



Smart Sheriff,

Smart Sheriff, Dumb Idea



Smart Sheriff, Dumb Idea

The wild west of government assisted parenting

presented by:

Abraham Aranguren - @7a_

Fabian Fäßler - @samuirai



A story about a Korean law...

- Some background information
- Case MOIBA: Smart Sheriff, Smart Dream
- Case mobile operators: KT, LGU, +SKT
- What now?

„In the end we hope you share our disbelief“

Takeaways from this talk

- Insight into South Korean culture and politics
- Some basics in Android reversing
- Difficulties with the ethics of disclosing issues

Who are we?



CURE53

Abraham Aranguren (@7a_) - blog.7-a.org

OWASP OWTF Project leader - owtf.org

abraham@cure53.de

Fabian Fäßler (@samuirai) - smrrd.de

fabian@cure53.de

Cure53 is led by handsome Mario Heiderich (@0x6D6172696F).

Bullshit free pentests, sometimes public 😊

<https://cure53.de/#publications>

Why did we do this?

OpenNet Korea brought this to Citizen Lab

<http://opennetkorea.org/>

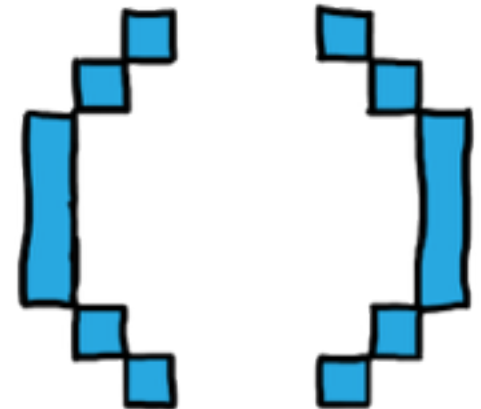
Citizen Lab, Toronto

"Citizen Lab Summer Institute on Monitoring Internet Openness and Rights 2015"

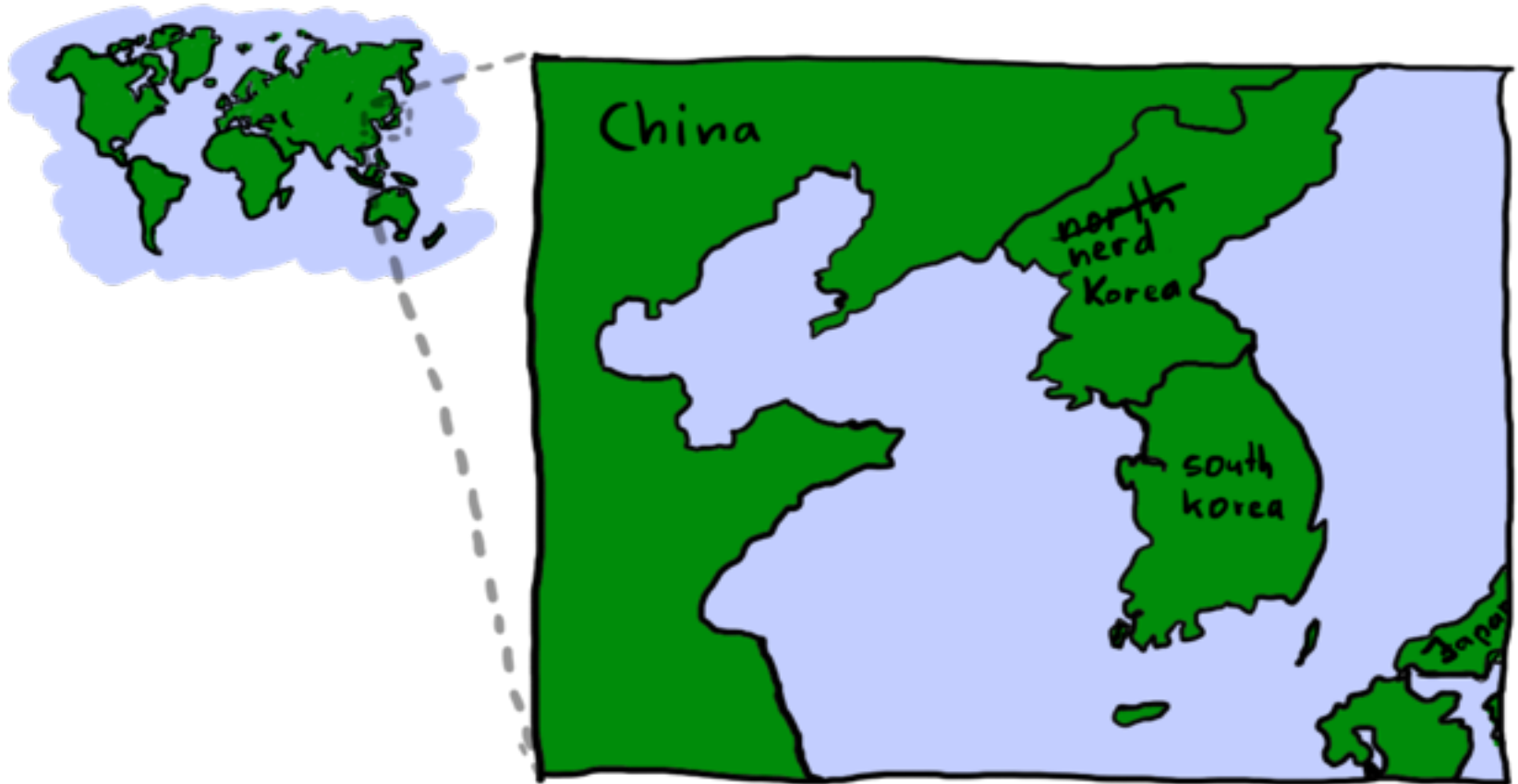
<http://citizenlab.org/>

Open Technology Fund supported it

<https://www.opentech.fund/>



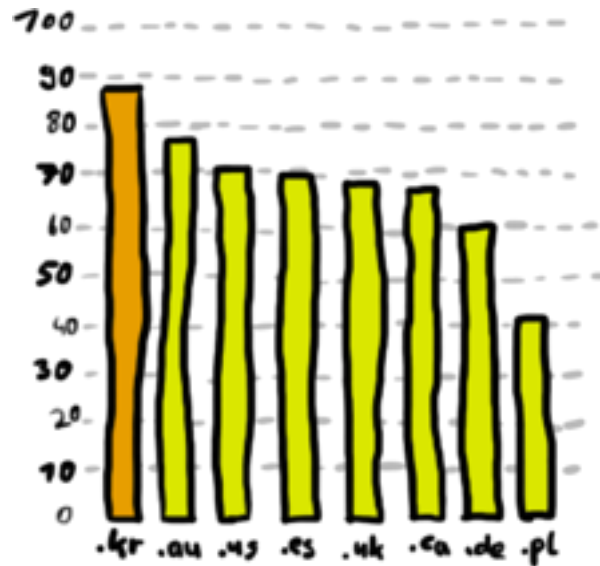
Once upon a time...



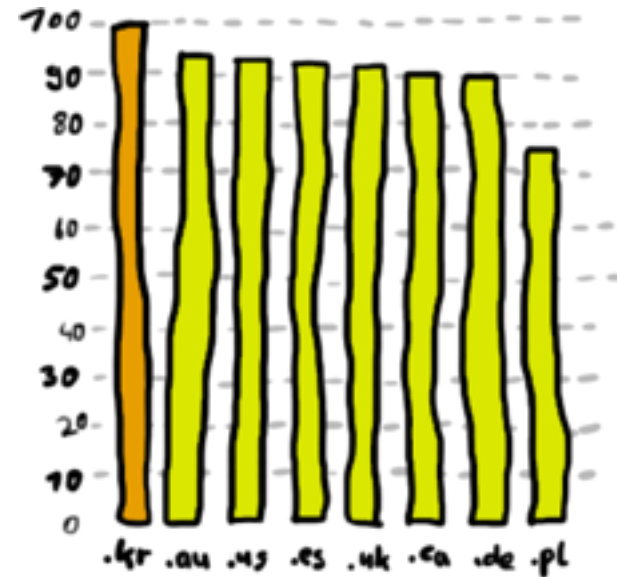
... in a country far far away.

South Korea – Smartphone Usage

% Total population



% 18-34 y/o population



... the country with the highest Smartphone usage on the planet!

South Korea – Child Protection Laws

Article 32, Section 7 of Korean Telecommunications Business Act

mobile network operators have to provide adult content filtering service for legal minors

Introduced 15.10.2014

...

South Korea – Child Protection Laws

Article 32, Section 7 of Korean Telecommunications Business Act

mobile network operators have to provide adult content filtering service for legal minors

Introduced 15.10.2014

...

Implementation Details Article 37, Section 8

Notify children and parents about features of the blocking
Monthly notification if the blocking means was deleted or had not been operated for more than 15 days

...

Introduced 14.04.2015

South Korea – Mandatory apps

Mandatory installation of a surveillance app when the phone is purchased for a teenager.



South Korea – Mandatory apps

Mandatory installation of a surveillance app when the phone is purchased for a teenager.

No opt-out.



South Korea – Mandatory apps

since May contractually obliged to provide means for blocking

apps have to be installed on juveniles' phones

alert after 15 days

“청소년 휴대폰”
유해물 차단 앱을 설치해야
이용할 수 있습니다

차단수단 제공자(KT, SK, LGU+)를 통해 청소년 및 법정대리인에게 안내

차단수단이 삭제되거나 15일 이상 작동하지 않을 경우 매월 법정대리인에게 고지

차단수단 선택 및 설치여부를 확인

한빛통신 SK Telecom kt LGU+ KAIT

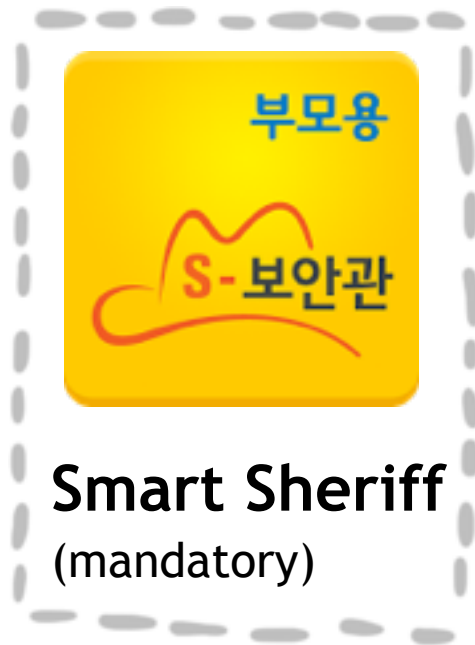
Mobile Internet Business Association (MOIBA)

The Korean Communications Commission (KCC) gave MOIBA **USD \$2.7 million** to create these mandatory apps



MOIBA - Smart Sheriff / Smart Dream

MOIBA created 2 mobile apps



Alternative Korean Child Protection Apps

- **KT Corporation:** <https://play.google.com/store/apps/details?id=com.kt.ollehkidsafe>



올레 자녀폰안심 프리

KT Corporation 라이프스타일

★★★★★ 2,050 호

USK: 전체이용가

기기가 없습니다.

위시리스트에 추가

설치

- **SKTelecom:** <https://play.google.com/store/apps/details?id=com.skt.thug.hazard>



T청소년유해차단

SKTelecom 라이프스타일

★★★★★ 173 호

USK: 전체이용가

기기가 없습니다.

위시리스트에 추가

설치

- **LG U+:** <https://play.google.com/store/apps/details?id=com.lguplus.cleanmobile>



U+ 자녀폰 지킴이

LG유플러스(LG Uplus Corporation) 라이프스타일

★★★★★ 501 호

USK: 전체이용가

기기 호환성 로드 중...

위시리스트에 추가

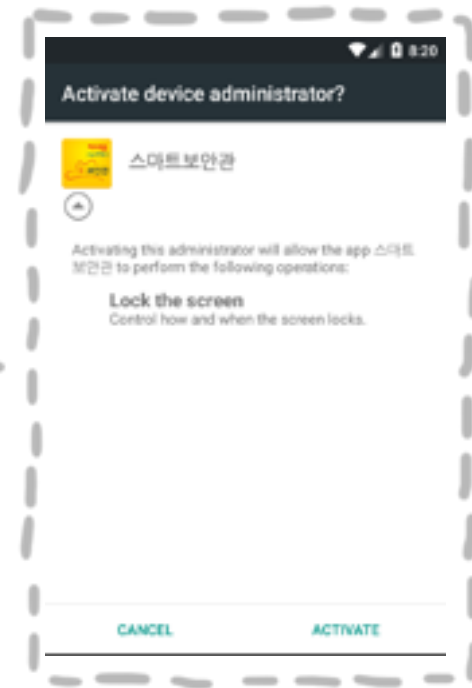
설치

Smart Sheriff: Parent vs. Child mode

- Operating mode chosen on first usage
- **Parent-Mode:** Smartphone usage management
- **Child-Mode:** For filtering and activity monitoring



Parent



Child

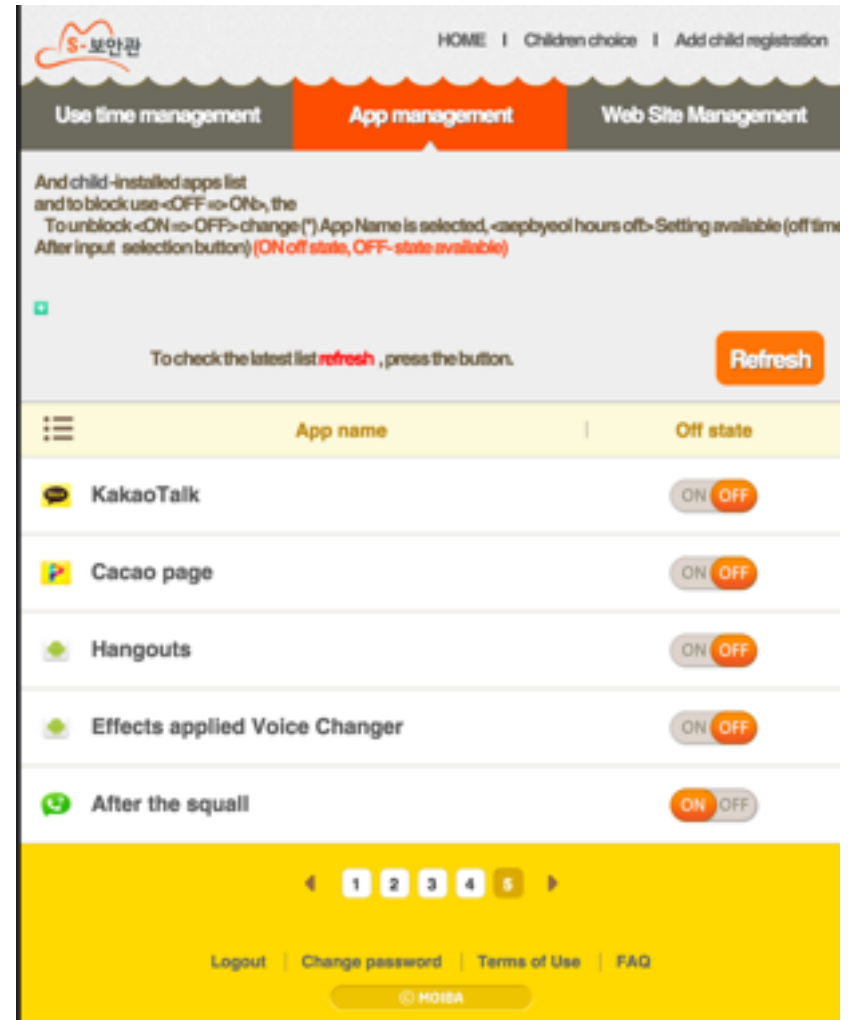
Smart Sheriff: Block phone access



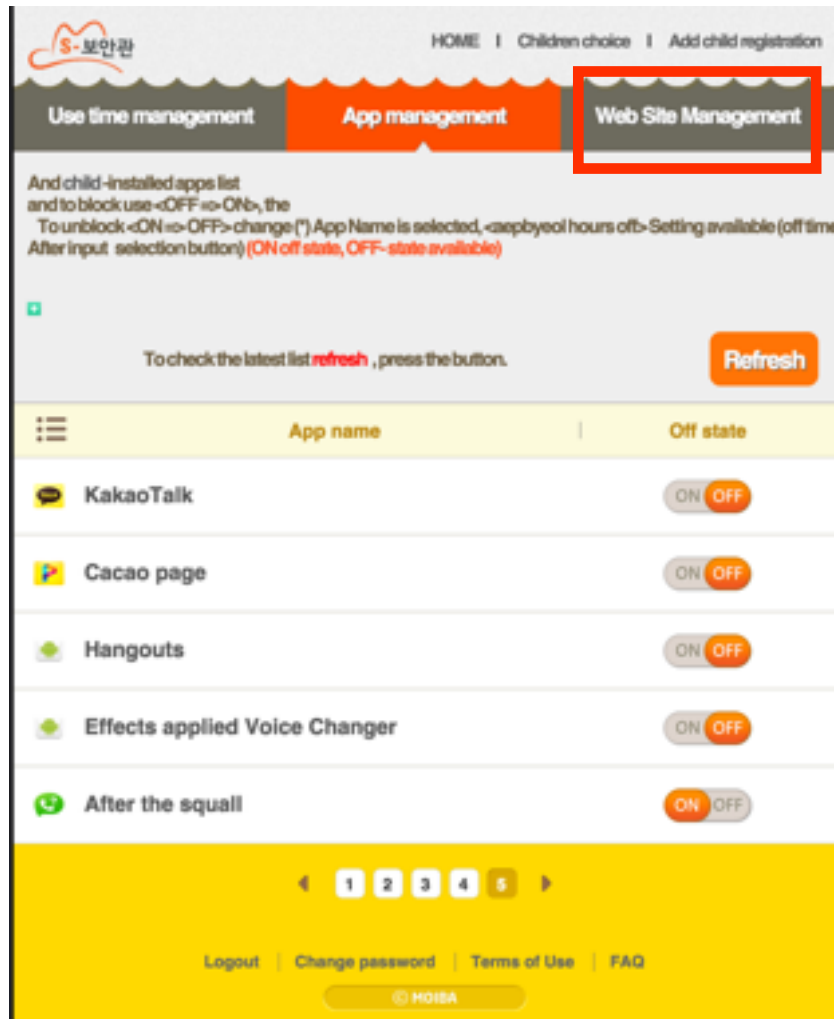
Parents can **deny phone access** for certain times for the child

Smart Sheriff: Installed apps

See installed apps on child's phone and deny or enable access to them.



Smart Sheriff: Websites



Manage/Block access to websites.

Implemented in the app, but not usable by parent.

Sensitive Data – Smart Sheriff (+others)

- Family Association (Parent - Child)
- Children's names, birthdays
- Installed apps and usage statistics
(time browsing or playing games)
- Visited/Blocked URLs

Smart Dream

- Private SMS and KakaoTalk messages (!)



Round 1 – Setup Challenges



Language Barrier

홍보안전관 HOME | 자네소개 | 자녀유기등록

 **010-XXXX-XXXX**

(*) 위 이용현황은 조회하신 기간 동안의 자녀가 이용한 평균 이용통계 정보입니다.

