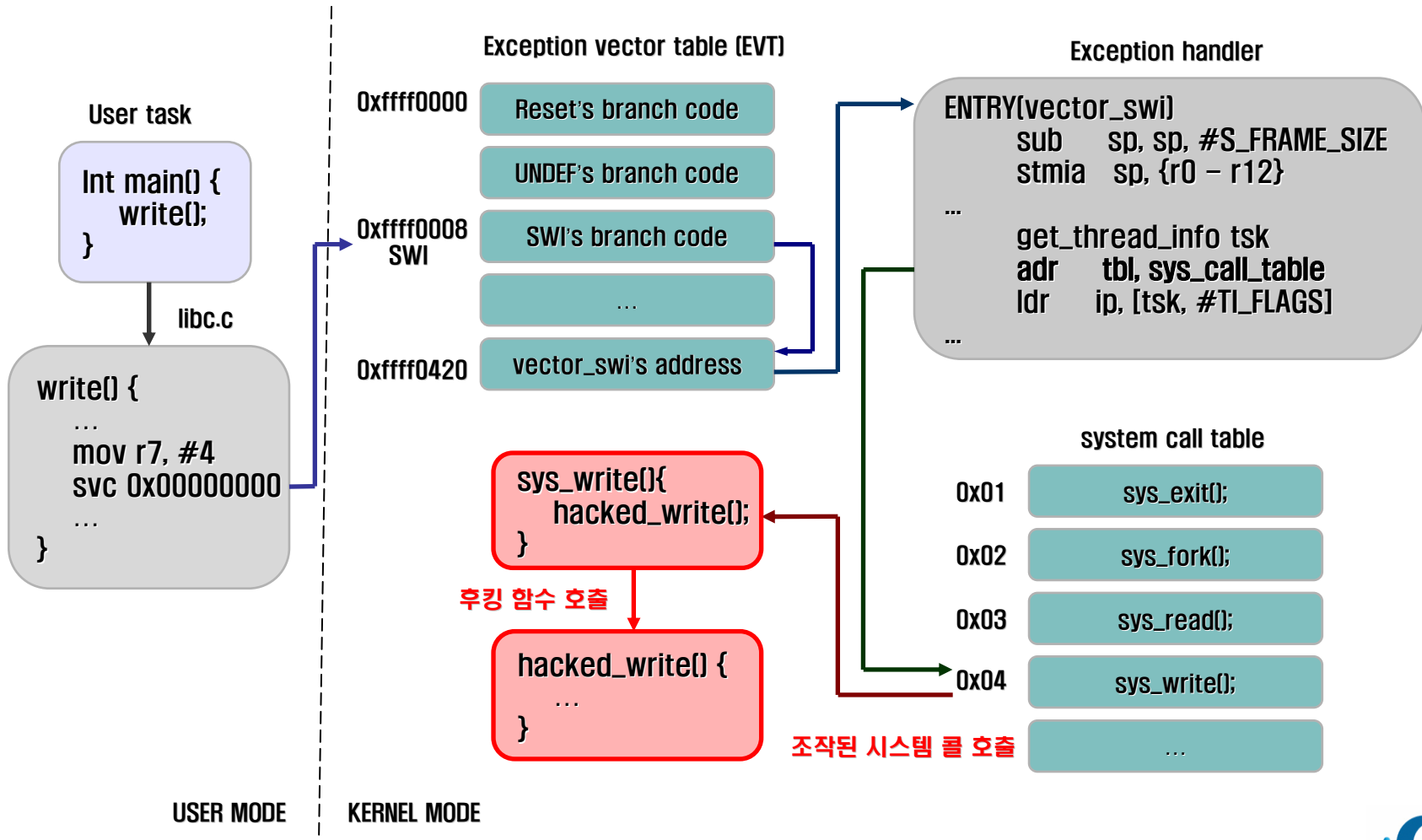
- **과거 Linux 기반 악성코드 패러다임의 변화**
 - 시스템 바이너리를 교체하는 파일 및 프로세스 은닉 방식
 - checksum 비교에 쉽게 탐지되는 것이 특징
 - 96년 이후 OS 커널 자체에 숨어서 동작하는 커널 기반 Rootkit 발견
 - 2010년 6월 최초 Android 스마트 플랫폼 커널 기반 Rootkit 발표
- **LKM (Loadable kernel module) 동적 적재를 통한 커널 접근 기술**
 - 런타임 커널 동적 모듈 적재 기능(LKM)을 플랫폼에서 기본으로 제공
 - 커널 컴파일, 재부팅 없이도 개발한 코드를 커널에 추가하거나 제거 가능
 - UTS_RELEASE 수정으로 vermagic 제한을 우회하여 LKM 커널 모듈 적재
 - sys_call_table 내에 저장된 함수 주소를 공격자의 함수로 변경하여 후킹

