AUTHSCOPE: Towards Automatic Discovery of Vulnerable Authorizations in Online Services

Chaoshun Zuo, Qingchuan Zhao, Zhiqiang Lin

University of Texas at Dallas

Nov 1st, 2017
Access Control In a Multi-User System

Users → Access Control → Database
Access Control In a Multi-User System
Access Control in a Multi-User System

- Users
  - Bob
  - Alice

- Database
  - Bob’s Data
  - Alice’s Data

Access Control
Access Control In a Multi-User System

Access Control

Users

Bob

Alice

Database

Bob’s Data

Alice’s Data
Access Control In a Multi-User System

- Users
  - Bob
  - Alice

- Database
  - Bob’s Data
  - Alice’s Data

Access Control
Access Control In a Multi-User System

Users → Access Control → Database
Access Control In a Multi-User System

Users -> Authentication -> Authorization -> Database
Challenges in Online Service

Access Control

Users Database
Challenges in Online Service

Users → Online Service → Database
Challenges in Online Service

Diagram showing the flow of users interacting with an online service, which then connects to a database.

- Users → Online Service → Database
Challenges in Online Service
Challenges in Online Service

Users → Online Service → Database

Users
Users
Users
Users

Users
Users
Users
Users

Database
Database
Database
Access Control in Online Service

Client

Authentication
Authorization

Server
Access Control in Online Service

Client → User Credential

Authentication

Authorization

Server
Access Control in Online Service

1. User Credential
2. Access Token

Client

Authentication

Authorization

Server
Access Control in Online Service

1. User Credential
2. Access Token
3. Access Token, Resource

Client → Authentication

Server → Authorization
Access Control in Online Service

1. User Credential
2. Access Token
3. Access Token, Resource
4. Response

Client → Authentication → Server

Client

Server
Access Control in Online Service

1 User Credential
2 Access Token
3 Access Token, Resource
4 Response
Possible Vulnerabilities

Vulnerabilities in Authorization

- No security token
Possible Vulnerabilities

Vulnerabilities in Authorization

- No security token
- No randomness of resource ID
Possible Vulnerabilities

Vulnerabilities in Authorization

- No security token
- No randomness of resource ID

https://www.overleaf.com/9357323vdzpzwzwmwdmx
Possible Vulnerabilities

Vulnerabilities in Authorization

- No security token
- No randomness of resource ID
Possible Vulnerabilities

Vulnerabilities in Authorization

- No security token
- No randomness of resource ID
- No access control enforcement
A Running Example

GET /api/v1/users/21690/notifications?in_app_token=e67315b35aa38d4ac8cac3cd9c7f88ae7f576d373f HTTP/1.1
Host: api.w****.com
Connection: close

HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
Content-Type: application/json
ETag: W/"5319d96924bb6d0a761b5f13b248919c"
Server: nginx/1.6.2
X-Request-Id: 5775d45e-cc3b-4665-8bc6-c2c7a2c9180d
X-Runtime: 0.027840
Content-Length: 191
Connection: Close


Alice’s first request and response message after login
A Running Example

GET /api/v1/users/21691/notifications?in_app_token=fb153b7d8c0a0c6ac841d7bfbd9446de627c642858 HTTP/1.1
Host: api.w****.com
Connection: close

HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
Content-Type: application/json
ETag: W/"6ee365b32e7f3e145d5c74778ea243cd"
Server: nginx/1.6.2
X-Request-Id: 4970cafb-9438-4a70-96e0-ca2f789f0d5d
X-Runtime: 0.022889
Content-Length: 192
Connection: Close


Bob’s first request and response message after login
A Running Example

GET /api/v1//users/21690/notifications?in_app_token=e67315b35aa38d4ac8cac3cd9c7f88ae7f576d373f HTTP/1.1
Host: api.w****.com
Connection: close

Alice’s first request message after login

GET /api/v1//users/21691/notifications?in_app_token=fb153b7d8c0a0c6ac841d7bfbd9446de627c642858 HTTP/1.1
Host: api.w****.com
Connection: close

Bob’s first request message after login
A Running Example

GET /api/v1/users/21690/notifications?in_app_token=e67315b35aa38d4ac8cac3cd9c7f88ae7f576d373f HTTP/1.1
Host: api.w****.com
Connection: close

GET /api/v1/users/21691/notifications?in_app_token=fb153b7d8c0a0c6ac841d7bfbd9446de627c642858 HTTP/1.1
Host: api.w****.com
Connection: close
A Running Example

GET /api/v1/users/21690/notifications?in_app_token=e67315b35aa38d4ac8cac3cd9c7f88ae7f576d373f HTTP/1.1
Host: api.w****.com
Connection: close

GET /api/v1/users/21691/notifications?in_app_token=fb153b7d8c0a0c6ac841d7bfb9446de627c642858 HTTP/1.1
Host: api.w****.com
Connection: close
A Running Example

GET /api/v1/users/21691/notifications?in_app_token=e67315b35aa38d4ac8cac3cd9c7f88ae7f576d373f HTTP/1.1
Host: api.w****.com
Connection: close
A Running Example

```
GET /api/v1/users/21691/notifications?in_app_token=e67315b35aa38d4ac8cac3cd9c7f88ae7f576d373f HTTP/1.1
Host: api.w****.com
Connection: close

HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
Content-Type: application/json
ETag: W/"6ee365b32e7f3e145d5c74778ea243cd"
Server: nginx/1.6.2
X-Request-Id: 4970cafb-9438-4a70-96e0-ca2f789f0d5d
X-Runtime: 0.022889
Content-Length: 192
Connection: Close