 **이용현황**

2015-06-01 ~ 2015-06-30 **조회**

일평균 이용시간	3시간 46.8분
주 이용 시간대 (앱+인터넷)	18시~24시 (2시간)
정보이용비중	앱(98.94%), 인터넷(1.06%)
정보별 주 이용시간대/ 카테고리	앱 : 18시~24시 (소셜콘텐츠) 사이트 : 18시~24시
앱 카테고리별 이용시간	소셜콘텐츠 (1시간 59.4분) 게임 (1시간 4.2분) 동영상 (31.2분) 커뮤니케이션 (4.8분) 엔터테인먼트 (3.6분)
주 이용 요일	월 (7시간 15.0분), 화 (5시간 22.2분)

앱 카테고리 유량보기

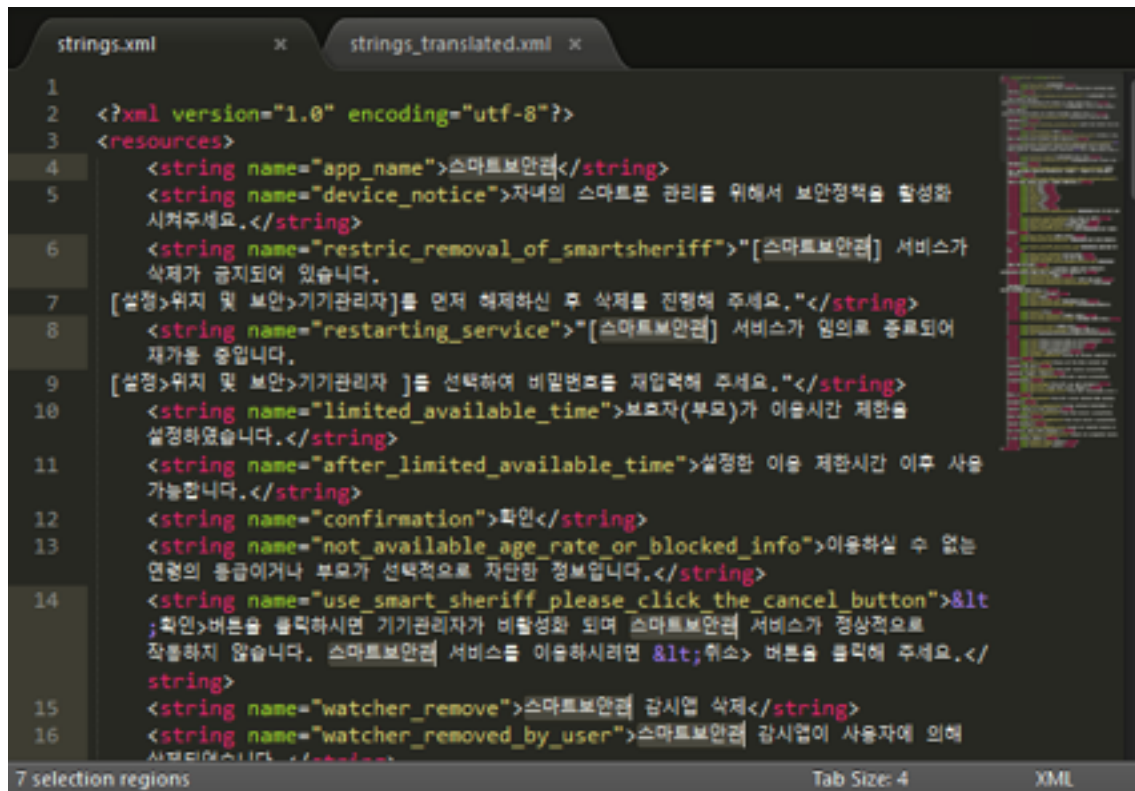
스마트 보안관 버전이 낮을 경우 데이터가 정상적으로 보이지 않을 수 있습니다.

스마트보안관은 청소년유해정보를 차단하고, 이용시간관리로 스마트폰 사용을 제한할 수 있습니다.

로그아웃 | 비밀번호 변경 | 이용약관 | FAQ

WTF DOES THIS?

Language Barrier



```
1
2 <?xml version="1.0" encoding="utf-8"?>
3 <resources>
4     <string name="app_name">스마트보안관</string>
5     <string name="device_notice">자녀의 스마트폰 관리를 위해서 보안정책을 활성화
        시켜주세요.</string>
6     <string name="restric_removal_of_smartsheriff">"[스마트보안관] 서비스가
        삭제가 금지되어 있습니다.
7     [설정>위치 및 보안>기기관리자]를 먼저 해제하신 후 삭제를 진행해 주세요."</string>
8     <string name="restarting_service">"[스마트보안관] 서비스가 임의로 종료되어
        재가를 중입니다.
9     [설정>위치 및 보안>기기관리자]를 선택하여 비밀번호를 재입력해 주세요."</string>
10    <string name="limited_available_time">보표자(부모)가 이용시간 제한을
        설정하였습니다.</string>
11    <string name="after_limited_available_time">설정한 이용 제한시간 이후 사용
        가능합니다.</string>
12    <string name="confirmation">확인</string>
13    <string name="not_available_age_rate_or_blocked_info">이용하실 수 없는
        연령의 통급이거나 부모가 선택적으로 차단한 정보입니다.</string>
14    <string name="use_smart_sheriff_please_click_the_cancel_button">&lt;
        ; 확인>버튼을 클릭하시면 기기관리자가 비활성화 되어 스마트보안관 서비스가 정상적으로
        작동하지 않습니다. 스마트보안관 서비스를 이용하시려면 &lt;취소> 버튼을 클릭해 주세요.</
        string>
15    <string name="watcher_remove">스마트보안관 감시업 삭제</string>
16    <string name="watcher_removed_by_user">스마트보안관 감시업이 사용자에 의해
        삭제되었습니다.</string>
```

unpack, translate,
repack with apktool

Language Barrier

unpack, translate,
repack with apktool

```
1 <?xml version="1.0" encoding="utf-8"?>
2 <resources>
3
4     <string name="app_name">스마트보안관</string>
5     <string name="device_notice">자녀의 스마트폰 관리를 위해서 보안정책을 활성화
6     시켜주세요.</string>
7     <string name="restric_removal_of_smartsheriff">
8     삭제가 금지되어 있습니다.
9     [설정>위치 및 보안>기기관리자]를 먼저 해제하신 후 삭제
10    <string name="restarting_service">[스마트
11    재가동 중입니다.
12    [설정>위치 및 보안>기기관리자]를 선택하여 비밀번호를 지
13    <string name="limited_available_time">보
14    설정하였습니다.</string>
15    <string name="after_limited_available_t">
16    가능합니다.</string>
17    <string name="confirmation">확인</string>
18    <string name="not_available_age_rate_or_blocked_info">
19    연령의 등급이거나 부모가 선택적으로 차단한 정보입니다
20    <string name="use_smart_sheriff_please">
21    ; 확인>버튼을 클릭하시면 기기관리자가 비활성화 되며
22    작동하지 않습니다. 스마트보안관 서비스를 이용하시려면
23    <string>
24    <string name="watcher_remove">스마트보안관
25    <string name="watcher_removed_by_user">
26    삭제되었습니다.</string>
27
```

7 selection regions

```
1 <?xml version="1.0" encoding="utf-8"?>
2 <resources>
3
4     <string name="app_name">smart sheriff</string>
5     <string name="device_notice">Please activate security policies to
6     manage your child's smartphone.</string>
7     <string name="restric_removal_of_smartsheriff">[Smart sheriff's]
8     service is deleted is forbidden. Settings> Location and Security>
9     Device Manager first, and then you release, please proceed to
10    delete.</string>
11    <string name="restarting_service">[smart sheriff] The restart of
12    the service is arbitrarily shut down. Select Settings> Location
13    and Security> Device Manager] Please re-enter your password.</
14    string>
15    <string name="limited_available_time">Guardians (parents) have
16    been set up limited hours.</string>
17    <string name="after_limited_available_time">Available since used
18    the time limit set.</string>
19    <string name="confirmation">confirm</string>
20    <string name="not_available_age_rate_or_blocked_info">Rating not
21    available in the information age, a parent or selectively blocking.
22    </string>
23    <string name="use_smart_sheriff_please_click_the_cancel_button">&lt;
24    ;If OK> button if you disable the device administrator smart
25    sheriff service is not working properly. To use smart sheriff
26    service &lt; Please click the Cancel> button.</string>
27    <string name="watcher_remove">Smart sheriff's
28    <string name="watcher_removed_by_user">
29
```

10 selection regions Spaces: 4 XML

Language Barrier

HOME | Children choice | Add child registration

010- [REDACTED]

[*] 위 이용현황은 조회하신 기간 동안의 자녀 이용현황입니다. (Statistical information for the period of your child with your inquiry.)

이용현황

2015-06-01 ~ 2015-06-30 [Lookup]

일평균 이용시간	3 hours 46.8 minutes
주 이용 시간대 (앱+인터넷)	18:00 o'clock to 24 (2 hours)
정보이용비중	앱(98.94%), Internet (1.06%).
정보별 주 이용시간대/ 카테고리	Apps: 18 am to 24 pm (Social) Sites: 18:00 to 24 o'clock
앱 카테고리별 이용시간	Social (1 hour 59.4 minutes) Video (31.2 minutes) Communication (4.8 minutes) Entertainment (3.6 minutes)
주 이용 요일	Monday (7:00 minutes), Tuesday (5 hours 12.2 minutes)

앱 카테고리 유형보기

스마트 보안관 버전이 낮을 경우 데이터가 정상적으로 보이지 않을 수 있습니다.

스마트보안관은 실시간 데이터를 제공하고, 이용시간관리로 다양한 통계를 제공할 수 있습니다.

로그아웃 | 비밀번호 변경 | 이용약관 | FAQ

Unfortunately ...

strings.xml is not enough for a app because WebViews

Language Barrier ... Google Translate

Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts

Intercept History Options

Filter: Showing all items

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	ES
14	https://211.253.14.71	GET	/js/com/util_ver1_2.js			200	44621	script	js
15	https://211.253.14.71	POST	/main/login			200	11056		
16	https://211.253.14.71	GET	/images/tit_userchoice.png			200	8875	PNG	png
17	https://211.253.14.71	GET	/css/reset.css			200	8187	CSS	css
18	https://211.253.14.71	POST	/main/login			200	11057		
19	https://211.253.14.71	GET	/images/bg_toproof.png			200	7005	PNG	png
20	https://211.253.14.71	GET	/images/bg_dotline_01.png			200	10833	PNG	png
21	https://211.253.14.71	GET	/images/bg_rybox.png			200	38315	PNG	png
22	https://211.253.14.71	GET	/images/bg_rybox_top.png			200	5167	PNG	png
23	https://211.253.14.71	GET	/images/icon_lock.png			200	1826	PNG	png
24	https://211.253.14.71	GET	/images/ic_lockscreen_emergency...			200	2897	PNG	png
25	https://211.253.14.71	GET	/images/footer_moiBa.png			200	4099	PNG	png
26	https://211.253.14.71	GET	/images/ic_lockscreen_forgotpass...			200	2272	PNG	png

Request Response

Raw Headers Hex

```
</tbody>
</table>
</dd>
</dl>
<p class="btncenter" style="margin-top:30px">
  <button type="button" id="login_bt" name="login_bt"
class="btn_orqbox" onclick="javascript:fn_login();" style="width:96.5%;
margin-right:0%;>로그인</button>
  <br><br>
  <button type="button" id="useStatus_bt" name="useStatus_bt"
class="btn_graybox" onclick="javascript:window.location='http://m.iapc.or.kr/iapc/iapcMain.mdo';">스마트폰 중독
진단</button>
  <button type="button" id="useStatus_bt" name="useStatus_bt"
class="btn_graybox" onclick="javascript:fn_restCenter();">스마트폰센터</button>
</p>
<dl class="ccenter" style="margin-top:10px">
  <dt>※ 비밀번호를 잊으셨나요? <a href="javascript:void(0);">비밀번호찾기</a></dt>
  <dt>※ 비밀번호를 잊으셨나요? <a href="javascript:void(0);">비밀번호찾기</a></dt>
</dl>
<br>
<div id="divCont" name="divCont"></div>
```

Type a search term 0 matches

HOME | Children choice | Add child registration

statistical information for the period of your child with your inquiry.

2015-06-30

Lookup

3 hours 48.8 minutes

18:00 o'clock to 24 (2 hours)

Apps (98.94%), Internet (1.06%).

Apps: 18 am to 24 pm (Social)
Sites: 18:00 to 24 o'clock

ocial (1 hour 59.4 minutes)
me (1 hour 4.2 minutes)
ideo (31.2 minutes)
unication (4.8 minutes)
inment (3.6 minutes)
0 minutes), Tuesday (5 hours
2.2 minutes)

Debugging

Patching debug messages in smali code for logging

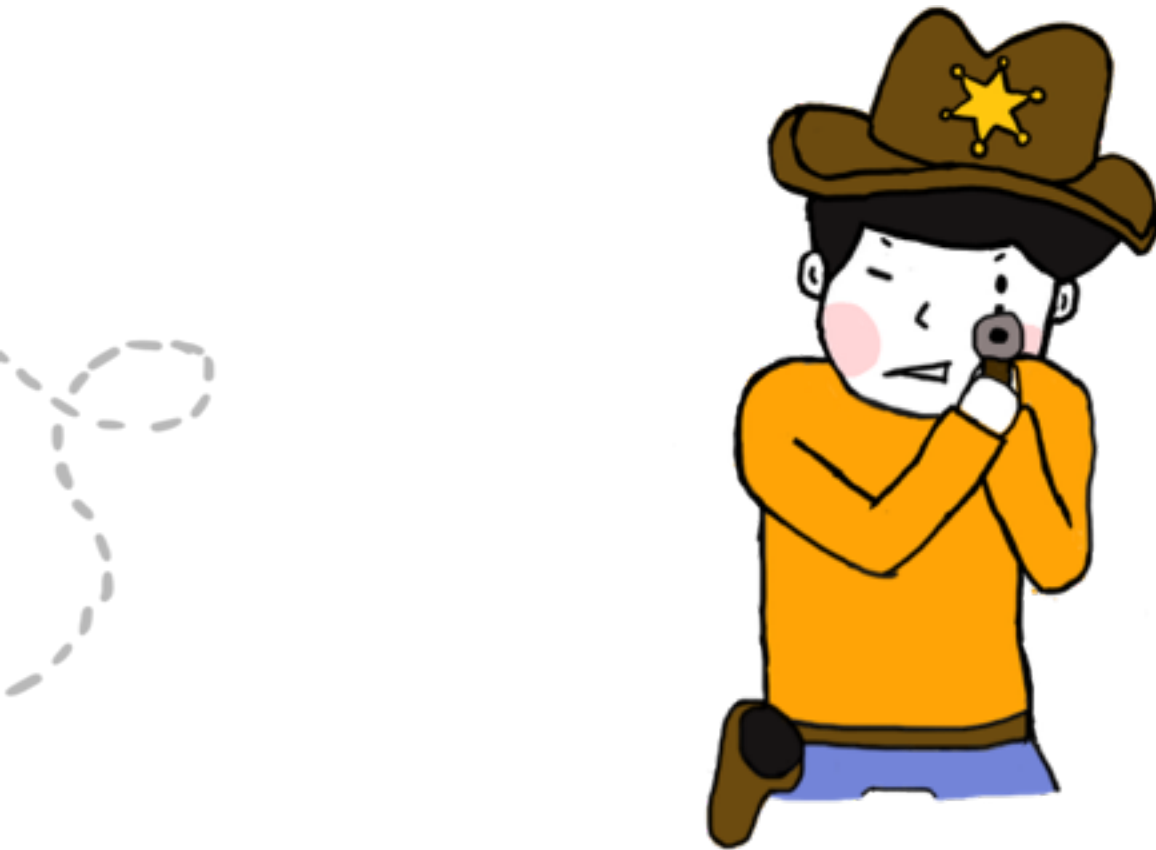
```
move-result-object v0  
const-string v1, "SAMU"  
invoke-static {v1, v0}, Landroid/util/Log;->i(Ljava/lang/String;Ljava/lang/String;)I
```

smali

java

```
private static final String TAG = "SAMU";  
Log.i(TAG, result);
```

Round 1 – Shoot



RCE with insecure WebView

Accessing Java methods from JavaScript in Android 2.4 to 4.1

```
String url = "http://ssweb.moiba.or.kr/pushAlarm";  
WebView webview = (WebView)findViewById(0x7f070000);  
webview.getSettings().setJavaScriptEnabled(true);  
webview.addJavascriptInterface(new JavaScriptInterface(),  
    "SmartSheriff");  
webview.postUrl(url, obj);
```

java
javascript

```
var String = window.jsinterface.getSomeString();  
// window.jsinterface.getClass().forName('java.lang.Runtime')
```

What is SSL?

```
String url = "http://ssweb.moiba.or.kr/pushAlarm";  
WebView webview = (WebView)findViewById(0x7f070000);  
webview.getSettings().setJavaScriptEnabled(true);  
webview.addJavascriptInterface(new JavaScriptInterface(),  
    "SmartSheriff");  
webview.postUrl(url, obj);
```


What is SSL?



```
String url = "http://ssweb.moiba.or.kr/pushAlarm";  
WebView webview = (WebView)findViewById(0x7f070000);  
webview.getSettings().setJavaScriptEnabled(true);  
webview.addJavascriptInterface(new JavaScriptInterface(),  
    "SmartSheriff");  
webview.postUrl(url, obj);
```



Fast forward to the fix...

Smart Sheriff – SSL v2.0

Smart Sheriff – How to SSL like a pro

SMS-01-003 No use of any SSL/TLS-based transport security **FIXED?**

https: //api.moiba.or.kr/MessageRequest_New



They switched to SSL for real O.o ?

Smart Sheriff – How to ~~SSL~~ like a pro

```
public final void onReceivedSslError(WebView  
paramWebView, SslErrorHandler paramSslErrorHandler,  
SslError paramSslError)  
{  
    paramSslErrorHandler.proceed();  
}
```

```
implements HostnameVerifier {  
    public final boolean verify(String paramString,  
SSLSession paramSSLSession)  
    {  
        return true;  
    }  
}
```

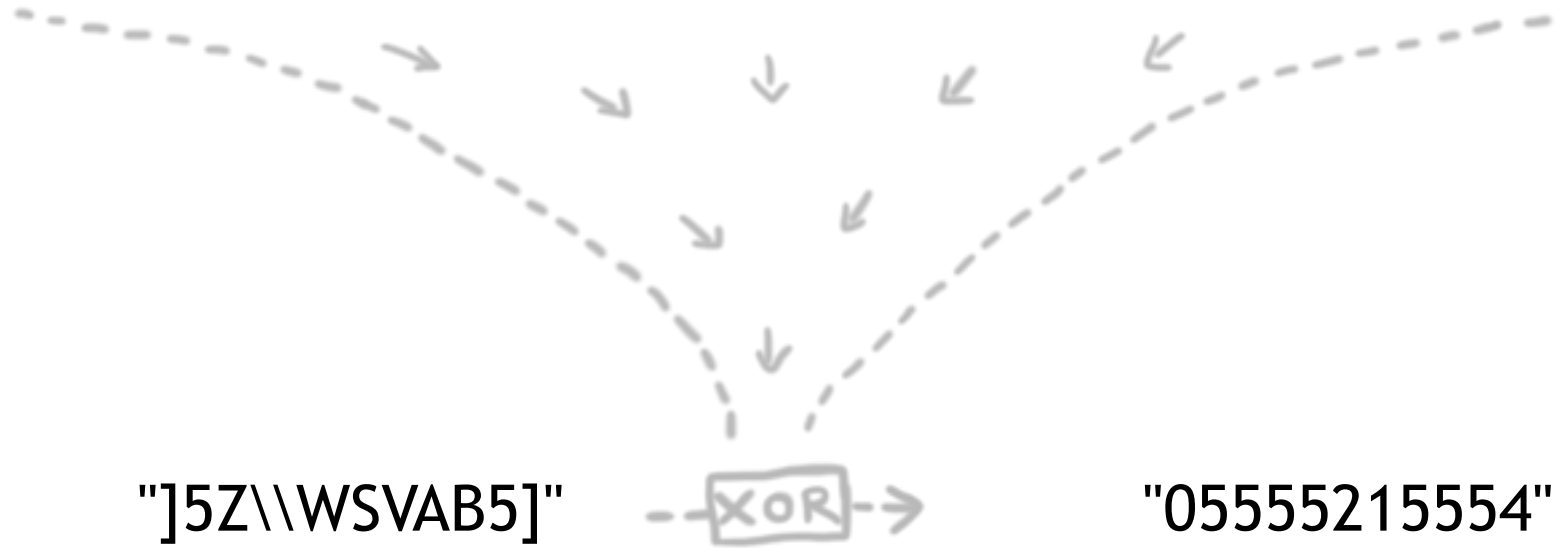
moibagtwigssystemsfightinghhhkkkkkok

- But SSL is not necessary, when you do your own crypto Layer...