- **KMEM device 접근을 통한 커널 메모리 접근 기술**
 - Silvio Cesare의 “런타임 KMEM 패칭” sd의 Phrack 58-7호에서 소개
 - /dev/mem, /dev/kmem 선형, 가상 메모리 �핑 파일을 통한 접근
 - 사용자 레벨에서 모듈 설치 없이 런타임 커널을 패치할 수 있는 장점 제공
 - 각 제조사에서 제공하는 다양한 커널 버전에 非 의존적, 독립적으로 동작
- **Android 플랫폼 sandbox 밖의 커널 모드 후킹 종류**
 - IDT exception vector table hooking
 - vector_swi (exception handler) hooking
 - sys_call_table hooking
 - kernel byte code patching

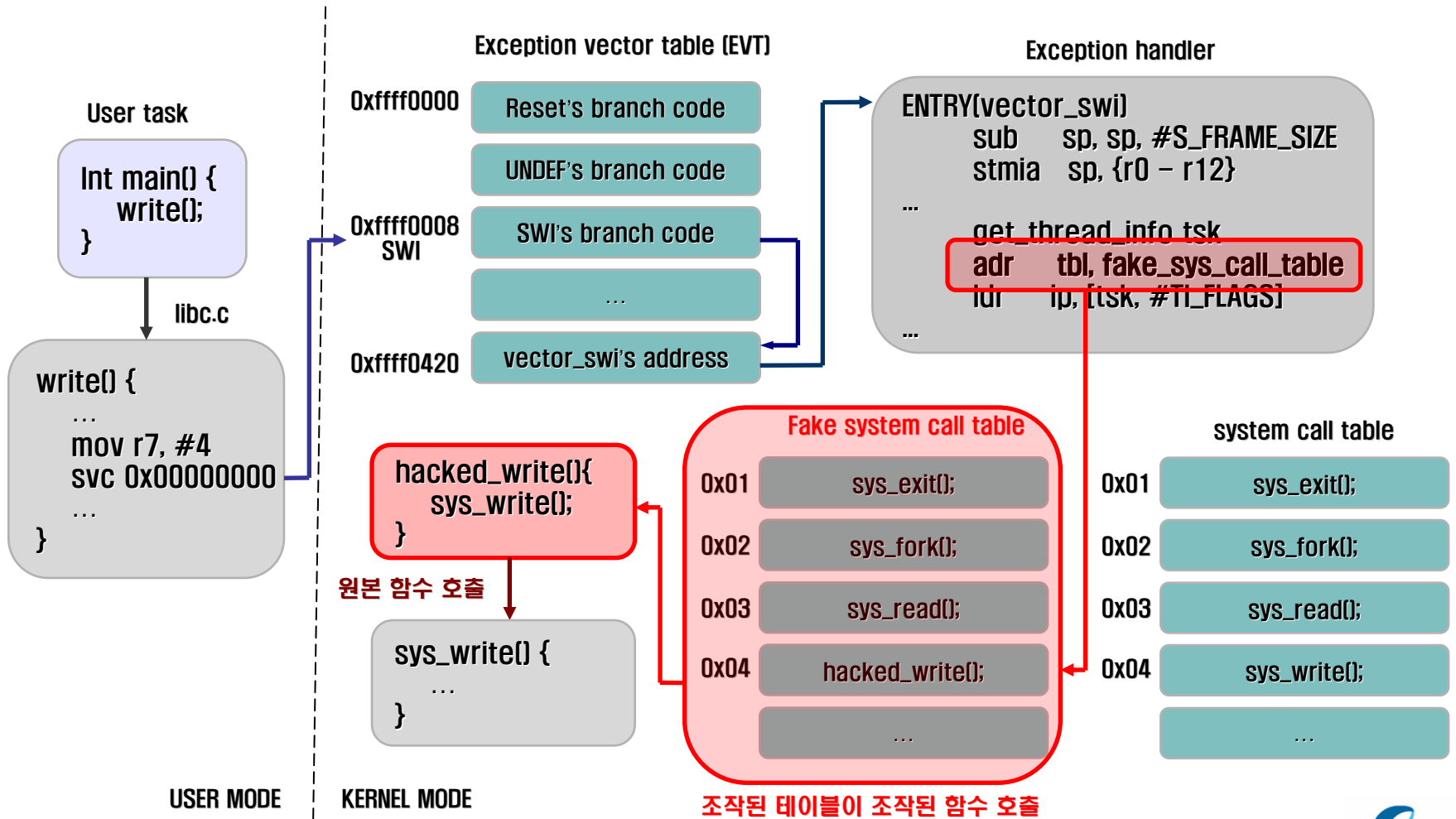
Android 플랫폼 커널 기반 악성코드 기술 #1



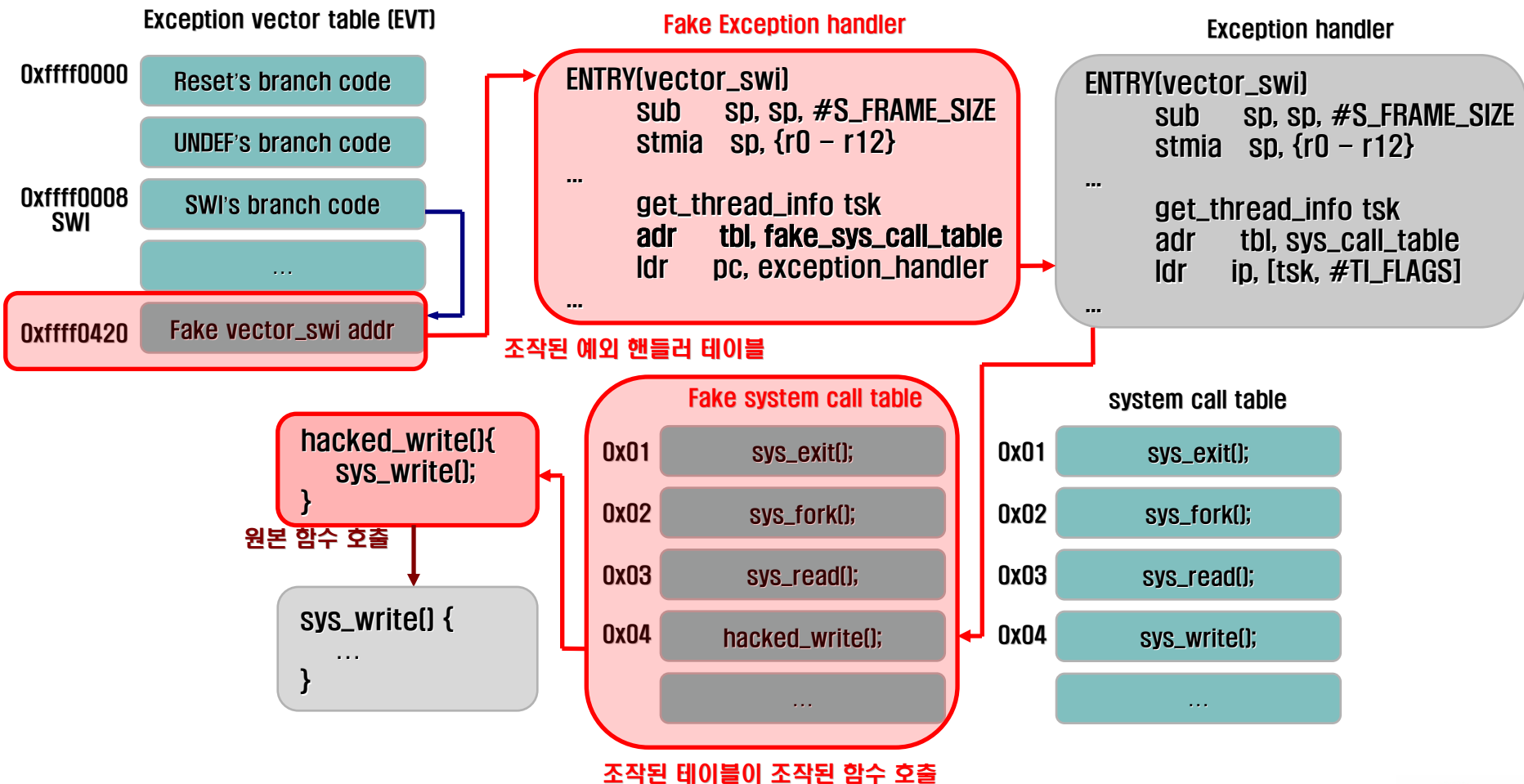
Android 플랫폼 커널 기반 악성코드 기술 #2



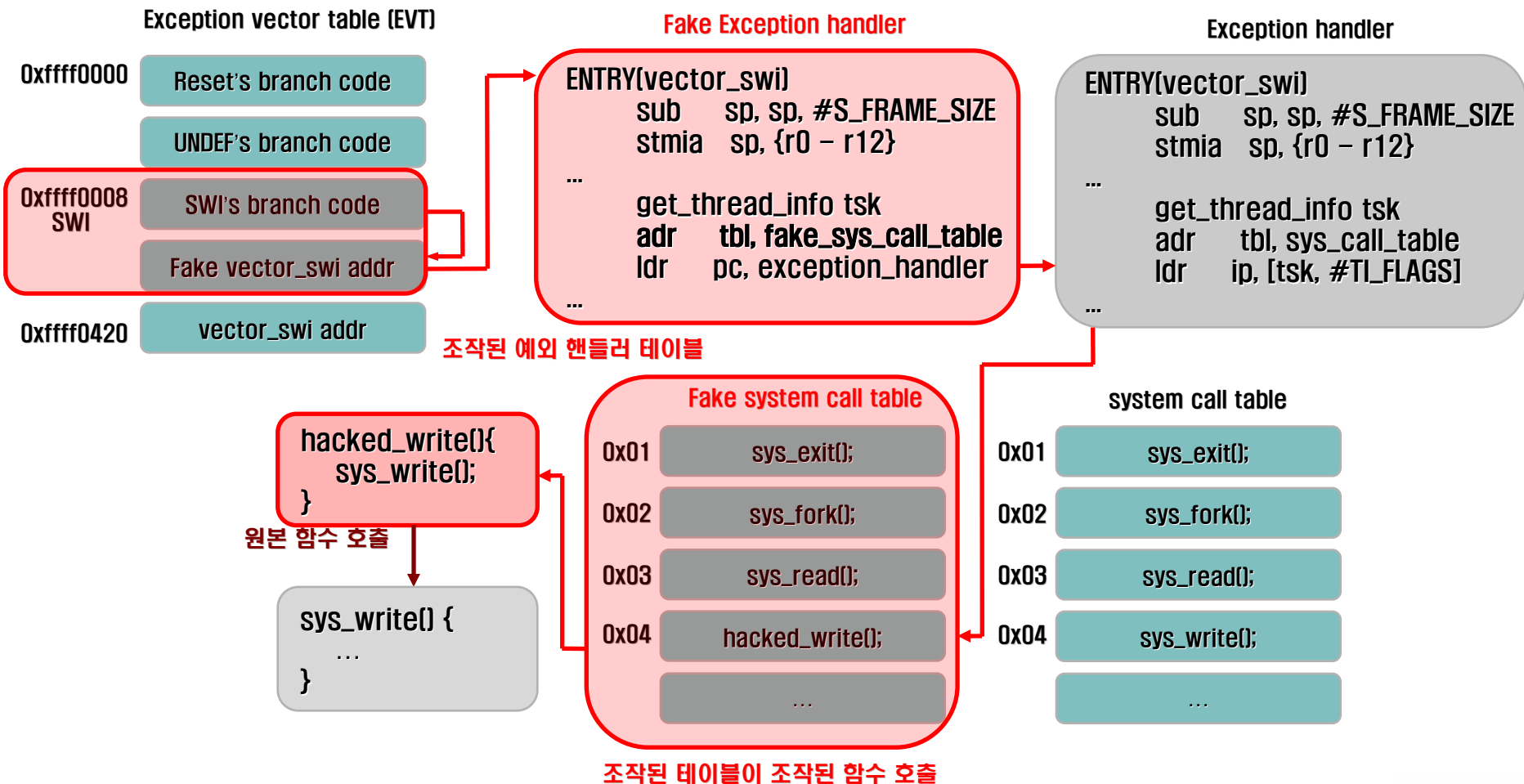
Android 플랫폼 커널 기반 악성코드 기술 #3



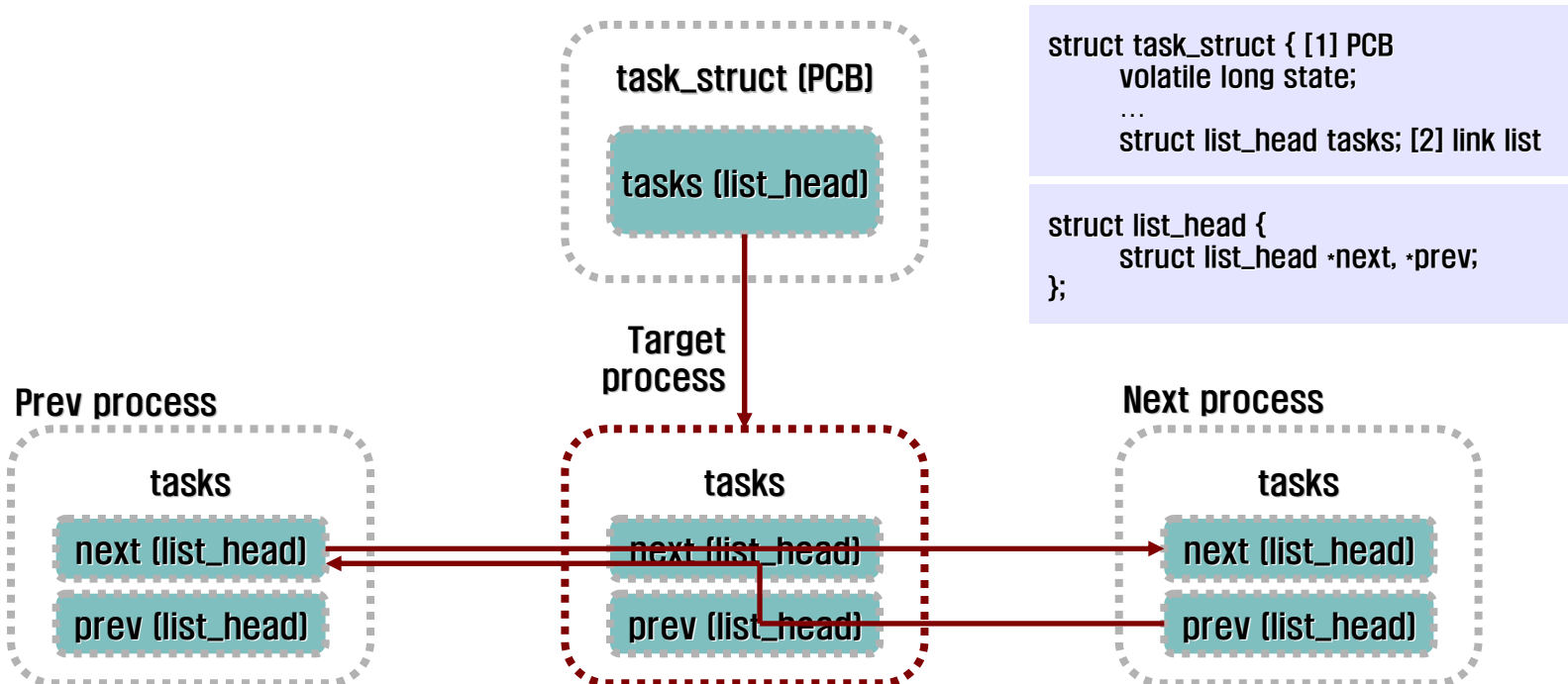
Android 플랫폼 커널 기반 악성코드 기술 #4



Android 플랫폼 커널 기반 악성코드 기술 #5



- Android 플랫폼 커널 기반 악성코드의 프로세스 은닉 원리
- Process hiding 원리
 - 실행 프로세스 정보가 담긴 PCB 구조체 내의 list_head 구조체 조작
 - 이전 프로세스 정보인 prev와 다음 프로세스 정보인 next를 병합



- Android 플랫폼 커널 기반 악성코드의 자원 정보 은닉 원리
- File & directory & Network status hiding 원리
 - EVT, vector_swi, sys_call_table 변경을 통한 시스템 콜 후킹 시도
 - getdents64 함수 후킹 후 dirent64 구조체 내의 객체 정보 제거
 - write, writev 함수 후킹 후 네트워크 자원 정보 조작 및 제거

```
hacked_getdents64(  
    unsigned int fd,  
    struct linux_dirent64 *dirp,  
    unsigned int count);
```

```
struct linux_dirent64 {  
    u64 d_ino;  
    s64 d_off;  
    unsigned short d_reclen;  
    unsigned char d_type;  
    char d_name[0];  
};
```

```
hacked_write(int fd,  
    struct iovec *vector,  
    int count);
```

```
struct iovec {  
    __ptr_t iov_base;  
    size_t iov_len;  
};
```

