Abusing Notification Services on Smartphones for Phishing and Spamming

Zhi Xu and Sencun Zhu
Department of Computer Science and Engineering
Pennsylvania State University
Outline

- Notification service
- Notification-based phishing attack
- Notification-based spam attack
- Attack on different platforms
- Defense mechanisms
Notification service

- Types of notification service
Types of notification service

- Pop-up notification
  - *Toast* on Android
  - *Dialog* on BlackBerry OS
  - *Alert* on iOS 5
  - *ShellToast* on Windows Phone 7
Types of notification service

- Pop-up notification
- Status bar notification
  - Status Bar notification on Android
  - Message List on BlackBerry OS
  - Notification Center on iOS 5
Notification service

- Types of notification service
  - Pop-up notification
  - Status bar notification
  - Icon notification
    - *Icon* on BlackBerry OS
    - *Badge* on iOS 5
    - *Tile* on Windows Phone 7
Notification service

- Types of notification service
  - Pop-up notification
  - Status bar notification
  - Icon notification
    - *Icon* on BlackBerry OS
    - *Badge* on iOS 5
    - *Tile* on Windows Phone 7
  - We will focus on
    - Pop-up notification
    - Status bar notification
Notification service (cont.)

- Notification customization
  - Trigger event
    - E.g., scheduled alarms, intent (ACTION_SCREEN_ON, BOOT_COMPLETED)
  - Notification view
    - E.g., text message, image and subviews
  - Allowed user operation
    - Operations which the user can perform on the displayed notification
    - The invoked actions of these operations
Concerns

- The sender application is anonymous
  - Authentication information is not mandatory
**Concerns**

- The sender application is anonymous
  - Authentication information is not mandatory
- The three aspects are all controlled by the sender application
  - Fabricate the notification view at will
  - Control the allowed user operations
Notification service (cont.)

- **Concerns**
  - The sender application is anonymous
    - Authentication information is not mandatory
  - The three aspects are all controlled by the sender application
    - Fabricate the notification view at will
    - Control the allowed user operations
  - An installed trojan app may use the notification service
    - Phishing attacks
    - Spam attacks
Goal

- To steal the user’s credentials for other installed applications, e.g., Facebook
**Goal**

- To steal the user’s credentials for other installed applications, e.g., Facebook
Notification-based phishing attack

- **Goal**
  - To steal the user’s credentials for other installed applications, e.g., Facebook
Goal

✓ To steal the user’s credentials for other installed applications, e.g., Facebook
**Goal**

- To steal the user’s credentials for other installed applications, e.g., Facebook

---

*E.g., to start the genuine Facebook app with intent:*

```java
intent.setClassName("com.facebook.katana", "com.facebook.katana.LoginActivity");
```
Difficult to notice the attack for the user
Notification-based spam attack

Goal

✓ To send spam notifications while hiding its identity from the user
**Notification-based spam attack**

- **Goal**
  - To send spam notifications while hiding its identity from the user

- **Using toasts**
  - Last for several seconds
  - Disappear automatically
  - No action allowed by the user
Notification-based spam attack (cont.)

- Using status bar notifications
  - Can even lead the user to a spam website when he tap on the notification view

![Notification example]

- Tens of thousands of satisfied customers worldwide.
- Get FREE Drug HERE
- This is a fake spam webpage for testing

![Spam website example]
Attack on different platforms

- Keys to the success of proposed attacks
  - Being able to send anonymous notifications
  - Being able to navigate the user to fraudulent views
Attack on different platforms

- Keys to the success of proposed attacks
  - Being able to send anonymous notifications
  - Being able to navigate the user to fraudulent views

- Summary of experimental results on different platforms

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Send Anonymous Notifications</th>
<th>Navigate To Fraudulent View</th>
</tr>
</thead>
<tbody>
<tr>
<td>Android 2.3</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Android 4.0</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>BlackBerry OS 7</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>iOS 5</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Jailbroken iOS 5</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Windows Phone 7.1</td>
<td>X</td>
<td>✔</td>
</tr>
</tbody>
</table>
Attack on different platforms

- Successful on BlackBerry
  - Phishing attacks
Attack on different platforms (cont.)

- Successful on BlackBerry
  - Spam attacks
Failed on iOS and Windows Phone

- Reason: NO customization is allowed

*Notification Center on iOS*
Failed on iOS and Windows Phone

- Reason: NO customization is allowed

*Notification Center on iOS*

*ShellToast on WP*
Defense mechanisms

- Notification authentication is needed
Defense mechanisms

- Notification authentication is needed
- Proposed defense mechanisms
  - Semi-OS-Controlled Notification
Defense mechanisms (cont.)

- **SecureView framework**
  - E.g., user login view
  - E.g., password entering view
Defense mechanisms (cont.)

- **SecureView framework**
  - E.g., user login view
  - E.g., password entering view

- **Notification logging service**
**Discussion**

- **Distribute spam content after publishing the trojan app**
  - Through app update
  - Through push notification service
  - Through the background service
Discussion

- Distribute spam content after publishing the trojan app
  - Through app update
  - Through push notification service
  - Through the background service

- Jailbroken iOS
  - Notification customization is fully supported
Discussion

- Distribute spam content after publishing the trojan app
  - Through app update
  - Through push notification service
  - Through the background service

- Jailbroken iOS
  - Notification customization is fully supported

- Incentive of proposed attacks
  - Building and publishing a new trojan app is easy and cheap
  - Identifying the trojan app is difficult
Related Work

- Spam attack on smartphones
  - SMS-based
  - AirPush, a status bar notification based adware
Related Work

- **Spam attack on smartphones**
  - SMS-based
  - AirPush, a status bar notification based adware

- **Phishing attack on smartphones**
  - Abusing mobile browser and email client
  - Abusing the view transfer
Conclusion

- Notification authentication is critical for notification service
- It is feasible to launch notification based phishing attacks and spam attack on Android and BlackBerry
- To prevent proposed attacks, the notification view must include notification authentication information

Future work

- View authentication
Thank you!