```

Alice reads Bob’s notifications
Challenge: Obtain the post-authentication messages

GET /api/v1//users/21690/notifications?in_app_token=e67315b35aa38d4ac8cac3cd9c7f88ae7f576d373f HTTP/1.1
Host: api.w****.com
Connection: close

Alice’s first request message after login

GET /api/v1//users/21691/notifications?in_app_token=fbl53b7d8c0a0c6ac841d7bfbd9446de627c642858 HTTP/1.1
Host: api.w****.com
Connection: close

Bob’s first request message after login
Challenge: Obtain the post-authentication messages

Alice’s first request message after login

```
GET /api/v1//users/21690/notifications?in_app_token=e67315b35aa38d4ac8c3ac3cd9c7f88ae7f576d373f HTTP/1.1
Host: api.w****.com
Connection: close
```

Bob’s first request message after login

```
GET /api/v1//users/21691/notifications?in_app_token=fb153b7d8c0a0c6ac841d7bfbd9446de627c642858 HTTP/1.1
Host: api.w****.com
Connection: close
```

Insights

Executing the app with single-sign-on.
Challenge: Recognize & Substitute fields of interest

Alice’s first request message after login

```
GET /api/v1/users/21690/notifications?in_app_token=e67315b35aa38d4ac8cac3cd9c7f88ae7f576d373f HTTP/1.1
Host: api.w****.com
Connection: close
```

Bob’s first request message after login

```
GET /api/v1/users/21691/notifications?in_app_token=fb153b7d8c0a0c6ac841d7bfbd9446de627c642858 HTTP/1.1
Host: api.w****.com
Connection: close
```
Challenge: Recognize & Substitute fields of interest

Alice’s first request message after login

GET /api/v1/users/21690/notifications?in_app_token=e67315b35aa30d4ac8c3d9f7f88ae7f576d373f HTTP/1.1
Host: api.w****.com
Connection: close

Bob’s first request message after login

GET /api/v1/users/21691/notifications?in_app_token=fbl53b7d8c0a0c6ac841d7bfbd9446de627642858 HTTP/1.1
Host: api.w****.com
Connection: close

Insights

Differential traffic analysis and small Euclidean distance.
Challenge: Identify the vulnerability

GET /api/v1//users/21691/notifications?in_app_token=e67315b35aa38d4ac8cac3cd9c7f88ae7f576d373f HTTP/1.1
Host: api.w****.com
Connection: close

HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
Content-Type: application/json
ETag: W/"6ee365b32e7f3e145d5c74778ea243cd"
Server: nginx/1.6.2
X-Request-Id: 4970cafb-9438-4a70-96e0-ca2f789f0d5d
X-Runtime: 0.022889
Content-Length: 192
Connection: Close


Alice reads Bob’s notifications
Challenge: Identify the vulnerability

GET /api/v1/users/\text{21691}/notifications?\text{in\_app\_token=e67315b35aa38d4ac8cac3cd9c7f88ae7f576d373f} HTTP/1.1
Host: api.w****.com
Connection: close

HTTP/1.1 200 OK
Cache-Control: max-age=0, private, must-revalidate
Content-Type: application/json
ETag: W/"6ee365b32e7f3e145d5c74778ea243cd"
Server: nginx/1.6.2
X-Request-Id: 4970cafb-9438-4a70-96e0-ca2f789f0d5d
X-Runtime: 0.022889
Content-Length: 192
Connection: Close

[{"id":\text{433227},"sender":null,"dog":null,"notification\_type":15,"notification\_text":"Welcome to w****.","object\_id":\text{21691},"is\_seen":true,"is\_read":false,"created\_at":"2017-01-28T23:56:40.533Z"}]

Alice reads Bob’s notifications

Insights
Labeling server response with differential traffic analysis.
Problem Statement

- Given a mobile app
- Automatically identify whether its server is vulnerable to access control violation
### Problem Statement
- Given a mobile app
- Automatically identify whether its server is vulnerable to access control violation

### Assumptions
- HTTP/HTTPS protocol
- Facebook login
Overview of AUTHSCOPE

Post-Authentication Message Generation

1. Alice’s Request
2. Alice’s Request
3. Bob’s Request

Field Recognition and Substitution

1. Alice’s Request
2. Alice’s Request
3. Bob’s Request

Response Message Labeling

4. Alice’s Response
5. Alice’s Response
6. Bob’s Response

7. Field-Substituted Alice’s Request Messages (for Bob)

8. Server Response Messages for the Field-Substituted Request

Smartphone

Man-in-the-Middle Proxy

Cloud
Post-Authentication Message Generation

1. Alice’s Request₁
2. Alice’s Request₂
3. Bob’s Request

Field Recognition and Substitution

1. Alice’s Request₁
2. Alice’s Request₂
3. Bob’s Request
4. Alice’s Response₁
5. Alice’s Response₂
6. Bob’s Response

Response Message Labeling

7. Field-Substituted Alice’s Request Messages (for Bob)

8. Server Response Messages for the Field-Substituted Request
Post-Authentication Message Generation

1. Alice’s Request
2. Alice’s Request
3. Bob’s Request

Field Recognition and Substitution

4. Alice’s Response
5. Alice’s Response
6. Bob’s Response

Response Message Labeling

7. Field-Substituted Alice’s Request Messages (for Bob)

8. Server Response Messages for the Field-Substituted Request

Smartphone  Man-in-the-Middle Proxy  Cloud

View Identification and Exploration
Post-Authentication Message Generation

1. Alice’s Request₁
2. Alice’s Request₂
3. Bob’s Request

Field Recognition and Substitution

4. Alice’s Response₁
5. Alice’s Response₂
6. Bob’s Response

Response Message Labeling

7. Field-Substituted Alice’s Request Messages (for Bob)

8. Server Response Messages for the Field-Substituted Request

Smartphone → Man-in-the-Middle Proxy → Cloud

- View Identification and Exploration
- Automatic Social-based Service Login
Post-Authentication Message Generation Cont
Post-Authentication Message Generation Cont
Post-Authentication Message Generation Cont