"]5Z\\WSVAB5]"  "05555215554"



moibagtwigssystemsfightinghhhkkkkok



XOR Key: m\x00oibagtw\x00igsyste\x00msfight\x00inghhhk\x00kkkok



Fast forward to the fixes...

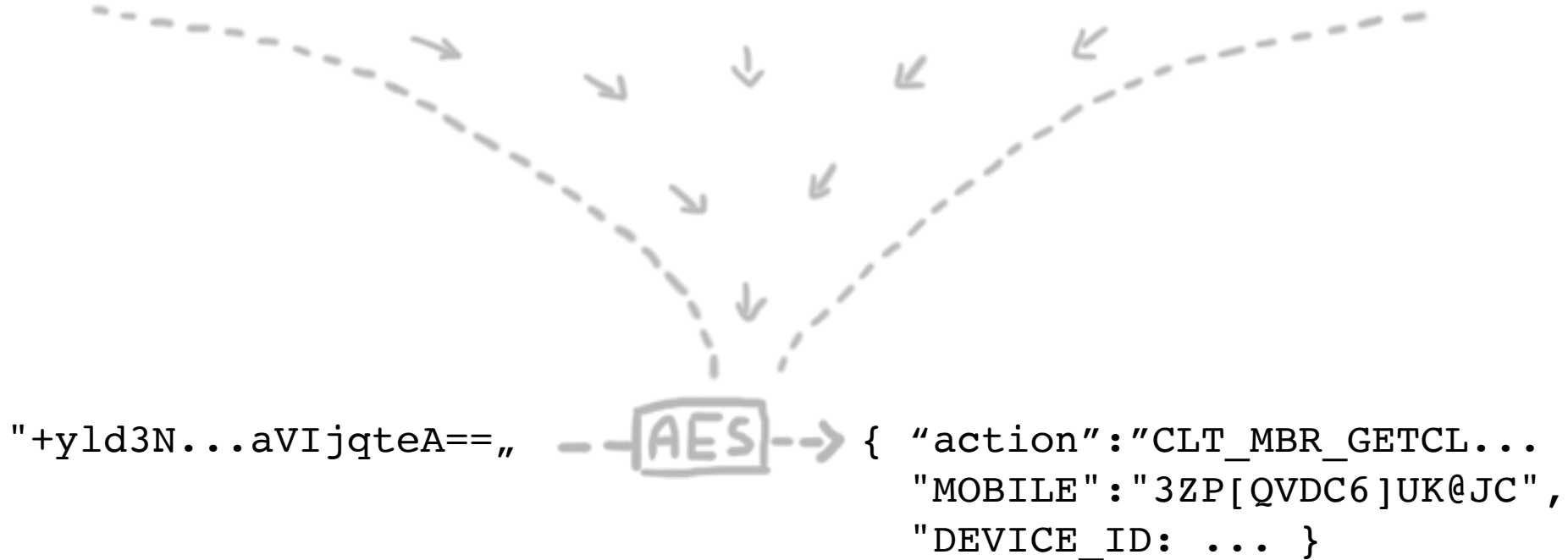
Smart Sheriff – Crypto v2.0

moiba1cybar8smart4sheriff4securi

"+yld3N...aVIjqteA==," --  { "action": "CLT_MBR_GETCL...",
"MOBILE": "3ZP[QVDC6]UK@JC",
"DEVICE_ID": ... }

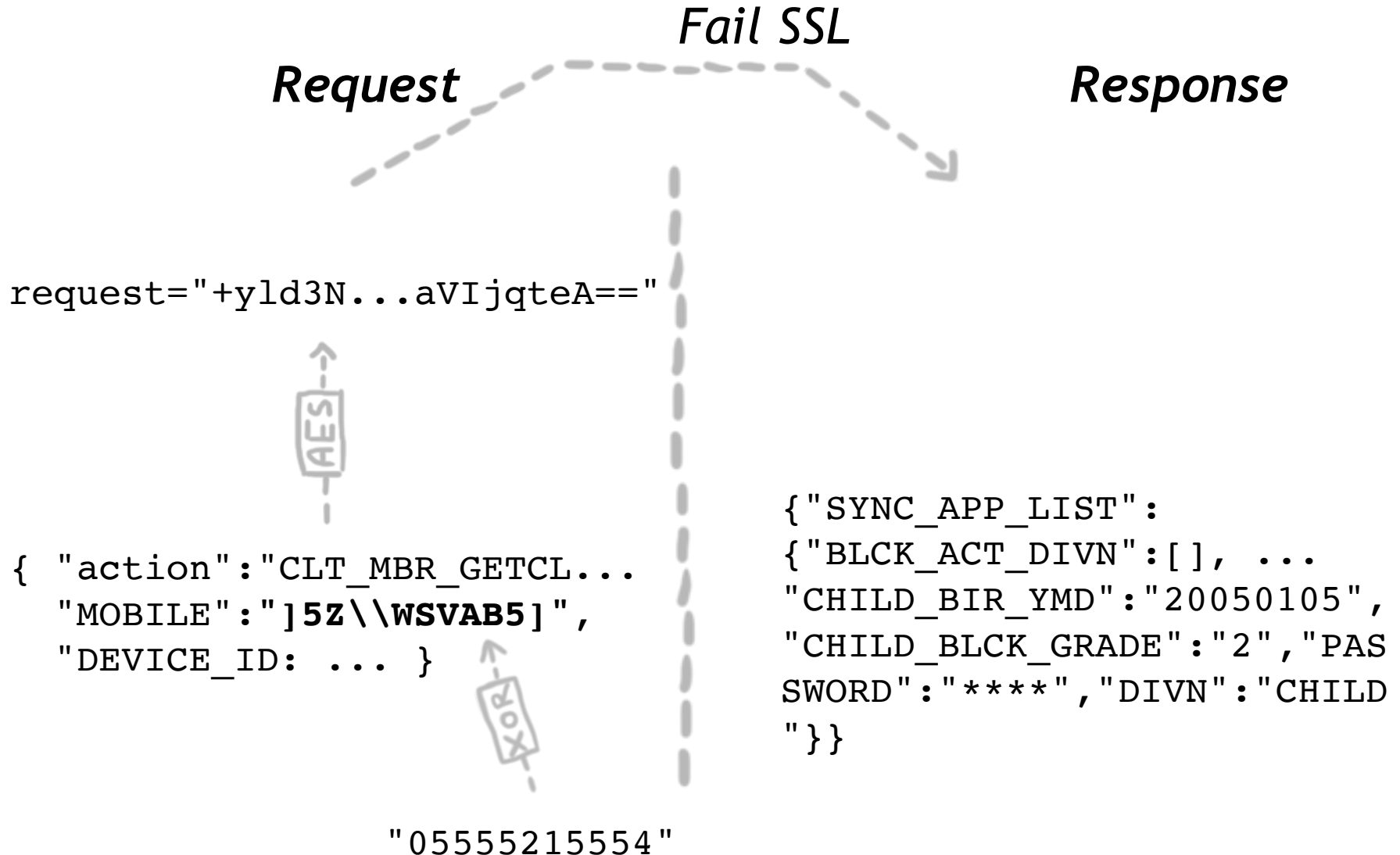
- MOIBA added more crypto...

moiba1cybar8smart4sheriff4securi



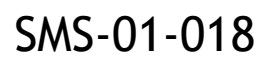
- Useless AES layer with static key

API Design

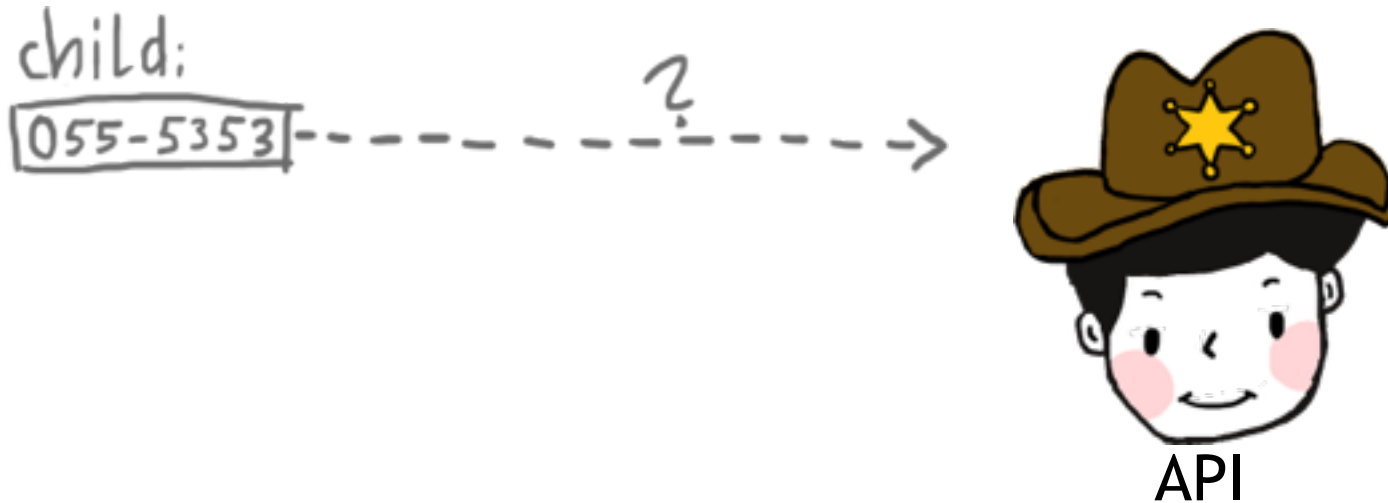


STORY TIME!

