Android apps in sheep's clothing

April 1\textsuperscript{st}, 2015
Tobias Ospelt, modzero AG
SIGS Special Event –
"It's not a joke - it can happen"
• 6 IT security experts
• We do all areas of technical HW & SW security analysis
  – Penetration Testing, Crypto, Web, embedded devices, etc.
Android

- Android has about 62% market share
We are going to see a User Interface (UI) attack today

History of UI attacks
Microsoft Windows 90ies overlay
Microsoft Windows 90ies overlay
Microsoft Windows 90ies overlay
Microsoft Windows 90ies overlay
Modern Windows Overlays

Remote Overlay Toolkit Makes Online Banking Fraud Easy

By Eduard Kovacs on January 14, 2015

A new toolkit discovered late last year by researchers at the Israeli antivirus company El dorado Cybersecurity has been used to launch online banking fraud campaigns and steal users’ financial information.

The toolkit, dubbed KL-Remote, is used for remote overlay attacks which enable cybercrooks to access online banking accounts directly from victims’ computers without raising too much suspicion.

The threat takes a screenshot of the banking website and displays it to the user. The cybercriminal then uses the tool to push a message on top of that image. The message is different for each website and it instructs victims to enter the information needed by the attacker to gain access to the banking account.
Browser Clickjacking

A malicious website presents a quiz: 97 + 3 = ? and 203 - 3 = ?. The user is directed to a logon page via a transparent iframe (not visible) at https://bank.com/logon. The iframe contains fields for Name: 100 and Password: 200. The user provides the answers and hits the "Next" button. All these clicks are hijacked by the invisible frame as its controls have higher (by default) Z order.
Android overlays

Chat while using other apps
Overlaying Android apps

Android apps in sheep's clothing
What

• Stealing credentials
  – When adding a Google account to Android
  – Or from all other apps with logins
    • Enterprise containers (Good, MobileIron, etc.)
    • Password safes
    • Social media, etc.

• Manipulating sensitive data that is displayed
  – Two-factor authentication mobile banking transaction signing
How

• What about sandboxing on the User Interface (UI) level?
Prerequisites for our attack

- Installed malware app on phone
- Permissions
  - GET_TASKS (must)
  - SYSTEM_ALERT_WINDOW (recommended but optional)
  - RECEIVE_BOOT_COMPLETED (optional)
  - INTERNET (optional)
Demo: Stealing Skype credentials
How did it work?

• Exactly when the Skype app is opening the login screen, we bring our app to the foreground and show our faked login screen
Bitte prüfen Sie

<table>
<thead>
<tr>
<th>ÜBERWEISUNG</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>IBAN</td>
<td>DE55555555555555555555555</td>
</tr>
<tr>
<td>BETRAG</td>
<td>1337,42 EUR</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>photoTAN</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7351946</td>
</tr>
</tbody>
</table>

Bitte geben Sie die TAN im Online-Banking ein, wenn die angezeigten Daten korrekt sind.
Enterprise containers – Example: MobileIron
Is it fixed?

Hint: won't fix
"[...] We don't consider this behavior to be a flaw in the Android security model. [...] the attack requires the victim to knowingly install an app that has permission to monitor foreground applications. [...] Google Play analyzes apps that get submitted [...] for phishing and other potentially harmful behavior. [...]"

...and analyzing for harmful behavior.

Let's talk about permissions...
Permission system is broken

• There is no opt-in/opt-out
  – Give it all permissions it wants or uninstall it

• Cyanogenmod (an alternative Android version) has permission opt-in/opt-out called "Privacy Guard". Why not on Android?
Facebook

needs access to

- Device & app history
- Identity
- Contacts/Calendar
- Location
  Uses the device's location
- SMS
- Phone
- Photos/Media/Files
- Camera/Microphone
- Wi-Fi connection information

ACCEPT
WHAT'S NEW

- Like posts, photos and Pages when you're offline
- Remove tags you've created
- Remove tags of yourself that your friends have created
WHAT'S NEW

- Like posts, photos and Pages when you’re offline
- Remove tags you've created
- Remove tags of yourself that your friends have created
Google is scanning for harmful behavior?

• What about other app stores?
• The malware app will be disguised as a legitimate app
  – Functionality will require those permissions
• Other malware made it in the Play store
• Our malware code can be loaded after the app is already in the store
Talking about quality assurance in the Google Play store...
"Given a choice between dancing pigs and security, users will pick dancing pigs every time."

– Edward Felten (Securing Java)
Demo: I just couldn't resist

Dancing pig
stefan meier

INSTALL

Personalisation  Similar

This is a very cute dancing pig showing whenever you are not in an app

READ MORE
I just couldn't resist

• Uploaded yesterday
• This particular demo works only on LG g3 with Android 5
• Download the malware:
I just couldn't resist
Is the attack still feasible on Android 5?
Demo: Android 5.0.2 (verified on 5.1)
What about BlackBerry?
Blackberry

• Blackberry supports Android apps
• You can attack another Android app on Blackberry
  – With our technique you are not able to figure out which native Blackberry app is in the foreground
Blackberry

Hello, I'm just a cool app. That means I'm usually a game or a torch app. But just for you, may I present, my loot: lootCollector?app=skype&username=fffff&password=bbbbbb

lootCollector?app=skype&username=lalala&password=fugu

lootCollector?app=skype&username=test123&password=test123

---
a totally cool app

Sign in

1 2 3 4 5 6 7 8 9 0
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M

Blackberry
Blackberry – spot the permission difference

Do you want to install this application?

**PRIVACY**
- Take pictures and videos

**DEVICE ACCESS**
- Full network access
- Retrieve running apps
- Run at startup
- Draw over other apps

---

**a totally cool app**

Do you want to install this application?

**PRIVACY**
- Take pictures and videos

**DEVICE ACCESS**
- Full network access
- Retrieve running apps
- Run at startup
- Draw over other apps

---

**a totally cool app**

Do you want to install this application?

**PRIVACY**
- Take pictures and videos

**DEVICE ACCESS**
- Full network access
- Retrieve running apps
- Run at startup
- Draw over other apps

---

**Kamera**

Erlaubt der App, Bilder aufzunehmen, Videos aufzuzeichnen und den Blitz zu verwenden.

**Freigegebene Dateien**


Sie können jederzeit die Seite "Sicherheit" in den "Systemeinstellungen" aufrufen, um Ihre Berechtigungen anzuzeigen.
Countermeasures

• If you have a HTML5 app (one WebView) the attack is "harder"
  – Android 5 situation on all Android versions
Summary

• Is this technique rocket-science? Not at all
• Does it matter? Yes, the impact is huge
• Android app separation is broken
  – Don't trust the sandboxing promises
• Bring-your-own-device is still a bad idea from a security perspective
  – private apps and business apps/data
• Come and play with devices here at the front
Thank you

- Twitter: @floyd_ch
- Twitter: @mod0
- http://floyd.ch