Button 1

Button 2
Post-Authentication Message Generation Cont

**FaceBook Login**

- **Button 1**
- **Button 2**
Field Recognition and Substitution

1. Alice’s Request₁
2. Alice’s Request₂
3. Bob’s Request

Field Recognition and Substitution

4. Alice’s Response₁
5. Alice’s Response₂
6. Bob’s Response

Response Message Labeling

7. Field-Substituted Alice’s Request Messages (for Bob)

8. Server Response Messages for the Field-Substituted Request

Post-Authentication Message Generation

Smartphone

Man-in-the-Middle Proxy

Cloud

Field Recognition and Substitution

- Parsing Message Fields
- Identifying Fields of Interest
- Substituting Enumerable Fields
Field Recognition and Substitution

Post-Authentication Message Generation

Smartphone → Man-in-the-Middle Proxy → Cloud

Parsing Message Fields
Field Recognition and Substitution

- Parsing Message Fields
- Identifying Fields of Interest
Field Recognition and Substitution

1. Alice’s Request
2. Alice’s Request
3. Bob’s Request

Field Recognition and Substitution

7. Field-Substituted Alice’s Request Messages (for Bob)

8. Server Response Messages for the Field-Substituted Request

Post-Authentication Message Generation

Response Message Labeling

Smartphone

Man-in-the-Middle Proxy

Cloud

- Parsing Message Fields
- Identifying Fields of Interest
- Substituting Enumerable Fields
Field Recognition and Substitution Cont

GET /api/v1/users/21690/notifications?in_app_token=e67315b35aa38d4ac8cac3cd9c7f88ae7f576d373f HTTP/1.1
Host: api.w****.com
Connection: close
Field Recognition and Substitution Cont

GET /api/v1/users/21690/notifications?in_app_token=e67315b35aa38d4ac8cac3cd9c7f88ae7f576d373f HTTP/1.1
Host: api.w****.com
Connection: close

<users, 21690>
<in_app_token, e67315b35aa38d4ac8cac3cd9c7f88ae7f576d373f>
Field Recognition and Substitution Cont
Field Recognition and Substitution Cont

<internal_state>

<users, 21690>
<in_app_token, e67315b35aa38d4ac8cac3cd9c7f88ae7f576d373f>
<timestamp, 1485612650>

<internal_state>

<users, 21690>
<in_app_token, e67315b35aa38d4ac8cac3cd9c7f88ae7f576d373f>
<timestamp, 1485612710>
Field Recognition and Substitution Cont

<users, 21690>
<in_app_token, e67315b35aa38d4ac8cac3cd9c7f88ae7f576d373f>
<timestamp, 1485612650>

<users, 21690>
<in_app_token, e67315b35aa38d4ac8cac3cd9c7f88ae7f576d373f>
<timestamp, 1485612710>
Field Recognition and Substitution Cont

<users, 21690>
<in_app_token, e67315b35aa38d4ac8cac3cd9c7f88ae7f576d373f>
## Field Recognition and Substitution Cont

<table>
<thead>
<tr>
<th>Field-Value of Alice vs. Field-Value of Bob</th>
<th>ED</th>
</tr>
</thead>
<tbody>
<tr>
<td>e67315b35aa38d4ac8cac3cd9c7f88ae7f576d373f</td>
<td>+∞</td>
</tr>
<tr>
<td>fb153b7d8c0a0c6ac841d7bfbd9446de627c642858</td>
<td></td>
</tr>
<tr>
<td>21690</td>
<td>1.0</td>
</tr>
<tr>
<td>21691</td>
<td></td>
</tr>
</tbody>
</table>
Response Message Labeling

Post-Authentication Message Generation

1. Alice’s Request
2. Alice’s Request
3. Bob’s Request

Field Recognition and Substitution

1. Alice’s Request
2. Alice’s Request
3. Bob’s Request
4. Alice’s Response
5. Alice’s Response
6. Bob’s Response

Response Message Labeling

7. Field-Substituted Alice’s Request Messages (for Bob)

8. Server Response Messages for the Field-Substituted Request

Smartphone

Man-in-the-Middle Proxy

Cloud

Response Message Labeling indicates vulnerability
Response Message Labeling

Labeling response messages indicate vulnerability
<id, 433222>
<sender, null>
<dog, null>
<notification_type, 15>
<notification_text, "Welcome to w****."
<object_id, 21690>
<is_seen, true>

Alice
Alice

<id, 433222>
<sender, null>
<dog, null>
<notification_type, 15>
<notification_text, "Welcome to w****.">
<object_id, 21690>
<is_seen, true>

Bob

<id, 433227>
<sender, null>
<dog, null>
<notification_type, 15>
<notification_text, "Welcome to w****.">
<object_id, 21691>
<is_seen, true>
Response Message Labeling Cont

Alice

Bob

New
Response Message Labeling Cont

Alice

Bob

New
Response Message Labeling Cont

Prune Public Interfaces
Prune Public Interfaces

- News App
Implementation

- Post-Authentication Message Generation
  - 1 Alice’s Request₁
  - 2 Alice’s Request₂
  - 3 Bob’s Request