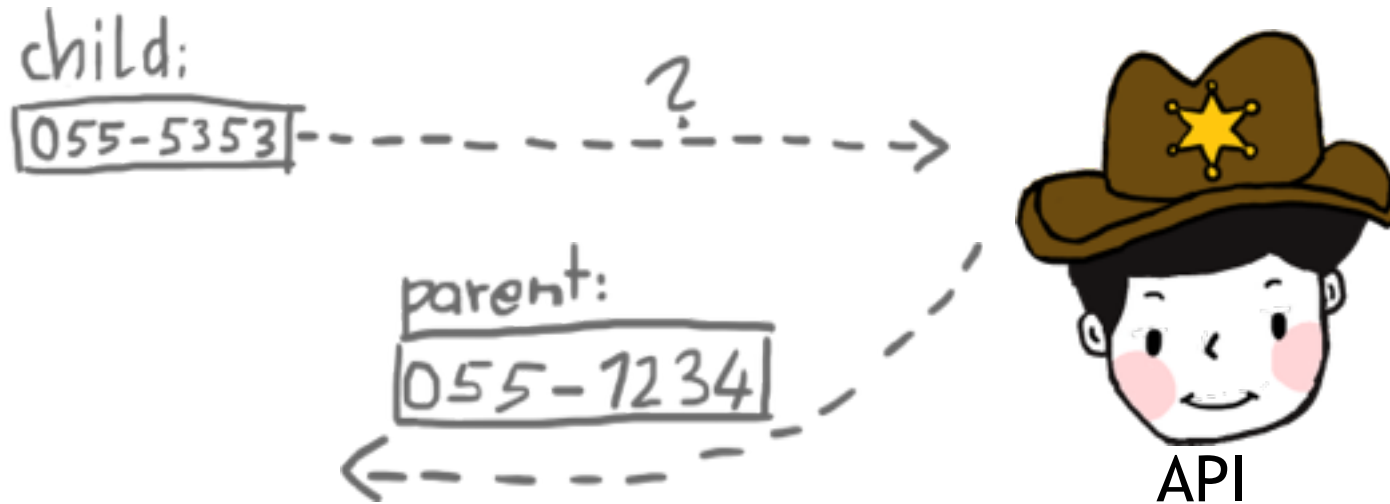




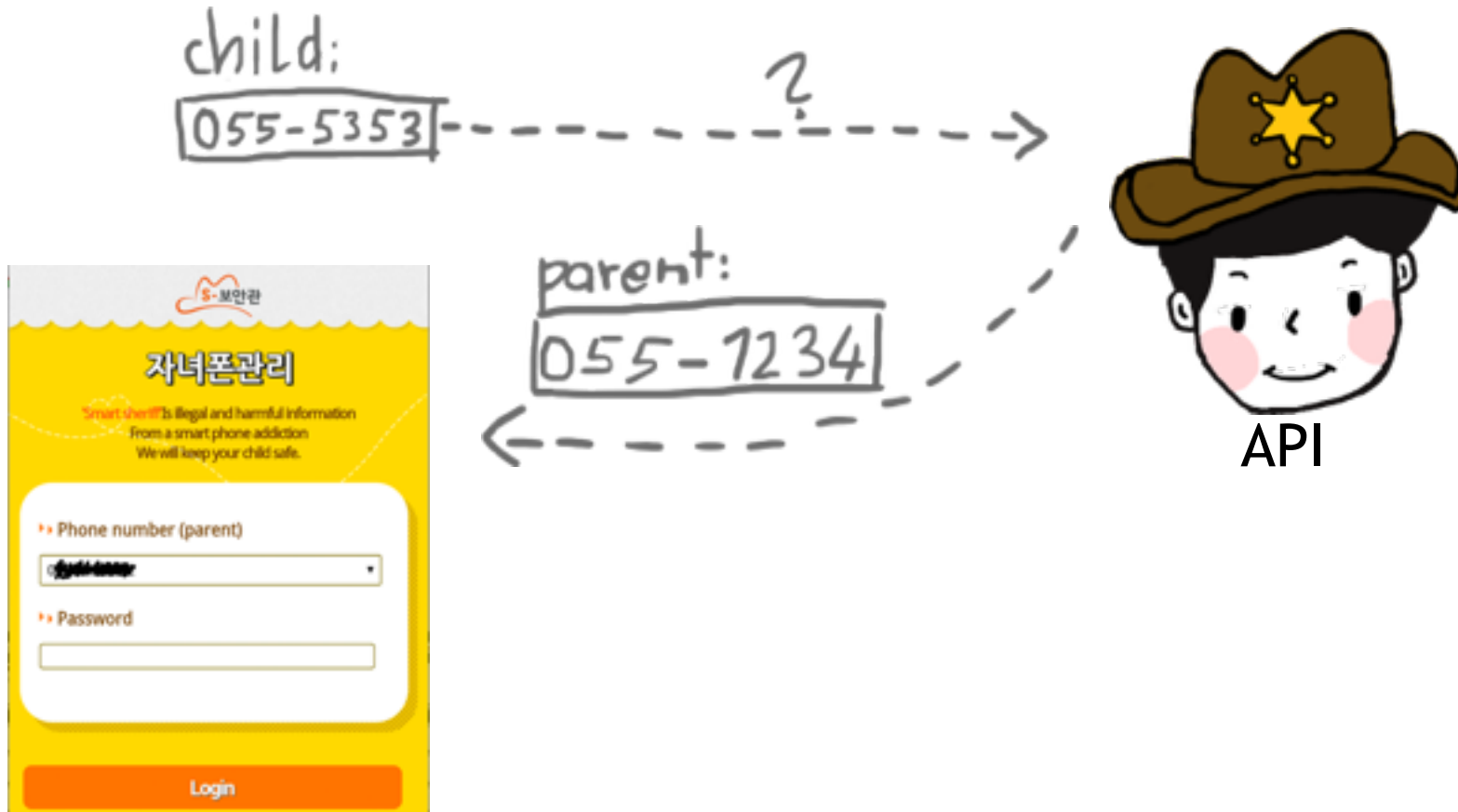
Smart Sheriff – Bully APITM



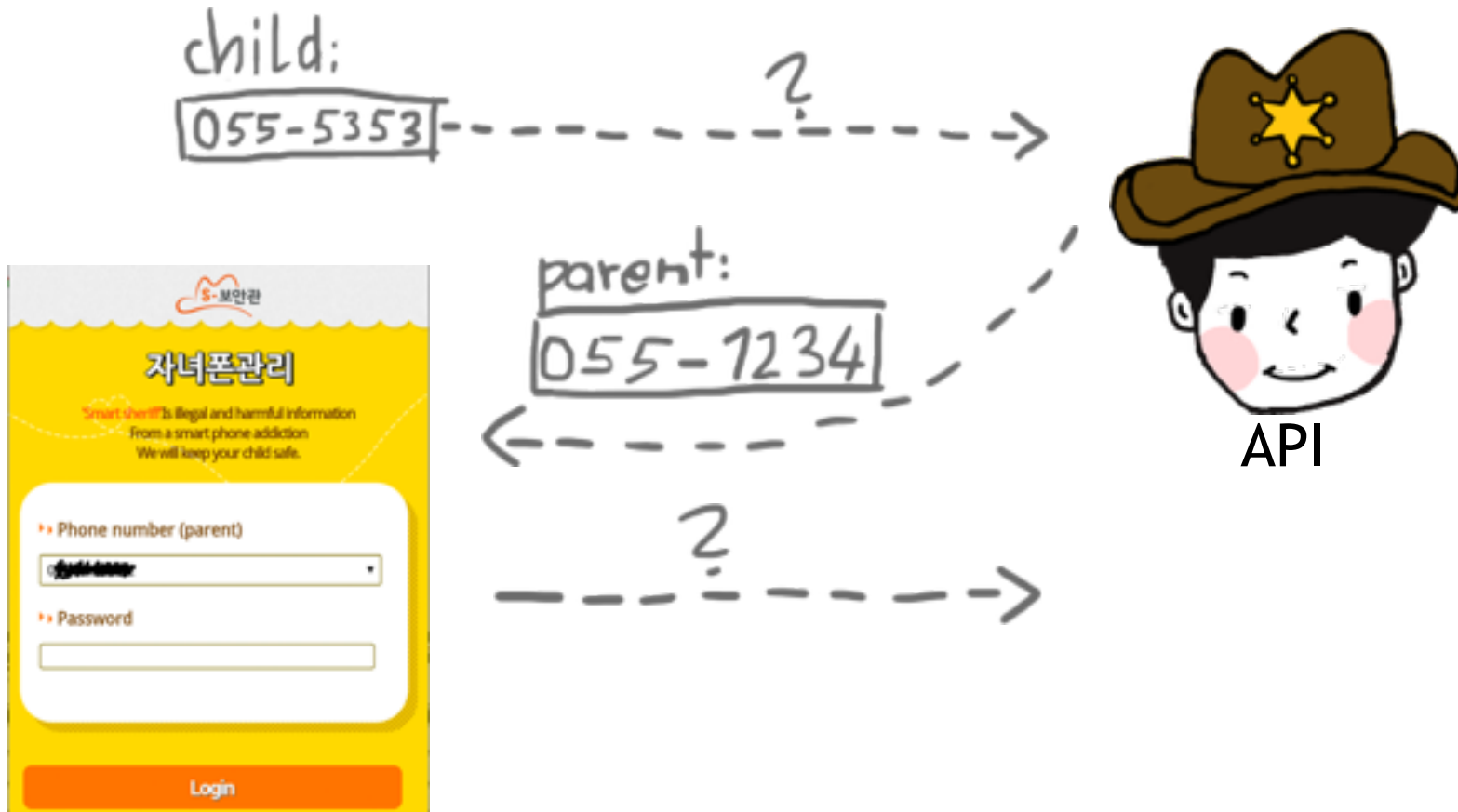
Smart Sheriff – Bully APITM



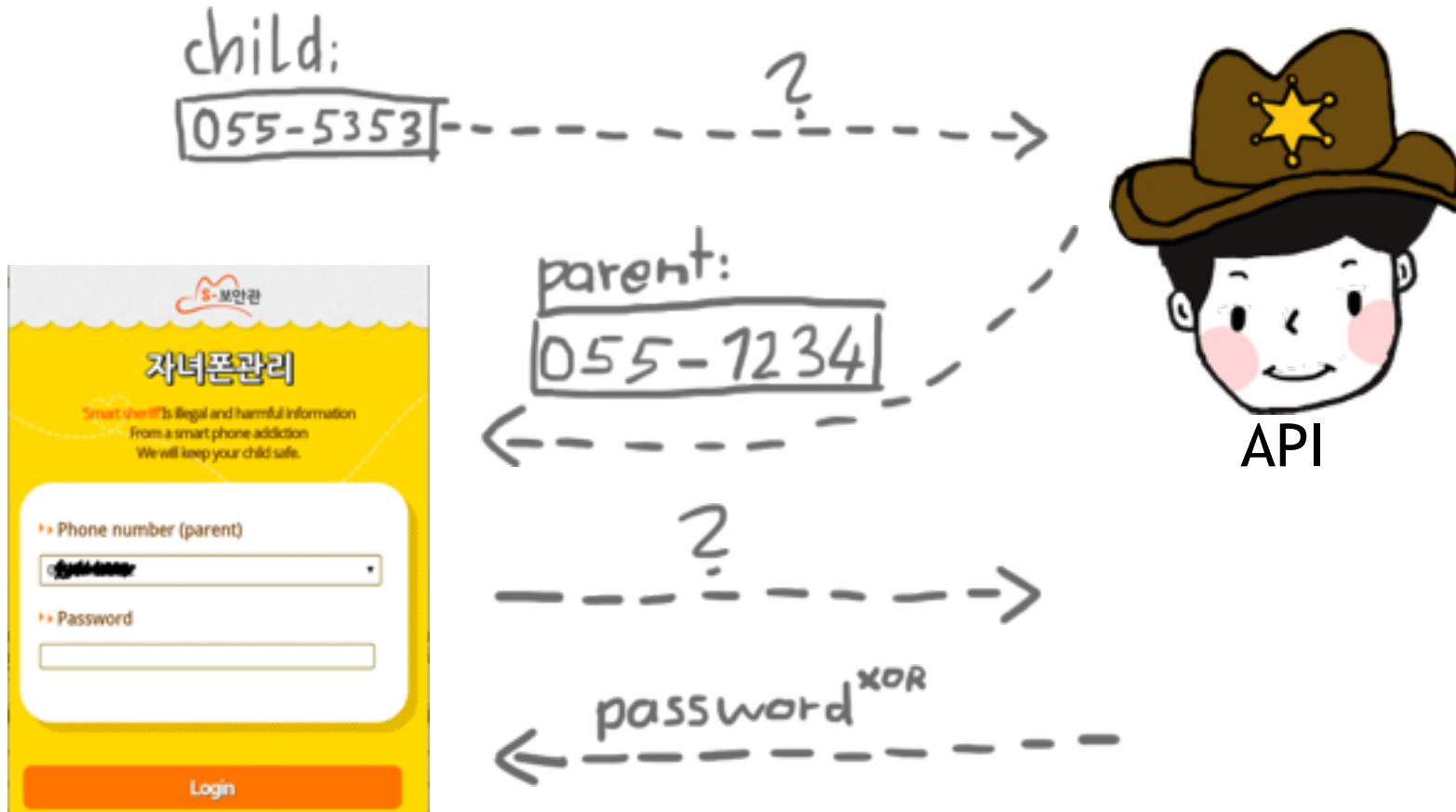
Smart Sheriff – Bully APITM



Smart Sheriff – Bully APITM



Smart Sheriff – Bully APITM



API response with the password (XORed)

Smart Sheriff – Bully APITM - Pass Leak

```
root@redstar-os $ curl -v -s 'http://api.moiba.or.kr/MessageRequest \
--data '{ "action":"CLT_MBR_GETCLIENTMEMBERINFO", "MOBILE_MACHINE_INFO":"XXX", "MOBILE":"\
\5Z\WSVAA5[" , "DEVICE_ID":"unknown" }'

> POST /MessageRequest HTTP/1.1
> Host: api.moiba.or.kr
> User-Agent: curl/7.48.0
> Accept: */*
> Content-Length: 141
> Content-Type: application/x-www-form-urlencoded
>
* upload completely sent off: 141 out of 141 bytes
< HTTP/1.1 200 OK
< Date: Sun, 15 Oct 2015 17:05:20 GMT
< Server: Apache/2.0.65 (Unix) DAV/2 mod_jk/1.2.37
< Content-Length: 242
< Content-Type: text/plain; charset=euc-kr
<
{"CHILD_GRADE_TYPE":"","CHILD_BIR_YMD":"","MEMBER_YN":"Y","CHILD_BLACK_GRADE":"","PASSWORD":"
\2\],"PARENT_MOBILE":"\5Z\WSVAA5[" , "REGISTRATION_ID":"","DIVN":"PARENT"}
```

\5Z\WSVAA5[--XOR--> 15555215652

\2\] --XOR--> 1234

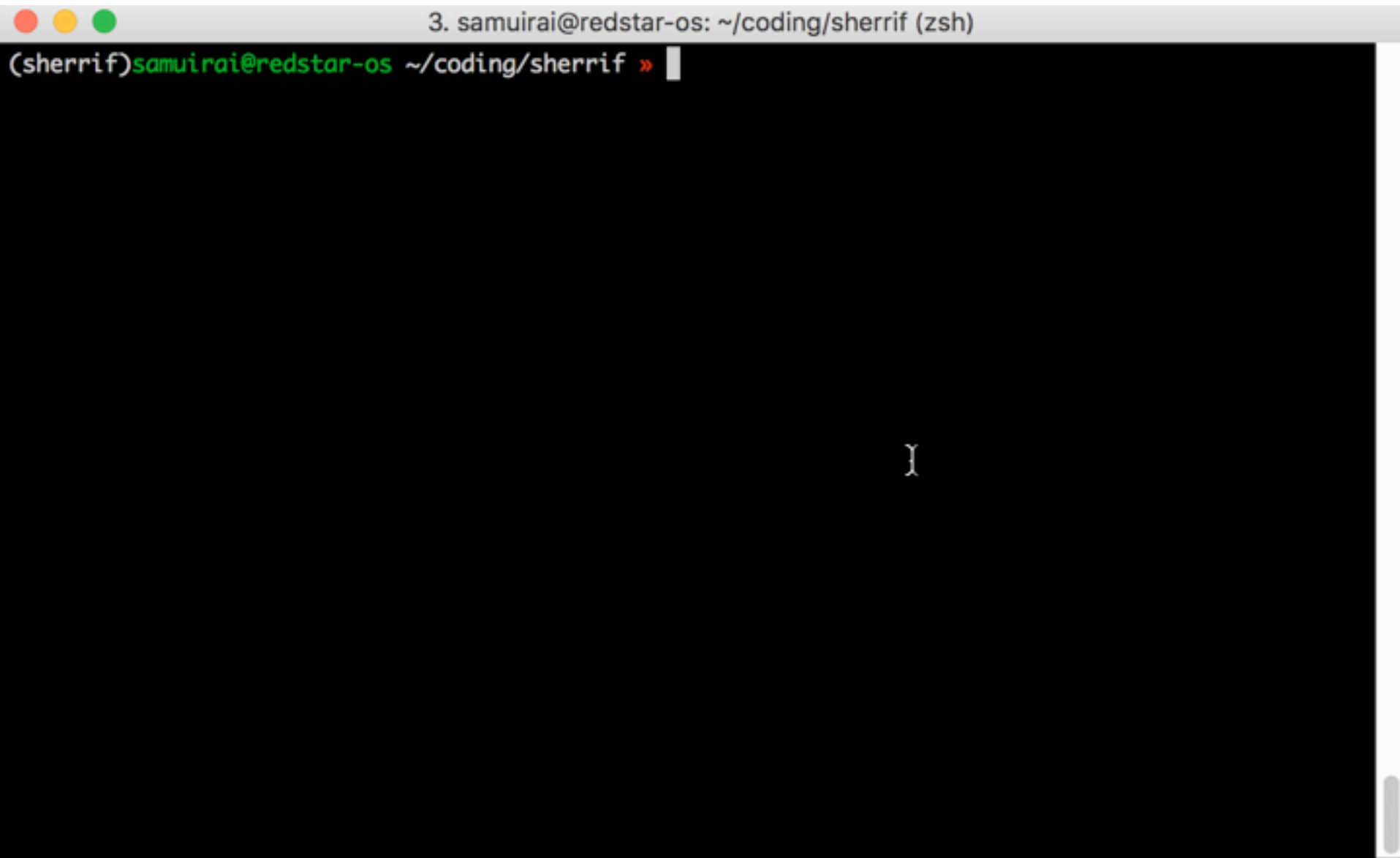
Smart Sheriff – Bully APITM

```
root@redstar-os $ python sheriff RAID.py
```

```
CHILD : 010XXXXXXXX - pw: 0879 -> parent number: 010XXXXXXXX
CHILD : 010XXXXXXXX - pw: 8493 -> parent number: 010XXXXXXXX
PARENT : 010XXXXXXXX - pw: 8493
PARENT : 010XXXXXXXX - pw: 0878
CHILD : 010XXXXXXXX - pw: 0878 -> parent number: 010XXXXXXXX
PARENT : 010XXXXXXXX - pw: 2580
CHILD : 010XXXXXXXX - pw: 2580 -> parent number: 010XXXXXXXX
CHILD : 010XXXXXXXX - pw: 2580 -> parent number: 010XXXXXXXX
PARENT : 010XXXXXXXX - pw: 5912
CHILD : 010XXXXXXXX - pw: 1004 -> parent number: 010XXXXXXXX
PARENT : 010XXXXXXXX - pw: 1004
```

Parent passwords. 4 digit strong!

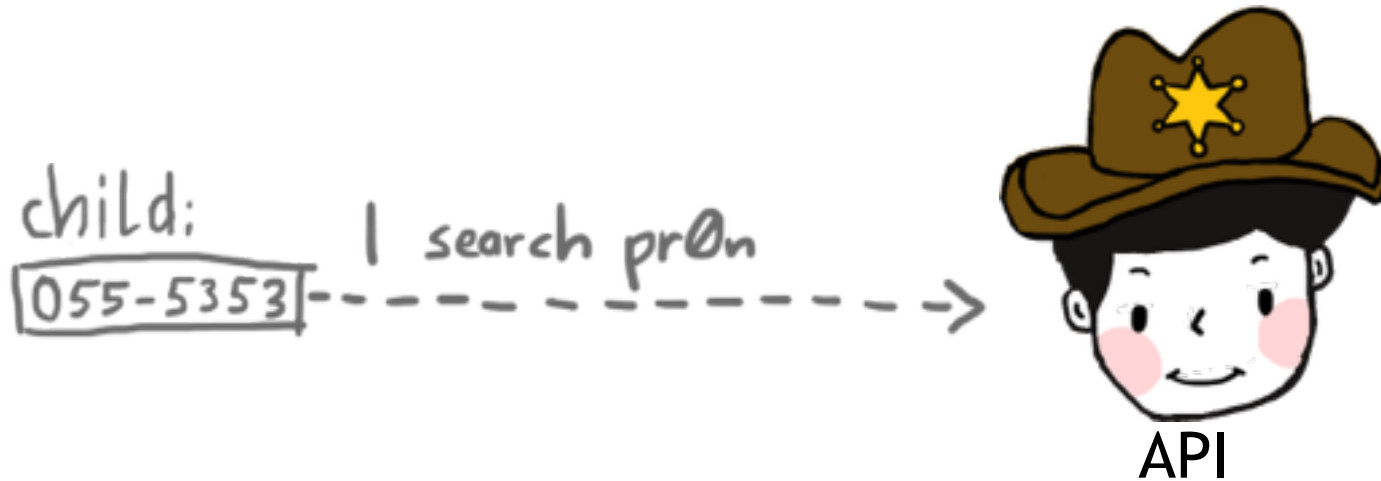
Smart sheriff has so many users, you can find valid phone numbers by just trying random numbers.

A terminal window with a light gray title bar containing three colored window control buttons (red, yellow, green) on the left. The title bar text reads "3. samuirai@redstar-os: ~/coding/sherrif (zsh)". The terminal area has a black background. The first line shows a prompt "(sherrif)samuirai@redstar-os ~/coding/sherrif" in green text, followed by a red double arrow "»" and a white cursor. The rest of the terminal is empty except for a single white character "I" centered on a line further down.

```
3. samuirai@redstar-os: ~/coding/sherrif (zsh)
(sherrif)samuirai@redstar-os ~/coding/sherrif » 
I
```

Bruteforce numbers - Skip to 2:54

Smart Sheriff – Bully APITM - Fake usage



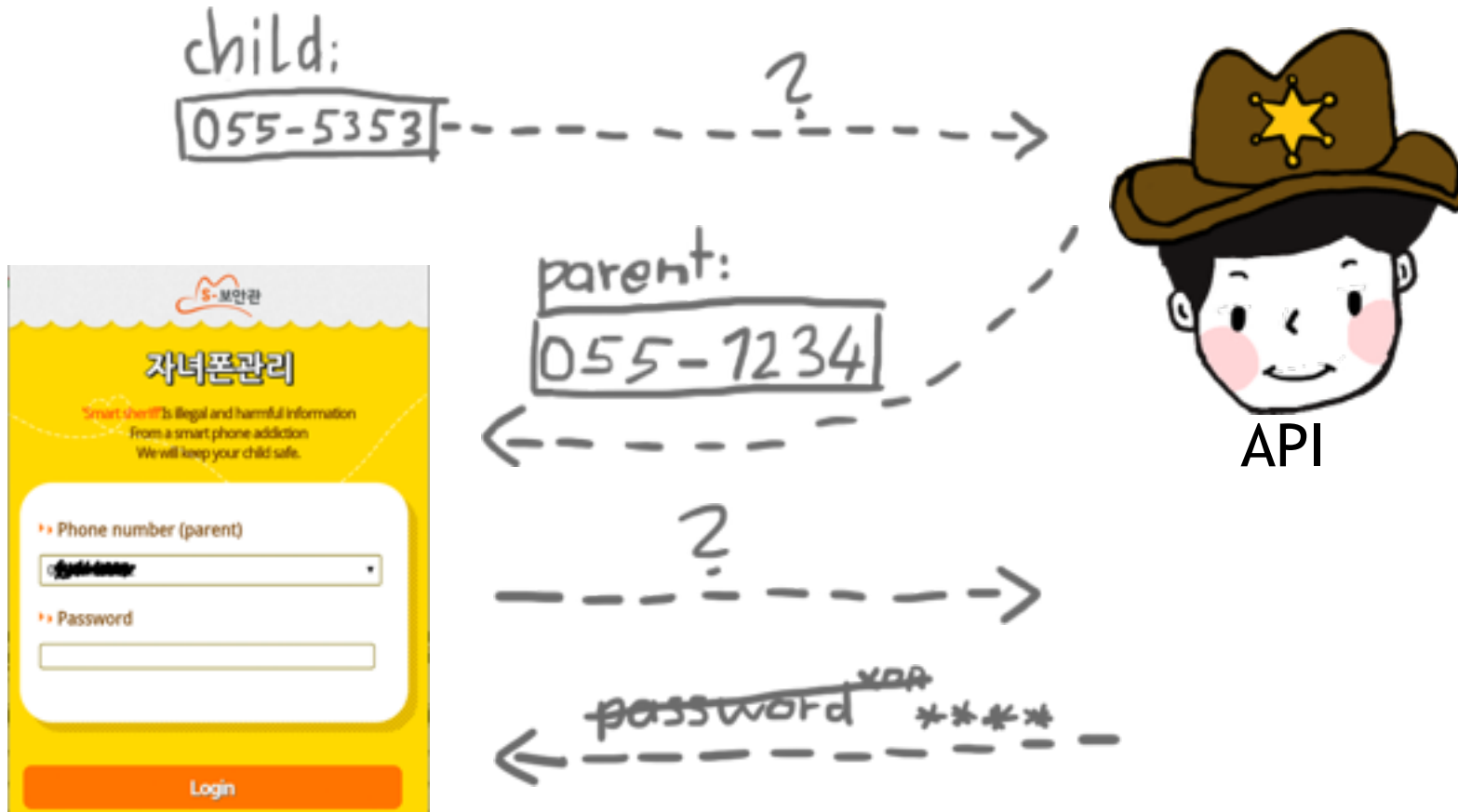
No authentication for the child application.

There is a `DEVICE_ID` as session cookie, but most API endpoints simply accept the phone number to perform updates.

Fast forward to the fixes...

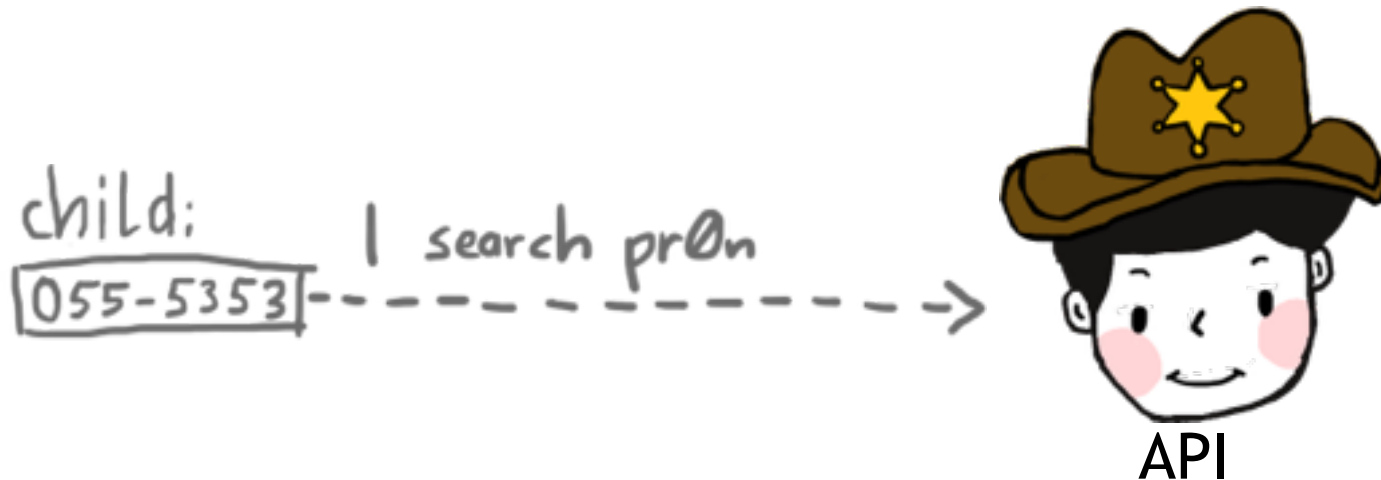
Smart Sheriff – Bully APITM v2.0

Smart Sheriff – Bully APITM



Guess what happened using a different User Agent :D

Smart Sheriff – Bully APITM v2.0



No authentication for the child application.

