AUTHSCOPE: Towards Automatic Discovery of Vulnerable Authorizations in Online Services

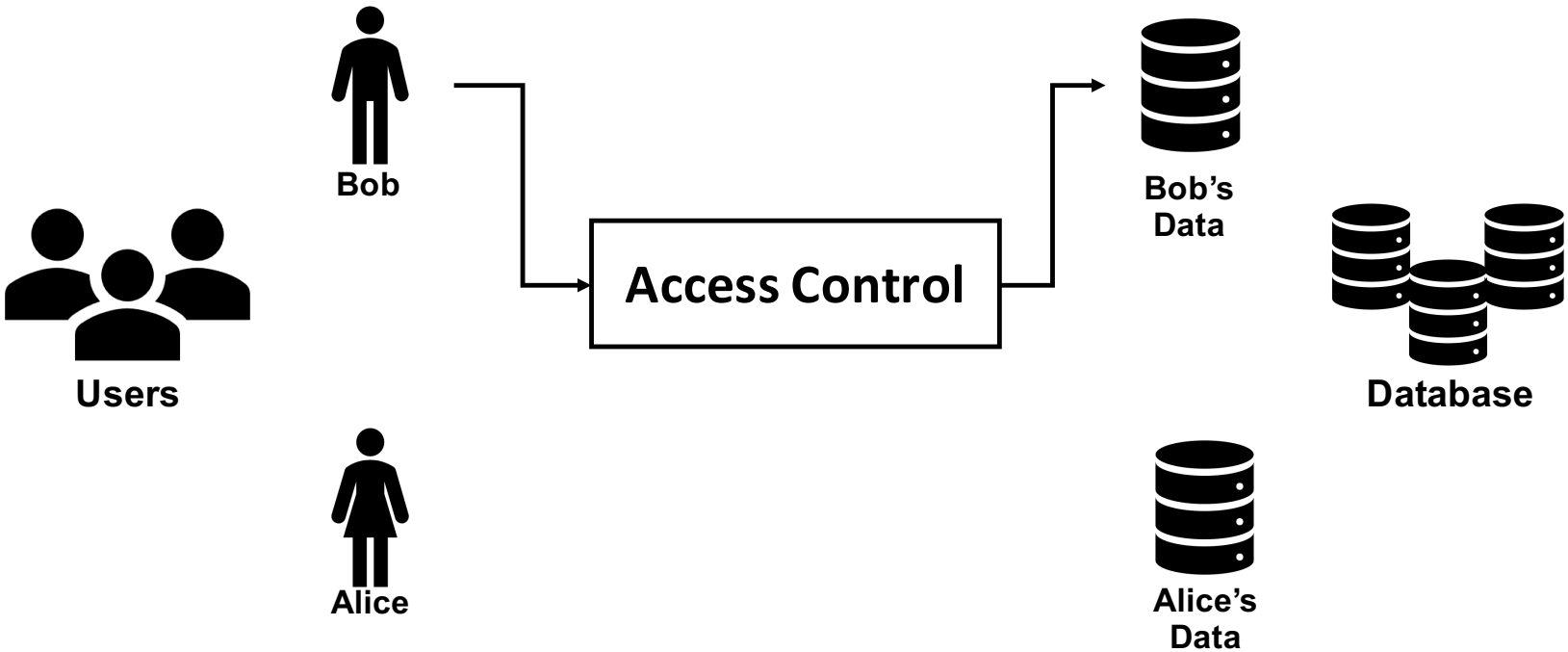
Chaoshun Zuo, **Qingchuan Zhao**, Zhiqiang Lin