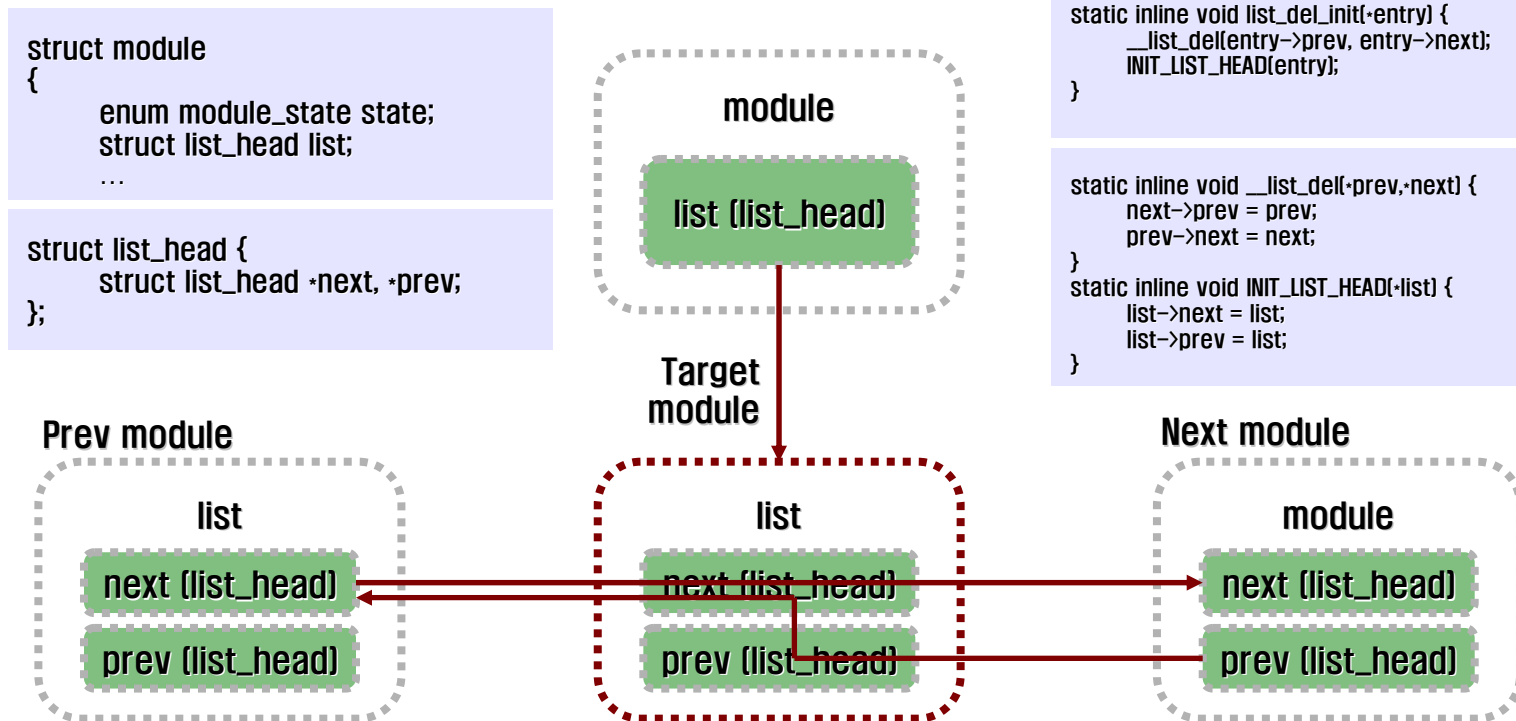
d_ino	d_off	d_reclen	d_type	d_name
6588...	271	16	4	net
6602...	272	16	4	kcore
7818...	273	16	4	18858
7020...	274	16	4	10054
...

엔트리 내에서 객체
정보 변조 및 제거

iov_base	iov_len
AAA BBB CCC DDD EEE	10
FFF GGG HHH	10

엔트리 내에서 객체
정보 변조 및 제거

- Android 플랫폼 커널 기반 악성코드의 모듈 정보 은닉 원리
- Kernel module driver hiding 원리
 - 로드된 모듈 정보가 담긴 module 구조체 내의 list_head 구조체 조작
 - 이전 모듈 구조체인 prev와 다음 모듈 구조체인 next를 병합



- Android 플랫폼을 위협하는 커널 기반 악성코드 종류 및 기능
 - 터치패드 입력 키 감시 (터치패드 인터럽트 후킹 방식)
 - 주요 전자금융 거래 내역 조작
 - 발전된 커널 기반 봇넷 (C&C 도구 및 커백션 채널 은닉)
 - Network 트래픽, 상태 정보 조작 및 은닉
 - 악성 코드 및 작업 디렉터리, 프로세스 은닉
 - 설치된 악성 커널 모듈 드라이버 은닉
 - 일반적인 커널 루트킷
 - 원격, 로컬 백도어 및 악성코드 정보 은닉