You can still **fake the phone usage** (kid installs p0rn app)

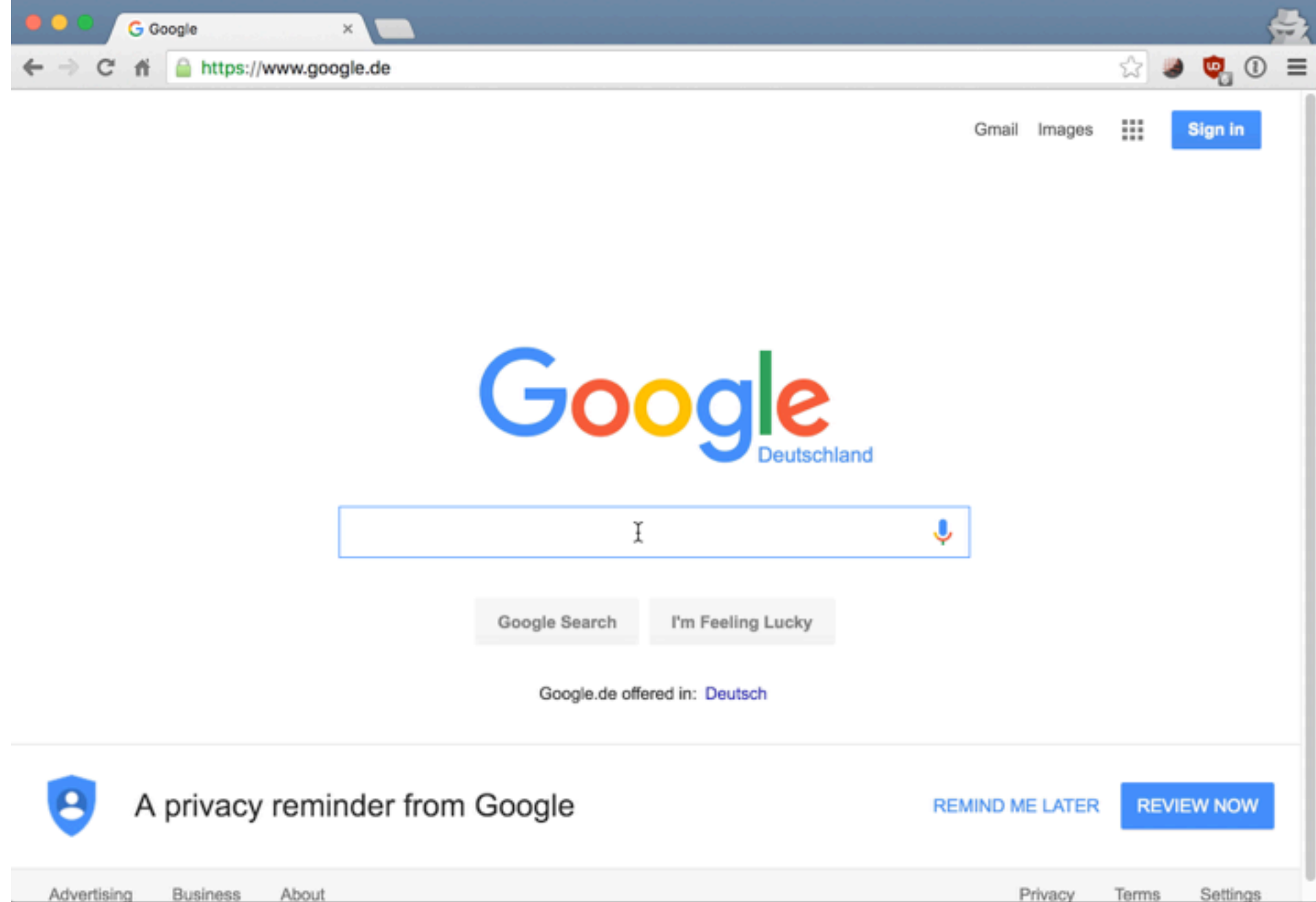
XSS



- SMS-01-008 Reflected XSS
on ssweb.moiba.or.kr via **CHILD_MOBILE** **FIXED!**

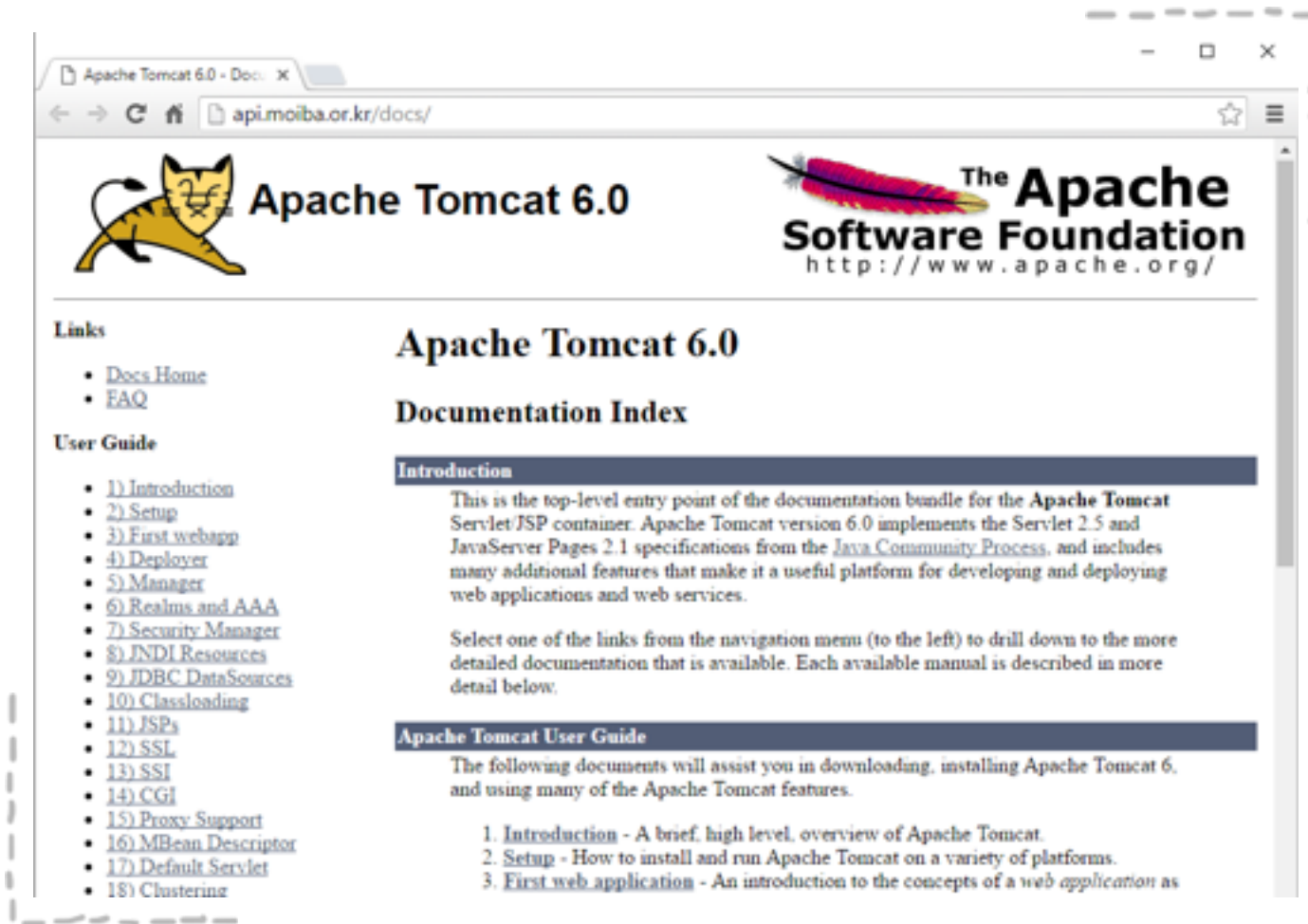
But...

- SMS-02-008 Reflected XSS
on ssweb.moiba.or.kr via **H_TYPE** **???**



You really screwed up when even Google indexes your vulns!

Why not? – Tomcat 6.0.29 (released 2009)



The screenshot shows a web browser window with the address bar displaying 'api.moiiba.or.kr/docs/'. The page title is 'Apache Tomcat 6.0'. The header features the Apache Tomcat logo (a yellow cat) and the Apache Software Foundation logo (a red feather) with the text 'The Apache Software Foundation' and the URL 'http://www.apache.org/'.

Links

- [Docs Home](#)
- [FAQ](#)

User Guide

- [1\) Introduction](#)
- [2\) Setup](#)
- [3\) First webapp](#)
- [4\) Deployer](#)
- [5\) Manager](#)
- [6\) Realms and AAA](#)
- [7\) Security Manager](#)
- [8\) JNDI Resources](#)
- [9\) JDBC DataSources](#)
- [10\) Classloading](#)
- [11\) JSPs](#)
- [12\) SSL](#)
- [13\) SSI](#)
- [14\) CGI](#)
- [15\) Proxy Support](#)
- [16\) MBean Descriptor](#)
- [17\) Default Servlet](#)
- [18\) Clustering](#)

Apache Tomcat 6.0

Documentation Index

Introduction

This is the top-level entry point of the documentation bundle for the **Apache Tomcat** Servlet/JSP container. Apache Tomcat version 6.0 implements the Servlet 2.5 and JavaServer Pages 2.1 specifications from the [Java Community Process](#), and includes many additional features that make it a useful platform for developing and deploying web applications and web services.

Select one of the links from the navigation menu (to the left) to drill down to the more detailed documentation that is available. Each available manual is described in more detail below.

Apache Tomcat User Guide

The following documents will assist you in downloading, installing Apache Tomcat 6, and using many of the Apache Tomcat features.

- [1. Introduction](#) - A brief, high level, overview of Apache Tomcat.
- [2. Setup](#) - How to install and run Apache Tomcat on a variety of platforms.
- [3. First web application](#) - An introduction to the concepts of a *web application* as

Block websites

```
function shouldOverrideUrlLoading()...
```

```
if(s.startsWith("market://") || s.startsWith("tel:")  
    || s.startsWith("http") && !s.contains("ssweb.moiba.or.kr"))  
    -----
```

blocked	allowed :D
http://blocked.com	http://blocked.com/?blah=ssweb.moiba.or.kr

Insecure Storage on SD card

```
Object obj = new File((new StringBuilder()  
obj.append(Environment.getDataDirectory());  
obj.append("/data/com.gt101.cleanwave/databases/SmartSheriff.db");  
Object obj1 = new File(Environment.getExternalStorageDirectory(), "");
```

Unlicensed Fonts

The screenshot shows a web browser's developer tools interface. At the top, a table lists several HTTP requests:

No.	URL	Method	Path	Status	Size	Content Type	File Name
54	https://211.253.14.71	GET	/fonts/fntPwd.woff	200	7145	woff	woff
55	https://211.253.14.71	GET	/images/bg_loginbox.png	200	8187	PNG	png
56	https://211.253.14.71	POST	/main/login	200	11057		
57	https://211.253.14.71	POST	/main/login	200	11057		

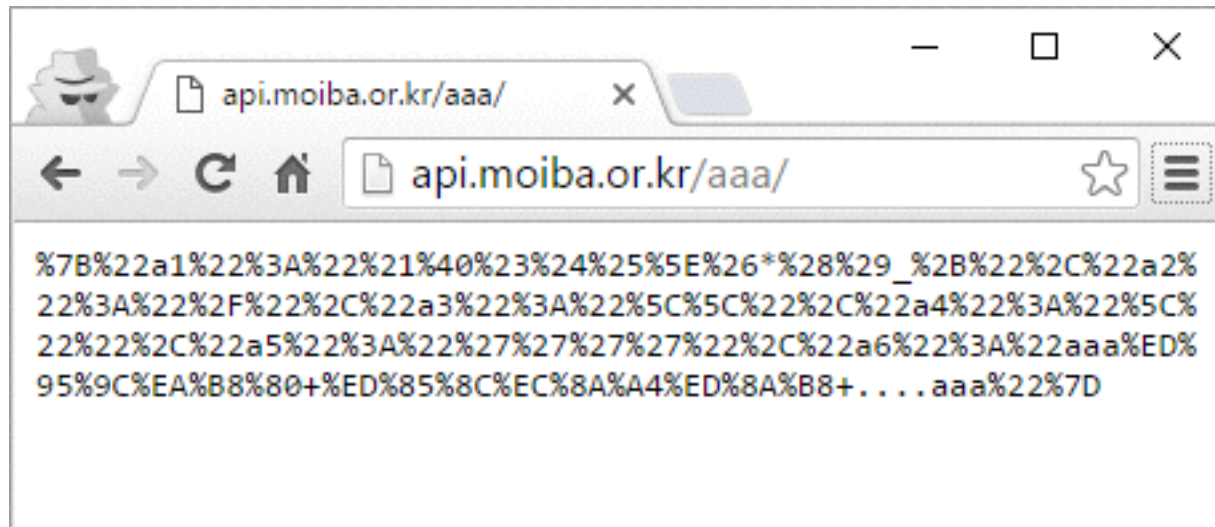
Below the table, the 'Response' tab is selected, showing the raw content of the selected request (the font file). The content is a mix of text and binary data, with a prominent copyright notice highlighted in yellow:

```
~ P 1 Typeface (your company). 2013. All Rights ReservedRegularpassword:Version 1.00Version 1.00 June 26, 2013, initial releaseThis font was created using FontCreator 7.0 from High-Logic.comThis font is made with the trial version of FontCreator. You may not use this font for commercial purposes.http://www.high-logic.com/fontcreator/fontlicense.htmlTypeface (your company). 2013. All Rights ReservedRegularpassword:Version 1.00Version 1.00 June 26, 2013, initial releaseThis font was created using FontCreator 7.0 from High-Logic.comThis font is made with the trial version of FontCreator. You may not use this font for commercial purposes.http://www.high-logic.com/fontcreator/fontlicense.html
```

At the bottom, there is a search bar with the text 'Type a search term' and a '0 matches' indicator.

*„This font is made with the trial version of FontCreator.
You may not use this font for commercial purposes.“*

Test and dev. snippets everywhere



...
{ "a1" : "!@#\$%^&* () _ +", "a2" : "/", "a3" : "\", "a4" : "\"", "a5" : "'", "a6" : "aaa한글 테스트aaa" }

Test URLs: <http://api.moiba.or.kr/test/>
<http://api.moiba.or.kr/aaa/>
<http://api.moiba.or.kr/aaa2/>

...

Test and dev. snippets everywhere

<http://220.117.226.129:8082> <http://hikdev.cafe24.com/demo-gcm-server>
<http://ssadm.moiba.or.kr/>

```
<li><a href=' /index'>관리자메인</a></li>
<li><a href=' /subMain'>서브메인메인</a></li>
<li><a href=' /harm/app/list'>유해정보관리</a>
  <ul>
    <li><a href="/harm/app/appList">앱관리</a></li>
    <li><a href="/harm/site/list">사이트관리</a></li>
    <li><a href="/harm/accept/acceptList_app">앱/사이트 접 관리</a></li>
  </ul>
</li>
<li><a href=' /member/admin/memberAdm'>가입자관리</a>
<li><a href=' /minwon/minwonList'>민원관리</a>
<li><a href=' /home/report/list'>홈이지</a></li>
</ul>
<p> <a href=' /html/filelist.html'>디자인</a><br/><br/>
<a href=' /minwon/minwonPushTest'>Push TEST</a><br/><br/>
<a href=' /minwon/livePushTest'>Live Push TEST</a><br/>
<a href="minwon/logPushTest">log Push Test</a></br>
```

Big pile of

- XSS
- Leaking personal data over the API
- No authentication
- No Transport Security
- Even a SQL injection inside their mobile app for the .db
-

Seriously:

https://cure53.de/pentest-report_smartsheriff.pdf

https://cure53.de/pentest-report_smartsheriff-2.pdf

Citizen Lab publishes the report



MOIBA Press Release 1

[20150806] 스마트보안관 1.7.6 업데이트 안내

| 2015-08-06

안녕하세요, 스마트보안관입니다.

스마트보안관 1.7.6 버전이 업데이트 되었습니다.

구글플레이 및 이통사 마켓을 통해 8/10일까지
반드시 업데이트 해 주시기 바라며,
8/11일 이후 이전 버전은 이용하실 수 없습니다.

이는 스마트보안관의 보안을 강화하기 위해
조치하는 사항으로 이용자들의 넓은 이해를 부탁드립니다.

앞으로도 스마트보안관은 지속적으로 보안을 강화하여
보다 안전하게 서비스를 이용하실 수 있도록 노력하겠습니다.

<업데이트 내용>

- SSL 적용으로 보안 강화(http -> https)

이번 업데이트에 대한 자세한 문의사항은 고객센터(1566-8274)로 전화 주시면
친절히 안내해 드리도록 하겠습니다.

감사합니다.

we continue
to improve
security!

enhanced security with SSL

MOIBA Press Release 2

[20150821] 스마트보안관 보안 강화 관련 공지 알림

2015-08-21

12

안녕하세요, 스마트보안관입니다.

먼저 스마트보안관을 이용해 주셔서 감사합니다.

지난 8월 6일 스마트보안관이 1.7.6 버전으로 업데이트 되면서 보안 강화를 위해 8/11일 이후 기존(1.7.5 이하) 버전의 경우 사용하실 수 없다는 내용을 홈페이지 및 메시지(Push) 전송을 통해 알려드린 바 있습니다.

deprecating old version
because of security

다만, 이러한 내용을 아직까지 확인하지 못한 분들이 계십니다. 그로 인해 이전 버전 사용자들의 경우 자녀폰에 이용시간 차단 등의 조치를 취해 놓으신 경우 자녀의 폰 사용 자체가 불가능해지는 현상이 발생하였습니다.

현재는 조치를 취하여 더 이상 문제가 발생하지 않게 되었으나, 예기치 못한 상황이 발생하여 이용에 불편을 드린 점에 대해 대단히 죄송하다는 말씀을 드립니다.

sorry for the inconvenience

단, 아직까지 스마트보안관을 업데이트 하지 않으신 이용자분들께서는 스마트보안관 보안 강화를 위해 마켓에 접속하셔서 최신 버전으로 반드시 업데이트 하여 주시기 바랍니다.

please update!!

특히 자녀가 스마트보안관을 이용하고 있는 이용자분들께서는 자녀폰에 설치된 스마트보안관 앱을 마켓을 통해 업데이트 하여 주시기 바랍니다.

