Investigating User Privacy in Android Ad Libraries

Ryan Stevens, Clint Gibler, Jon Crussell, Jeremy Erickson
Hao Chen

UC Davis Computer Security Lab
Motivation
Motivation
Motivation

Previous work has focused on the trustworthiness of application code:

- TaintDroid - Enck, “OSDI 2010”
- AndroidLeaks - Gibler, “Trust 2012”
Motivation

But what about ad code?
Goals

• Identify unique privacy concerns in Android app advertising
• Discover privacy threats resulting from these concerns
• Analyze popular Android ad libraries for these threats
• Propose guidelines to alleviate these threats
Goals

- Identify unique privacy concerns in Android app advertising
Goals

- Identify unique privacy concerns in Android app advertising
- Discover privacy threats resulting from these concerns
Goals

- Identify unique privacy concerns in Android app advertising
- Discover privacy threats resulting from these concerns
- Analyze popular Android ad libraries for these threats
Goals

• Identify unique privacy concerns in Android app advertising

• Discover privacy threats resulting from these concerns

• Analyze popular Android ad libraries for these threats

• Propose guidelines to alleviate these threats
Permissions

- Specified by the application
Permissions

• Specified by the application

• Allows the app to access privileged device functionality
Permissions

• Specified by the application

• Allows the app to access privileged device functionality

• Examples of permissions are:
  • INTERNET
Permissions

- Specified by the application

- Allows the app to access privileged device functionality

- Examples of permissions are:
  - INTERNET
  - ACCESS_FINE_LOCATION
Permissions

- Specified by the application

- Allows the app to access privileged device functionality

- Examples of permissions are:
  - INTERNET
  - ACCESS_FINE_LOCATION
  - ACCESS_NETWORK_STATE
Application Advertising

App APK

Ad Library SDK
Application Advertising

- App APK
- Ad Library
- SDK
- Ad Server
- Ad Request
Application Advertising

Diagram:

- **App APK**
- **Ad Library SDK**
- **Ad Server**

Flow:
- **Ad Request** from **Ad Server** to **Ad Library SDK**
- **Advertisement** from **Ad Library SDK** to **App APK**
Threat Model

Device

Profile Data
(Device ID, GPS, phone type...)

Internet

Ad Provider
Threat Model - Unscrupulous Ad Provider

Device -> Internet

Profile Data
(Device ID, GPS, phone type...)

Internet -> Ad Provider
Threat Model - Network Snooper

Device

Profile Data
(Device ID, GPS, phone type...)

Internet

Network Snooper

Ad Provider
Unique Privacy Concerns in Android App Advertising

1. No privilege separation between app and ad code
   • No same origin policy

2. Greater access to detailed user data
   • SMS, calendar, etc.

3. More persistent user identifiers
   • UDIDs – ANDROID ID, DEVICE ID (IMEI, MEID, ...)
   • More persistent than Web cookies and IP addresses
Unique Privacy Concerns in Android App Advertising

1. No privilege separation between app and ad code
   - No *same origin policy*
Unique Privacy Concerns in Android App Advertising

1. No privilege separation between app and ad code
   - No *same origin policy*

2. Greater access to detailed user data
   - SMS, calendar, etc.
Unique Privacy Concerns in Android App Advertising

1. No privilege separation between app and ad code
   - No *same origin policy*

2. Greater access to detailed user data
   - SMS, calendar, etc.

3. More persistent user identifiers
   - UDIDs – `ANDROID_ID`, `DEVICE_ID` (IMEI, MEID, ...)
   - More persistent than Web cookies and IP addresses
Unique Privacy Concerns in Android App Advertising

1. **No privilege separation between app and ad code**

2. Greater access to detailed user data

3. More persistent user identifiers
Undocumented Permissions

- Required
- Optional

Ad Provider Documentation
Undocumented Permissions

* A.P. Felt et al. *Android Permissions Demystified*. “CCS 2011”
Undocumented Permissions

* A.P. Felt et al. *Android Permissions Demystified*. “CCS 2011”
## Undocumented Permissions

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>admob (4.3.1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>inmobi (3.0.1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>millenialmedia (4.5.1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mobclix (3.2.0)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>smaato (2.5.4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Undocumented Permissions

<table>
<thead>
<tr>
<th>Ad Library (version)</th>
<th>INTERNET</th>
<th>ACCESS_NET_STATE</th>
<th>READ_PHONE_STATE</th>
<th>ACCESS_LOCATION</th>
<th>CAMERA</th>
<th>READ CALENDAR</th>
<th>WRITE CALENDAR</th>
<th>READ CONTACTS</th>
<th>WRITE CONTACTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>admob (4.3.1)</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>inmobi (3.0.1)</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>millennialmedia (4.5.1)</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mobclix (3.2.0)</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>smaato (2.5.4)</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