Smart Phone Malware

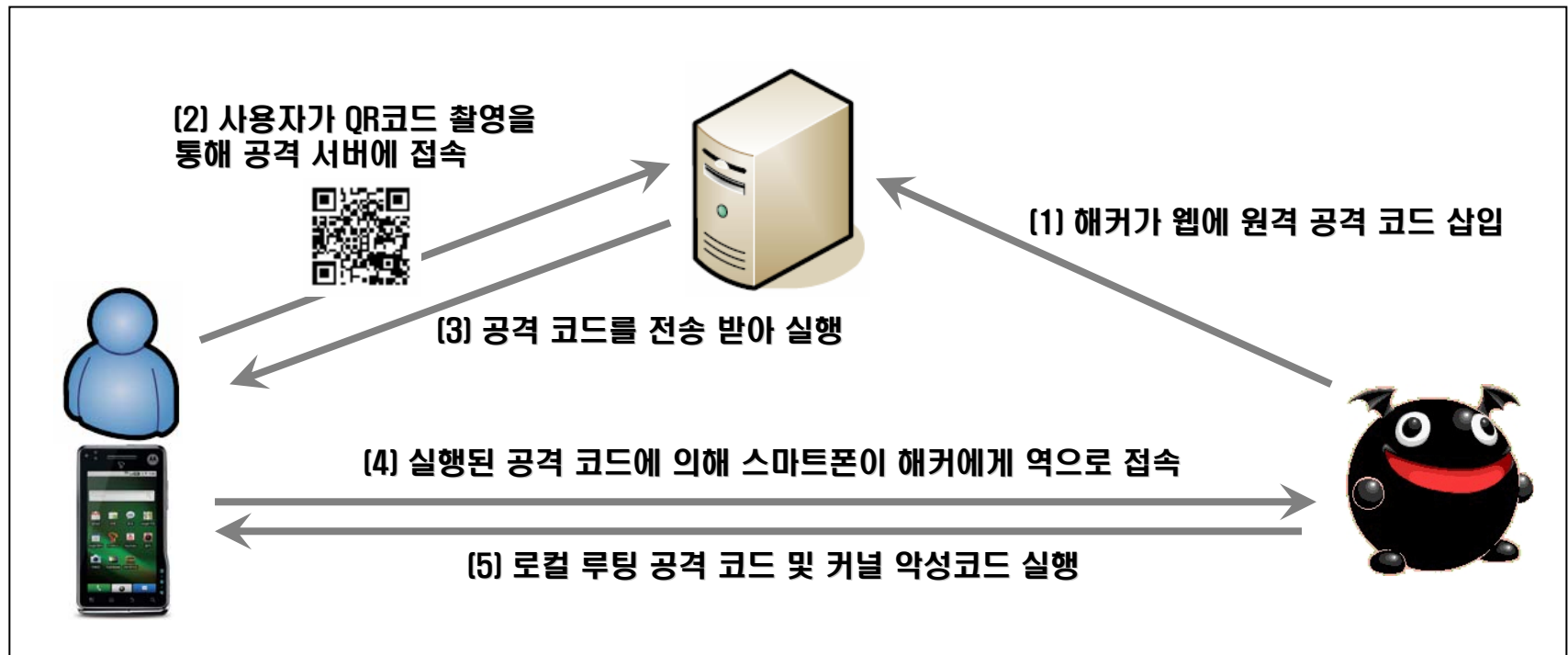
Android 커널 악성코드 시연

- **Android platform 커널 기반 악성코드 시연 환경**
 - 하드웨어: 모토로이 XT720, 운영체제 소프트웨어: Android 2.1 (Eclair)
Linux version 2.6.29-omap1 (w21679@zkr30mdb05) (gcc version 4.4.0 (GCC))
 - 하드웨어: 갤럭시 S, 갤럭시 탭, 운영체제 소프트웨어: Android 2.2 (Froyo)
Linux version 2.6.32.9 (root@SEI-27) (gcc version 4.4.1 (Sourcery G++ Lite 2009q3-67))
 - 하드웨어: 옵티머스 one, 운영체제 소프트웨어: Android 2.2 (Froyo)
Linux version 2.6.32.9 (mclab1@s-ibm06-desktop) (gcc version 4.4.0 (GCC))