그 외의 추가적인 사항이나 상세한 설명을 원하시는 분들은 1566-8274로 연락 주시면 안내해 드리도록 하겠습니다.

다시 한 번 이용에 불편을 드리게 된 점에 대해 죄송하다는 말씀을 드리며, 앞으로도 스마트보안관은 지속적으로 보안을 강화하여 보다 안전하게 서비스를 이용하실 수 있도록 노력하겠습니다.

we continue to strengthen
the security

감사합니다.

Some media attention

CBCnews | Technology & Science

Home	World	Canada	Politics	Business	Health	Arts & Entertainment	Technology & Science	Trending	Video
Technology & Science Quirks & Quarks Blog Spark Photo Galleries									

Smart Sheriff child surveillance app leaves South Korean kids vulnerable to hackers

Citizen Lab, Cure 53 find government-mandated app has 'literally no security at all'

The Associated Press Posted: Sep 21, 2015 9:59 AM ET | Last Updated: Sep 21, 2015 10:29 AM ET

... but reaction was a bit underwhelming

스마트폰 통제 앱 '스마트보안관'...개인정보 노출 무방비

정부와 생체 의무화—자녀 스마트폰 관리해라다가 해커들에게 정보 파수는 꿈
개인정보 전혀 암호화하지 않아 위험 높아

등록 2015-09-21 10:18 수정 2015-09-21 10:05

공식 + -    



The infographic features a central smartphone displaying the 'Smart Sheriff' app interface. Surrounding the phone are several circular icons with Korean text, each representing a feature or concern: a lightbulb for 'Security protection' (보안 관리), a shield for 'Personal information protection' (개인정보 관리), a clock for 'Time management' (시간 관리), a location pin for 'Location management' (위치 관리), a smartphone with a lock for 'App management' (앱 관리), and a document with a checkmark for 'Usage management' (사용 관리). The main text on the left reads: '자녀의 부모님 스마트폰에 "스마트보안관"을 설치하시면 불법·유해정보 차단 뿐 아니라 자녀 스마트폰 관리를 위한 다양한 서비스를 이용할 수 있습니다.' (If you install 'Smart Sheriff' on your child's parent's smartphone, you can not only block illegal and harmful information but also use various services for managing your child's smartphone.) At the bottom, there is a button that says '스마트보안관 이용안내 바로가기' (Go to Smart Sheriff usage guide) and a small disclaimer at the very bottom: '국립사이버보안지능센터가 '스마트보안관'이 자녀의 개인정보를 해커들에게 노출시킨다는 보안문제자들의 경고가 나왔다. (자녀를 자녀-한국인터넷진흥원(KISA)의 스마트보안관 홈페이지)' (A warning from the National Cyber Security Intelligence Center that 'Smart Sheriff' exposes children's personal information to hackers was issued. (Parents, visit the Korea Internet & Security Agency's Smart Sheriff homepage))

„Thanks for the free pentest!“



It kinda backfired...

Did we just help improving surveillance software?



Citizen Lab publishes updated report



MOIBA reacts and pulls the app

[스마트보안관 서비스 이용 안내] | 2015-11-11

안녕하세요, 스마트보안관입니다.

저희 스마트보안관은 스마트폰을 통해 유통되는 음란물 및 유해정보로부터 청소년을 보호하기 위하여 '12년부터 무료로 서비스를 제공해왔습니다.

'13년 이후 폭발적인 스마트폰 확산(현재 청소년의 80%이상 스마트폰 보유)과 더불어 유해정보로부터 청소년을 보호하기 위한 정책의 필요성이 대두됨에 따라, 국회 및 정부는 관련 법 개정('15.4.16)을 통해 전기통신사업자에게 청소년의 휴대용 가입시 유해정보 차단 수단을 의무적으로 제공하도록 하였습니다.

이에 금년 10월부터, 모든 전기통신사업자가 유해정보 차단 SW를 무료로 제공함에 따라, 민간 업 시장의 발전과 중박사업 발전을 위해 11월 1일부터 '스마트보안관'은 신규 가입자를 받지 않기로 하였으며, 기존가입자의 경우는 민간사업자가 제공하는 서비스로 전환하는 것으로 결정되었습니다.

따라서, 기존 가입자의 경우는 해당 통신사 또는 민간 업 사업자가 제공하는 유료 또는 무료 유해정보 차단 SW 중 선택 (자단수단 안내는 와이즈유저 홈페이지) 서비스 전환을 하여 주시기 바랍니다.

저희 스마트보안관은 향후 사용자 여러분들께 조금의 불편함도 없이 서비스 전환이 이루어지도록 최선을 다하겠습니다.

감사합니다.

이전글 ^ [스마트보안관 보안 관련 안내] 2015-11-11

다음글 v [20150825] 스마트보안관 1.7.7 버전 업데이트 안내 2015-08-25

we offer free service for 12 years

80% of kids have a phone that's why there is this new law since 15.4.16

decide to stop smart sheriff

please move to another blocking service

News about the app removal

smart sheriff disappeared

slow news

미디어 ▾ 정치 ▾ 사회 ▾ 테크 ▾ 문화 ▾ 비즈니스 ▾ 사람들 ▾ 특집 ▾ 연재 ▾ 비어트 ▾ 전체 기사 ▾

현재 위치: 홈 > 사회 > 스마트폰안관은 사라졌지만 감시는 계속된다

스마트보안관은 사라졌지만 감시는 계속된다

일자: 오픈넷 작성일: 2015-11-16 카테고리: 사회, 테크 | 댓글: 1

 공유하기  44  6

방통위가 청소년들을 유해정보에서 구해내겠다며 청소년들의 스마트폰에 배포한 스마트보안관이라는 모바일 앱이 있다. 방통위는 2013년부터 무려 이 앱을 위해 약 30억 원의 예산을 들였고 이통3사와 한국우선인터넷산업연합회(이하 MOIBA)가 함께 개발을 했다.

스마트보안관을 실행시키면 이 앱이 계속 스마트폰에 상주해있으면서 이용자, 즉 청소년이 스마트폰을 통해 하는 모든 행동이 모두 모니터링 되는 방식으로 작동한다. 주요 기능은 아래와 같다.

- 청소년에게 유해하다고 판단된 정보에 접근하는 것을 원천적으로 차단한다.
- 부모에게 청소년 자녀의 스마트폰 일평균 이용시간, 주 이용시간대, 주 이용정보 카테고리 등의 정보를 제공한다.
- 부모가 청소년 자녀의 스마트폰 이용을 통제한다. (시간별, 앱별 등)
- 스마트폰에 설치된 스마트보안관을 청소년이 임의로 삭제할 수 없게 한다.

slow news
느리지만 꼼꼼한 슬로우뉴스에게
커피 한 잔의 여유를 후원해주세요
국민은행 653201-04-035401
(유)슬로우미디어

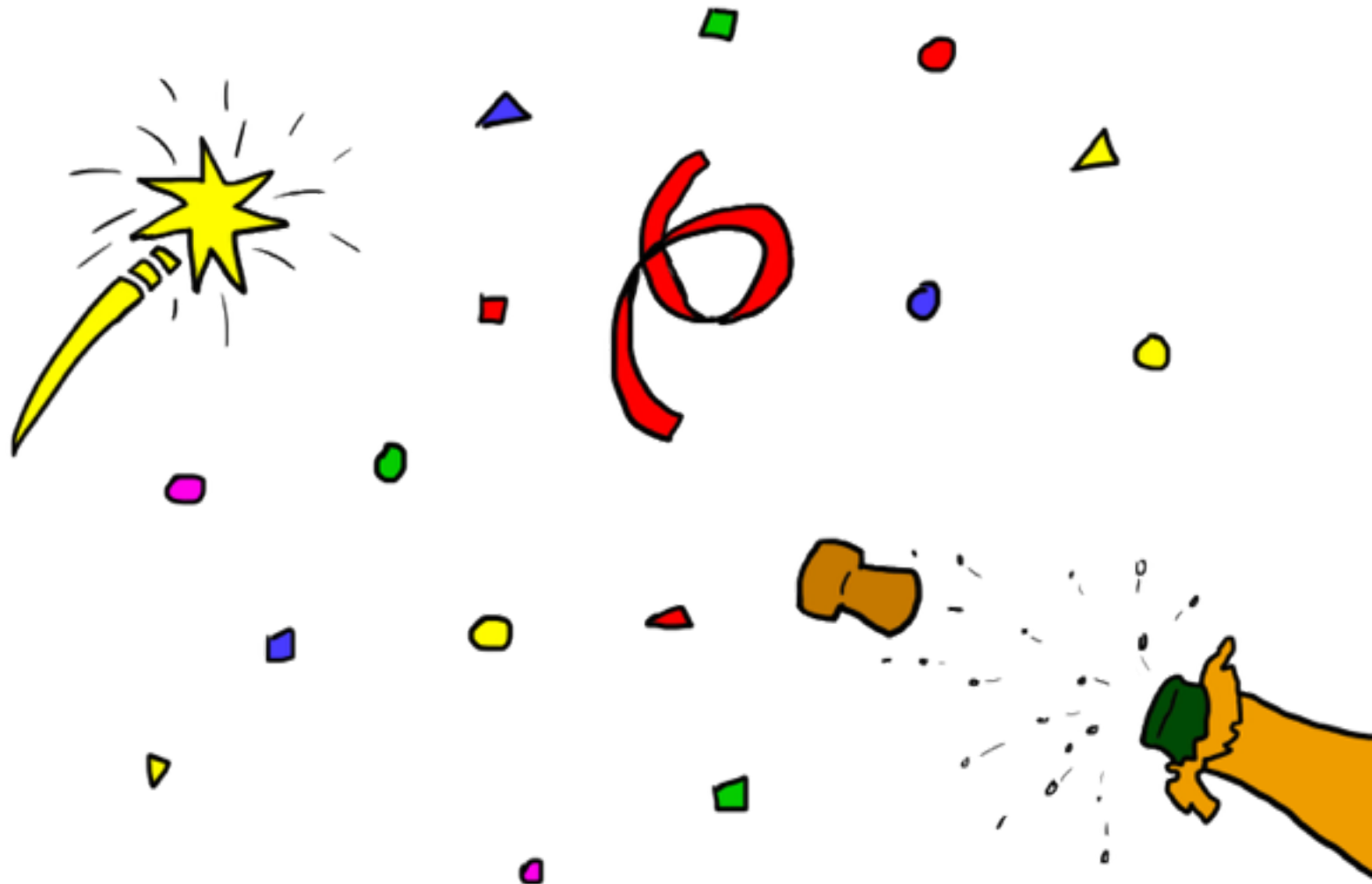


최근 기사

 **철집 아메리카 3부작, 그 서사와 창작에 관하여**
9월 15, 2016

 **열린 커리큘럼 방문들, 아름다운 동화 '슬랄'이 지운 것들**
9월 15, 2016

Time to celebrate!



But something is shady...



NOTE: On October 31, 2015, Citizen Lab learned that MOIBA removed the Smart Sheriff application from the Google Play Store. However, the Smart Sheriff API remains available and therefore constitutes a continued security risk to users. Additionally, MOIBA appears to have republished Smart Sheriff under another name (사이버안심존 – translated as “Cyber Safety Zone”) on the Google Play store. A brief inspection of version 1.7.8 indicates that, beyond cosmetic changes, the application is functionally the same as Smart Sheriff 1.7.7 – which we analyze here. This new program inherits all the same security concerns as the original application.

minor children and parental users of the application at serious risk.

- MOIBA, the Korean industry consortium responsible for the Smart Sheriff application, has been slow to respond to the issues raised (of which it was notified more than 90 days ago); the fixes that have been applied do not adequately or effectively address the issues, especially for users; and MOIBA has not communicated transparently to the public about Smart Sheriff's known risks.
- The Citizen Lab recommends immediate withdrawal of Smart Sheriff from the public market, and that existing users discontinue their use of the application.

NOTE: On October 31, 2015, Citizen Lab learned that MOIBA removed the Smart Sheriff application from the Google Play Store. However, the Smart Sheriff API remains available and therefore constitutes a continued security risk to users. Additionally, MOIBA appears to have republished Smart Sheriff under another name (사이버안심존 – translated as “Cyber Safety Zone”) on the Google Play store. A brief inspection of version 1.7.8 indicates that, beyond cosmetic changes, the application is functionally the same as Smart Sheriff 1.7.7 – which we analyze here. This new program inherits all the same security concerns as the original application.

Did we fail?

T-store
www.tstore.co.kr/userpoc/game/view?pid=0000691902

store

게임
앱
영화
TV방송
만화
eBook
음악
이벤트
고객센터

내 폰에 설치하기

OK! 앱이 폰으로 전송

지녀용 (LITE)
사이버 안심존

★★★★☆ 18
26 people participated

공여요 8

Use Class Everyone
Self Member MOBA
Support equipment Read More

Cyber relief zone (-LITE version for children)
By blocking adult content, including pornography and violence on the smartphone, the app high and gambling items.

Price **Free**
Downloads 2684
Added 2015-08-25
Updated 2015-11-09
Capacity 8,479Kb
Platform Android
Product Description

[Cyber assured John]
pornography, including adult content and violence, gambling by blocking high apps and Internet site access protection for our children to use, games, chat, apps and to restrict Internet usage time too much of a child's smart phone on the smartphone this service can prevent.

우리아이 스마트폰 지킴이!
사이버안심존
Loading...

우리아이 스마트폰 지킴이!
사이버안심존
사이버존 안에서 청소년 유해정보를 차단해
부모의 마음을 조금이라도 덜어드립니다.

앱의 특징

항목	내용
이용시간	2시간 12.0분
주 이용 시간대 (월~일요일)	12시~18시 (40.4명)
정보이용비율	앱(96.55%), 인터넷(0.45%)
정보별 주 이용시간대/카테고리	앱: 12시~18시 (연차평균) 카테고리: 12시~18시
앱 사용고려해 이용시간	연차평균 (1.42) 34.2명 게임 (22.2명) 커뮤니케이션 (1.3명) 유희 (1.3명)
주 이용요일	수 (44.0) 35.4명, 화 (24.0) 48.6명

청소년 이용정보
해당 콘텐츠는 청소년에게도
적당히 사용할 수 있습니다.

고객센터: 1566-827

Find the difference!

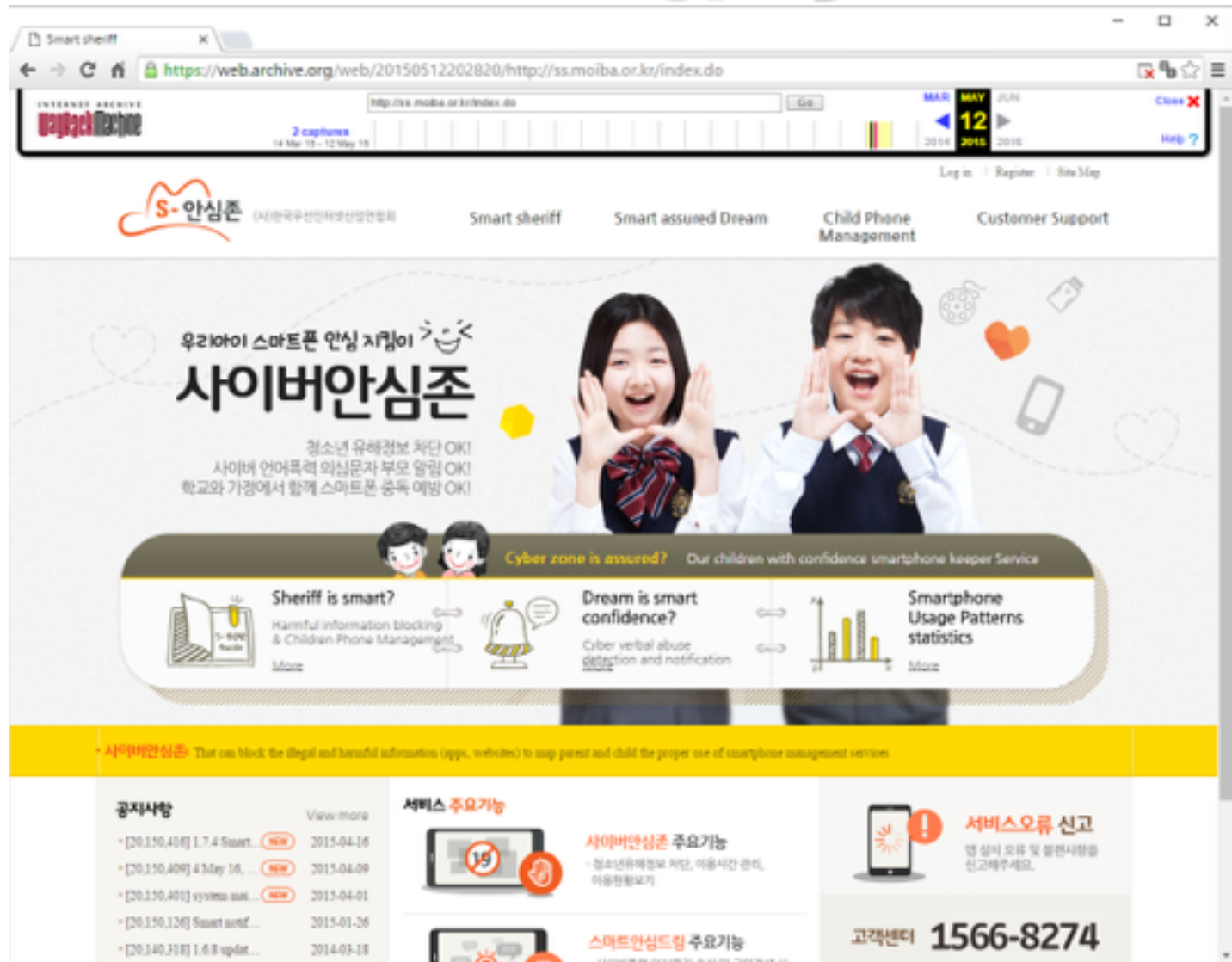


스마트보안관
(Smart Sheriff)



사이버안심존
(Cyber Safety Zone)

The old MOIBA



The new MOIBA



Web Interface – Cyber Safety Zone

The screenshot displays a web browser window with the URL `https://ss.moelba.or.kr/childPhone/introduce_03.do?ms=1`. The page is titled "사이버안심존" (Cyber Safety Zone) and features a navigation menu with links: "사이버안심존", "스마트안심드림", "자녀 폰 관리" (Child Phone Management), and "고객지원".

The main content area is titled "사이버안심존 - 자녀 폰 관리" (Cyber Safety Zone - Child Phone Management). It includes a sub-header "자녀 스마트폰에 아이폰인 경우 인터넷사이트관리, 자녀추가만 이용가능" (If your child's smartphone is an iPhone, you can only use internet site management and add children). Below this, there are tabs for "View Usage", "Use time management", "Manage apps" (selected), "Internet site management", and "Additional child".

The "Manage apps" section is titled "John assured cyber-kids phone management". It contains a note: "* If your child a smartphone, the iPhone Internet site management, available only add children". Below this, it states: "Children can look up the list of apps installed on your smartphone, and you can direct parents to block or revoked." (Note: The text "해지 불가" is crossed out with a red 'X').