University of Texas at Dallas

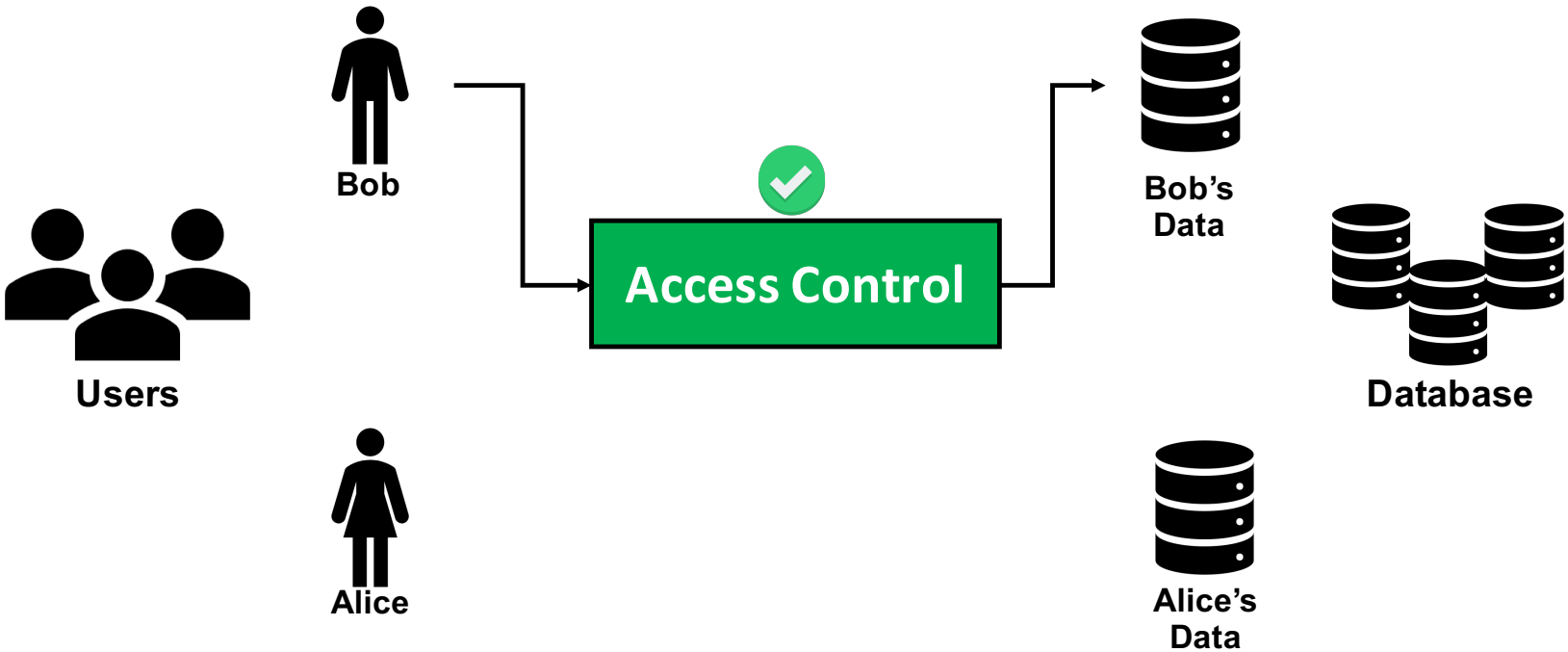
Nov 1^{st}, 2017

Access Control In a Multi-User System

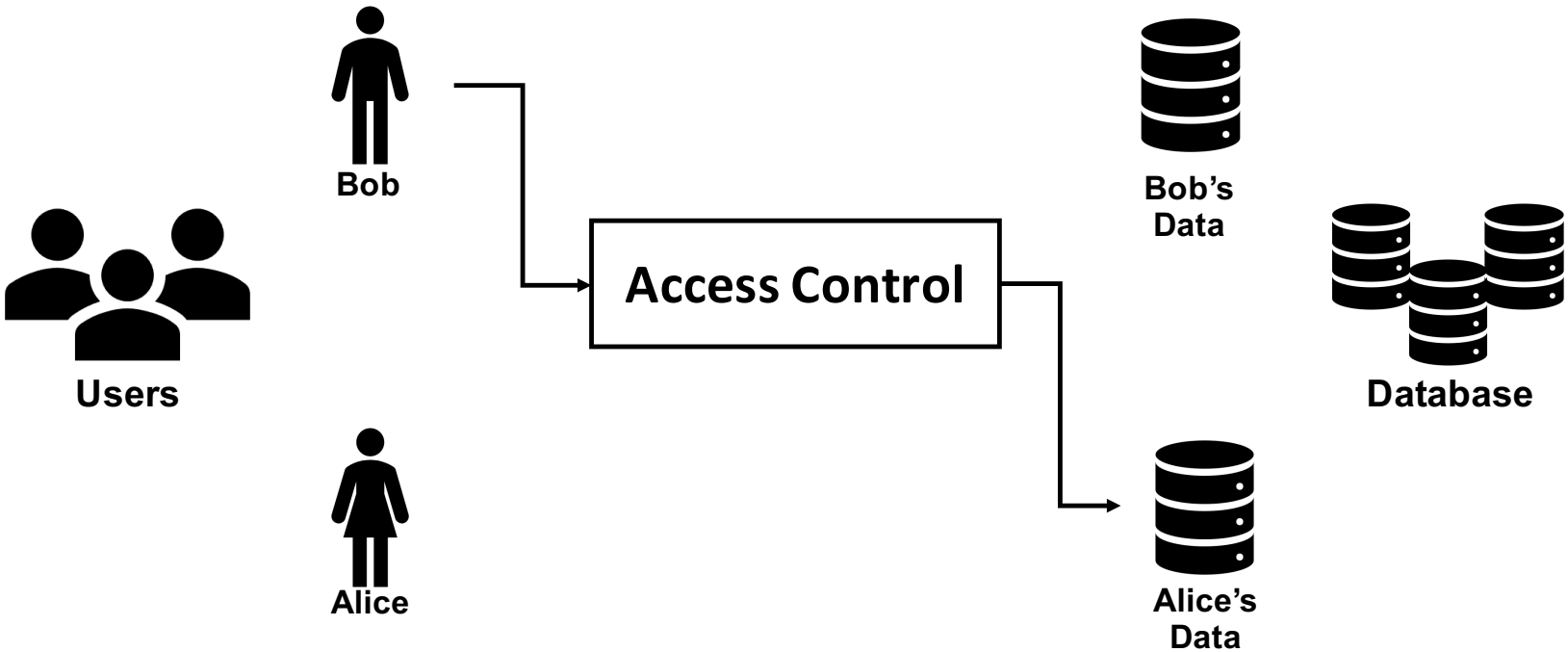
Access Control In a Multi-User System



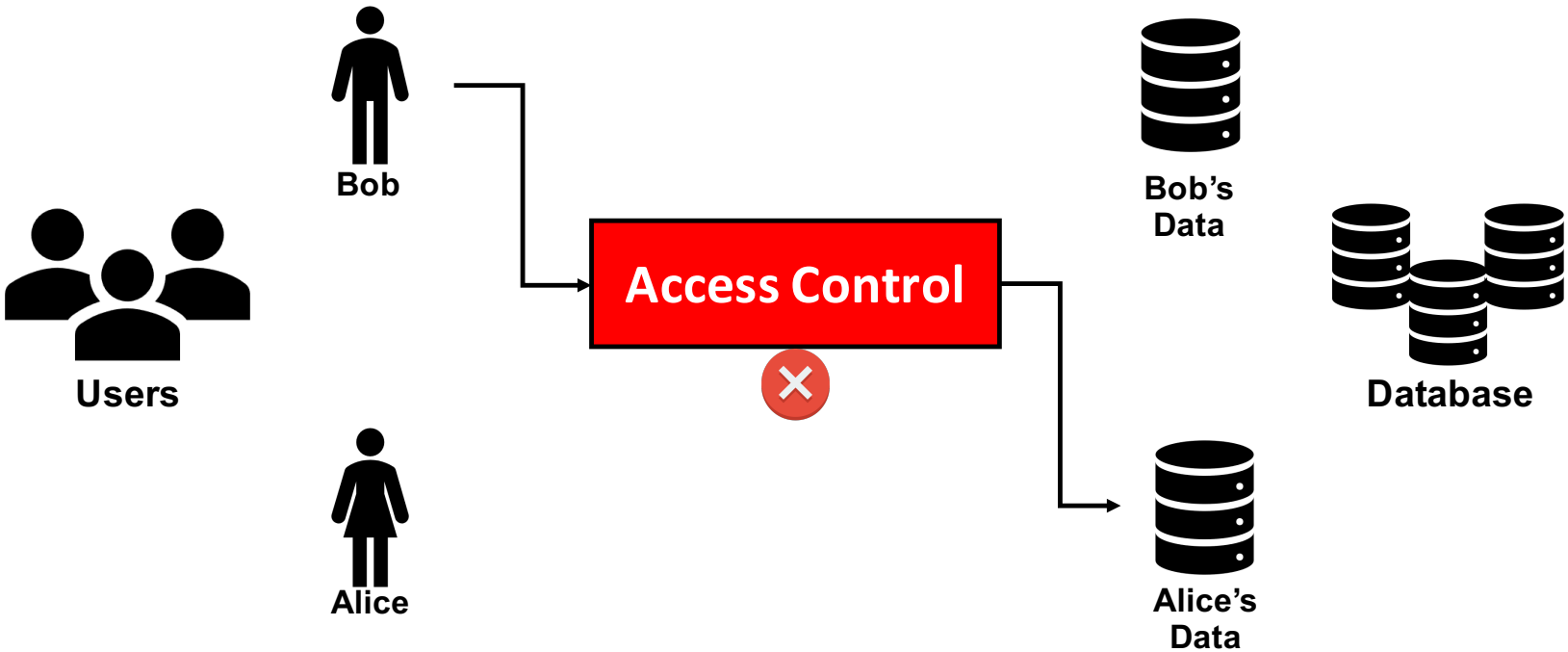
Access Control In a Multi-User System



Access Control In a Multi-User System

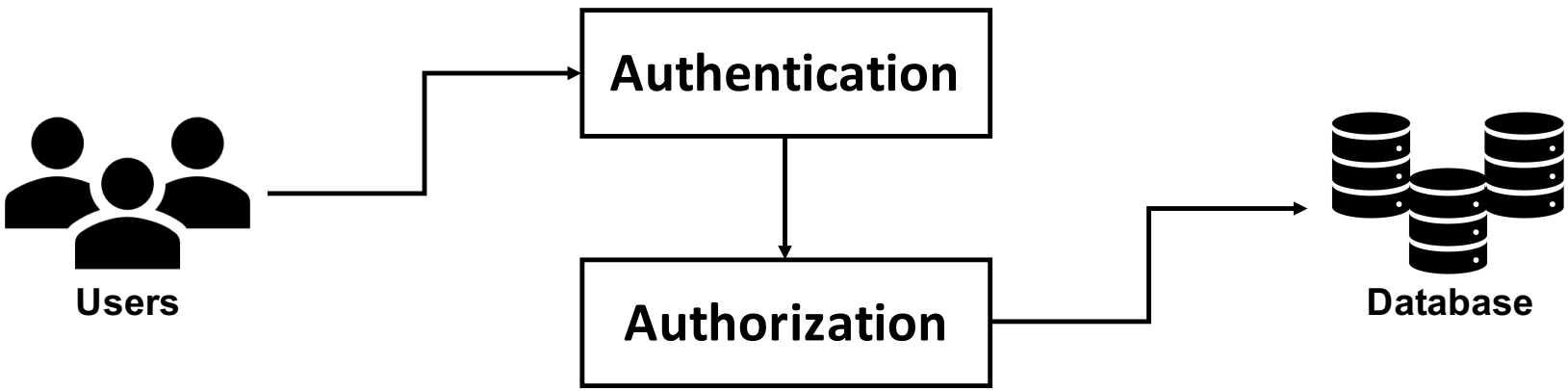


Access Control In a Multi-User System



Access Control In a Multi-User System

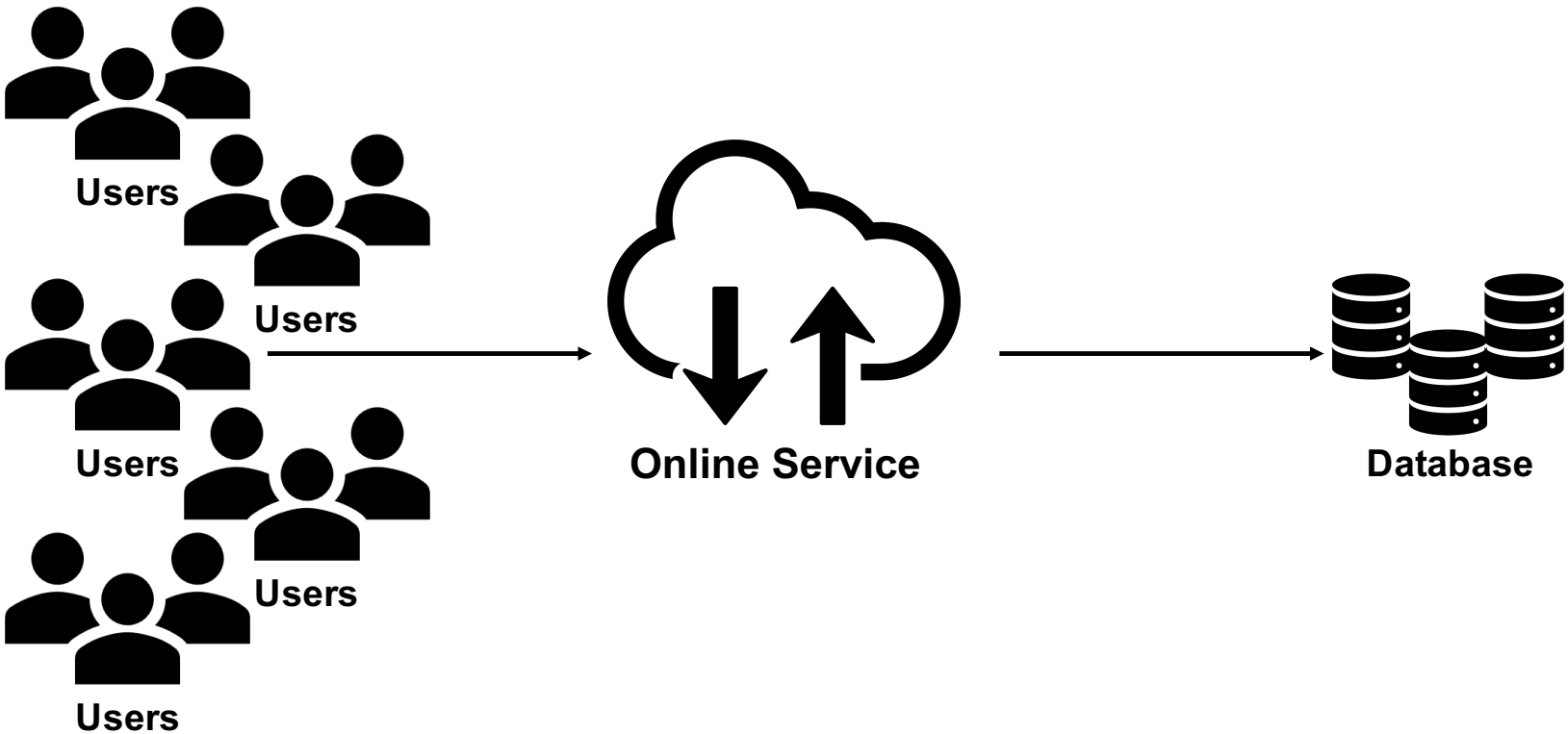
Access Control In a Multi-User System



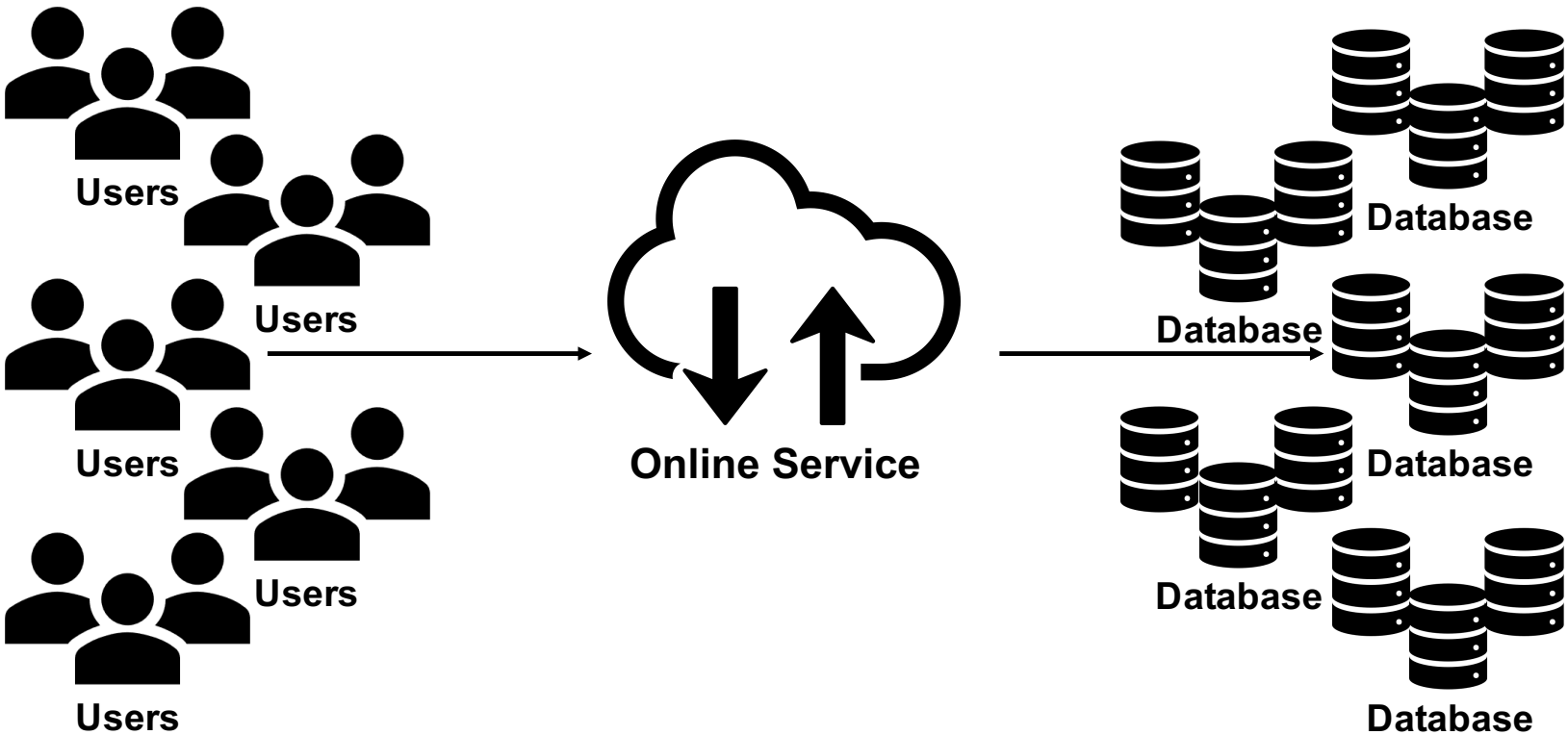
Challenges in Online Service

Challenges in Online Service

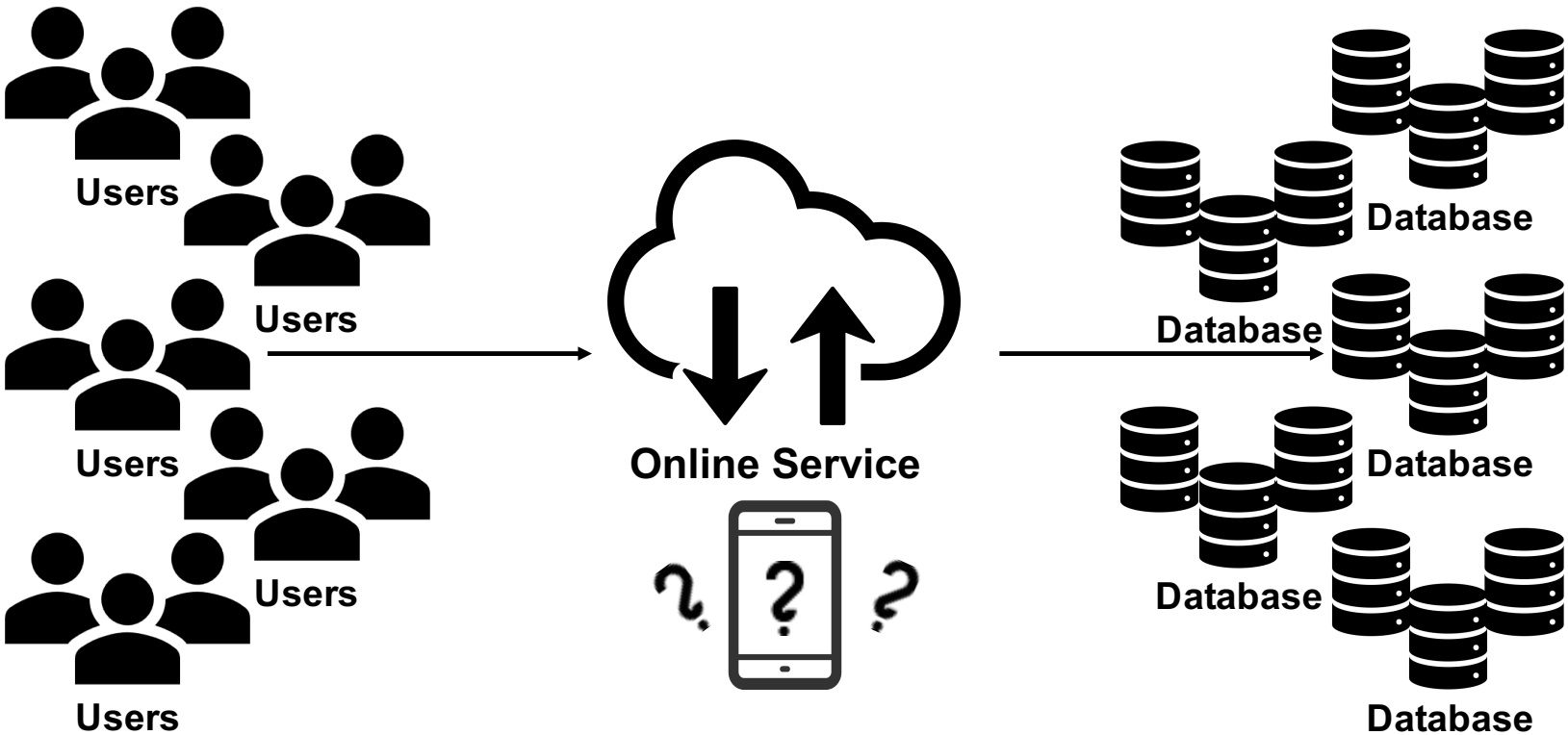
Challenges in Online Service



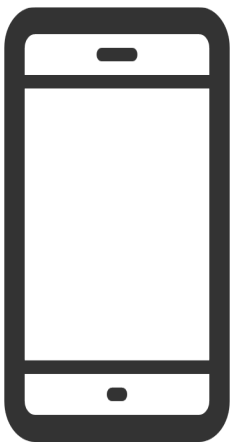
Challenges in Online Service



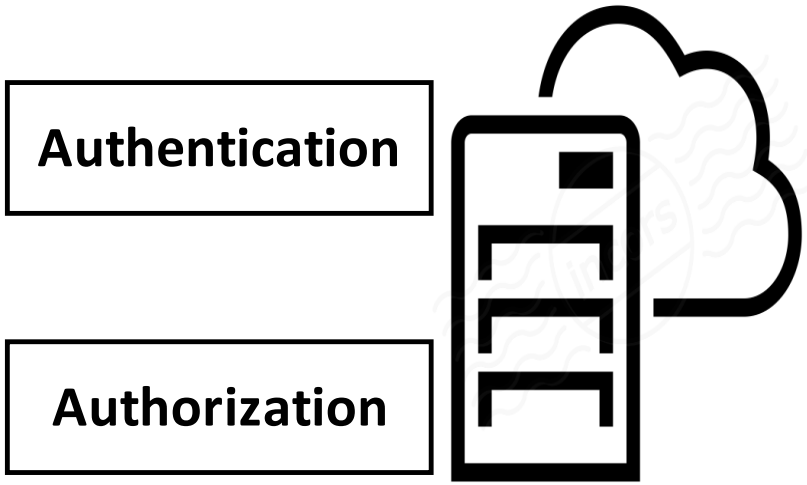
Challenges in Online Service



Access Control in Online Service

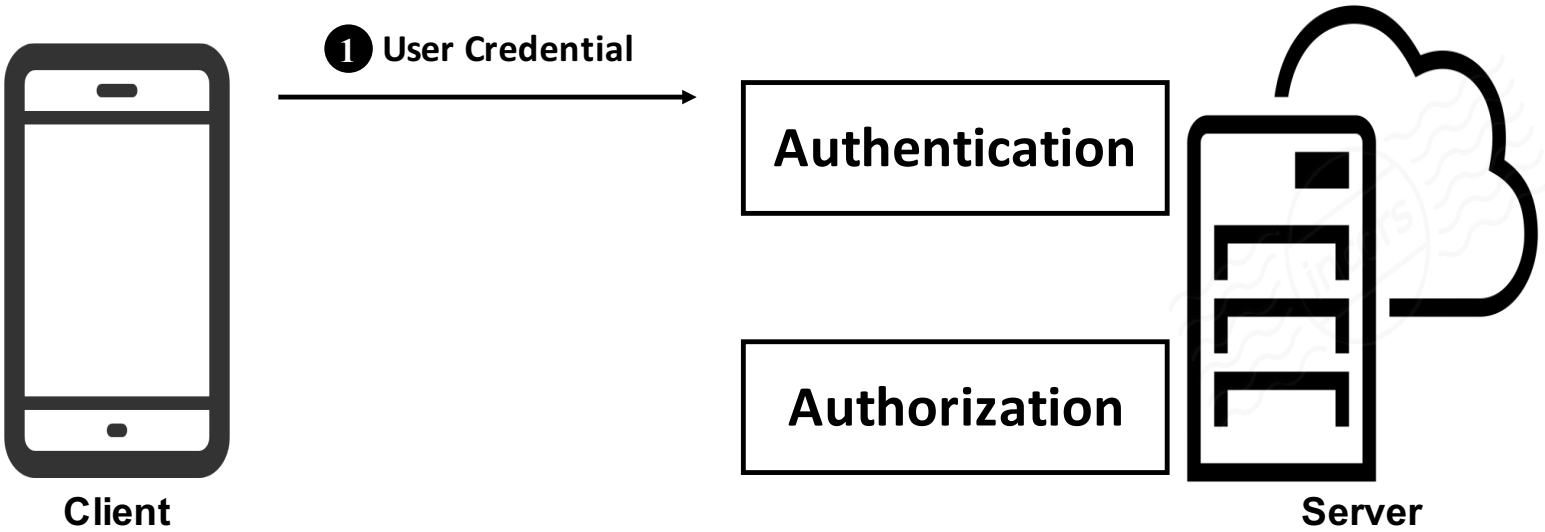


Client

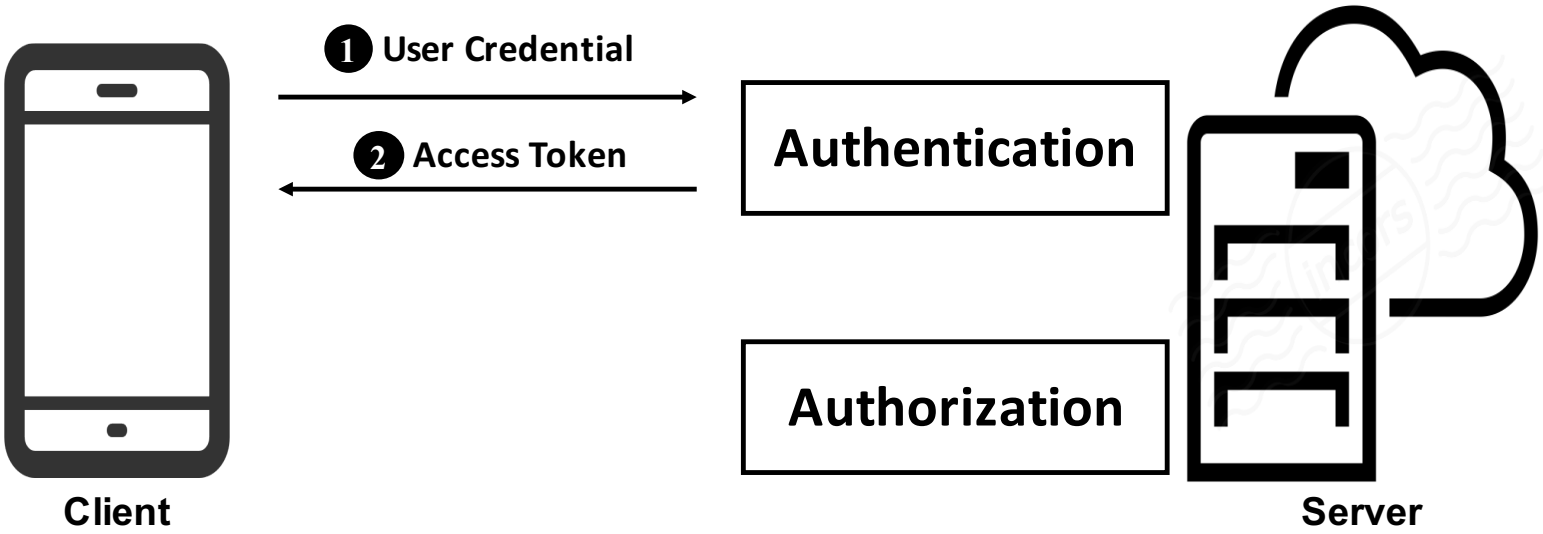


Server

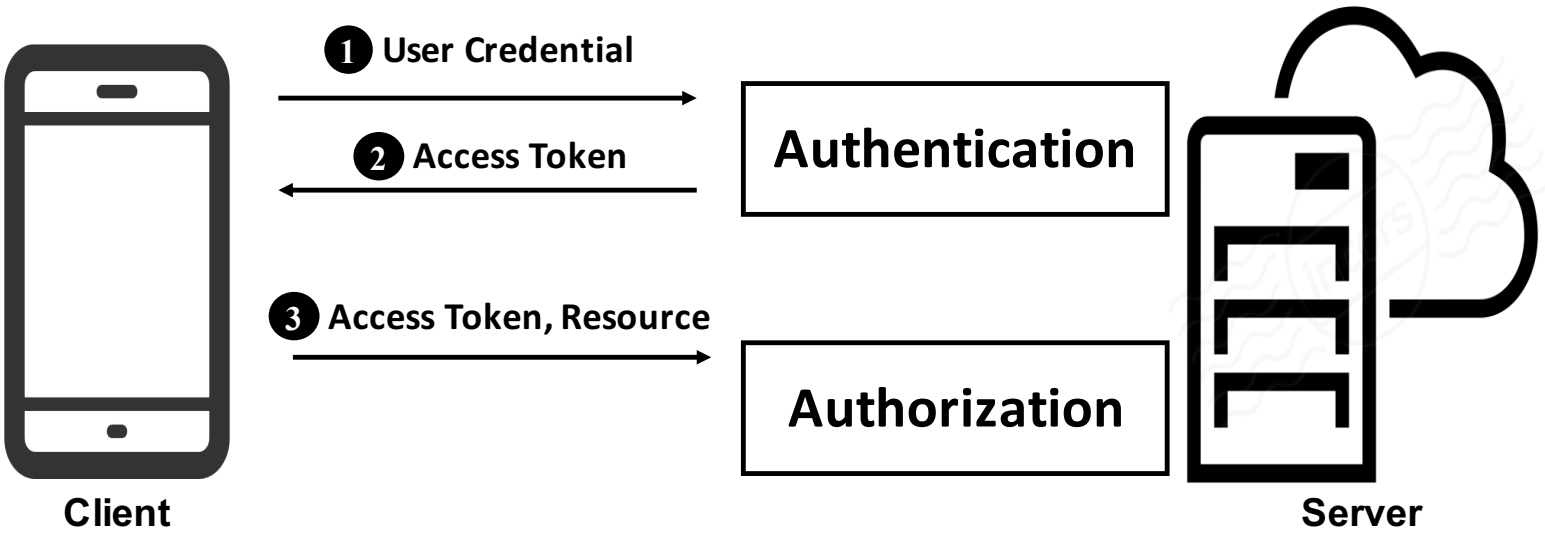
Access Control in Online Service



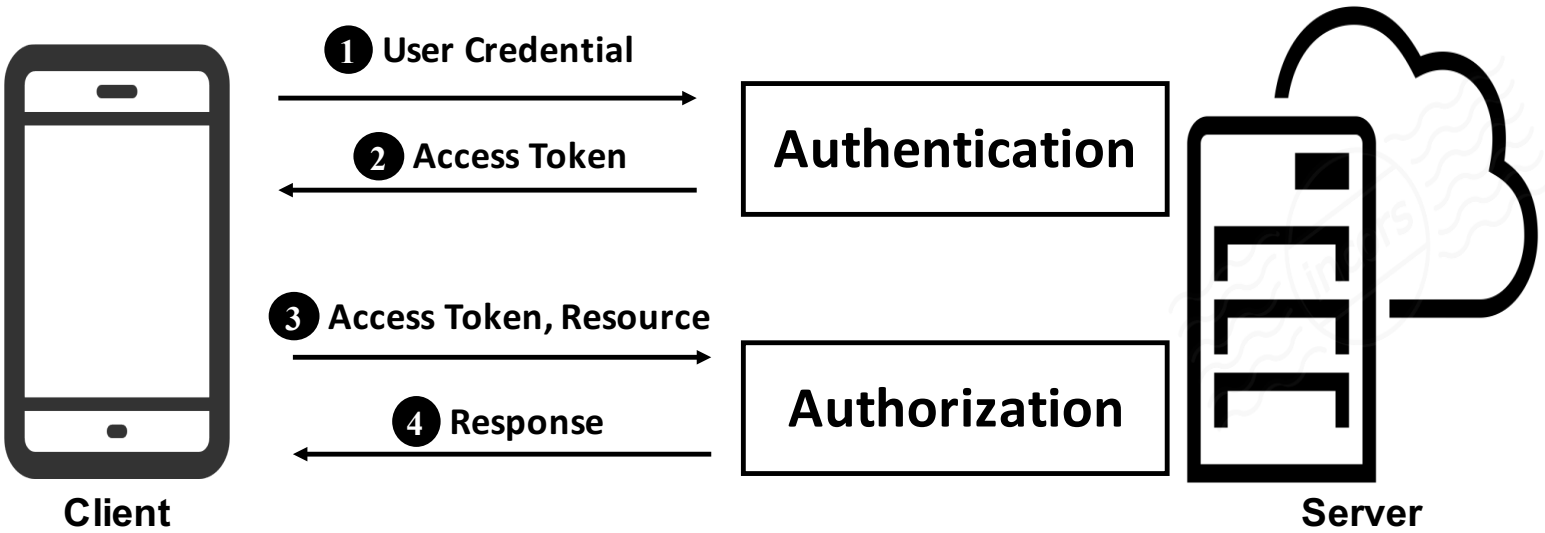
Access Control in Online Service



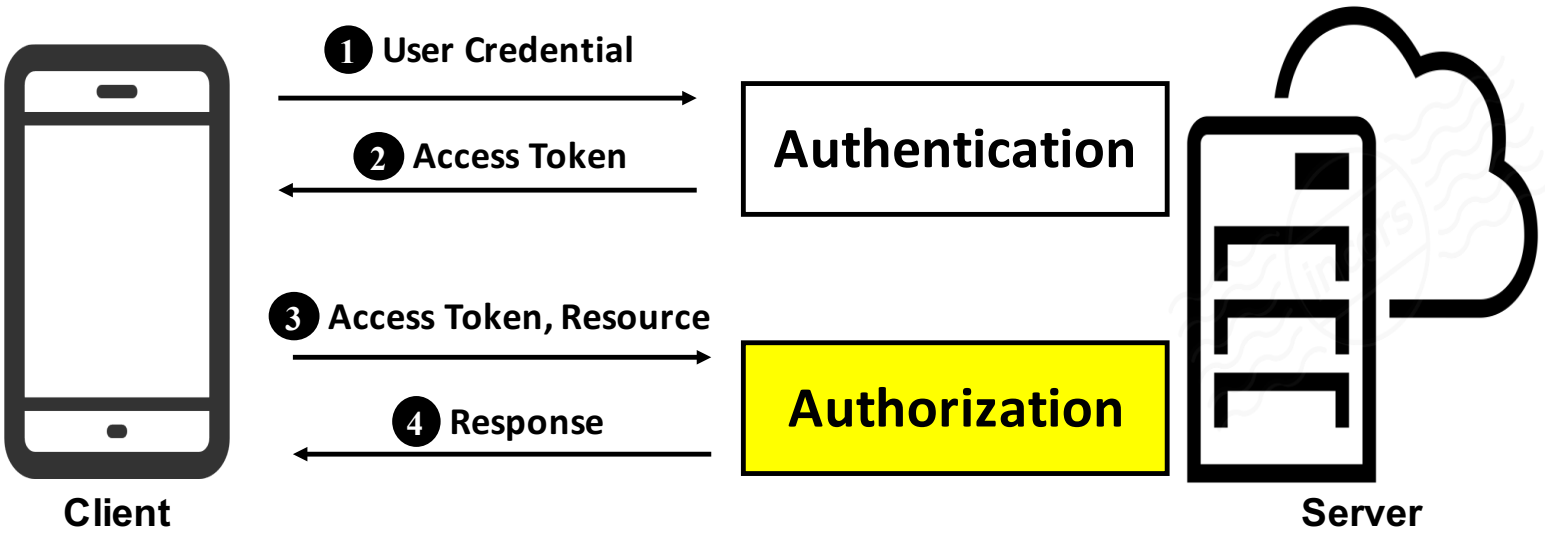
Access Control in Online Service



Access Control in Online Service



Access Control in Online Service



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
  $https://www.overleaf.com/9357323vdzpzwzmwdmx$

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=e67315b35aa3
8d4ac8cac3cd9c7f88ae7f576d373f 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