- Field Recognition and Substitution
  - Field-Substituted Alice’s Request Messages (for Bob)
    - 1 Alice’s Request₁
    - 2 Alice’s Request₂
    - 3 Bob’s Request

- Response Message Labeling
  - 4 Alice’s Response₁
  - 5 Alice’s Response₂
  - 6 Bob’s Response

- Server Response Messages for the Field-Substituted Request

Smartphone → Man-in-the-Middle Proxy → Cloud

- Atop Android 4.4 with Xposed framework
Implementation

- **Post-Authentication Message Generation**
  - 1. Alice’s Request
  - 2. Alice’s Request
  - 3. Bob’s Request

- **Field Recognition and Substitution**
  - 1. Alice’s Request
  - 2. Alice’s Request
  - 3. Bob’s Request

- **Response Message Labeling**
  - 4. Alice’s Response
  - 5. Alice’s Response
  - 6. Bob’s Response

- **Server Response Messages for the Field-Substituted Request**
  - 7. Field-Substituted Alice’s Request Messages (for Bob)

- **Burp Suite for man-in-the-middle proxy**
Implementation

Post-Authentication Message Generation

1. Alice’s Request
2. Alice’s Request
3. Bob’s Request

Field Recognition and Substitution

1. Alice’s Request
2. Alice’s Request
3. Bob’s Request

Response Message Labeling

4. Alice’s Response
5. Alice’s Response
6. Bob’s Response

Server Response Messages for the Field-Substituted Request

7. Field-Substituted Alice’s Request Messages (for Bob)

Smartphone

Man-in-the-Middle Proxy

Cloud

- 5,000 lines of Java and 300 lines of Python
## Experiment Setup

### Dataset Collection

- Top 10% free mobile apps from Google Play, totally 200,000 apps
- Filtered out the app that does not have Facebook libraries, remaining 33,950 apps
- Filtered out the app that has no Facebook login button or invoking code, finally we have 4,838 apps
Experiment Setup

Dataset Collection
- Top 10% free mobile apps from Google Play, totally 200,000 apps
- Filtered out the app that does not have Facebook libraries, remaining 33,950 apps
- Filtered out the app that has no Facebook login button or invoking code, finally we have 4,838 apps

Testing Environment
- LG Nexus 4 with Android 4.4
- Ubuntu 14.04 on Intel i7-6700k CPU with 8G memory
- Two Facebook accounts: Alice: alice4testapp@gmail.com & Bob: bob4testapp@gmail.com
Experiment Setup
# Overall Experiment Result

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total # Apps</td>
<td>4,838</td>
</tr>
</tbody>
</table>
## Overall Experiment Result

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total # Apps</td>
<td>4,838</td>
</tr>
<tr>
<td>Total Time of testing (hours)</td>
<td>562.4</td>
</tr>
</tbody>
</table>
## Overall Experiment Result

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total # Apps</td>
<td>4,838</td>
</tr>
<tr>
<td>Total Time of testing (hours)</td>
<td>562.4</td>
</tr>
<tr>
<td>Total # Request Messages</td>
<td>3,220,886</td>
</tr>
</tbody>
</table>
## Overall Experiment Result

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total # Apps</td>
<td>4,838</td>
</tr>
<tr>
<td>Total Time of testing (hours)</td>
<td>562.4</td>
</tr>
<tr>
<td>Total # Request Messages</td>
<td>3,220,886</td>
</tr>
<tr>
<td>Total # Suspicious Interfaces</td>
<td>2,976</td>
</tr>
</tbody>
</table>
## Overall Experiment Result

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total # Apps</td>
<td>4,838</td>
</tr>
<tr>
<td>Total Time of testing (hours)</td>
<td>562.4</td>
</tr>
<tr>
<td>Total # Request Messages</td>
<td>3,220,886</td>
</tr>
<tr>
<td>Total # Suspicious Interfaces</td>
<td>2,976</td>
</tr>
<tr>
<td>Total # Public Interfaces</td>
<td>2,379</td>
</tr>
</tbody>
</table>
## Overall Experiment Result

<table>
<thead>
<tr>
<th>Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total # Apps</td>
<td>4,838</td>
</tr>
<tr>
<td>Total Time of testing (hours)</td>
<td>562.4</td>
</tr>
<tr>
<td>Total # Request Messages</td>
<td>3,220,886</td>
</tr>
<tr>
<td>Total # Suspicious Interfaces</td>
<td>2,976</td>
</tr>
<tr>
<td>Total # Public Interfaces</td>
<td>2,379</td>
</tr>
<tr>
<td>Total # Vulnerable Interfaces</td>
<td>597</td>
</tr>
</tbody>
</table>
Distribution of the Vulnerable Interfaces
### Detailed Results for Top Tested App in Each Category