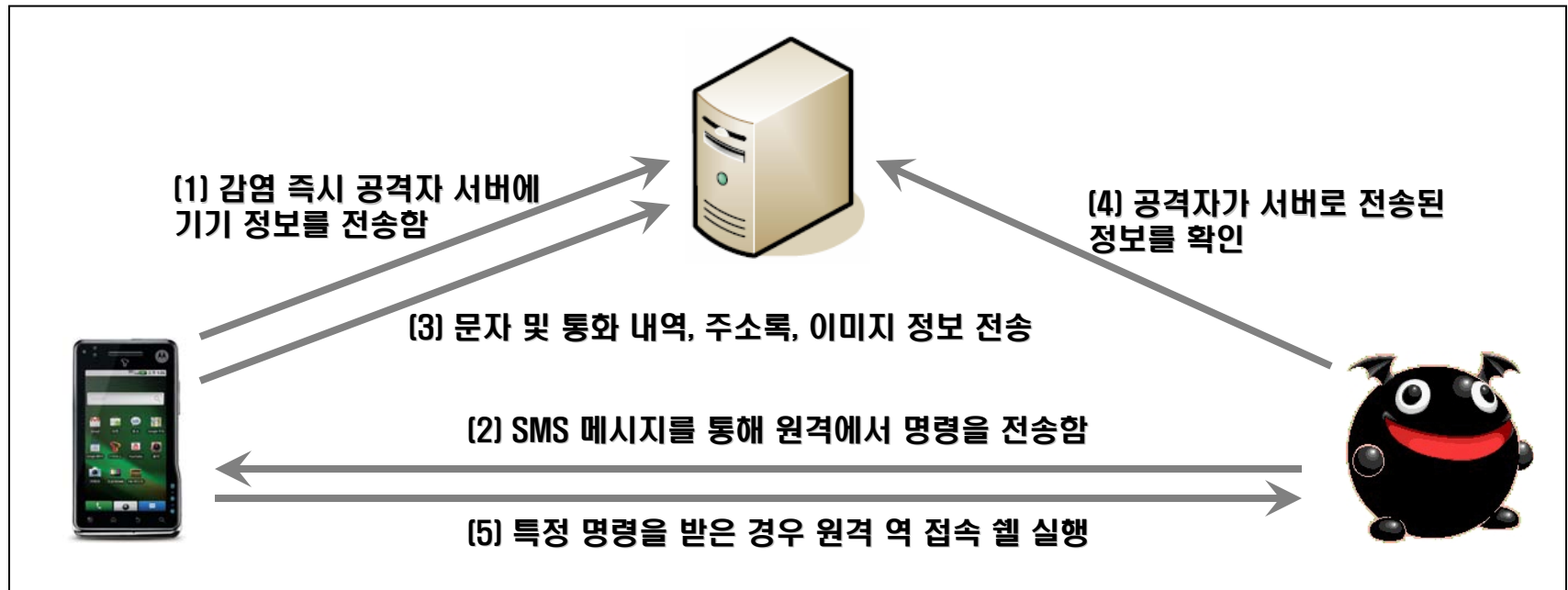
■ 원격 침입 및 로컬 루팅 공격 시연

- QR 코드를 통한 원격 셸 획득 및 로컬 rooting 시연
- Android remote webkit library use-after-free 취약점
- CVE-2009-3547 linux kernel local pipe 함수 rooting 취약점



■ 커널 기반 악성코드 공격 시연

- 커널 기반 악성코드 활성화 및 중요 정보 획득 시연
[기기 정보, 문자 및 통화 내역, 주소록, 이미지, GPS 정보 등]
- 파일 및 디렉터리, 프로세스, LKM 모듈 은닉 시연
- remote reverse shell connection 시연



Demonstration of Smart Phone Malware



Smart Phone Malware

Android 커널 악성코드 대응

- **Linux 서버용 커널 기반 악성코드 탐지 도구**
 - kstat, btrom, stmichael, carbonite (프로세스만 검사)
 - 커널 모듈 형태의 탐지 도구는 커널 버전에 의존적으로 동작하는 단점 존재
 - chkrootkit, rootcheck, rkhunter
 - 사용자 어플리케이션 형태의 탐지 도구는 정확한 탐지가 불가능한 단점 존재

- **Android 플랫폼용 커널 기반 악성코드 탐지 도구**
 - Coelacanth core (x86/arm)
 - 펌웨어, 부트섹터, 주요 커널 구조체, 메모리 무결성 검사
 - EVT, vector_swi, sys_call_table, 주요 커널 함수 변조 검사
 - 숨겨진 프로세스, 디렉터리, 파일 분석
 - 숨겨진 네트워크 상태 정보 분석
 - 숨겨진 커널 모듈 드라이버 분석

- **스마트 플랫폼 커널 기반 악성코드 대응 결론**
 - App 보안성 검증 대책 마련
 - OS 커널에 은닉된 악성 코드까지 탐지할 수 있는 백신 필요
 - 취약점 악용을 최소화하기 위한 OS 차원의 보안 업데이트 체계 구현
 - 스마트 플랫폼 보호를 위한 보안 솔루션 도입
 - 근본적인 스마트 플랫폼(sandbox & OS) 통합 보안 정책 필요

Q & A



참고 자료

■ 참고 자료

- [http://en.wikipedia.org/wiki/Android_\(operating_system\)](http://en.wikipedia.org/wiki/Android_(operating_system))
- <http://www.exploit-db.com>
- Linux Kernel 2.x sock_sendpage() Local Root Exploit (Android Edition)
- CVE-2009-2692: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2692>
- CVE-2010-1807: <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1807>
- Security Threats for Smart Phone Users: <http://www.youtube.com/watch?v=UZgf32wVTd4>
- <http://hakim.ws/DEFCON18/Trustwave-Spiderlabs/DEFCON-18-Trustwave-Spiderlabs-Android-Rootkit.pdf>
- Android Anti-Rootkit – INetCop Security
- [Phrack] Android platform based linux kernel rootkit – INetCop Security
- [Usenix-WOOT] Android platform based linux kernel rootkit – INetCop Security

Thank you !



By "dong-hoon yoU" (Xpl017Elz), in INetCop(c).
MSN & E-mail: szoahc(at)hotmail(dot)com
Home: <http://x82.inetcop.org>