[{"id":433222,"sender":null,"dog":null,"notification_type":15,"n
otification_text":"Welcome to w****.","object_id":21690,"is_seen
":true,"is_read":true,"created_at":"2017-01-28T23:54:59.831Z"}]
```

Alice's first request and response message after login

A Running Example

```
GET /api/v1//users/21691/notifications?in_app_token=fb153b7d8c0a
0c6ac841d7bfbd9446de627c642858 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":433227,"sender":null,"dog":null,"notification_type":15,"n
otification_text":"Welcome to w****.","object_id":21691,"is_seen
":true,"is_read":false,"created_at":"2017-01-28T23:56:40.533Z"}]
```

Bob's first request and response message after login

A Running Example

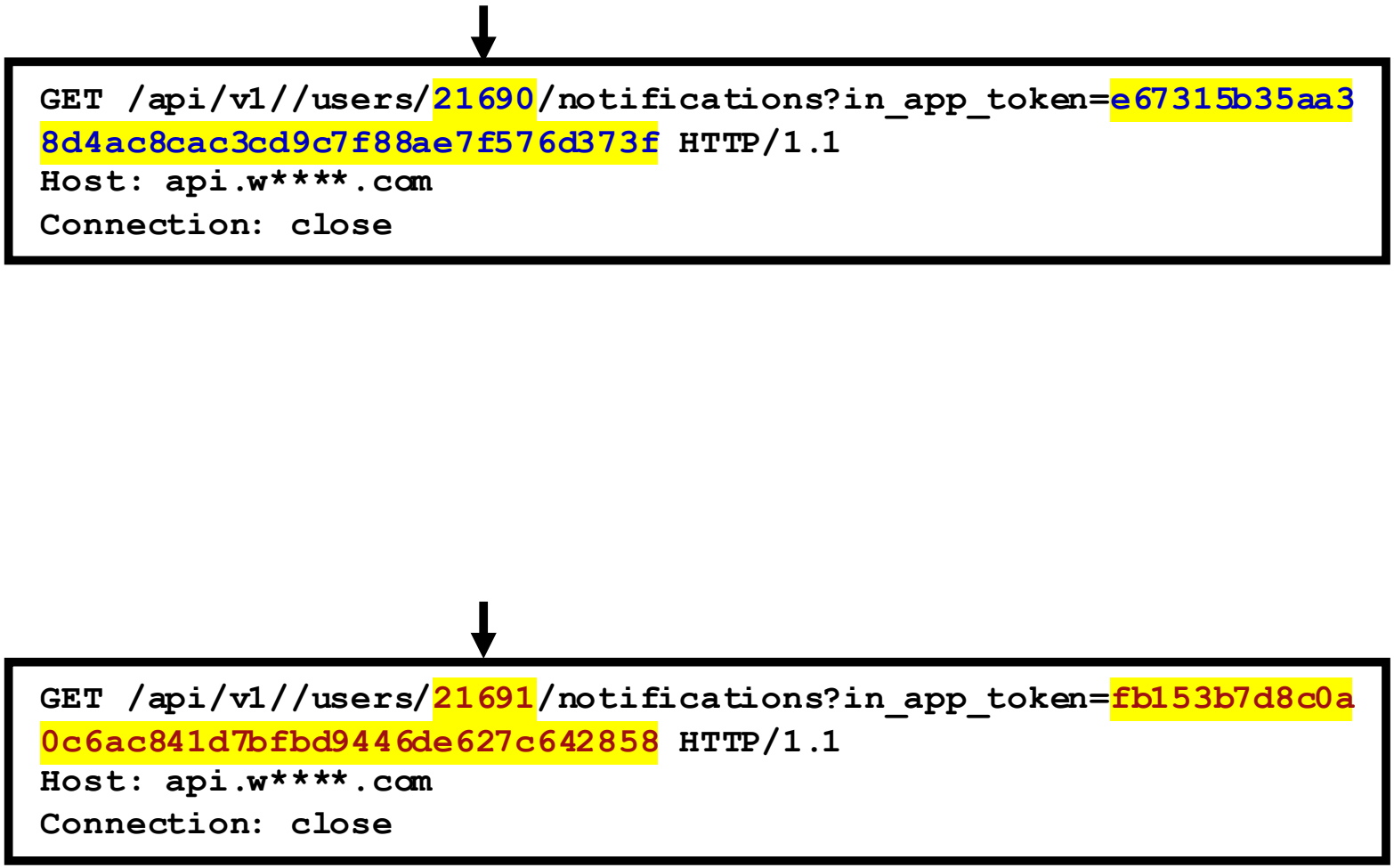
```
GET /api/v1//users/21690/notifications?in_app_token=e67315b35aa3
8d4ac8cac3cd9c7f88ae7f576d373f HTTP/1.1
Host: api.w****.com
Connection: close
```

Alice's first request message after login

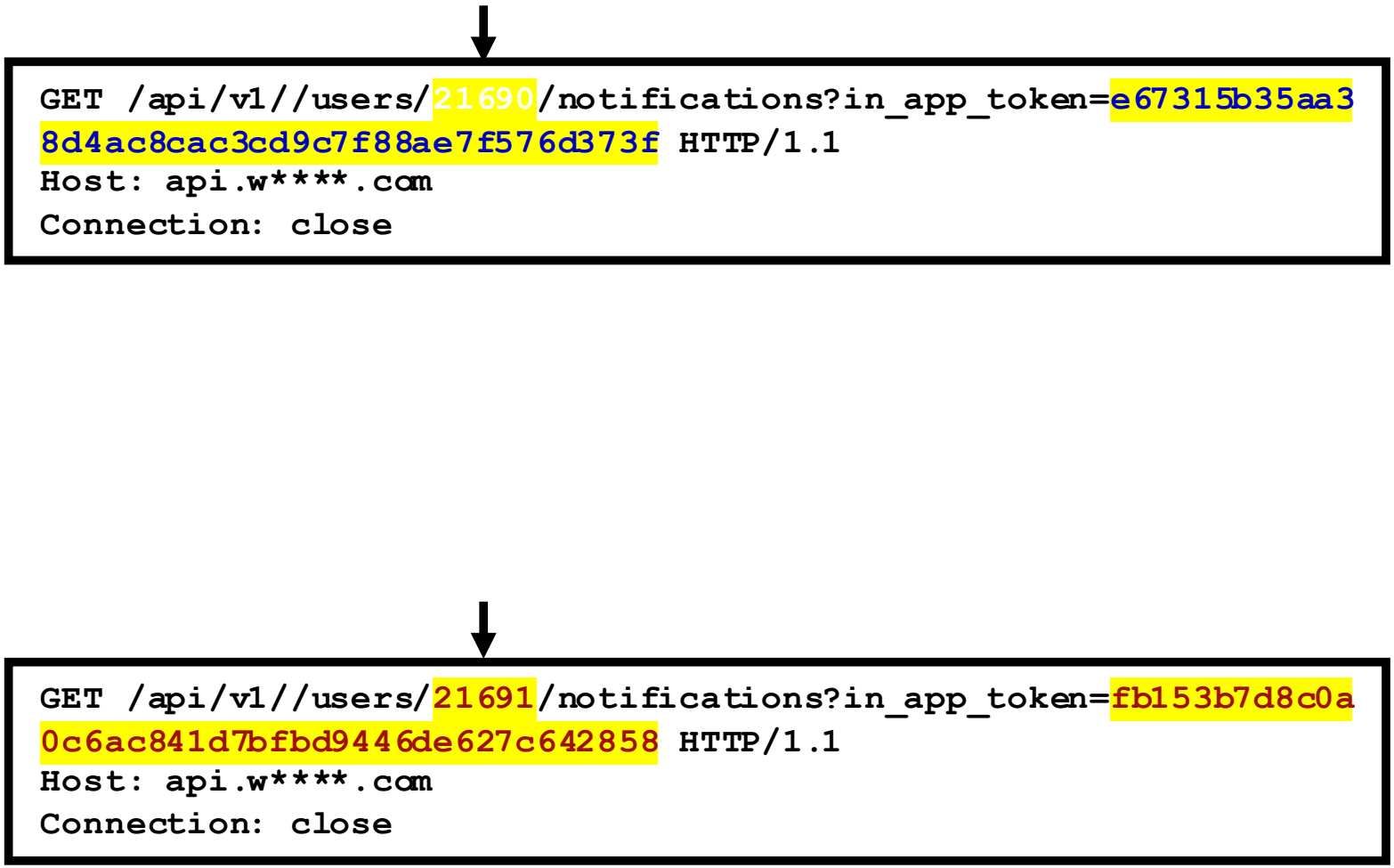
```
GET /api/v1//users/21691/notifications?in_app_token=fb153b7d8c0a
0c6ac841d7bfbd9446de627c642858 HTTP/1.1
Host: api.w****.com
Connection: close
```

Bob's first request message after login

A Running Example



A Running Example



A Running Example

```
GET /api/v1//users/21691/notifications?in_app_token=e67315b35aa3
8d4ac8cac3cd9c7f88ae7f576d373f HTTP/1.1
Host: api.w****.com
Connection: close
```

A Running Example

```
GET /api/v1//users/21691/notifications?in_app_token=e67315b35aa3
8d4ac8cac3cd9c7f88ae7f576d373f 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":433227,"sender":null,"dog":null,"notification_type":15,"n