<table>
<thead>
<tr>
<th>Category</th>
<th>Package Name</th>
<th># Activities</th>
<th># Views</th>
<th>Time to Login (s)</th>
<th>#Request Messages</th>
<th>#Mutated Fields</th>
<th>#Public Interfaces</th>
<th>#Vulnerable Interfaces</th>
</tr>
</thead>
<tbody>
<tr>
<td>Books &amp; Reference</td>
<td>com.&quot;e&quot;&quot;</td>
<td>3</td>
<td>288</td>
<td>45</td>
<td>975</td>
<td>16</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>Business</td>
<td>com.&quot;k&quot;&quot;</td>
<td>8</td>
<td>1,224</td>
<td>30</td>
<td>927</td>
<td>12</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Communication</td>
<td>com.&quot;w&quot;&quot;</td>
<td>18</td>
<td>970</td>
<td>41</td>
<td>727</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Entertainment</td>
<td>com.&quot;.&quot;&quot;</td>
<td>3</td>
<td>184</td>
<td>32</td>
<td>739</td>
<td>2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Finance</td>
<td>com.&quot;m&quot;&quot;</td>
<td>8</td>
<td>549</td>
<td>16</td>
<td>790</td>
<td>7</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Food &amp; Drink</td>
<td>com.&quot;h&quot;&quot;</td>
<td>10</td>
<td>924</td>
<td>21</td>
<td>1,032</td>
<td>8</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>Games</td>
<td>com.&quot;.&quot;&quot;</td>
<td>7</td>
<td>609</td>
<td>20</td>
<td>1,050</td>
<td>7</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Health &amp; Fitness</td>
<td>com.&quot;.u&quot;&quot;</td>
<td>12</td>
<td>788</td>
<td>15</td>
<td>966</td>
<td>10</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Lifestyle</td>
<td>com.&quot;&quot;&quot;</td>
<td>17</td>
<td>1,938</td>
<td>25</td>
<td>1,229</td>
<td>29</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Maps &amp; Navigation</td>
<td>com.&quot;.&quot;&quot;&quot;&quot;&quot;&quot;&quot;</td>
<td>11</td>
<td>667</td>
<td>26</td>
<td>490</td>
<td>12</td>
<td>7</td>
<td>1</td>
</tr>
<tr>
<td>Medical</td>
<td>com.&quot;.&quot;&quot;&quot;&quot;&quot;&quot;&quot;</td>
<td>18</td>
<td>1,616</td>
<td>23</td>
<td>927</td>
<td>9</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Music &amp; Audio</td>
<td>com.&quot;&quot;&quot;</td>
<td>2</td>
<td>456</td>
<td>25</td>
<td>933</td>
<td>15</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>News &amp; Magazines</td>
<td>com.&quot;.&quot;&quot;&quot;&quot;&quot;&quot;&quot;</td>
<td>5</td>
<td>462</td>
<td>37</td>
<td>880</td>
<td>9</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Photography</td>
<td>com.&quot;.&quot;&quot;&quot;&quot;&quot;&quot;&quot;</td>
<td>15</td>
<td>909</td>
<td>26</td>
<td>965</td>
<td>7</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Productivity</td>
<td>com.&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;</td>
<td>15</td>
<td>1,347</td>
<td>32</td>
<td>882</td>
<td>10</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>Shopping</td>
<td>com.&quot;.&quot;&quot;&quot;&quot;&quot;&quot;&quot;</td>
<td>8</td>
<td>795</td>
<td>44</td>
<td>961</td>
<td>10</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Social</td>
<td>com.&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;</td>
<td>10</td>
<td>645</td>
<td>20</td>
<td>1,068</td>
<td>20</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Tools</td>
<td>com.mediaingea.uptodown.lite</td>
<td>7</td>
<td>1,347</td>
<td>112</td>
<td>1,276</td>
<td>25</td>
<td>6</td>
<td>1</td>
</tr>
<tr>
<td>Travel &amp; Local</td>
<td>com.&quot;&quot;&quot;&quot;&quot;&quot;&quot;&quot;</td>
<td>5</td>
<td>321</td>
<td>35</td>
<td>1,024</td>
<td>10</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Video Players &amp; Editors</td>
<td>com.&quot;.&quot;&quot;&quot;&quot;&quot;&quot;&quot;</td>
<td>4</td>
<td>218</td>
<td>25</td>
<td>821</td>
<td>5</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
# User Privacy & Vulnerability Details

<table>
<thead>
<tr>
<th>Category</th>
<th>Detailed Privacy Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>User E-Profile</td>
<td>① Email, ② User ID, ③ Registration Date, ④ IP Address, ⑤ Last Login Date, ⑥ Last Update Date</td>
</tr>
<tr>
<td>User Physical-Profile</td>
<td>⑦ Real Name, ⑧ Birthday, ⑨ Geo-location, ⑩ Home Address, ⑪ Phone Number, ⑫ Body Information</td>
</tr>
<tr>
<td>User Secrets</td>
<td>⑬ Token, ⑭ Password, ⑮ Pass Code</td>
</tr>
<tr>
<td>App Specific Private Data</td>
<td>⑯ In App Messages, ⑰ Shopping History, ⑱ Book Shelf, ⑲ Favorites or Subscription, ⑳ Account Balance</td>
</tr>
<tr>
<td></td>
<td>㉑ Contacts Information, ㉒ Payment Information, ㉓ Private Activity Information</td>
</tr>
</tbody>
</table>
## User Privacy & Vulnerability Details