At the bottom, there is a search form with the following fields:

- Child mobile phone number: `asd [010-1111-1122]`
- Inquiry period: `[ ] - [ ]`
- Search button: `Search`

Web Interface – Cyber Safety Zone

The screenshot displays the 'Cyber Safety Zone' web interface in a browser window. The address bar shows the URL: https://ss.moiba.or.kr/childPhone/introduce_03.do?ms=1. The page features a header with the '사이버안심존' (Cyber Safety Zone) logo and navigation links: '사이버안심존', '스마트안심드림', '자녀 폰 관리' (Child Phone Management), and '고객지원' (Customer Support). A large banner image shows a family (father, mother, and child) with a violin and a book.

The main content area is titled '자녀 폰 관리' (Child Phone Management) and '사이버안심존 - 자녀 폰 관리'. It includes a sub-header: '자녀 스마트폰에 아이폰인 경우 인터넷사이트관리, 자녀추가만 이용가능' (If the child's smartphone is an iPhone, only internet site management and adding children are available). Below this are tabs: 'View Usage', 'Use time management', 'Manage apps' (selected), 'Internet site management', and 'Additional child'.

A pop-up window titled 'S-보안관' (S-Security Guard) is overlaid on the bottom left. It has three main sections: 'Use time management' (highlighted in orange), 'App management', and 'Web Site Management'. The 'Use time management' section contains text: 'And child-installed apps and internet sites can use the time off (off time after setting [selection button]) and use time blocking specific apps are available at <app management> (*) hours off each day of the week. www.smartSheriff.kr'. Below this is a 'Parent-off time' section with a clock icon and a time range '00:00 ~ 06:00' displayed in a grey bar. A red 'X' button is next to the time range. The pop-up also includes a search bar with the text 'asd' and a 'Search' button.

Smart Sheriff / Cyber Safety Zone

- MOIBA didn't deprecate the API
- MOIBA renamed the app
- MOIBA is trying to hide the issues

But what is up with Smart Dream?



The new MOIBA – Login for Parents

로그인 Login 자녀의 스마트폰에 사이버안심존 / 스마트안심드림을 설치하셨다면 설치 시 등록된 부모님의 휴대전화번호와 비밀번호를 입력하시면 로그인 할 수 있습니다. ✕



— 유해정보차단 & 중독예방 **사이버안심존** 이용하기 —

부모님 휴대폰 전화

010 - -

비밀번호

로그인

[회원가입](#) | [비밀번호찾기](#)



— 사이버언어폭력 감지&알림 **스마트안심드림** 이용하기 —

부모님 휴대폰 전화

010 - -

비밀번호

로그인

[회원가입](#) | [비밀번호찾기](#)



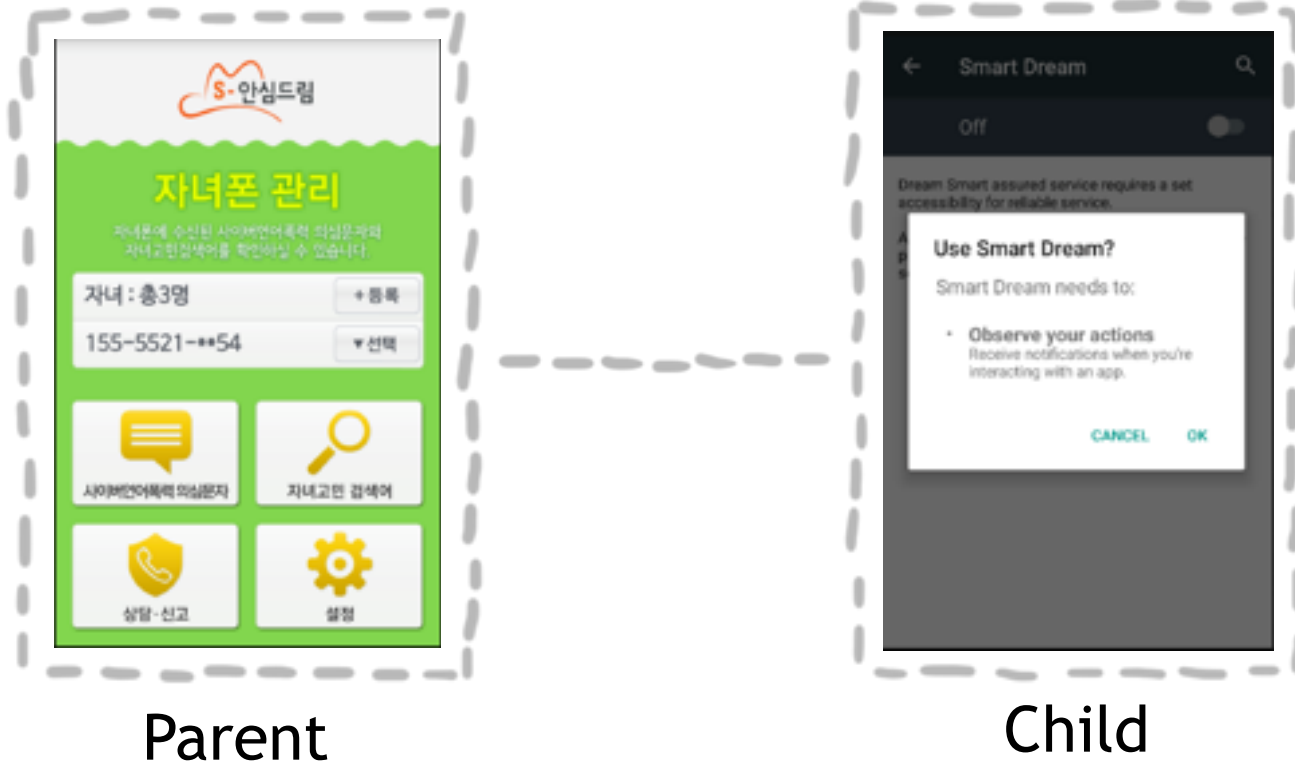
Smart Sheriff / Cyber Safety Zone



Smart Dream

Smart ~~Dream~~ Nightmare

- **Parent-Mode:** Check messages and searches containing dangerous words
- **Child-Mode:** Monitoring SMS/KakaoTalk and google searches. installs as accessibility service



How do they read KakaoTalk?

- **Very clever solution** - request accessibility permissions
- Abusing functionality intended for text2speech, ...

Dream Smart assured service requires a set accessibility for reliable service.

Web Interface – Smart Dream

The screenshot displays the '사이버안심존' (Cyber Safe Zone) web interface. The browser address bar shows the URL: `sd.moiba.or.kr/SmartDream/mng_child/child_trouble_list.do`. The page features a header with the site logo and navigation links: '사이버안심존', '스마트안심드림', '자녀 폰 관리' (Child Phone Management), and '고객지원' (Customer Support). A large banner image depicts a family scene with a violin and a book.

The main content area is titled '자녀 폰 관리' (Child Phone Management) and '사이버안심존 - 자녀 폰 관리'. It includes a sub-header: '자녀 스마트폰이 아이폰인 경우 인허넷사이트관리, 자녀주거만 이용가능' (If the child's smartphone is an iPhone, it can be used only for the Inhetnet site management and child's residence). The interface has three tabs: 'Cyber harass suspected inquiry letter', 'Views Keywords child worries' (which is active), and 'Add Child'.

Below the tabs, there is a text block: 'Cyber verbal abuse is suspected character list, ※ character storage period is 30 days. However, the historical character cyber harass doubt confirming in the parent app can be held until cleared.' This is followed by a 'Select Child' dropdown menu and a '선택' (Select) button.

The 'Receive History' section shows 'Total 0건' (Total 0 cases). Below this is a table with columns: 'No.', 'Pause detection', 'keyword', and 'Results confirmed'. The table is currently empty, with a message 'There is no detection search.' displayed below it. A 'delete' button is located at the bottom right of the table area.

Smart Dream Nightmare

Parent App monitoring SMS

☰

155-5521-**54

🔔

사이버언어폭력 의심문자 : 총 0/2건

※Suspicious letter to let you know my parents are preferable to judgment after checking the entire text content because extracting only a word that implies abusive, bullying, extortion, etc...

발신자 : *****56
수신건 : 0건 (총 2건)
최근수신일자 : 2016-05-11 00:08:44

• Character information

📱

2016-05-11 00:08:44 폭언(ac)
teacher whispering 헐박 to herself today?

📱

2016-05-11 00:07:13 헐박(되겠)
되겠

Parent Web Backend

사이버안심드림

자녀 폰 관리
Management for Children

사이버안심드림

자녀 폰 관리

자녀 스마트폰이 악의적인 경우 인터넷 사이트관리, 자녀추가할 이용가능

사이버언어폭력 의심문자 조회

자녀 42명 검색어 조회

자녀 추가

사이버언어폭력 의심문자 리스트입니다.
※ 문자보관 기간은 30일입니다. 단, 부모앱에서 확인하신 사이버언어폭력 의심문자내역은 삭제전까지 보존가능합니다.

자녀 선택

155-5521-**54

선택

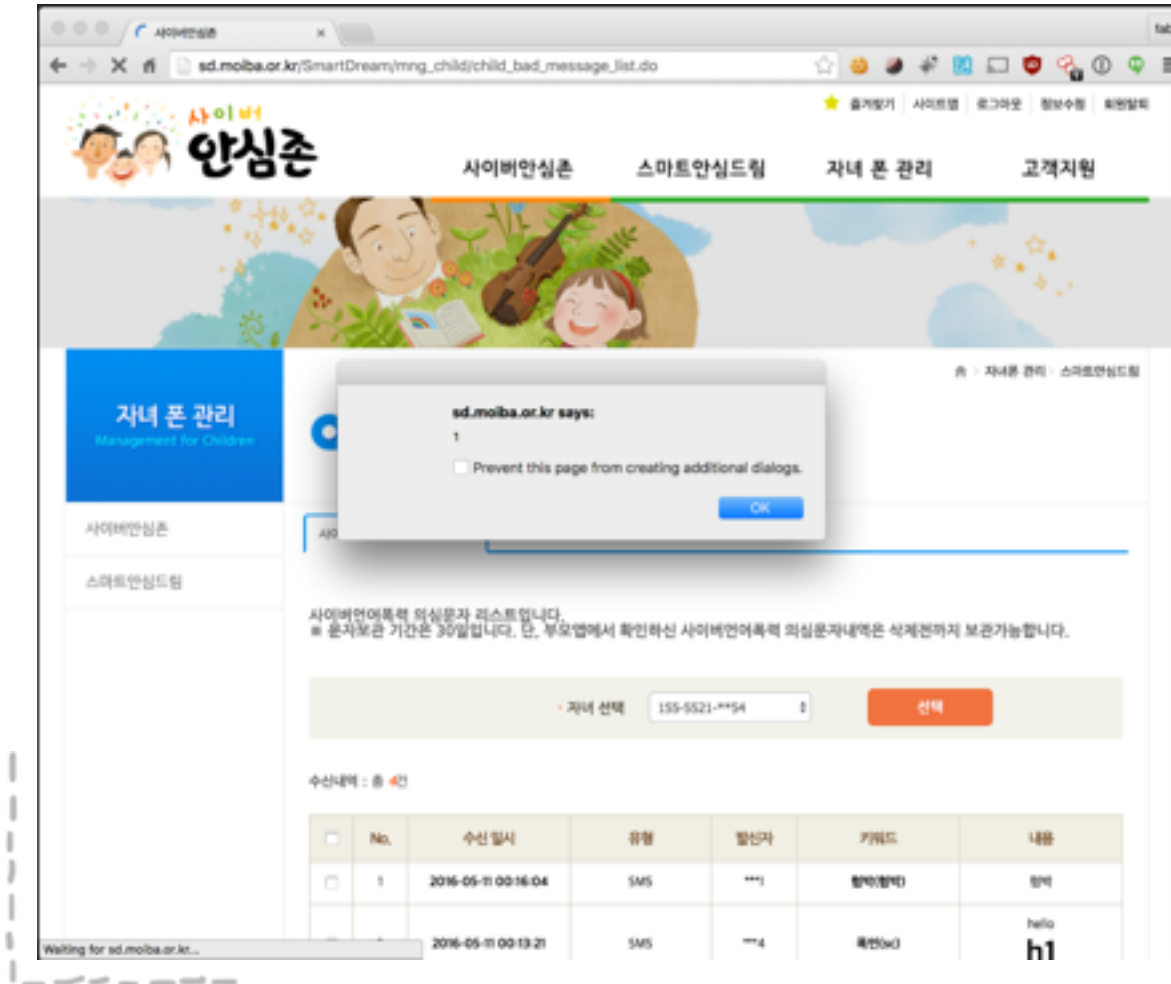
수신내역 : 총 4건

☐	No.	수신 일시	유형	발신자	키워드	내용
☐	1	2016-05-11 00:16:04	SMS	***1	헐박(헐박)	헐박
☐	2	2016-05-11 00:13:21	SMS	***4	폭언(ac)	hello h1
☐	3	2016-05-11 00:13:08	SMS	***4	폭언(ac)	hello h1
☐	4	2016-05-11 00:07:13	SMS	*****56	헐박(되겠)	되겠

삭제

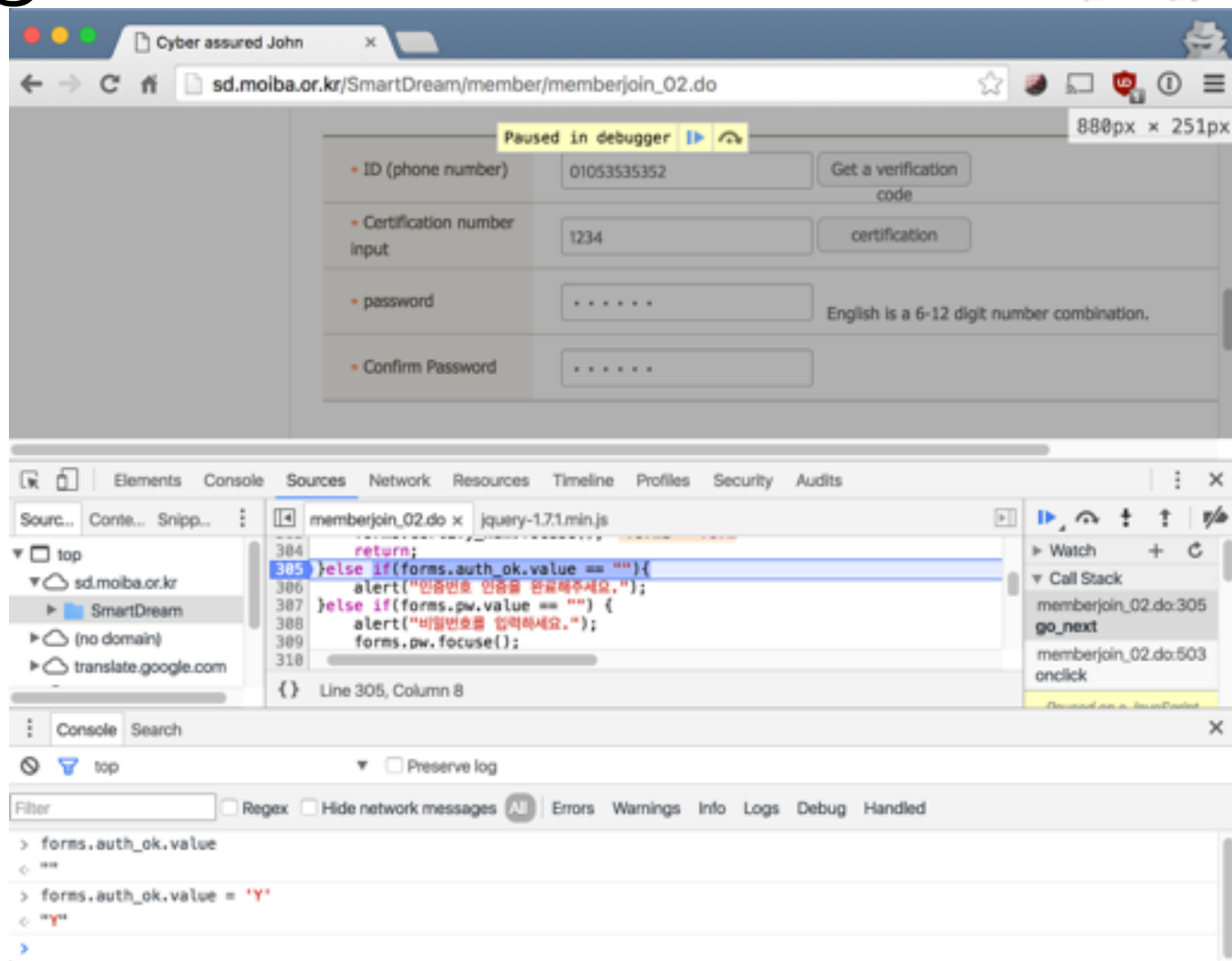
guess why the
h1 is so big ;)

Smart Dream Nightmare



XSS via SMS/KakaoTalk messages (no authentication)... and no SSL?

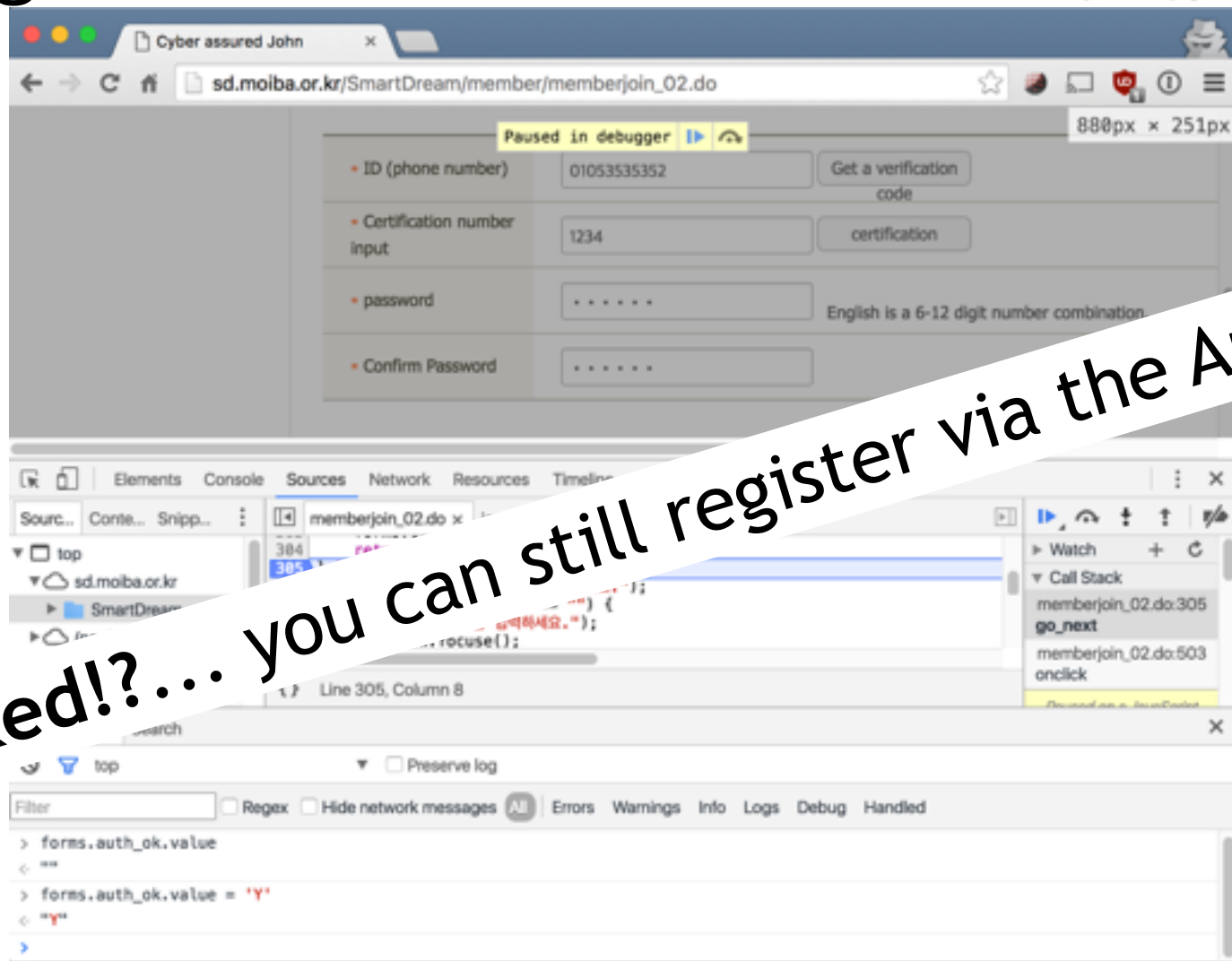
Register an account



Korean number needed. And wait for verification SMS...
Or simply change `forms.auth_ok.value = "1"`

Register an account

Fixed!?... you can still register via the App 🤔



Korean number needed. And wait for verification SMS...
Or simply change `forms.auth_ok.value = "1"`

+700k Messages from +55k Children

```
root@redstar-os $ python nightmare.py
```

```
### Messages from Child:
```

```
From: ".인터넷" (5)
```

1. [KakaoTalk] (violence/gang up): "투명성성인기회"
2. [KakaoTalk] (blackmail/money): "깡패?"
3. [KakaoTalk] (violence/맞다): "한!!국교!!"
4. [KakaoTalk] (blackmail/빌려달라): "보안어린이개방성사랑정?"
5. [KakaoTalk] (threat/kill): "성인성인괴상한해킹비밀한국성인강남스타일모바일,,

```
From: ".사이버억압♡" (2)
```

1. [KakaoTalk] (rant/crazy girl acting as child): "투명♡♡"
2. [KakaoTalk] (abuse/fuck it): "비 밀사 이버비? 밀번역 조 화정부 기 회개인 성 인 어린이정 ..."

```
From: "010XXXXXXX" (3)
```

1. [SMS] (harass/desperate): "어린이강남스?타일인터넷"
2. [SMS] (harass/): "깡패구글괴상한"
3. [SMS] (harass/desperate): "부패교육감?"

```
From: ".사이버투♥" (3)
```

1. [KakaoTalk] (threat/kill): "해킹 평등"
2. [KakaoTalk] (harass/desperate): "자 기 검열보?"
3. [KakaoTalk] (violence/gang up): "강남스타일!!!"