otification_text":"Welcome to w****.","object_id":21691,"is_seen
":true,"is_read":false,"created_at":"2017-01-28T23:56:40.533Z"}]
```

Alice reads Bob's notifications

Challenge: Obtain the post-authentication messages

```
GET /api/v1//users/21690/notifications?in_app_token=e67315b35aa3
8d4ac8cac3cd9c7f88ae7f576d373f 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=fb153b7d8c0a
0c6ac841d7bfbd9446de627c642858 HTTP/1.1
Host: api.w****.com
Connection: close
```

Bob's first request message after login

Challenge: Obtain the post-authentication messages

```
GET /api/v1//users/21690/notifications?in_app_token=e67315b35aa3
8d4ac8cac3cd9c7f88ae7f576d373f HTTP/1.1
Host: api.w****.com
Connection: close
```

Alice's first request message after login

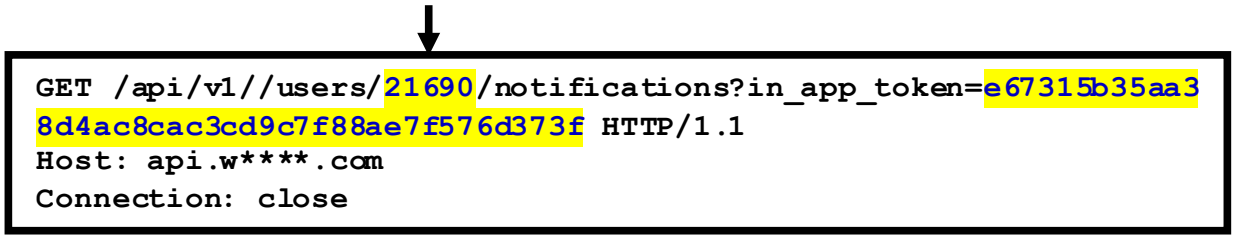
```
GET /api/v1//users/21691/notifications?in_app_token=fb153b7d8c0a
0c6ac841d7bfbd9446de627c642858 HTTP/1.1
Host: api.w****.com
Connection: close
```

Bob's first request message after login

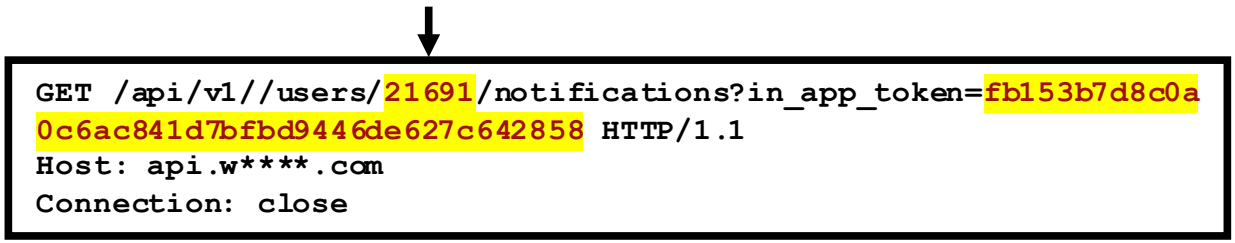
Insights

Executing the app with single-sign-on.

Challenge: Recognize&Substitute fields of interest

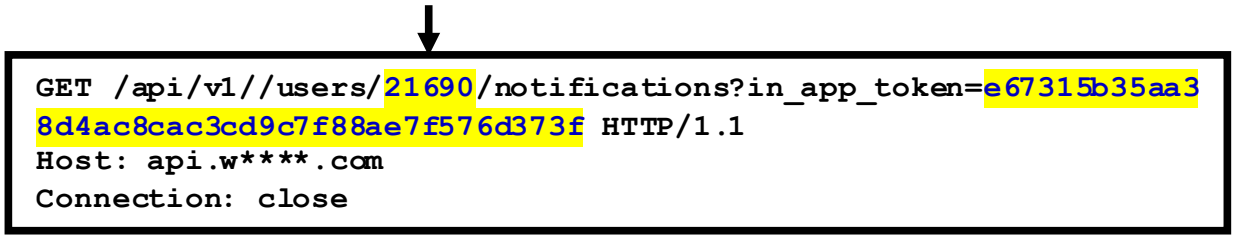


Alice's first request message after login

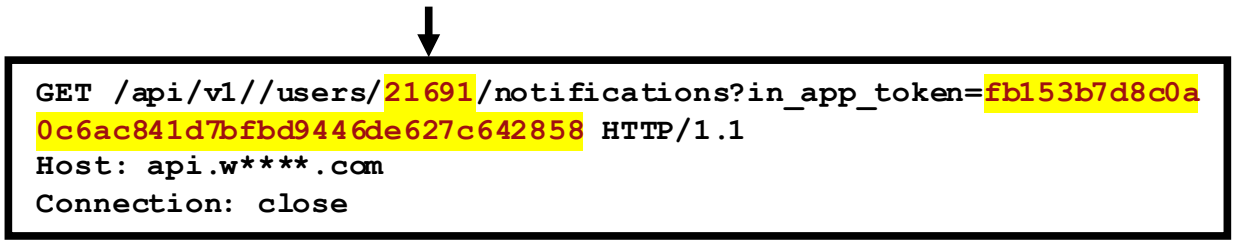


Bob's first request message after login

Challenge: Recognize&Substitute fields of interest



Alice's first request message after login



Bob's first request message after login

Insights

Differential traffic analysis and small Euclidean distance.

Challenge: Identify the vulnerability