R = Required
## Undocumented Permissions

<table>
<thead>
<tr>
<th>Ad Library (version)</th>
<th>INTERNET</th>
<th>ACCESS_NET_STATE</th>
<th>READ_PHONE_STATE</th>
<th>ACCESS_LOCATION</th>
<th>CAMERA</th>
<th>READCALENDAR</th>
<th>WRITECALENDAR</th>
<th>READCONTACTS</th>
<th>WRITECONTACTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>admob (4.3.1)</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>inmobi (3.0.1)</td>
<td>R</td>
<td>O</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>millennialmedia (4.5.1)</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mobclix (3.2.0)</td>
<td>R</td>
<td>O</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>smaato (2.5.4)</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

R = Required  O = Optional
# Undocumented Permissions

<table>
<thead>
<tr>
<th>Ad Library (version)</th>
<th>INTERNET</th>
<th>ACCESS_NET_STATE</th>
<th>READ_PHONE_STATE</th>
<th>ACCESS_LOCATION</th>
<th>CAMERA</th>
<th>READ_CALENDAR</th>
<th>WRITE_CALENDAR</th>
<th>READ_CONTACTS</th>
<th>WRITE_CONTACTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>admob (4.3.1)</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>inmobi (3.0.1)</td>
<td>R</td>
<td>O</td>
<td>O</td>
<td>O</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>millennialmedia (4.5.1)</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mobclix (3.2.0)</td>
<td>R</td>
<td>O</td>
<td>R</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>smaato (2.5.4)</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>O</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

R = Required  \hspace{1cm} O = Optional  \hspace{1cm} X = Undocumented
Unique Privacy Concerns in Android App Advertising

1. No privilege separation between app and ad code

2. Greater access to detailed user data

3. More persistent user identifiers
Private Data on the Network

**Goal:** Discover if private data is sent in ad requests
Private Data on the Network

**Goal:** Discover if private data is sent in ad requests

**Method:** Observed ad requests from each library in
- Android emulator
- Live traffic
## Private Data on the Network

<table>
<thead>
<tr>
<th>Ad Library (version)</th>
<th>App Package Name</th>
<th>GPS Coordinates</th>
<th>Connection Type</th>
<th>Device Make and Model</th>
<th>Wireless Carrier</th>
<th>Age</th>
<th>Gender</th>
<th>Income Level</th>
<th>Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>admob (4.3.1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>inmobi (3.0.1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>millennialmedia (4.5.1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mobclix (3.2.0)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>smaato (2.5.4)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Private Data on the Network

<table>
<thead>
<tr>
<th>Ad Library (version)</th>
<th>App Package Name</th>
<th>GPS Coordinates</th>
<th>Connection Type</th>
<th>Device Make and Model</th>
<th>Wireless Carrier</th>
<th>Age</th>
<th>Gender</th>
<th>Income Level</th>
<th>Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>admob (4.3.1)</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>inmobi (3.0.1)</td>
<td>A</td>
<td></td>
<td>A</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>millennialmedia (4.5.1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mobclix (3.2.0)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>smaato (2.5.4)</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\(A = \text{Always automatically}\)
## Private Data on the Network

<table>
<thead>
<tr>
<th>Ad Library (version)</th>
<th>App Package Name</th>
<th>GPS Coordinates</th>
<th>Connection Type</th>
<th>Device Make and Model</th>
<th>Wireless Carrier</th>
<th>Age</th>
<th>Gender</th>
<th>Income Level</th>
<th>Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>admob (4.3.1)</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>inmobi (3.0.1)</td>
<td>A</td>
<td>P</td>
<td>P</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>millennialmedia (4.5.1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>mobclix (3.2.0)</td>
<td>P</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>smaato (2.5.4)</td>
<td>A</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A = Always automatically  

P = Automatically, with permissions
## Private Data on the Network

<table>
<thead>
<tr>
<th>Ad Library (version)</th>
<th>App Package Name</th>
<th>GPS Coordinates</th>
<th>Connection Type</th>
<th>Device Make and Model</th>
<th>Wireless Carrier</th>
<th>Age</th>
<th>Gender</th>
<th>Income Level</th>
<th>Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>admob (4.3.1)</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>inmobi (3.0.1)</td>
<td>A</td>
<td>P</td>
<td>P</td>
<td>A</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>millennialmedia (4.5.1)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
<tr>
<td>mobclix (3.2.0)</td>
<td>P</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>D</td>
</tr>
<tr>
<td>smaato (2.5.4)</td>
<td>A</td>
<td>P</td>
<td>P</td>
<td>P</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
<td>D</td>
</tr>
</tbody>
</table>

A = *Always automatically*  
P = *Automatically, with permissions*  
D = *Developer chosen*
Unique Privacy Concerns in Android App Advertising

1. No privilege separation between app and ad code

2. Greater access to detailed user data

3. More persistent user identifiers
## Tracking Users

<table>
<thead>
<tr>
<th>Device</th>
<th>App 1</th>
<th>App 2</th>
<th>App 3</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Tracking Users

Device

App 1
App 2
App 3

Internet

SHA-1(UDID)
SHA-1(UDID)
SHA-1(UDID)

Ad Provider
Tracking Users

Device

App 1

App 2

App 3

Internet

Ad Provider

SHA-1(UDID)