<table>
<thead>
<tr>
<th>Category</th>
<th>Detailed Privacy Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>User E-Profile</td>
<td>① Email, ② User ID, ③ Registration Date, ④ IP Address, ⑤ Last Login Date, ⑥ Last Update Date</td>
</tr>
<tr>
<td>User Physical-Profile</td>
<td>⑦ Real Name, ⑧ Birthday, ⑨ Geo-location, ⑩ Home Address, ⑪ Phone Number, ⑫ Body Information</td>
</tr>
<tr>
<td>User Secrets</td>
<td>⑬ Token, ⑭ Password, ⑮ Pass Code</td>
</tr>
<tr>
<td>App Specific Private Data</td>
<td>⑯ In App Messages, ⑰ Shopping History, ⑱ Book Shelf, ⑲ Favorites or Subscription, ⑳ Account Balance</td>
</tr>
<tr>
<td></td>
<td>㉑ Contacts Information, ㉒ Payment Information, ㉓ Private Activity Information</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>APP</th>
<th>Version</th>
<th>Credential Type</th>
<th>User E-Profile</th>
<th>User Physical-Profile</th>
<th>User Secrets</th>
<th>App Specific Private Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>com.*** .c***</td>
<td>2.2</td>
<td>N</td>
<td>①②</td>
<td>⑦⑧⑨⑩</td>
<td>⑬⑭</td>
<td>⑯⑰⑱⑲⑳</td>
</tr>
<tr>
<td>com.*** .k***</td>
<td>2.0.11</td>
<td>E</td>
<td>①②③④⑤</td>
<td>⑦⑧⑨⑩</td>
<td>⑬⑭⑮</td>
<td>⑯⑰⑱⑲⑳</td>
</tr>
<tr>
<td>com.*** .w***</td>
<td>1.0.5</td>
<td>F</td>
<td>①②③④⑤</td>
<td>⑦⑧⑨⑩</td>
<td>⑬⑭⑮</td>
<td>⑯⑰⑱⑲⑳</td>
</tr>
<tr>
<td>com.g*** .c***</td>
<td>2.4.1</td>
<td>E</td>
<td>①②③④⑤</td>
<td>⑦⑧⑨⑩</td>
<td>⑬⑭</td>
<td>⑯⑰⑱⑲⑳</td>
</tr>
<tr>
<td>com.*** .m***</td>
<td>1.6.8</td>
<td>N</td>
<td>①②③④⑤</td>
<td>⑦⑧⑨⑩</td>
<td>⑬⑭</td>
<td>⑯⑰⑱⑲⑳</td>
</tr>
<tr>
<td>com.*** .h***</td>
<td>2.5.6.0</td>
<td>E</td>
<td>①②③④⑤</td>
<td>⑦⑧⑨⑩</td>
<td>⑬⑭</td>
<td>⑯⑰⑱⑲⑳</td>
</tr>
<tr>
<td>com.*** .c***</td>
<td>2.6.1</td>
<td>F</td>
<td>①②③④⑤</td>
<td>⑦⑧⑨⑩</td>
<td>⑬⑭</td>
<td>⑯⑰⑱⑲⑳</td>
</tr>
<tr>
<td>com.*** .u***</td>
<td>2.0.3</td>
<td>N</td>
<td>①②③④⑤</td>
<td>⑦⑧⑨⑩</td>
<td>⑬⑭</td>
<td>⑯⑰⑱⑲⑳</td>
</tr>
<tr>
<td>com.m***</td>
<td>7.3.0</td>
<td>N</td>
<td>①②③④⑤</td>
<td>⑦⑧⑨⑩</td>
<td>⑬⑭</td>
<td>⑯⑰⑱⑲⑳</td>
</tr>
<tr>
<td>com.***** .c***</td>
<td>7.5.5v</td>
<td>F</td>
<td>①②③④⑤</td>
<td>⑦⑧⑨⑩</td>
<td>⑬⑭</td>
<td>⑯⑰⑱⑲⑳</td>
</tr>
<tr>
<td>com.*** .a***</td>
<td>3.0.9</td>
<td>F</td>
<td>①②③④⑤</td>
<td>⑦⑧⑨⑩</td>
<td>⑬⑭</td>
<td>⑯⑰⑱⑲⑳</td>
</tr>
<tr>
<td>com.b***</td>
<td>2.0.4</td>
<td>N</td>
<td>①②③④⑤</td>
<td>⑦⑧⑨⑩</td>
<td>⑬⑭</td>
<td>⑯⑰⑱⑲⑳</td>
</tr>
<tr>
<td>com.*** .a***</td>
<td>2.3.2</td>
<td>N</td>
<td>①②③④⑤</td>
<td>⑦⑧⑨⑩</td>
<td>⑬⑭</td>
<td>⑯⑰⑱⑲⑳</td>
</tr>
<tr>
<td>com.*** .f***</td>
<td>2.7.4</td>
<td>F</td>
<td>①②③④⑤</td>
<td>⑦⑧⑨⑩</td>
<td>⑬⑭</td>
<td>⑯⑰⑱⑲⑳</td>
</tr>
<tr>
<td>com.*** .d***</td>
<td>2.4.2</td>
<td>E</td>
<td>①②③④⑤</td>
<td>⑦⑧⑨⑩</td>
<td>⑬⑭</td>
<td>⑯⑰⑱⑲⑳</td>
</tr>
<tr>
<td>cl.***** .d***</td>
<td>2.1.0</td>
<td>N</td>
<td>①②③④⑤</td>
<td>⑦⑧⑨⑩</td>
<td>⑬⑭</td>
<td>⑯⑰⑱⑲⑳</td>
</tr>
<tr>
<td>in.v***</td>
<td>4.4.5.2</td>
<td>N</td>
<td>①②③④⑤</td>
<td>⑦⑧⑨⑩</td>
<td>⑬⑭</td>
<td>⑯⑰⑱⑲⑳</td>
</tr>
<tr>
<td>com.mediaingea.uptodown.lite</td>
<td>3.18</td>
<td>F</td>
<td>①②③④⑤</td>
<td>⑦⑧⑨⑩</td>
<td>⑬⑭</td>
<td>⑯⑰⑱⑲⑳</td>
</tr>
<tr>
<td>com.t***</td>
<td>1.4.0</td>
<td>F</td>
<td>①②③④⑤</td>
<td>⑦⑧⑨⑩</td>
<td>⑬⑭</td>
<td>⑯⑰⑱⑲⑳</td>
</tr>
<tr>
<td>cz.*** .n***</td>
<td>4.8</td>
<td>F</td>
<td>①②③④⑤</td>
<td>⑦⑧⑨⑩</td>
<td>⑬⑭</td>
<td>⑯⑰⑱⑲⑳</td>
</tr>
<tr>
<td>Statistics</td>
<td>8 4 8</td>
<td>14 16 05 02 01 01</td>
<td>15 06 06 07 06 01</td>
<td>13 01 01</td>
<td>11 02 01 13 04 02 02 03</td>
<td></td>
</tr>
</tbody>
</table>
Impact