```
GET /api/v1//users/21691/notifications?in_app_token=e67315b35aa3
8d4ac8cac3cd9c7f88ae7f576d373f 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":433227,"sender":null,"dog":null,"notification_type":15,"n
otification_text":"Welcome to w****.","object_id":21691,"is_seen
":true,"is_read":false,"created_at":"2017-01-28T23:56:40.533Z"}]
```

Alice reads Bob's notifications

Challenge: Identify the vulnerability

```
GET /api/v1//users/21691/notifications?in_app_token=e67315b35aa3
8d4ac8cac3cd9c7f88ae7f576d373f 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":433227,"sender":null,"dog":null,"notification_type":15,"n
otification_text":"Welcome to w****.","object_id":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 & Assumption

Problem Statement

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

Problem Statement & Assumption

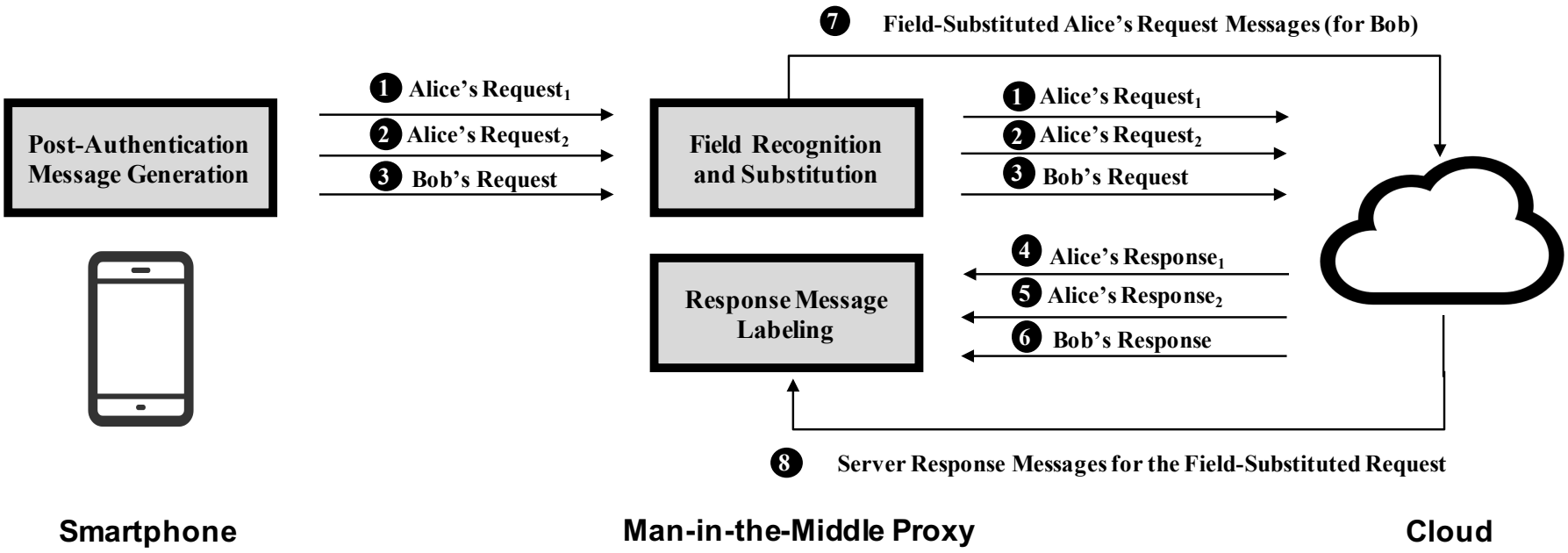
Problem Statement

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

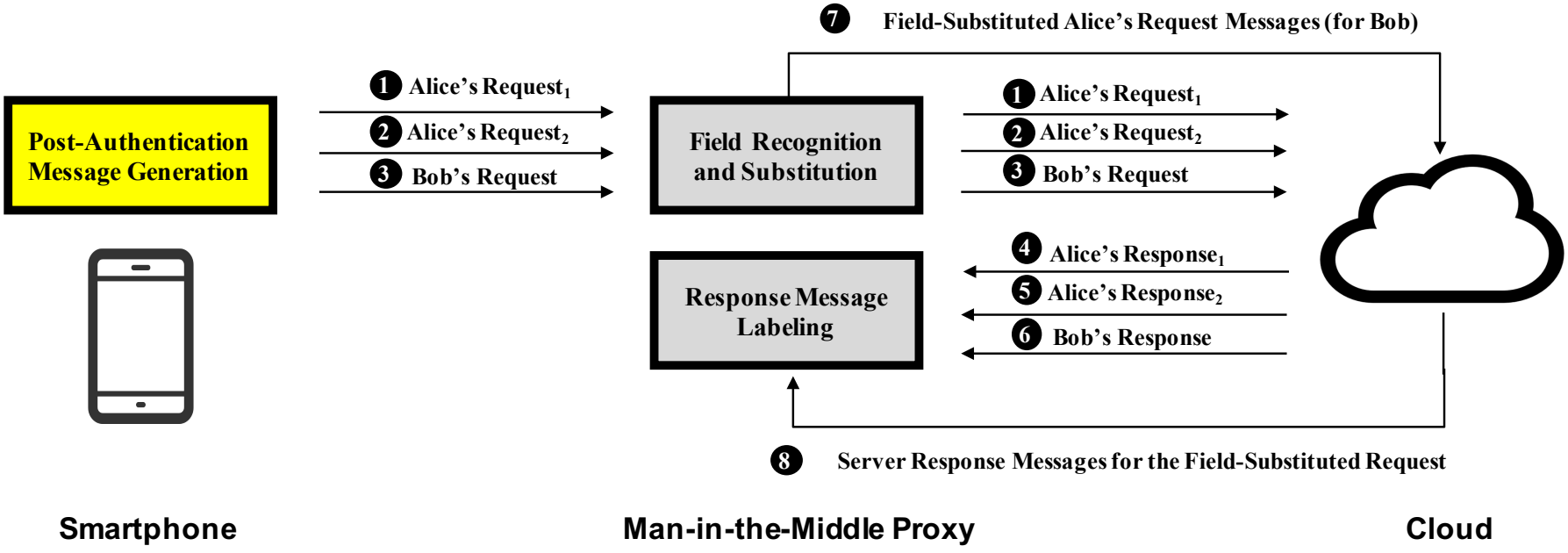
Assumptions

- HTTP/HTTPS protocol
- Facebook login

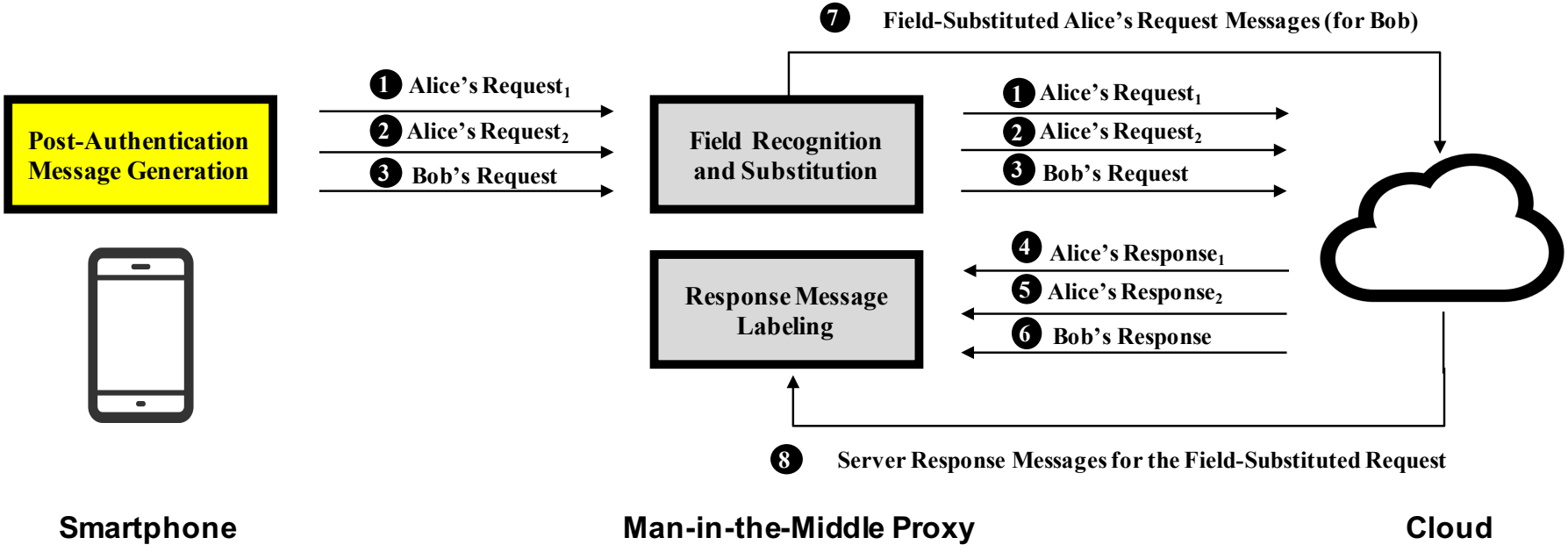
Overview of AUTHSCOPE



Post-Authentication Message Generation

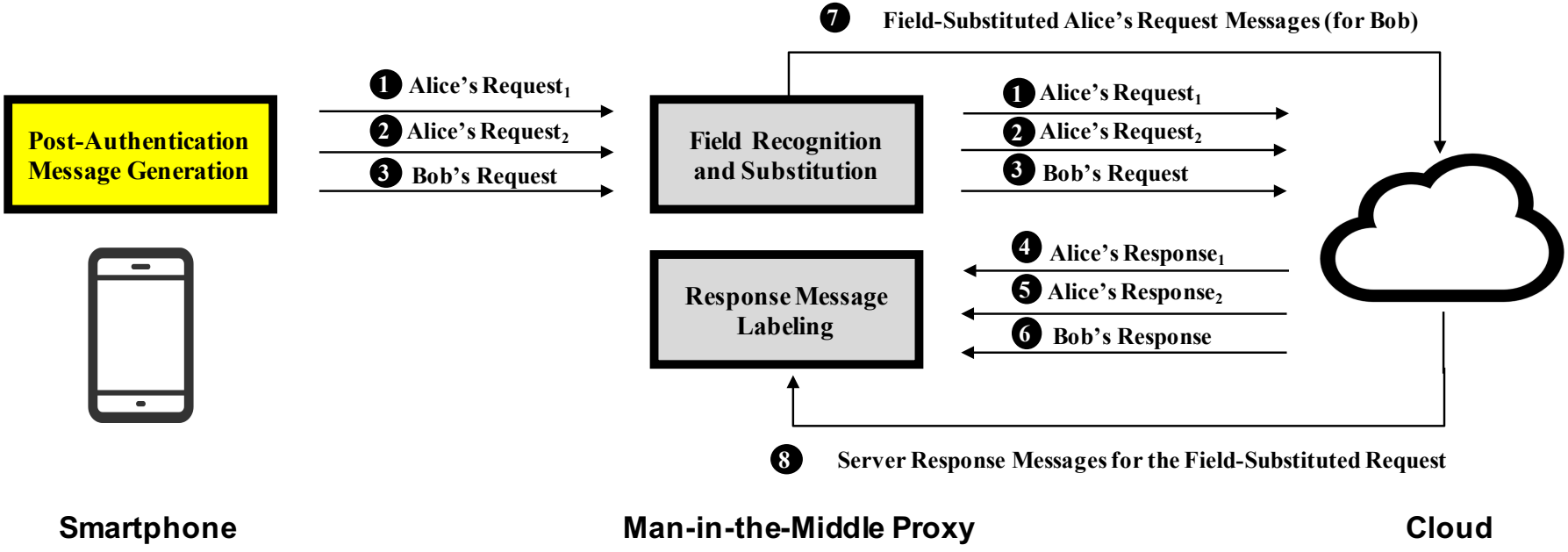


Post-Authentication Message Generation



- View Identification and Exploration

Post-Authentication Message Generation



- View Identification and Exploration
- Automatic Social-based Service Login

Post-Authentication Message Generation Cont

Post-Authentication Message Generation Cont

Button 1

Post-Authentication Message Generation Cont

Button 1

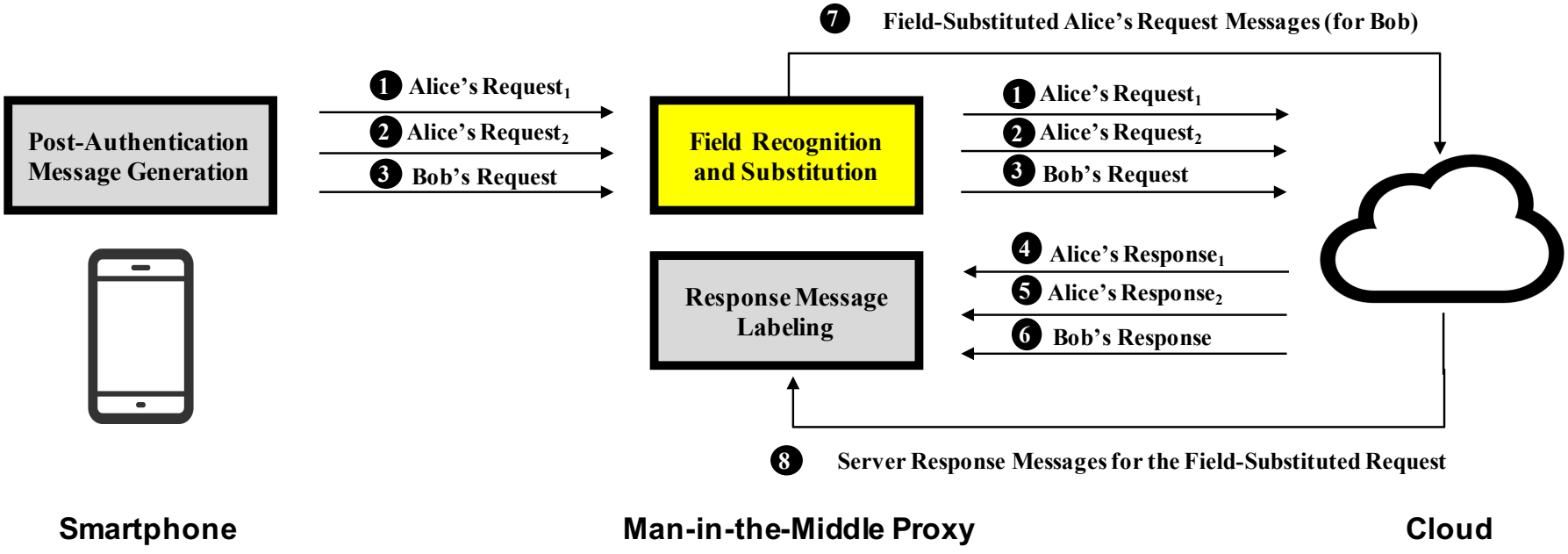
Button 2

Post-Authentication Message Generation Cont

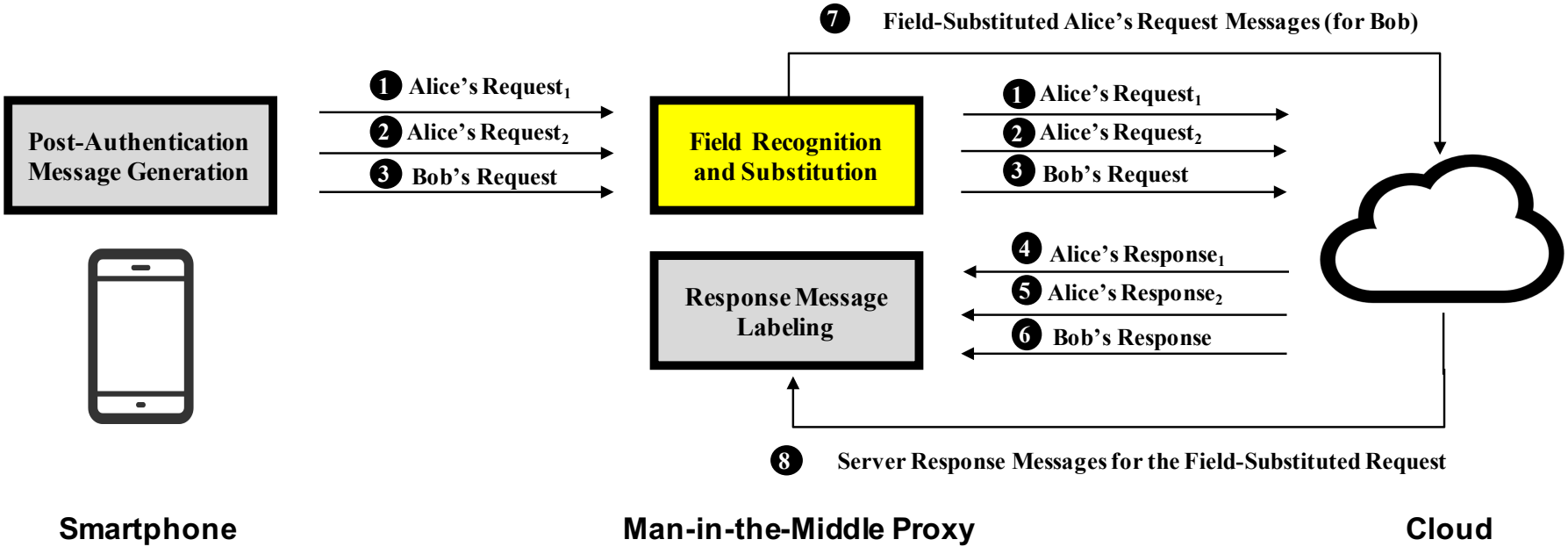
Button 1 → FaceBook Login

Button 2

Field Recognition and Substitution

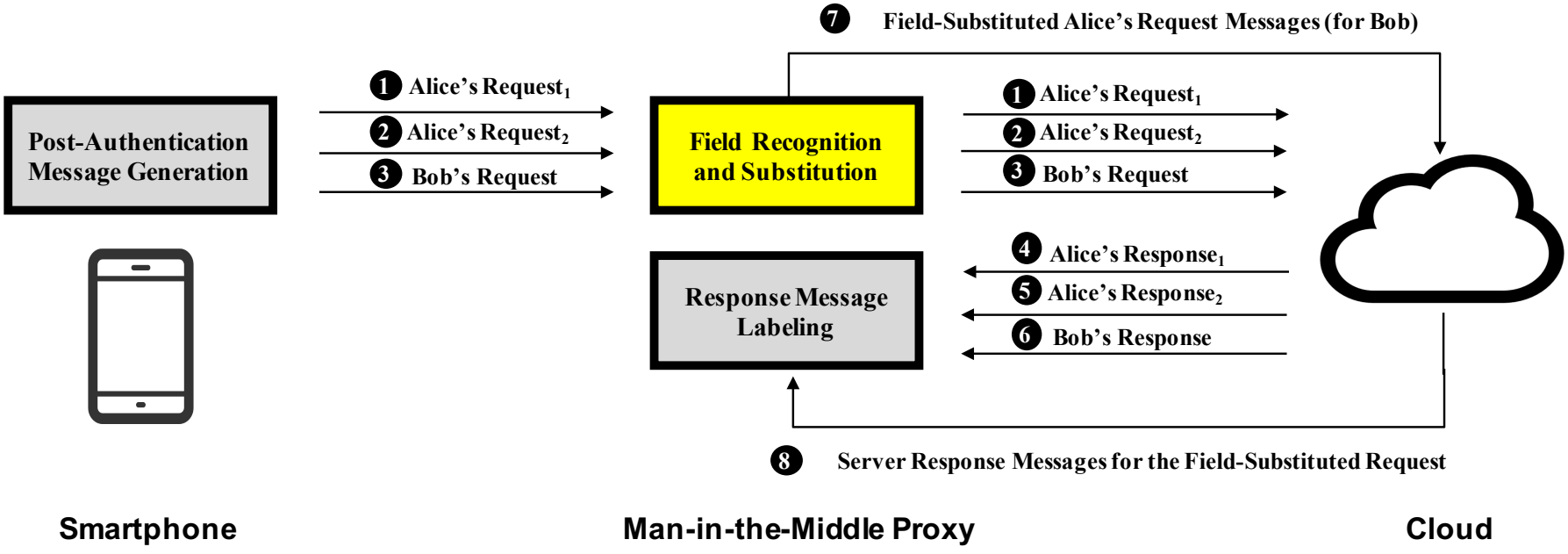


Field Recognition and Substitution



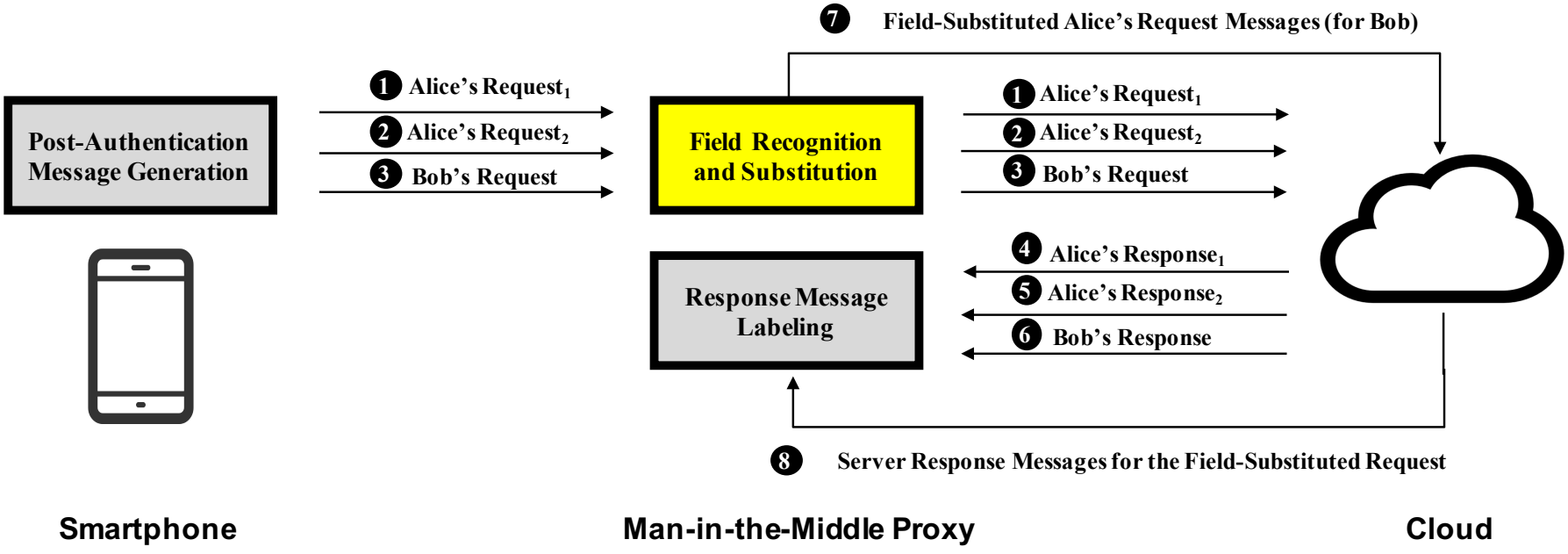
- Parsing Message Fields

Field Recognition and Substitution



- Parsing Message Fields
- Identifying Fields of Interest

Field Recognition and Substitution

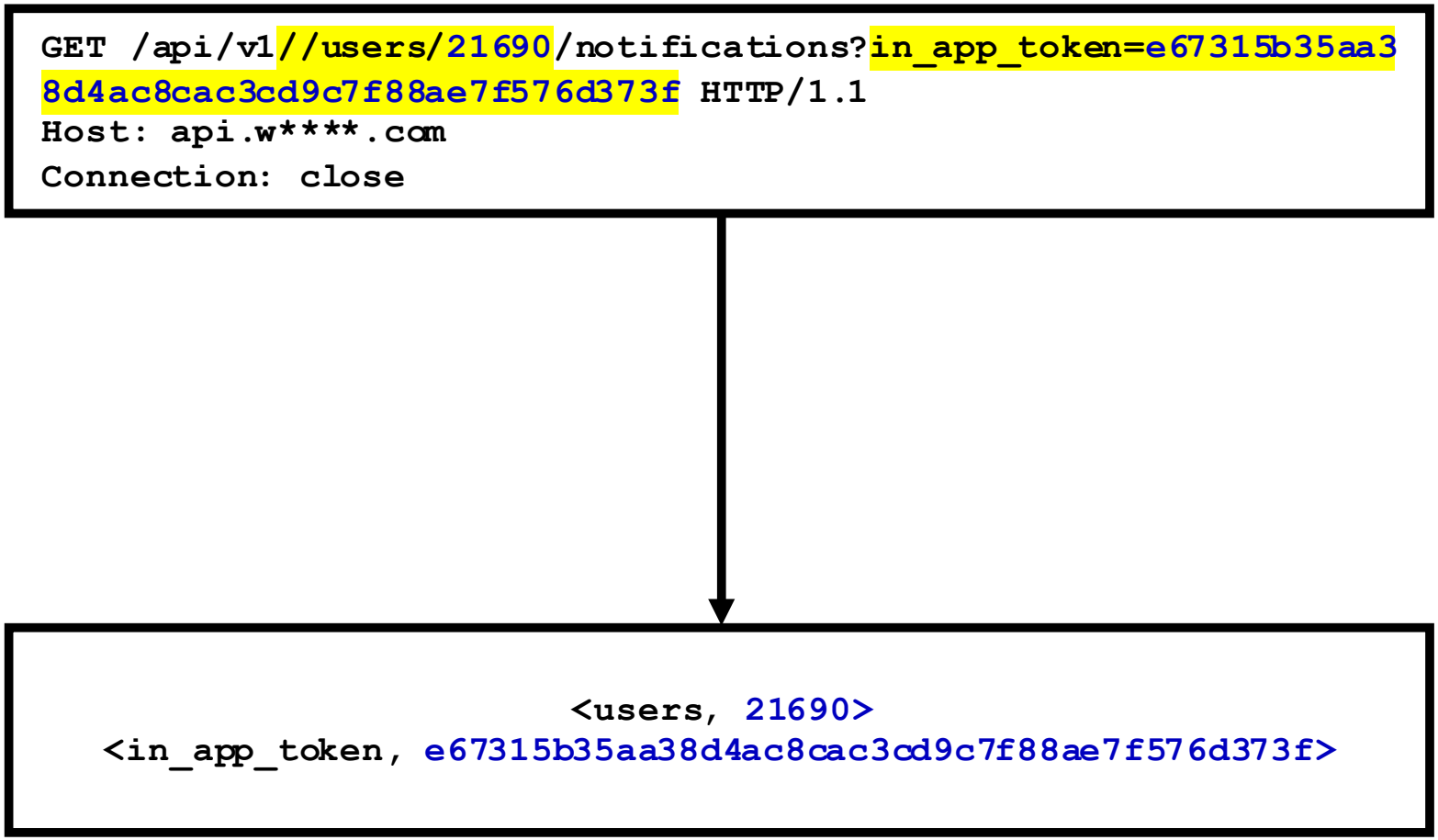


- Parsing Message Fields
- Identifying Fields of Interest
- Substituting Enumerable Fields

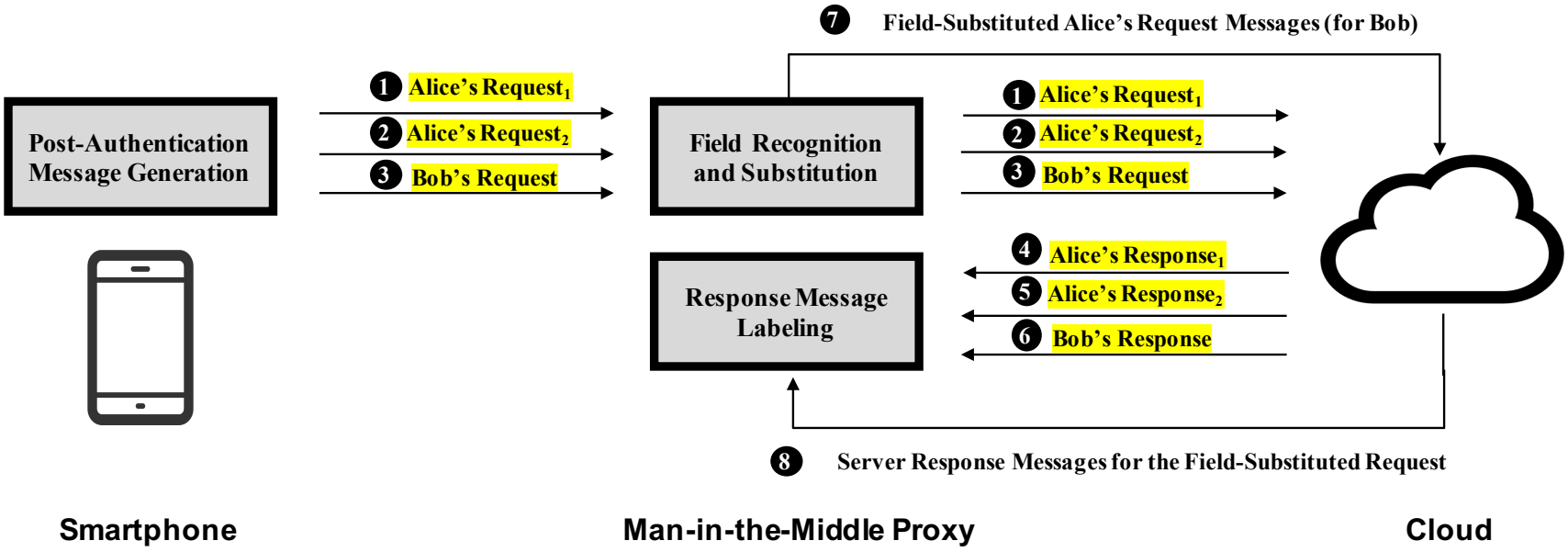
Field Recognition and Substitution Cont

```
GET /api/v1//users/21690/notifications?in_app_token=e67315b35aa3
8d4ac8cac3cd9c7f88ae7f576d373f HTTP/1.1
Host: api.w****.com
Connection: close
```