SHA-1(UDID)

SHA-1(UDID)

Network Snooper
Tracking Users

Device

App 1

App 2

App 3
Tracking Users

Device

App 1
App 2
App 3

Internet

UDID
MD5(UDID)
SHA-1(UDID)

Ad Provider 1
Ad Provider 2
Ad Provider 3
Tracking Users

- UDID
- MD5(UDID)
- SHA-1(UDID)

Device

- App 1
- App 2
- App 3

Internet

Ad Provider 1

Ad Provider 2

Ad Provider 3

Network Snooper
## Tracking Users

<table>
<thead>
<tr>
<th>Ad Library (version)</th>
<th>DEVICE_ID</th>
<th>ANDROID_ID</th>
<th>md5(ANDROID_ID)</th>
<th>sha1(ANDROID_ID)</th>
</tr>
</thead>
<tbody>
<tr>
<td>admob (4.3.1)</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>inmobi (3.0.1)</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>millenialmedia (4.5.1)</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>mobclix (3.2.0)</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>smaato (2.5.1)</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Hashing Device Identifiers

- Prevent correlating ad requests across multiple ad providers: hash(ad provider || UDID)
- Prevent correlating ad requests across multiple applications: hash(ad provider || package name || UDID)
Hashing Device Identifiers

Prevent correlating ad requests across multiple ad providers:

\[ hash(\text{ad provider} \ || \ \text{UDID}) \]
Hashing Device Identifiers

Prevent correlating ad requests across multiple ad providers:

\[ \text{hash}(\text{ad provider } \|	ext{ UDID}) \]

Prevent correlating ad requests across multiple applications:

\[ \text{hash}(\text{ad provider } \|	ext{ package name } \|	ext{ UDID}) \]
Encrypting Ad Requests

Problem:
SSL is expensive and allows for less concurrency on the server

Desirable properties of advertising encryption:
- Low overhead - minimal session state
- Lightweight - preferably symmetric key
Encrypting Ad Requests

**Problem:** SSL is expensive and allows for less concurrency on the server.
Encrypting Ad Requests

**Problem:** SSL is expensive and allows for less concurrency on the server.

Desirable properties of advertising encryption:
- Low overhead - minimal session state
Encrypting Ad Requests

**Problem:** SSL is expensive and allows for less concurrency on the server

Desirable properties of advertising encryption:

- Low overhead - minimal session state
- Lightweight - preferably symmetric key
Separating Ad and App Code

Splitting library and application code is not trivial in the Android framework.
Separating Ad and App Code

Splitting library and application code is not trivial in the Android framework.

Potential solutions:
- AdDroid – “Asia CCS 2012”
Splitting library and application code is not trivial in the Android framework

Potential solutions:
- AdDroid – “Asia CCS 2012”
Conclusions

1. No privilege separation between app and ad code
   • Problem: Undocumented permissions
   • Solution: AdDroid, AdSplit

2. Greater access to detailed user data
   • Problem: Private user data on network
   • Solution: Lightweight encryption

3. More persistent user identifiers
   • Problem: Correlating user profile data over time
   • Solution: Proper hashing, lightweight encryption
Conclusions

1. No privilege separation between app and ad code
Conclusions

1. No privilege separation between app and ad code
   • Problem: Undocumented permissions
Conclusions

1. No privilege separation between app and ad code
   - Problem: Undocumented permissions
   - Solution: AdDroid, AdSplit
Conclusions

1. No privilege separation between app and ad code
   - Problem: Undocumented permissions
   - Solution: AdDroid, AdSplit

2. Greater access to detailed user data
Conclusions

1. No privilege separation between app and ad code
   - Problem: Undocumented permissions
   - Solution: AdDroid, AdSplit

2. Greater access to detailed user data
   - Problem: Private user data on network
Conclusions

1. No privilege separation between app and ad code
   - Problem: Undocumented permissions
   - Solution: AdDroid, AdSplit

2. Greater access to detailed user data
   - Problem: Private user data on network
   - Solution: Lightweight encryption
Conclusions

1. No privilege separation between app and ad code
   • Problem: Undocumented permissions
   • Solution: AdDroid, AdSplit

2. Greater access to detailed user data
   • Problem: Private user data on network
   • Solution: Lightweight encryption

3. More persistent user identifiers
Conclusions

1. No privilege separation between app and ad code
   - Problem: Undocumented permissions
   - Solution: AdDroid, AdSplit

2. Greater access to detailed user data
   - Problem: Private user data on network
   - Solution: Lightweight encryption

3. More persistent user identifiers
   - Problem: Correlating user profile data over time
Conclusions

1. No privilege separation between app and ad code
   - Problem: Undocumented permissions
   - Solution: AdDroid, AdSplit

2. Greater access to detailed user data
   - Problem: Private user data on network
   - Solution: Lightweight encryption

3. More persistent user identifiers
   - Problem: Correlating user profile data over time
   - Solution: Proper hashing, lightweight encryption
Questions/Comments?

Presenter:

Ryan Stevens

rcstevens@ucdavis.edu