Up to 61 MILLION mobile users
Case Study-App K

```
00 {
01  "pk_i_id": "163126",
02  "dt_reg_date": "2017-04-30 23:21:59",
03  "dt_mod_date": "2017-04-30 23:36:58",
04  "s_name": "Bob Ccs",
05  "s_username": "163126",
06  "s_password": "7c4a8d09ca3762af61e59520943dc26494f8941b",
07  "s_secret": "6stgMaAb",
08  "s_email": "bob4testapp@gmail.com",
09  "s_website": "bob.ccs\index.html",
10  "s_phone_mobile": "469585213",
11  "s_pass_ip": null,
12  "fk_c_country_code": null,
13  "s_country": "Tanzania",
14  "s_address": "15246 Sni Rd. APT 252 Tanzania",
15  "fk_i_region_id": "17",
16  "s_region": "Mara",
17  "d_coord_lat": null,
18  "d_coord_long": null,
19  "b_company": "0",
20  "i_items": "1",
21  "i_comments": "0",
22  "dt_access_date": "2017-04-30 23:46:05",
23  "s_access_ip": "",
24  "b_prefer_phone": "1",
25  "s_dialing_code": "+255",
26  "fk_i_category_id": "22",
27  "s_facebook_page": "http:\/\/",
28  ...
29 }
```
Case Study-App K

### User Privacy

```json
00 {
01  "pk_i_id": "163126",
02  "dt_reg_date": "2017-04-30 23:21:59",
03  "dt_mod_date": "2017-04-30 23:36:58",
04  "s_name": "Bob Ccs",
05  "s_username": "163126",
06  "s_password": "7c4a8d09ca3762af61e59520943dc26494f8941b",
07  "s_secret": "6stgMaAb",
08  "s_email": "bob4testapp@gmail.com",
09  "s_website": "bob.ccs/index.html",
10  "s_phone_mobile": "469585213",
11  "s_pass_ip": null,
12  "fk_c_country_code": null,
13  "s_country": "Tanzania",
14  "s_address": "15246 Sni Rd. APT 252 Tanzania",
15  "fk_i_region_id": "17",
16  "s_region": "Mara",
17  "d_coord_lat": null,
18  "d_coord_long": null,
19  "b_company": "0",
20  "i_items": "1",
21  "i_comments": "0",
22  "dt_access_date": "2017-04-30 23:46:05",
23  "s_access_ip": "",
24  "b_prefer_phone": "1",
25  "s_dialing_code": "+255",
26  "fk_i_category_id": "22",
27  "s_facebook_page": "http://",
28  ...
29 }
```
### Case Study - App K

**User Privacy**

<table>
<thead>
<tr>
<th>Registration Date</th>
<th>Last Update Date</th>
<th>User ID</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>&quot;163126&quot;</td>
<td>&quot;<a href="mailto:bob4testapp@gmail.com">bob4testapp@gmail.com</a>&quot;</td>
</tr>
</tbody>
</table>

尤为注意的是，该用户隐私数据的注册日期为2017年4月30日，最后更新日期为同日。
User Privacy

Real Name

Phone Number

Home Address

Geo Location

```json
01 { "pk_i_id": "163126", 
02  "dt_reg_date": "2017-04-30 23:21:59", 
03  "dt_mod_date": "2017-04-30 23:36:58", 
04  "s_name": "Bob Ccs", 
05  "s_username": "163126", 
06  "s_password": "7c4a8d09ca3762af61e59520943dc26494f8941b", 
07  "s_secret": "6stgMaAb", 
08  "s_email": "bob4testapp@gmail.com", 
09  "s_website": "bob.ccs\index.html", 
10  "s_phone_mobile": "4695855213", 
11  "s_pass_ip": null, 
12  "fk_c_country_code": null, 
13  "s_country": "Tanzania", 
14  "s_address": "15246 Sni Rd. APT 252 Tanzania", 
15  "fk_i_region_id": "17", 
16  "s_region": "Mara", 
17  "d_coord_lat": null, 
18  "d_coord_long": null, 
19  "b_company": "0", 
20  "i_items": "1", 
21  "i_comments": "0", 
22  "dt_access_date": "2017-04-30 23:46:05", 
23  "s_access_ip": "", 
24  "b_prefer_phone": "1", 
25  "s_dialing_code": "+255", 
26  "fk_i_category_id": "22", 
27  "s_facebook_page": "http:\", 
28  ...
29 }
```
Case Study-App I

```json
00 {
01  ...
02  "response":{
03    "user":{
04      "idnum":false,
05      "name":"Bob",
06      "lastname":"Ccs",
07      "birthday":"1990-04-26",
08      "gender":"M",
09      "email":"bob4testapp@gmail.com",
10      "type":"EMAIL",
11      "firstlogin":1,
12      "country":{
13        "id":"10",
14        "name":"United States",
15        ...
16      },
17      "post_on_activities":"disabled",
18      "bananas_count":0,
19      "id":"673491",
20      "fbid_number":"10661716575863",
21      "current_latitude":"30.9863214",
22      "current_longitude":"-86.7501116",
23      "bananas_history":"https:\/\/profile.i*****.com\/bananas\/store\/673491\/?accesstoken=debda35ccd92f4b8e06f0bfff3b6e49279a557&latitude=30.9863214&longitude=-86.7501116&lang=",
24      ...
25    }
26  }
27 }
```
Case Study-App I