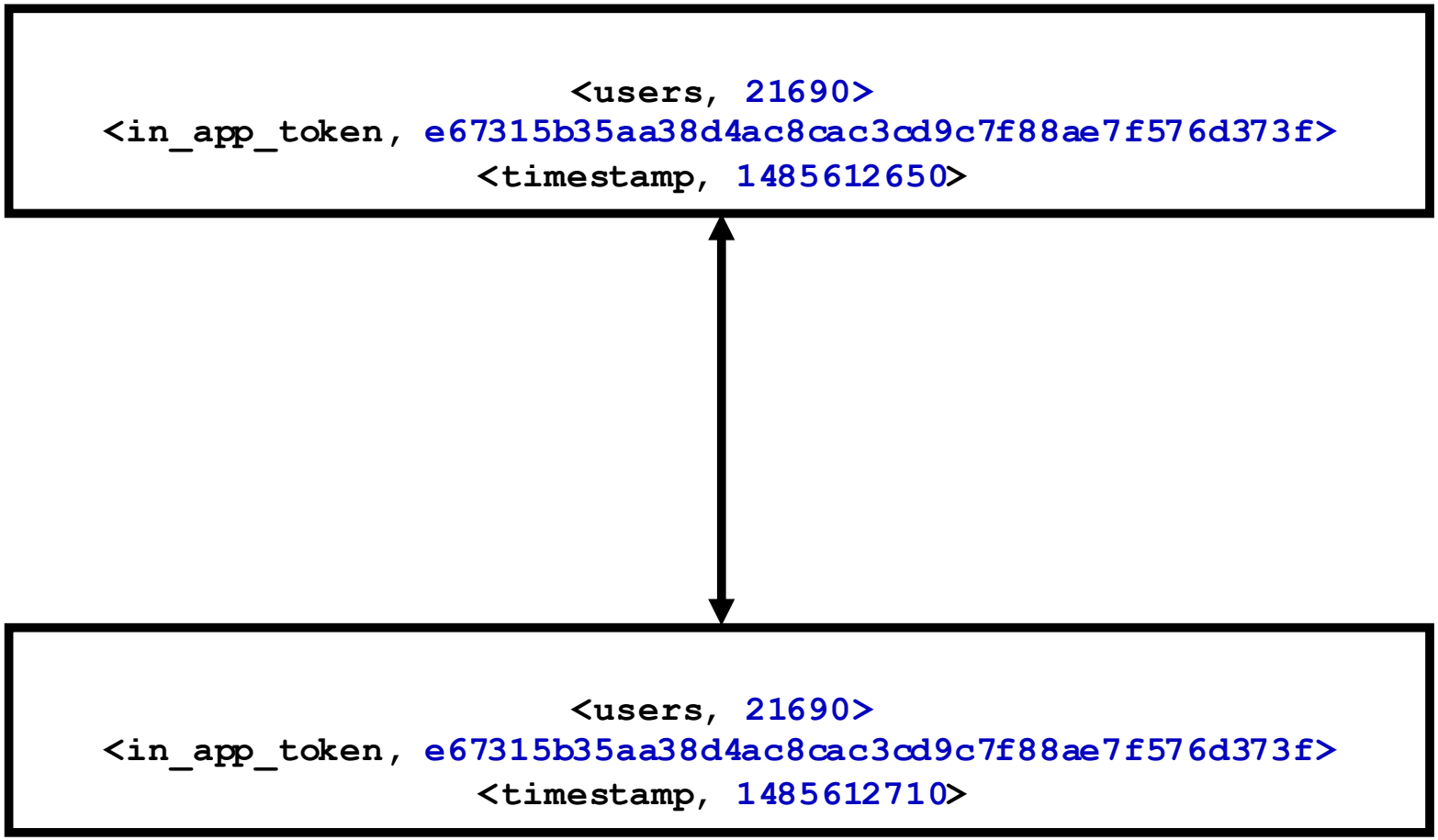
Field Recognition and Substitution Cont



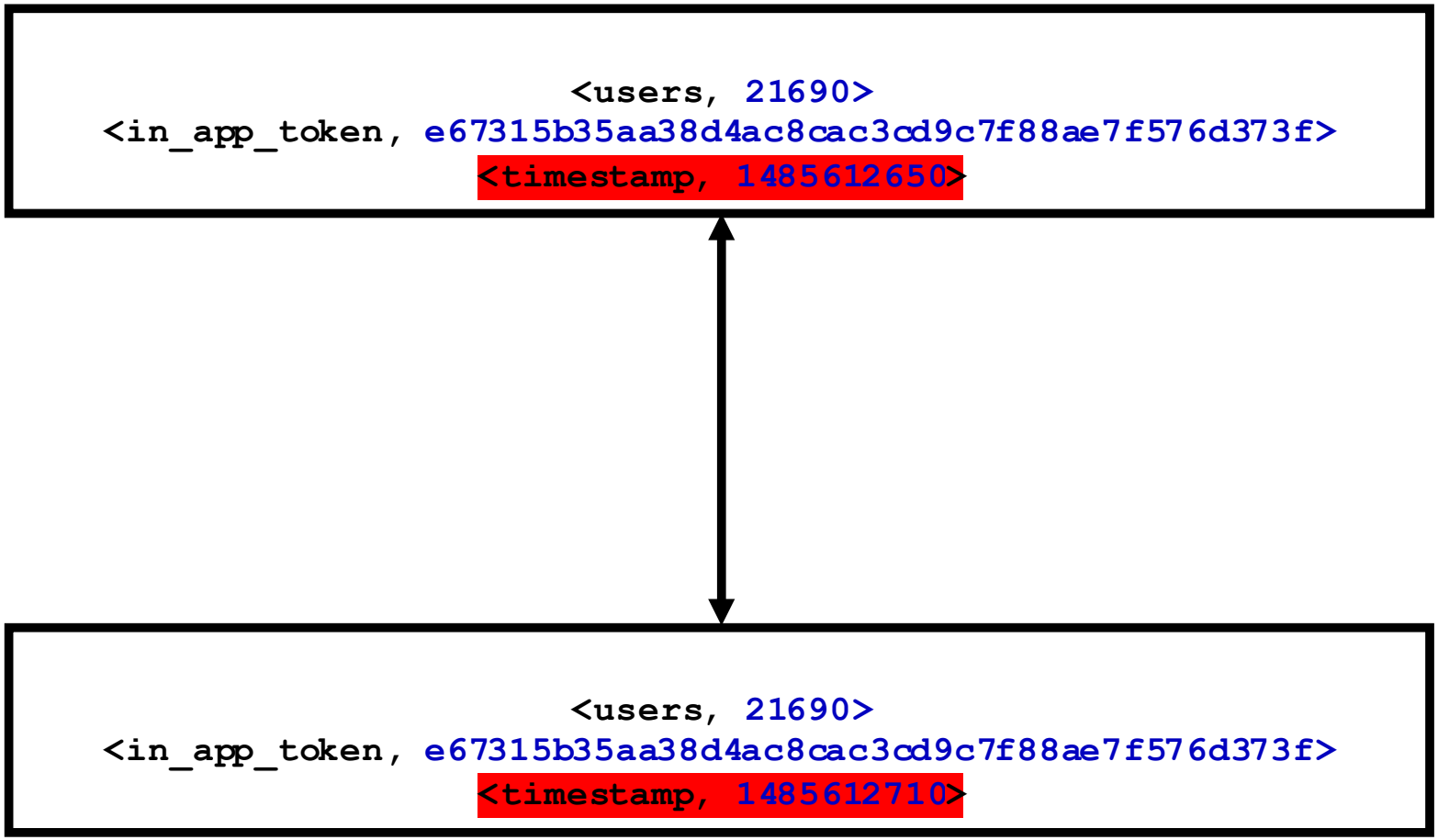
Field Recognition and Substitution Cont



Field Recognition and Substitution Cont



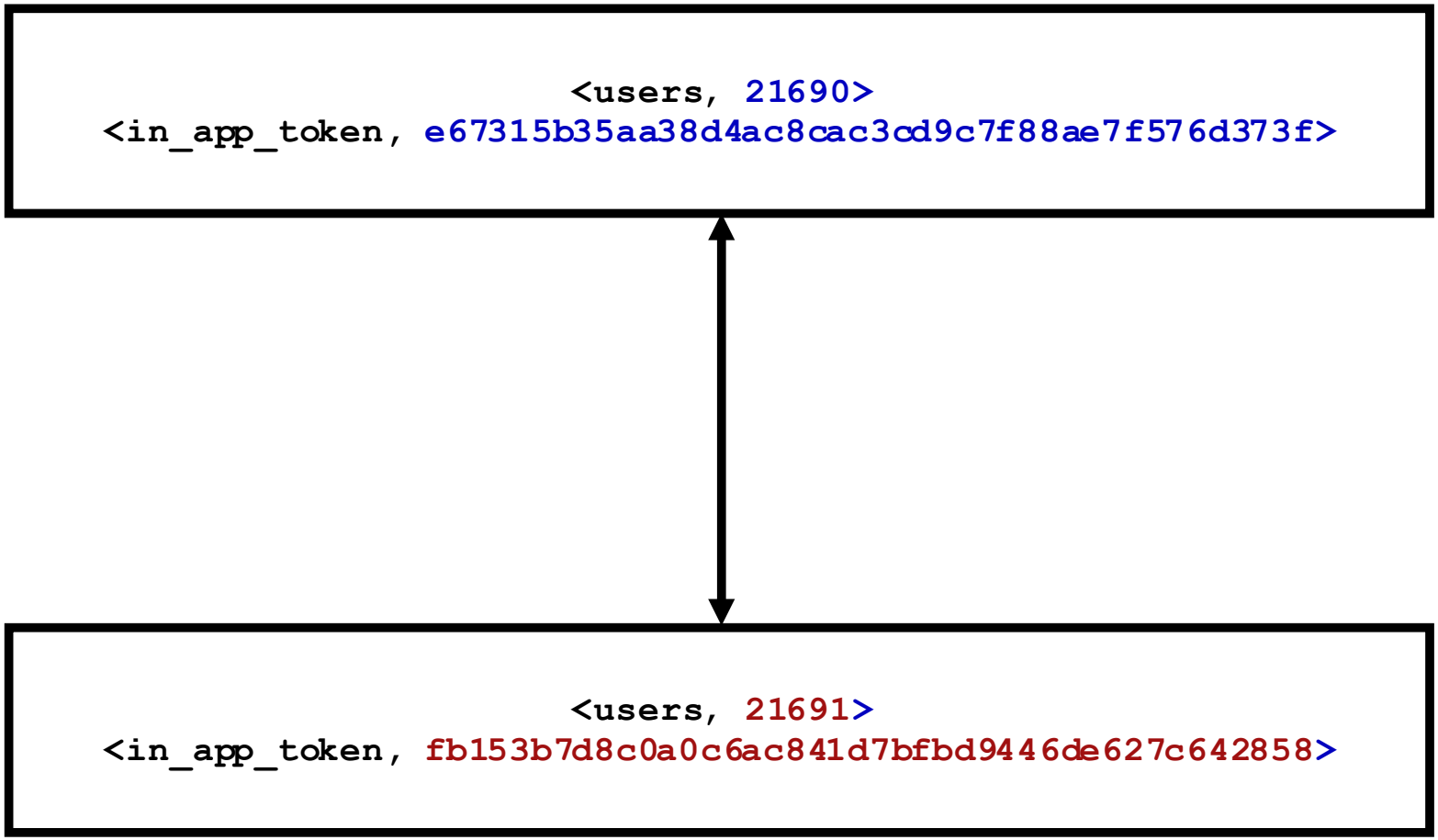
Field Recognition and Substitution Cont



Field Recognition and Substitution Cont

```
<users, 21690>
<in_app_token, e67315b35aa38d4ac8cac3cd9c7f88ae7f576d373f>
```

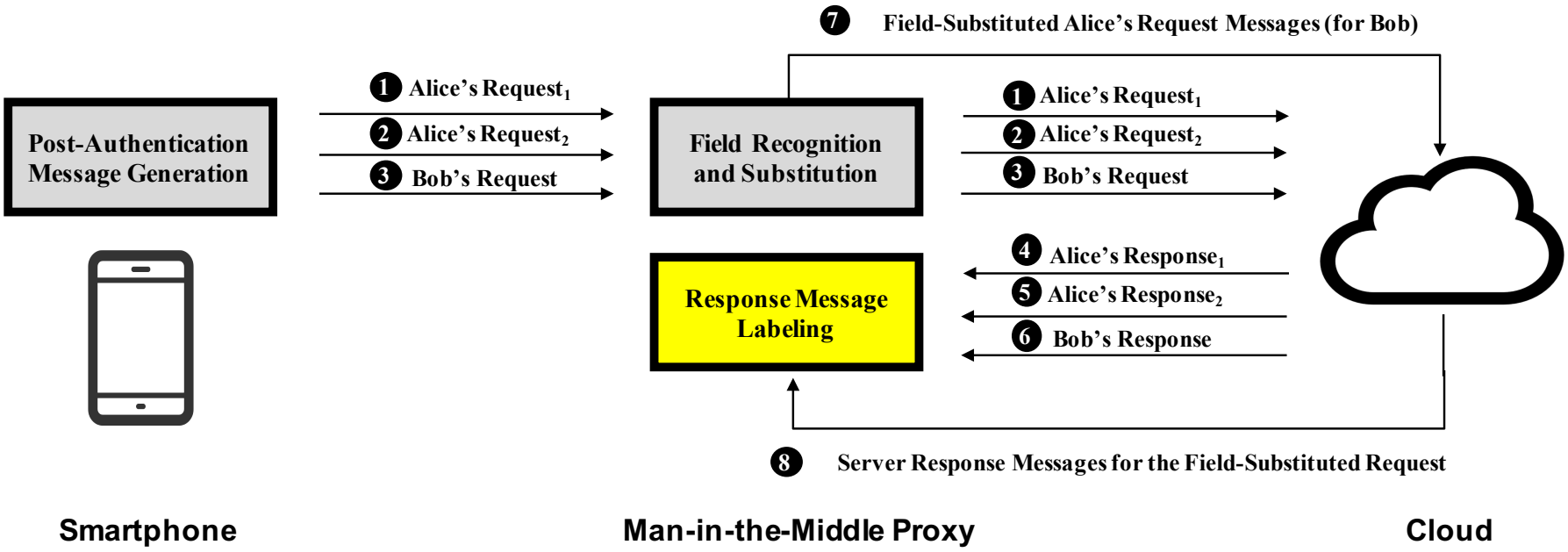
Field Recognition and Substitution Cont



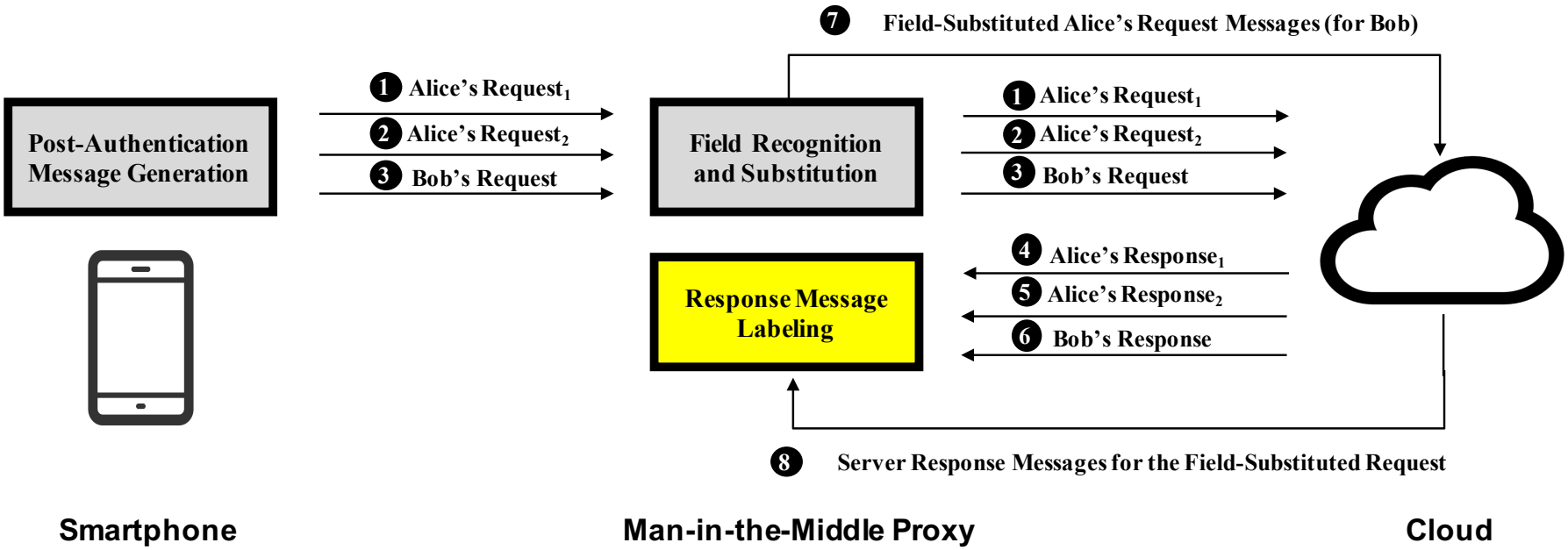
Field Recognition and Substitution Cont

Field-Value of Alice vs. Field-Value of Bob	ED
e67315b35aa38d4ac8cac3cd9c7f88ae7f576d373f	$+\infty$
fb153b7d8c0a0c6ac841d7bfbd9446de627c642858	
21690	1.0
21691	