↑
tagged
meaning

↑
some fake messages.
But that's how it would look like

1. samuirai@redstar-os: ~/pentest/2015_10_smartsherif (zsh)

(2015_10_smartsherif)samuirai@redstar-os ~/pentest/2015_10_smartsherif » python smart_nightmare.py



The Most Offensive Slide :O



The 1086 "*harmful*" words that are monitored by smart dream

The Most Offensive Slide :O

Example words:

divorce, single parent,
remarriage, adoption,
earn money, *multiculturalism*,
menstruation, breast, stress,
I hate ..., girlfriend, boyfriend,
break up, dating, lie, *beer*,
person/friend/guy/girl I like,
r-rated, sex, discrimination,
black history, going to school,
borrow, *sarcasm*, fanboy,
gangster, disability,
reporting to police, ...



The 1086 "harmful" words that are monitored by smart dream

MOIBA's guide to fixing vulns

issue	fix plan
Lack of Authentication	Important parameters will be encrypted with AES256
Hardcoded API key	1. Put API key into NDK binaries 2. Each user get's own key
XSS with messages	Before sending SMS message, escape and replace special chars

Another big pile of

- XSS
- No SSL
- Lack of Authentication and Authorization
- Accessing stored messages and searches
- ...

But what about the other apps?



T 청소년유해차단

SKTelecom 라이프스타일

★★★★★ 173 호

USK: 전체이용가

기기가 없습니다.

위시리스트에 추가

설치



올레 자녀폰안심 프리

KT Corporation 라이프스타일

★★★★★ 2,050 호

USK: 전체이용가

기기가 없습니다.

위시리스트에 추가

설치



U+ 자녀폰 지킴이

LG유플러스(LG Uplus Corporation) 라이프스타일

★★★★★ 501 호

USK: 전체이용가

기기 호환성 로드 중...

위시리스트에 추가

설치

But what about the other apps?



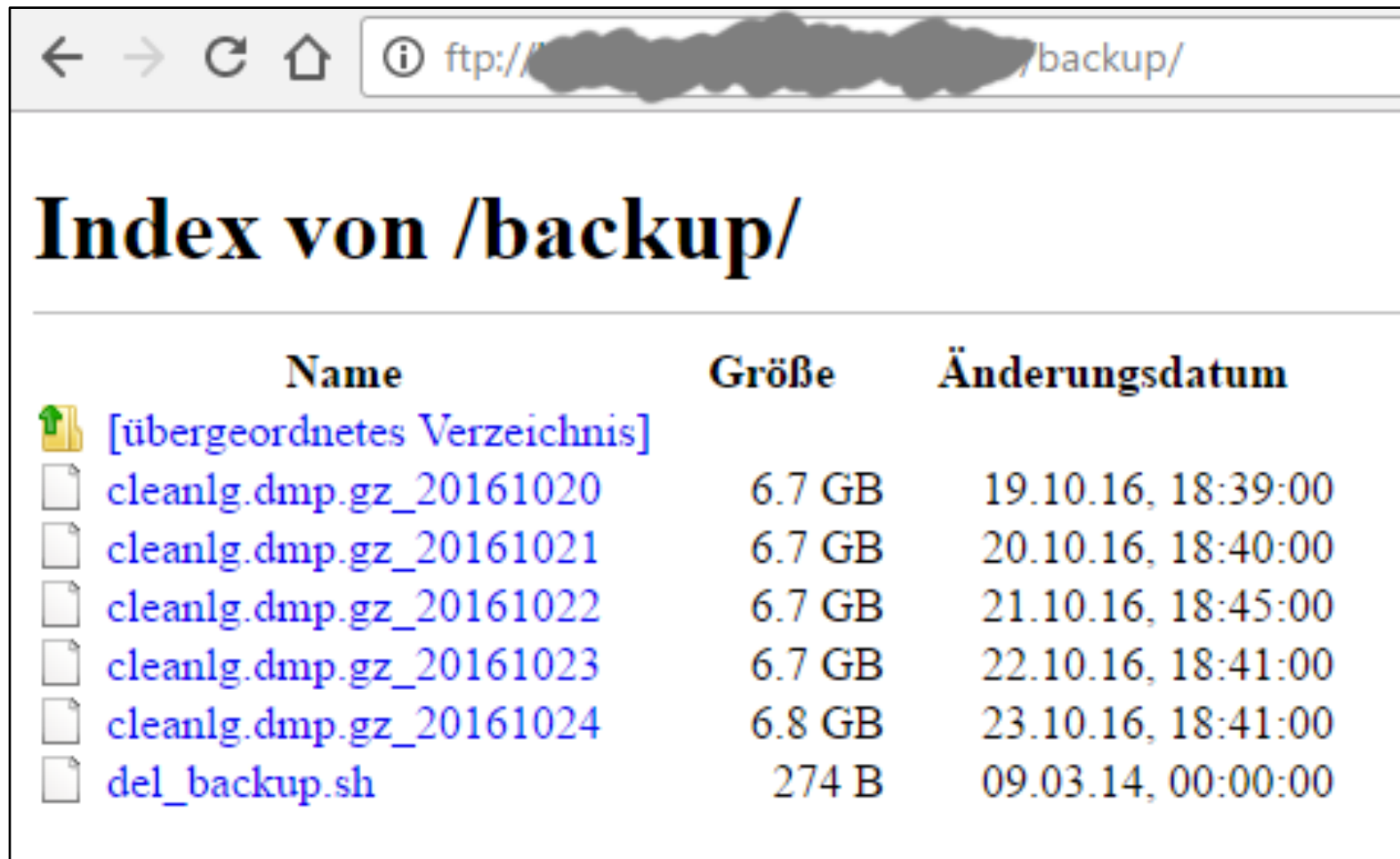
We love you too, Plantynet ❤️

Found as a string inside a Java class:

`DamnYouHackerwHAt1sy0UrBENefitwhEnDeComPil2Th1saPpplEas2DOn0td1sTurbUs`

“Damn You Hacker what is your benefit when decompile this app please dont disturb us”

... guess why they don't want people looking



Index von /backup/		
Name	Größe	Änderungsdatum
 [übergeordnetes Verzeichnis]		
 cleanlg.dmp.gz_20161020	6.7 GB	19.10.16, 18:39:00
 cleanlg.dmp.gz_20161021	6.7 GB	20.10.16, 18:40:00
 cleanlg.dmp.gz_20161022	6.7 GB	21.10.16, 18:45:00
 cleanlg.dmp.gz_20161023	6.7 GB	22.10.16, 18:41:00
 cleanlg.dmp.gz_20161024	6.8 GB	23.10.16, 18:41:00
 del_backup.sh	274 B	09.03.14, 00:00:00

SKTelecom



T 청소년유해차단

SKTelecom 라이프스타일

★★★★★ 173 호

USK: 전체이용가

기기가 없습니다.

위시리스트에 추가

설치



올레 자녀폰안심 프리

KT Corporation 라이프스타일

★★ 2,050 호

USK: 전체이용가

기기가 없습니다.

위시리스트에 추가

설치



U+ 자녀폰 지킴이

LG유플러스(LG Uplus Corporation) 라이프스타일

★★ 52 호

USK: 전체이용가

기기가 없습니다.

위시리스트에 추가

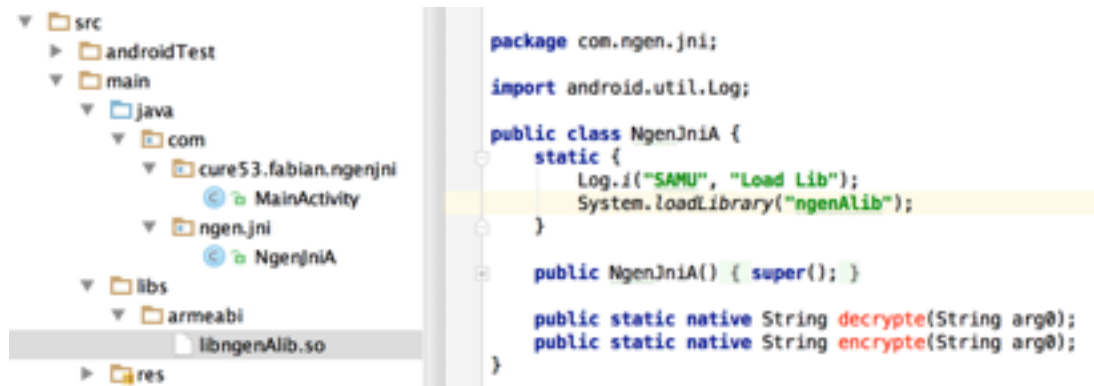
설치

SKT Corporation

- Encrypted/obfuscated application implemented via native library 

Defeat Obfuscation – Lame Strategy

- Encrypted/obfuscated application implemented via native library



```
Log.i("SAMU3", "Load Lib");
Log.i("SAMU3", NgenJniA.decrypte("sEeZQsl1M8sH8gtneZRU0Q3Rh1ZiEbBtGDx7qsr4o/hqv2ZFy8AL8pg7PErE9IVlgZ6/dB5VbgA="));
Log.i("SAMU3", NgenJniA.decrypte("LAhRhoz+RbuY6LoFOH4Jhtrr/86Smt0Li2iB1YvKaI6NRaN9xRrm6XzjK5CroC/eYgGz0/9mhNaVC2ByN
Log.i("SAMU3", NgenJniA.decrypte("Rlp0mMdnYtB1R3KblIJEQ8pG4nKCANTe12iB1YvKaI6NRaN9xRrm6faN0MMMQ05o4PvETMTvH+KfLLiU
Log.i("SAMU3", NgenJniA.decrypte("A052XK+Ukh0oY9Dq547kiETTj/JpBryS5jW4tFAaDFjMthTo4mhbNLgY7cyKrm2NiVvdKwPIPE="));
Log.i("SAMU3", NgenJniA.decrypte("hrYzXZ/h+3CM+X3E5LPwHdoAia9WxIwVlyP57ZFb4F50p+T+h8vX6egoLCqskfHp653KTSFitKJ0ZGtL
Log.i("SAMU3", NgenJniA.decrypte("Ru224e7qk/0rg5a2hnsEib9RxcA7eICG0A4UX1/X3W5w/2kmMhXZM0jasHsjD0ZiX2twyBplZo4Z3xY/d
Log.i("SAMU3", NgenJniA.decrypte("JwvGSj5Qd+eJy4PAqjbTz8BeXyBd/W/dG1IzD4/Xqg8Ht3scik395MAzHt3mS1kgqN2dXw+4Jsg="));
Log.i("SAMU3", NgenJniA.decrypte("5qjN4pWfTw0LEQH4/qmkVgmu98sL0pf60A4UX1/X3W5w/2kmMhXZM0sm47jS7FebsatAmdTHIDQ4dAT0
Log.i("SAMU3", NgenJniA.decrypte("06/kSNpbY18n463AB55f0Q/C45m0mZpyF5f+HcLbsfH/lxoiWYzG2gyp8jLiBAx10Ad4oneuGrom"));
Log.i("SAMU3", NgenJniA.decrypte("i2lePtDCybnN9F9+LYK7Udm29d4E+0ilg7VfNiCN6u7d6GLzPQEKmfniURFaxAL1Nvq4ESF8zqpQ1P67
Log.i("SAMU3", NgenJniA.decrypte("9Zv577n6LP4uMXABxnDNTvGjuuPSf/LDF5f+HcLbsfH/lxoiWYzG2jH4i2PEsStfeRC/BI+Qi20="));
Log.i("SAMU3", NgenJniA.decrypte("wtIUhPh5IvTBsTwg5W68/onBsMc2zA2bvTR5BCDwFbfl6JvJphlCA+i21qsXp0ufo/hexpZslQ="));
Log.i("SAMU3", NgenJniA.decrypte("SjMIztB1DvmAwR0giBDg3Cl6xsGjWEjRFSf+HcLbsfH/lxoiWYzG2hMH/oGf7ZoeWDAiqopCdM="));
```

Defeat Obfuscation – Cool Strategy

- Jeff from CitizenLab reverse engineered the binary



- AES key unwrapping (RFC 3394)
- PBKDF2 HMAC
- AES ECB

```
1 #!/usr/bin/env python3
2 import base64, hashlib, struct
3 from Crypto.Cipher import AES
4
5 MASKS = [0x23, 0xF5, 0xC8, 0x90, 0x3C, 0x88, 0x1A, 0x0A,
6          0xA3, 0x5B, 0xD2, 0x33, 0x98, 0x1E, 0xF5, 0xD7]
7
8 SALT = b'\xb9\x89\x0c\xa27\x127\x06c\x127\x09f|\xab\xad\x1c\x01'
9
10 DBLE = struct.Struct('>I')
11 QUAD = struct.Struct('>Q')
12
13 def aes_unwrap(kek, wrapped, iv=0xa6a6a6a6a6a6a6a6):
14     # AES key unwrapping as defined in RFC 3394
15     # Code derived from https://gist.github.com/doublereedkurt/4173118
16     n = len(wrapped) // 8 - 1
17     R = [wrapped[i * 8 : i * 8 + 8] for i in range(1, n + 1)]
18     A = QUAD.unpack(wrapped[:8])[0]
19     cipher = AES.new(kek)
20     for j in range(5, -1, -1):
21         for i in range(n, 0, -1):
22             ciphertext = QUAD.pack(A ^ (n * j + 1)) + R[i - 1]
23             B = cipher.decrypt(ciphertext)
24             A = QUAD.unpack(B[:8])[0]
25             R[i - 1] = B[8:]
26     if A != iv:
27         raise RuntimeError('AES unwrap integrity check failed')
28     return b''.join(R)
29
30 def decrypt(string):
31     buf = base64.b64decode(string)
32     unwrapped_aes_key = buf[:24]
33     password = bytes(b ^ m for b, m in zip(buf[24:40], MASKS))
34     password_encoded = base64.b64encode(password)
35     kek = hashlib.pbkdf2_hmac('sha1', password_encoded, SALT, 18, 16)
36     unwrapped_aes_key = aes_unwrap(kek, unwrapped_aes_key)
37     unwrapped_aes_key_encoded = base64.b64encode(unwrapped_aes_key)
38     aes_key = hashlib.pbkdf2_hmac('sha1', unwrapped_aes_key_encoded, SALT, 18, 16)
39     cipher = AES.new(aes_key, AES.MODE_ECB)
40     plain = cipher.decrypt(buf[40:])
41     padding = plain[-1]
42     if 0 < padding <= 16 and all(b == padding for b in plain[-padding:]):
43         plain = plain[:padding]
44     else:
45         raise RuntimeError('Invalid padding\n')
46     plain = plain.rstrip(b'\x00')
47     plain_decoded = base64.b64decode(plain)
48     return plain_decoded.decode('utf-8')
49
50 if __name__ == '__main__':
51     import sys
52     string = sys.stdin.read()
53     print(decrypt(string))
54
```

SKTelecom - Issues

- No HTTPS
- XSS



A note for reflexion

- Take a step back
- Imagine these apps were magically 100% secure
- Would you trust **any company or government...**
- **... to have a database with all that information?**
 - Phone usage statistics (times, apps)
 - SMS/IM Messages
 - Knowing family associations
 - Names and birthdays



What is happening next?

- The Korean government proposed a new bill to make opt-out possible
- OpenNet Korea submitted a constitutional complaint about the law
 - final decision in 2-3 years
- Should there be regulations for parental/child-protection apps?
 - eg. no cloud service, only local

Reports

- *[20 September 2015]* Are the Kids Alright? Digital Risks to Minors from South Korea's Smart Sheriff Application - <https://citizenlab.org/2015/09/digital-risks-south-korea-smart-sheriff/>
- *[1 November 2015]* The Kids are Still at Risk: Update to Citizen Lab's "Are the Kids Alright?" Smart Sheriff report - <https://citizenlab.org/2015/11/smart-sheriff-update/>
- *[21 September 2015]* Submission to the 113th Session of the UN Human Rights Committee for Fourth Periodic Report of the Republic of Korea - http://opennetkorea.org/en/wp/wp-content/uploads/2016/03/INT_CCPR_KOR_OPEN_NETSmart-Sheriff.pdf

Some News Articles

- *[19 May 2015]* Don't text 'beer' in Korea: Words that trigger teen alerts - <http://www.japantimes.co.jp/news/2015/05/19/asia-pacific/dont-text-beer-korea-words-trigger-teen-alerts/>
- *[16 June 2015]* South Korea provokes teenage smartphone privacy row - <http://www.bbc.com/news/technology-33091990>
- *[21 September 2015]* Smart Sheriff child surveillance app leaves South Korean kids vulnerable to hackers - <http://www.cbc.ca/news/technology/smart-sheriff-1.3236682>

Questions/Comments/ Discussion



Abraham Aranguren (@7a_) - abraham@cure53.de

Fabian Fäßler (@samuirai) - fabian@cure53.de

Reports: <https://cure53.de/#publications>



CURE53