User Privacy

Email

User ID

```json
00 {
01 ... 02 "response":{
03 "user":{
04 "idnum":false,
05 "name":"Bob",
06 "lastname":"Ccs",
07 "birthday":"1990-04-26",
08 "gender":"M",
09 "email":"bob4testapp@gmail.com",
10 "type":"EMAIL",
11 "firstlogin":"1",
12 "country":{
13 "id":"10",
14 "name":"United States",
15 ... 16 
17 "post_on_activities":"disabled",
18 "bananas_count":0,
19 "id":673491,
20 "fbid":"10661716575863",
21 "current_latitude":30.9863214,
22 "current_longitude":-86.7501116,
23 "bananas_history":https://profile.i*****.com/bananas/store/673491/?accessstoken=debda35ccd92f4b8e06f0bffe7b6e49279a557&latitude=30.9863214&longitude=-86.7501116&lang",
24 ... 25 
26 } 27 }
```
Case Study-App I

User Privacy

Real Name

Birthday

Geo Location

```json
00 {
01  ...
02  "response": {
03    "user": {
04      "idnum": false,
05      "name": "Bob",
06      "lastname": "CCs",
07      "birthday": "1990-04-26",
08      "gender": "M",
09      "email": "bob4testapp@gmail.com",
10      "type": "EMAIL",
11      "firstlogin": "1",
12      "country": {
13        "id": "10",
14        "name": "United States",
15        ...
16      },
17      "post_on_activities": "disabled",
18      "bananas_count": 0,
19      "id": "675491",
20      "fbid_number": "106611716575863",
21      "current_latitude": "30.9863214",
22      "current_longitude": "-86.7501116",
23      "bananas_history": "https://profile.i*****.com/bananas/store/673491/?accesstoken=debda35cd92f4b8e06f0b7f3b6e49279a557&latitude=30.9863214&longitude=-86.7501116&lang=",
24      ...
25    }
26  }
27 }
```
Case Study-App I

User Privacy

Account

Balance

```json
00 {
01 ...  
02 "response":{
03 "user":{
04 "idnum":false,
05 "name":"Bob",
06 "lastname":"Ccs",
07 "birthday":"1990-04-26",
08 "gender":"M",
09 "email":"bob4testapp@gmail.com",
10 "type":"EMAIL",
11 "firstlogin":"1",
12 "country":{
13 "id":"10",
14 "name":"United States",
15 ...  
16 },
17 "post_on_activities":"disabled",
18 "bananas_count":0,
19 "id":"673491",
20 "fbid_number":"10661716575863",
21 "current_latitude":"30.9863214",
22 "current_longitude":"-86.7501116",
23 "bananas_history":"https:\/\/profile.i******.com\bananas\store\/673491\?accessstoken=debda35c9d92f4b8e2e06f0bf3b6e49279a557d&latitude=30.9863214&longitude=-86.7501116&lang=",
24 ...  
25 }
26 }
27 }
```
Limitation and Future work

Limitations

- Only Facebook Login
- Only authorization vulnerabilities that lead to information leakage and account hijacking
- Only Android Platform and HTTP/HTTPS protocol

Future Work

Addressing the first two limitations
Extend to other platforms and protocols
Limitation and Future work

Limitations
- Only Facebook Login
- Only authorization vulnerabilities that lead to information leakage and account hijacking
- Only Android Platform and HTTP/HTTPS protocol

Future Work
- Addressing the first two limitations
- Extend to other platforms and protocols
Vulnerability Discovery in Online Service. SQL injection [HVO06], cross-site-scripting [VNJ+07], cross-site-forgery [BJM08], broken authentication [DKZ09], application logic vulnerabilities [WCWQ11, PB14, WZC+13, XCWC13]

Access Control in Online Service. security with single-sign on [WCW12, ZE14], oauth [SB12, CPC+14], authentication vulnerability scanning [BLM+13], password brute-force attacks with online services [ZWWL16]
Related Work

- **Dynamic Analysis of Mobile Apps.** Monkey [mon17], Robotium [Rob], AppsPlayground [RCE13], DynoDroid [MTN13], symbolic execution [ANHY12, MMP+12, WL16, ZL17]

- **Protocol Reverse Engineering.** Analyzing network messages [Bed17, MLK+06, CKW07, CFL+17], and instructions traces [CS07, WMKK08, LJXZ08, LZ08, CPC+08, MWKK09] to discover protocol formats. Inspired by the protocol informatics project [Bed17], and uses a customized Needleman-Wunsch algorithm [NW70] to align and diff the protocol messages and infer only the fields of our interest.
Conclusion

AUTHSCOPE

- Automatically identify whether an app’s server is vulnerable to access control violation
- 597 vulnerable implementations in 306 mobile apps over 4,838 apps
Field Recognition and Substitution
Response Message Labeling

1. Alice’s Request
2. Alice’s Request
3. Bob’s Request

4. Alice’s Response
5. Alice’s Response
6. Bob’s Response

7. Field-Substituted Alice’s Request Messages (for Bob)

8. Server Response Messages for the Field-Substituted Request

To contact us
{chaoshun.zuo, qingchuan.zhao, zhiqiang.lin}@utdallas.edu
References I


Giancarlo Pellegrino and Davide Balzarotti, Toward black-box detection of logic flaws in web applications., NDSS, 2014.