Response Message Labeling

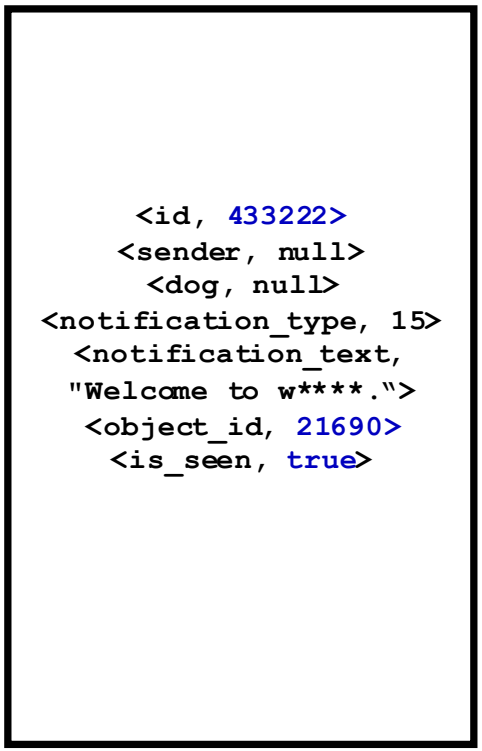


Response Message Labeling

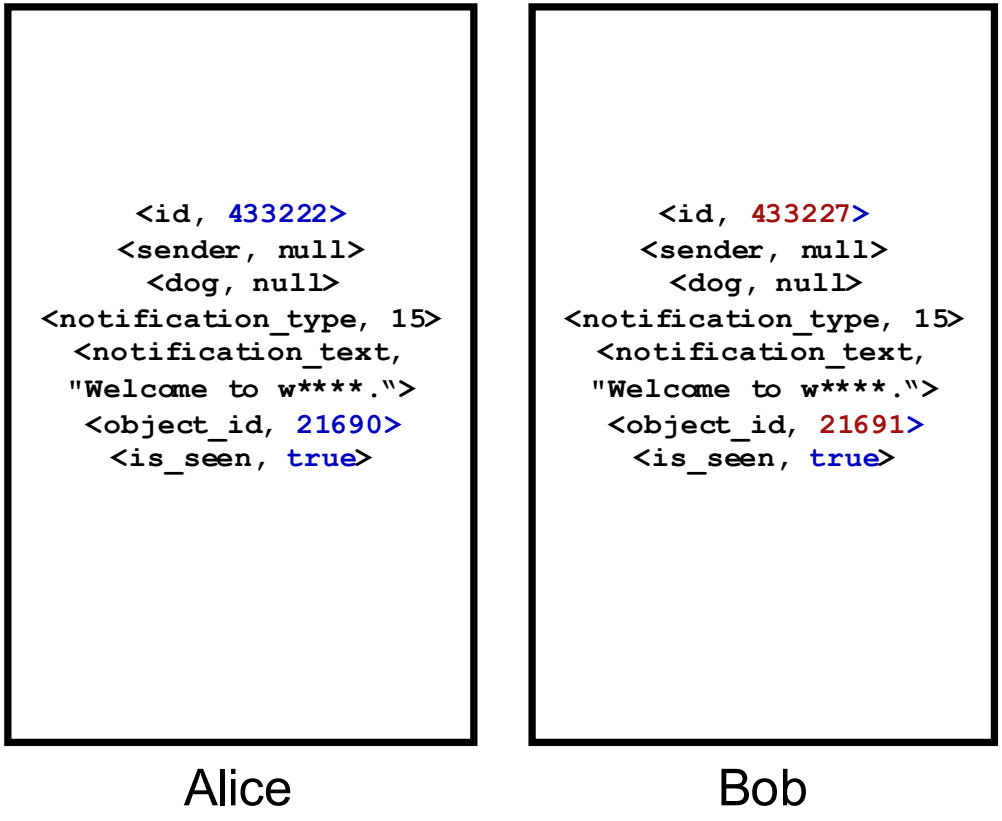


- Labeling response messages indicate vulnerability

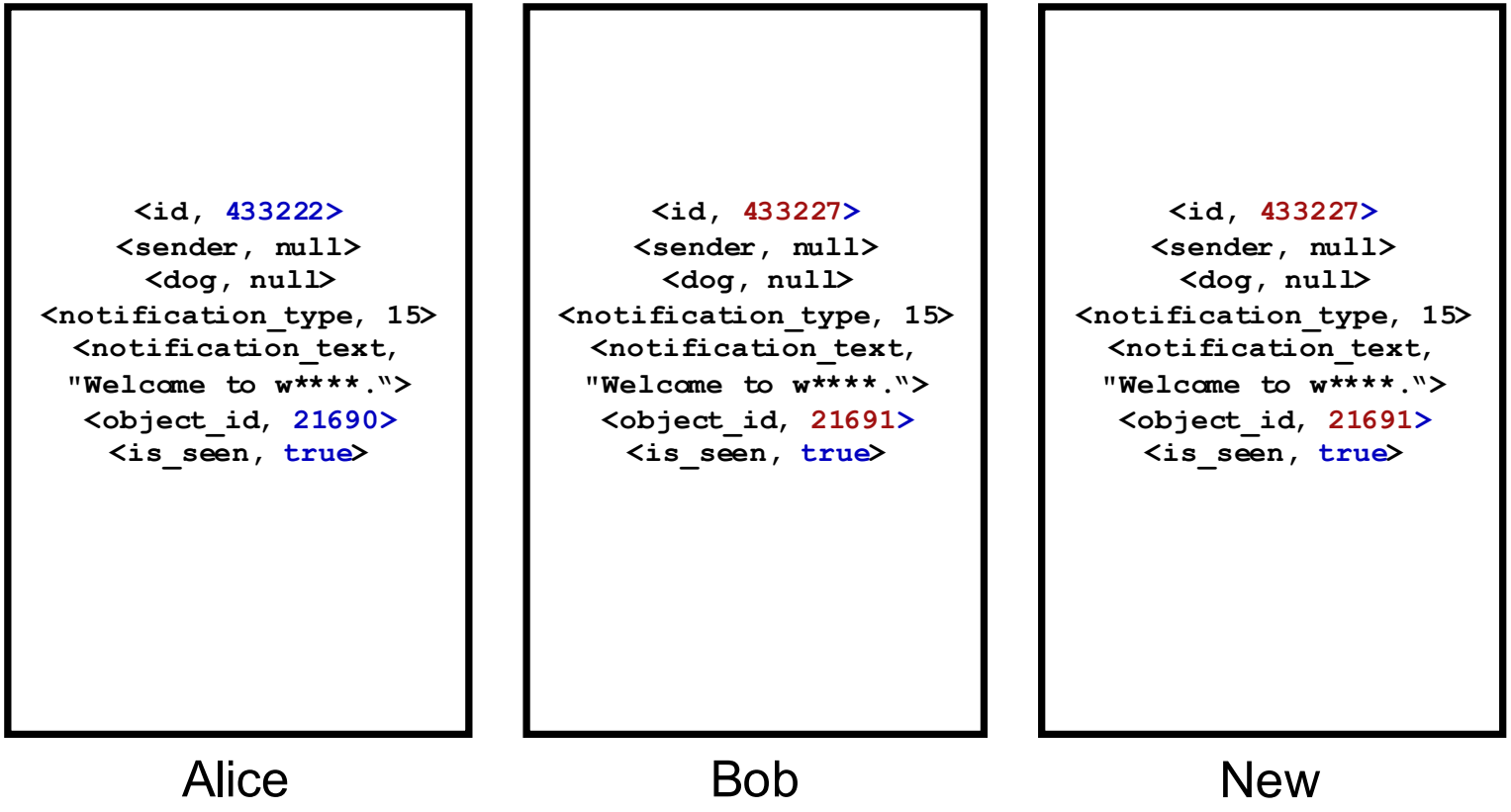
Response Message Labeling Cont



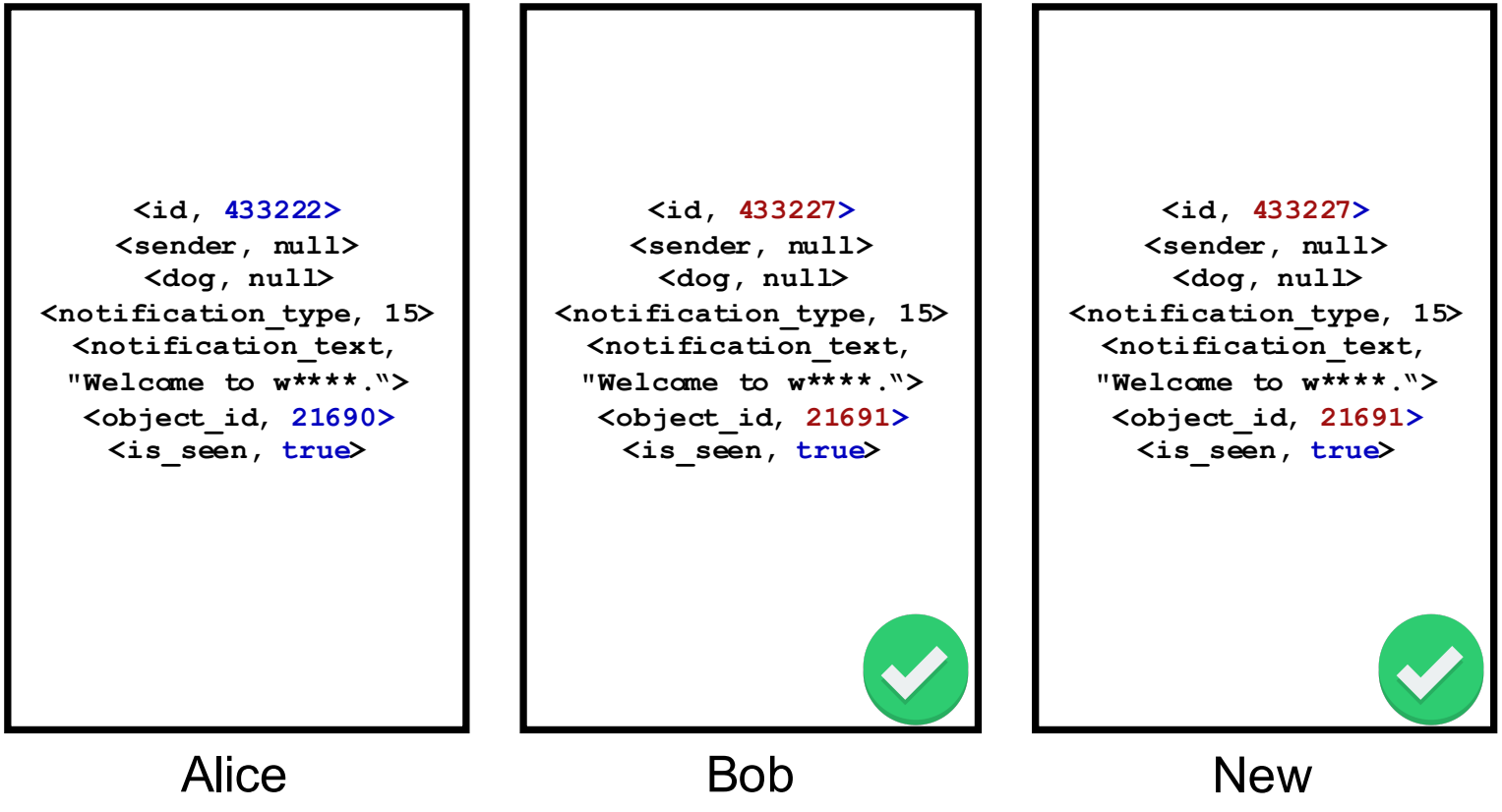
Response Message Labeling Cont



Response Message Labeling Cont



Response Message Labeling Cont



Response Message Labeling Cont

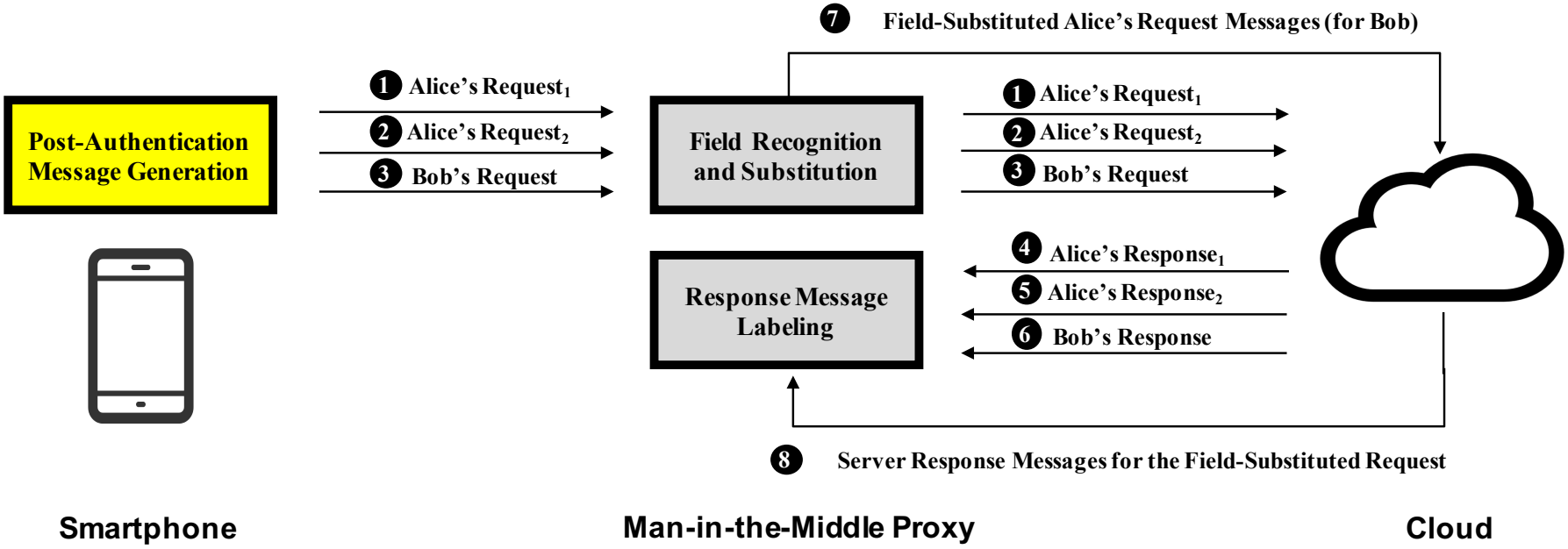
Prune Public Interfaces

Response Message Labeling Cont

Prune Public Interfaces

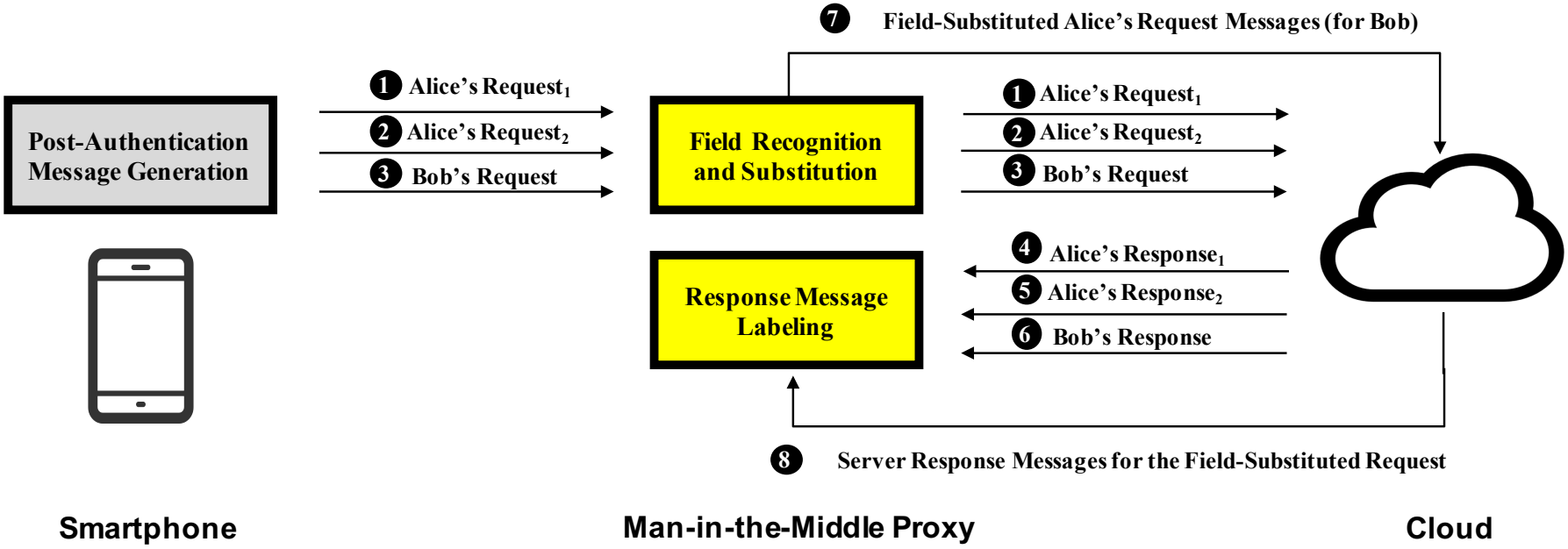
- News App

Implementation



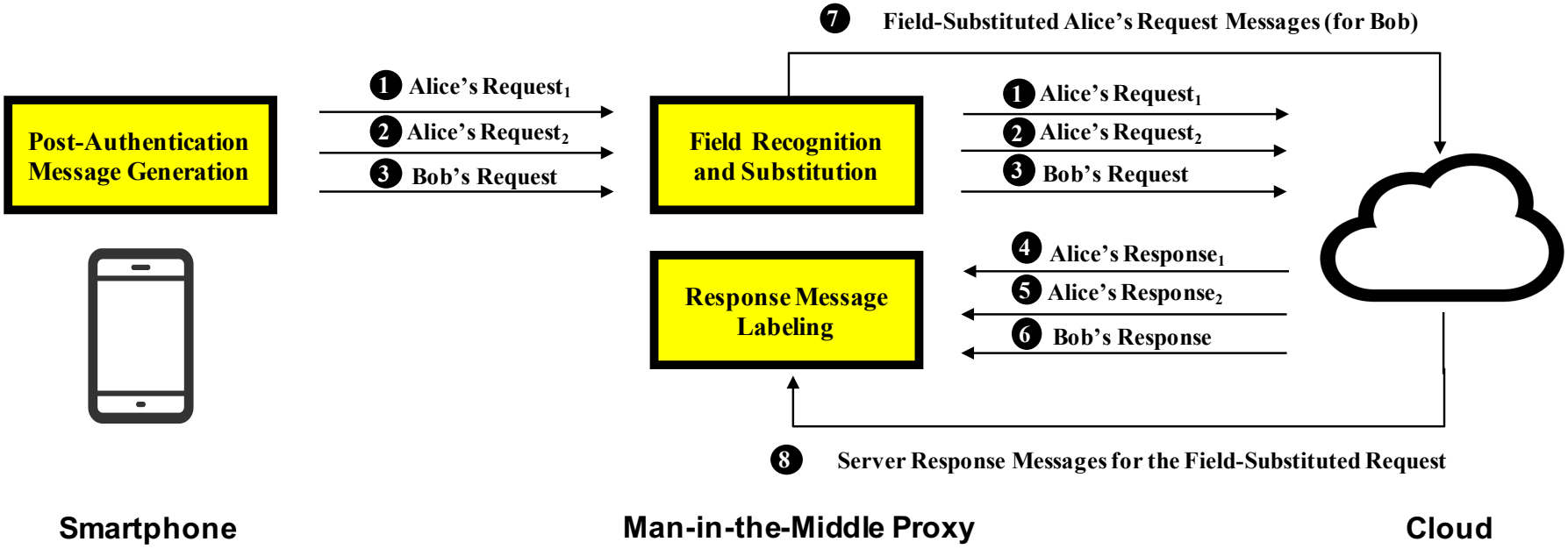
- Atop Android 4.4 with Xposed framework

Implementation



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

Implementation



- 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

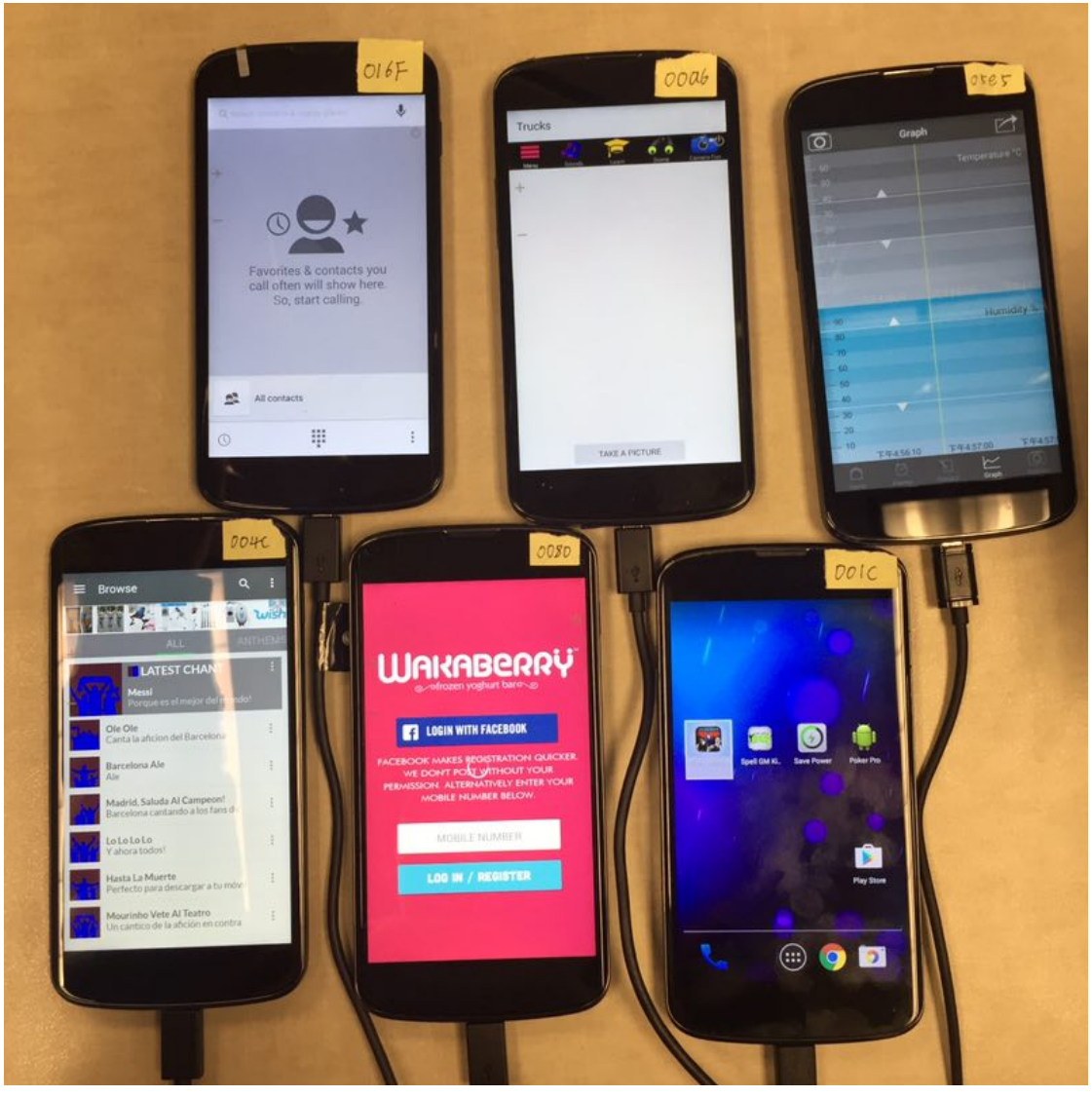
Dataset Collection

- 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

Item	Value
Total # Apps	4,838

Overall Experiment Result

Item	Value
Total # Apps	4,838
Total Time of testing (hours)	562.4

Overall Experiment Result

Item	Value
Total # Apps	4,838
Total Time of testing (hours)	562.4
Total # Request Messages	3,220,886

Overall Experiment Result

Item	Value
Total # Apps	4,838
Total Time of testing (hours)	562.4
Total # Request Messages	3,220,886
Total # Suspicious Interfaces	2,976

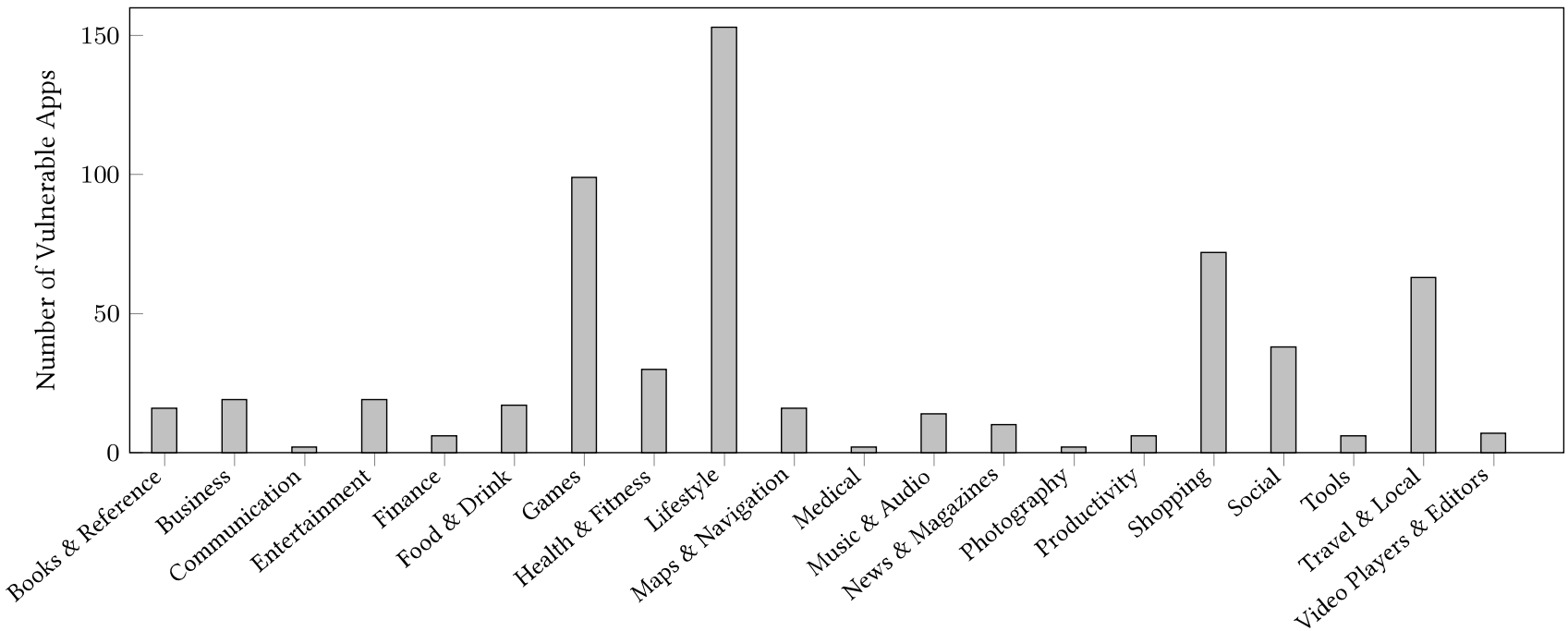
Overall Experiment Result

Item	Value
Total # Apps	4,838
Total Time of testing (hours)	562.4
Total # Request Messages	3,220,886
Total # Suspicious Interfaces	2,976
Total # Public Interfaces	2,379

Overall Experiment Result

Item	Value
Total # Apps	4,838
Total Time of testing (hours)	562.4
Total # Request Messages	3,220,886
Total # Suspicious Interfaces	2,976
Total # Public Interfaces	2,379
Total # Vulnerable Interfaces	597

Distribution of the Vulnerable Interfaces



Detailed Results for Top Tested App in Each Category

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

User Privacy & Vulnerability Details

Category	Detailed Privacy Type
User E-Profile	⑴ Email, ⑵ User ID, ⑶ Registration Date, ⑷ IP Address, ⑸ Last Login Date, ⑹ Last Update Date
User Physical-Profile	⑺ Real Name, ⑻ Birthday, ⑼ Geo-location, ⑽ Home Address, ⑾ Phone Number, ⑿ Body Information
User Secrets	⒀ Token, ⒁ Password, ⒂ Pass Code
App Specific Private Data	⒃ In App Messages, ⒄ Shopping History, ⒅ Book Shelf, ⒆ Favorites or Subscription, ⒇ Account Balance
	(21) Contacts Information, (22) Payment Information, (23) Private Activity Information

User Privacy & Vulnerability Details

Category	Detailed Privacy Type
User E-Profile	⑴ Email, ⑵ User ID, ⑶ Registration Date, ⑷ IP Address, ⑸ Last Login Date, ⑹ Last Update Date
User Physical-Profile	⑺ Real Name, ⑻ Birthday, ⑼ Geo-location, ⑽ Home Address, ⑾ Phone Number, ⑿ Body Information
User Secrets	⒀ Token, ⒁ Password, ⒂ Pass Code
App Specific Private Data	⒃ In App Messages, ⒄ Shopping History, ⒅ Book Shelf, ⒆ Favorites or Subscription, ⒇ Account Balance ㉑ Contacts Information, ㉒ Payment Information, ㉓ Private Activity Information

APP	Version	Credential Type	User E-Profile	User Physical-Profile	User Secrets	App Specific Private Data
com.***.e***	2.2	N	⑴⑵	⑺⑻ ⑽⑾		⑱
com.***.k***	2.0.11	E	⑴⑵⑶⑷ ⑹	⑺ ⑼⑽⑾	⒀⒁	⑰ ⑲
com.***.w***	1.0.5	F	⑴⑵	⑺	⒀	⑯ ⑲ ㉑
com.g***.c***	2.4.1	E	⑴⑵	⑾	⒀	⑰ ⑳
com.***.m***	1.6.8	N	⑴⑵	⑺ ⑼⑽⑾	⒂	⑯ ⑳ ㉒
com.***.h***	2.5.6.0	E	⑴⑵		⒀	⑯ ⑲
com.***.c***	2.6.1	F	⑴	⑺ ⑽	⒀	⑲
com.***.u***	2.03	N	⑴⑵⑶	⑺⑻ ⑿		⑯ ⑲
com.m***	7.3.0	N	⑵	⑺⑻ ⑽		⑯ ⑲⑳
com.******.c***	7.5.5v	F	⑴⑵	⑺ ⑼⑽⑾	⒀	⑲ ㉒
com.***.a***	3.09	F	⑴⑵	⑺	⒀	⑯ ⑲
com.b***	2.0.4	N				⑲
com.***.a***	2.3.2	N	⑴ ⑶⑷⑸	⑺⑻⑼	⒀	⑯ ⑲
com.***.j***	2.7.4	F	⑴⑵⑶	⑺	⒀	⑯ ⑲
com.***.d***	2.4.2	E	⑵⑶	⑺ ⑼	⒀	㉓
cl.******.i***	2.1.0	N	⑴⑵	⑺⑻⑼		⑳
in.v***	4.4.5.2	N		⑺⑻		⑯ ⑲ ㉑
com.mediaingea.uptodown.lite	3.18	F	⑵		⒀	⑯ ⑲
com.t***	1.4.0	F	⑴⑵	⑽⑾	⒀	⑯ ㉓
cz.***.n***	4.8	F	⑵	⑺	⒀	㉓
Statistics		8 4 8	14 16 05 02 01 01	15 06 06 07 06 01	13 01 01	11 02 01 13 04 02 02 03

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": "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 K

User Privacy

Password

```
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": "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 K

User Privacy
Registration Date
Last Update Date
User ID
Email


```
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": "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 K

User Privacy
Real Name
Phone Number
Home Address
Geo Location


```
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": "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

```
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":"106611716575863",
21    "current_latitude":”30.9863214",
22    "current_longitude":”-86.7501116",
23    "bananas_history":"https:\/\/profile.i******.com\/bananas\
/store\/673491\/?accesstoken=debda35ccd92f4b8e2e06f0bff3b6e49279
a557d&latitude=30.9863214&longitude=-86.7501116&lang=",
24    ...
25   }
26  }
27 }
```

Case Study-App I

User Privacy

Email

User ID

```
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":"106611716575863",
21    "current_latitude":”30.9863214",
22    "current_longitude":”-86.7501116",
23    "bananas_history":"https:\/\/profile.i******.com\/bananas\
/store\/673491\/?accesstoken=debda35ccd92f4b8e2e06f0bff3b6e49279
a557d&latitude=30.9863214&longitude=-86.7501116&lang=",
24    ...
25   }
26  }
27 }
```

Case Study-App I

User Privacy

Real Name

Birthday

Geo Location

```
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":"106611716575863",
21    "current_latitude":”30.9863214",
22    "current_longitude":”-86.7501116",
23    "bananas_history":"https:\/\/profile.i******.com\/bananas\
/store\/673491\/?accesstoken=debda35ccd92f4b8e2e06f0bff3b6e49279
a557d&latitude=30.9863214&longitude=-86.7501116&lang=",
24    ...
25   }
26  }
27 }
```

Case Study-App I

User Privacy

Account Balance

```
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":"106611716575863",
21    "current_latitude":"30.9863214",
22    "current_longitude":"-86.7501116",
23    "bananas_history":"https:\/\/profile.i******.com\/bananas\
/store\/673491\/?accesstoken=debda35ccd92f4b8e2e06f0bff3b6e49279
a557d&latitude=30.9863214&longitude=-86.7501116&lang=",
24    ...
25   }
26  }
27 }
```

Limitation and Future work

Limitations

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

Limitation and Future work

Limitations

- Only Facebook Login
- Only authrization vulnerabilities that leads 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

Related Work

- **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

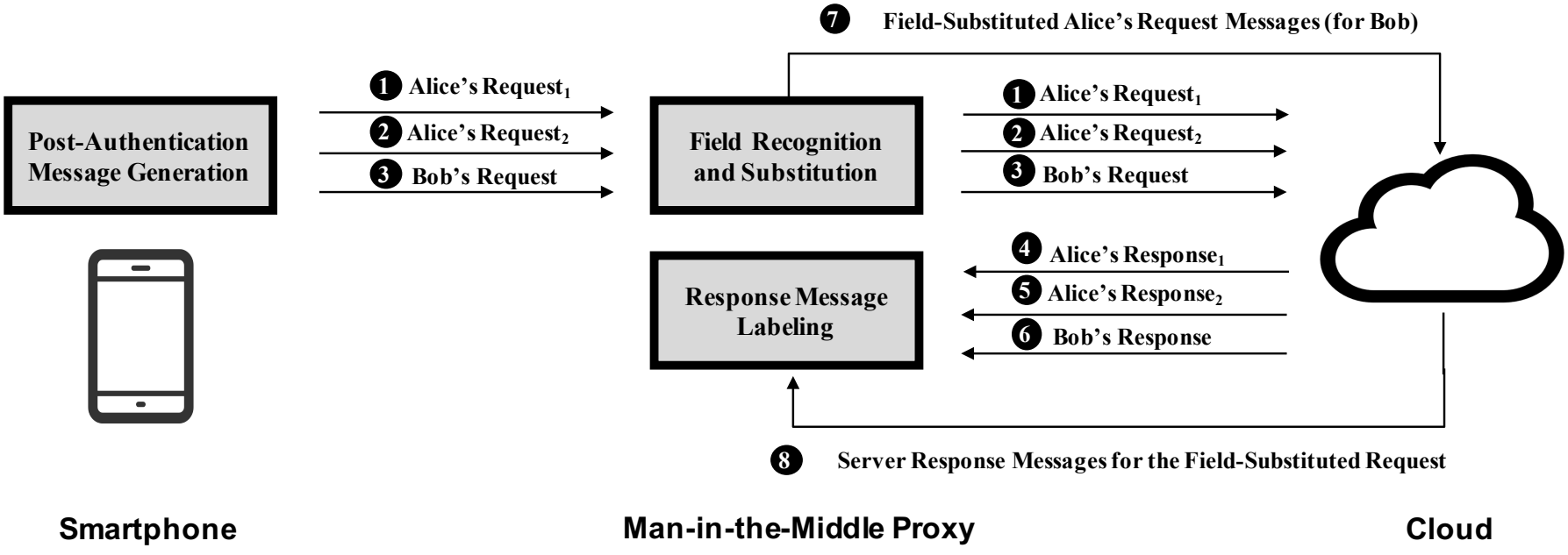
- **Dynamic Analysis of Mobile Apps.** Monkey [mon17], Robotium [Rob], AppsPlayground [RCE13], DynoDroid [MTN13], symbolic execution [ANHY12, MMP+12, WL16, ZL17]
- **Protocol Reverse Engineering.** Analyzing network messages [Bed17, MLK+06, CKW07, CFL+17], and instructions traces [CS07, WMKK08, LJXZ08, 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

Thank you



To contact us

{chaoshun.zuo, qingchuan.zhao, zhiqiang.lin}@utdallas.edu

References I

Saswat Anand, Mayur Naik, Mary Jean Harrold, and Hongseok Yang, Automated concolic testing of smartphone apps, Proceedings of the ACM SIGSOFT 20th International Symposium on the Foundations of Software Engineering (New York, NY, USA), FSE '12, ACM, 2012, pp. 59:1–59:11.

Marshall Beddoe, The protocol informatics project, 2017, https://github.com/wolever/Protocol-Informatics.

Adam Barth, Collin Jackson, and John C Mitchell, Robust defenses for cross-site request forgery, Proceedings of the 15th ACM conference on Computer and communications security, ACM, 2008, pp. 75–88.

Guangdong Bai, Jike Lei, Guozhu Meng, Sai Sathyanarayan Venkatraman, Prateek Saxena, Jun Sun, Yang Liu, and Jin Song Dong, Authscan: Automatic extraction of web authentication protocols from implementations., NDSS, 2013.

Andrea Continella, Yanick Fratantonio, Martina Lindorfer, Alessandro Puccetti, Ali Zand, Christopher Kruegel, and Giovanni Vigna, Obfuscation-resilient privacy leak detection for mobile apps through differential analysis, Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS), 2017, pp. 1–16.

Weidong Cui, Jayanthkumar Kannan, and Helen J. Wang, Discoverer: Automatic protocol reverse engineering from network traces, Proceedings of the 16th USENIX Security Symposium (Security'07) (Boston, MA), August 2007.

Weidong Cui, Marcus Peinado, Karl Chen, Helen J. Wang, and Luis Irun-Briz, Tupni: Automatic reverse engineering of input formats, Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS'08) (Alexandria, Virginia, USA), October 2008, pp. 391–402.

References II


Eric Y Chen, Yutong Pei, Shuo Chen, Yuan Tian, Robert Kotcher, and Patrick Tague, Oauth demystified for mobile application developers, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, ACM, 2014, pp. 892–903.


Juan Caballero and Dawn Song, Polyglot: Automatic extraction of protocol format using dynamic binary analysis, Proceedings of the 14th ACM Conference on Computer and and Communications Security (CCS'07) (Alexandria, Virginia, USA), 2007, pp. 317–329.


Michael Dalton, Christos Kozyrakis, and Nickolai Zeldovich, Nemesis: Preventing authentication & access control vulnerabilities in web applications., USENIX Security Symposium, 2009, pp. 267–282.


William G Halfond, Jeremy Viegas, and Alessandro Orso, A classification of sql-injection attacks and countermeasures, Proceedings of the IEEE International Symposium on Secure Software Engineering, vol. 1, IEEE, 2006, pp. 13–15.


Zhiqiang Lin, Xuxian Jiang, Dongyan Xu, and Xiangyu Zhang, Automatic protocol format reverse engineering through context-aware monitored execution, Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS'08) (San Diego, CA), February 2008.


Zhiqiang Lin and Xiangyu Zhang, Deriving input syntactic structure from execution, Proceedings of the 16th ACM SIGSOFT International Symposium on Foundations of Software Engineering (FSE'08) (Atlanta, GA, USA), November 2008.


Justin Ma, Kirill Levchenko, Christian Kreibich, Stefan Savage, and Geoffrey M. Voelker, Unexpected means of protocol inference, Proceedings of the 6th ACM SIGCOMM on Internet measurement (IMC'06) (Rio de Janeriro, Brazil), ACM Press, 2006, pp. 313–326.

References III


Nariman Mirzaei, Sam Malek, Corina S Păsăreanu, Naeem Esfahani, and Riyadh Mahmood, Testing android apps through symbolic execution, ACM SIGSOFT Software Engineering Notes **37** (2012), no. 6, 1–5.


Ui/application exerciser monkey, https://developer.android.com/tools/help/monkey.html, 2017.


Aravind Machiry, Rohan Tahiliani, and Mayur Naik, Dynodroid: An input generation system for android apps, Proceedings of the 2013 9th Joint Meeting on Foundations of Software Engineering, ACM, 2013, pp. 224–234.


Paolo Milani Comparetti, Gilbert Wondracek, Christopher Kruegel, and Engin Kirda, Prospex: Protocol Specification Extraction, IEEE Symposium on Security & Privacy (Oakland, CA), 2009, pp. 110–125.


Saul B Needleman and Christian D Wunsch, A general method applicable to the search for similarities in the amino acid sequence of two proteins, Journal of molecular biology **48** (1970), no. 3, 443–453.


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


Vaibhav Rastogi, Yan Chen, and William Enck, AppsPlayground: Automatic Security Analysis of Smartphone Applications, Third ACM Conference on Data and Application Security and Privacy, 2013.


Robotium, https://code.google.com/p/robotium/, last accessed in May 2017.

References IV


San-Tsai Sun and Konstantin Beznosov, The devil is in the (implementation) details: an empirical analysis of oauth sso systems, Proceedings of the 2012 ACM conference on Computer and communications security, ACM, 2012, pp. 378–390.


Philipp Vogt, Florian Nentwich, Nenad Jovanovic, Engin Kirda, Christopher Kruegel, and Giovanni Vigna, Cross site scripting prevention with dynamic data tainting and static analysis., NDSS, vol. 2007, 2007, p. 12.


Rui Wang, Shuo Chen, and XiaoFeng Wang, Signing me onto your accounts through facebook and google: A traffic-guided security study of commercially deployed single-sign-on web services, Security and Privacy (SP), 2012 IEEE Symposium on, IEEE, 2012, pp. 365–379.


Rui Wang, Shuo Chen, XiaoFeng Wang, and Shaz Qadeer, How to shop for free online–security analysis of cashier-as-a-service based web stores, Security and Privacy (SP), 2011 IEEE Symposium on, IEEE, 2011, pp. 465–480.


Michelle Y Wong and David Lie, Intellidroid: A targeted input generator for the dynamic analysis of android malware, Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS'16) (San Diego, CA), February 2016.


Gilbert Wondracek, Paolo Milani, Christopher Kruegel, and Engin Kirda, Automatic network protocol analysis, Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS'08) (San Diego, CA), February 2008.


Rui Wang, Yuchen Zhou, Shuo Chen, Shaz Qadeer, David Evans, and Yuri Gurevich, Explicating sdks: Uncovering assumptions underlying secure authentication and authorization., USENIX Security, vol. 13, 2013.

References V

Luyi Xing, Yangyi Chen, XiaoFeng Wang, and Shuo Chen, Integuard: Toward automatic protection of third-party web service integrations., NDSS, 2013.

Yuchen Zhou and David Evans, Ssoscan: Automated testing of web applications for single sign-on vulnerabilities., USENIX Security, 2014, pp. 495–510.

Chaoshun Zuo and Zhiqiang Lin, Exposing server urls of mobile apps with selective symbolic execution, Proceedings of the 26th World Wide Web Conference (Perth, Australia), April 2017.

Chaoshun Zuo, Wubing Wang, Rui Wang, and Zhiqiang Lin, Automatic forgery of cryptographically consistent messages to identify security vulnerabilities in mobile services, Proceedings of the 21st Annual Network and Distributed System Security Symposium (NDSS'16) (San Diego, CA), February 2016.