SecurityScorecard

Hidden Risks of Advertisements

Doina Cosovan and Catalin Valeriu Lita

Virus Bulletin 2020

Advertising is (almost) everywhere

- Mobile apps and games
- Websites with ‘free’ content in general
- Youtube, facebook, google search results

Ad mediation platform examples: AdMob, ironSource, Mopub, ...

Ad network examples: AppLovin, AdMob, AdColony, …

Verizon Media Native ad network states that it has 1B monthly active users

Sinkholing opportunities

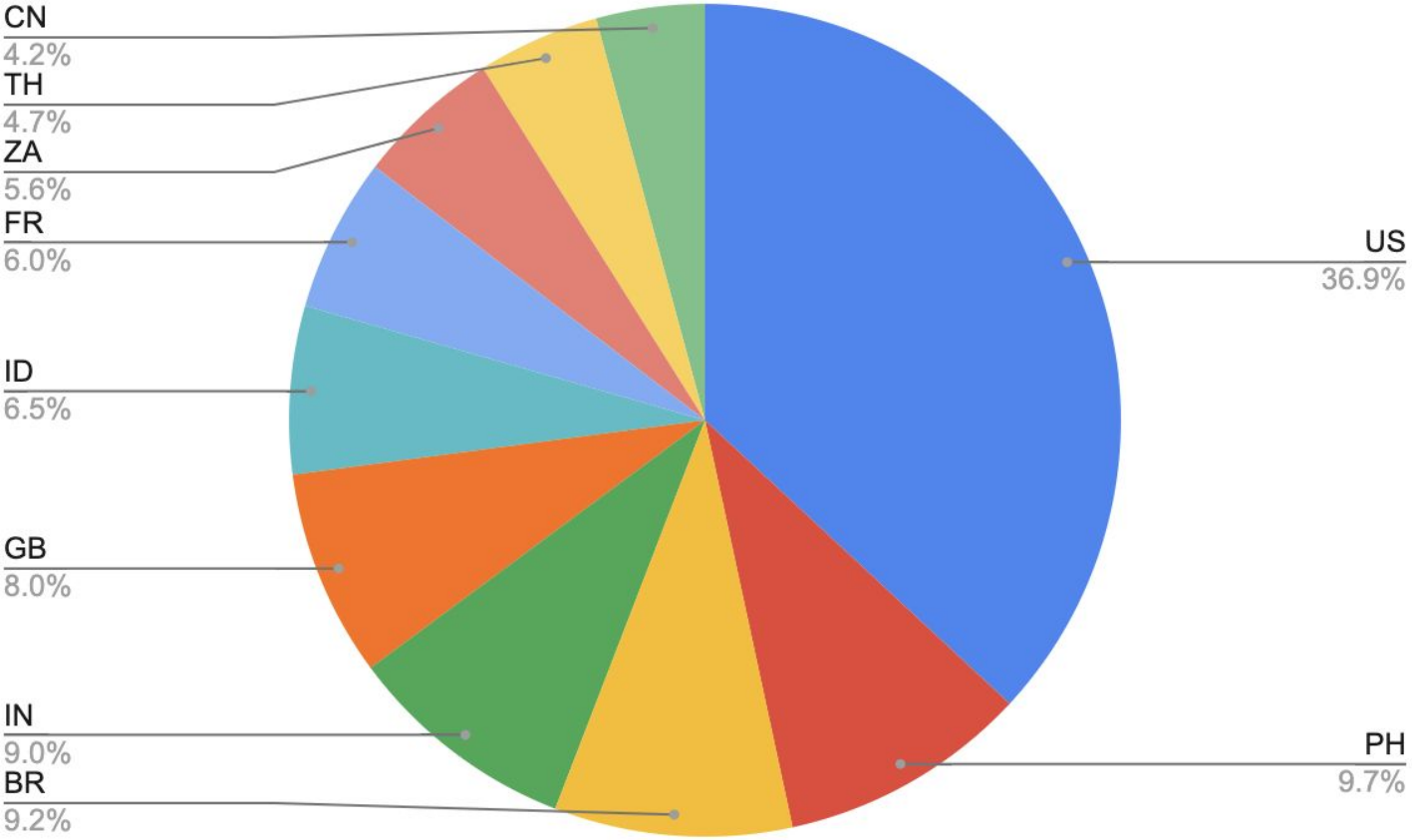
- expired hardcoded domains (2 use cases)
- usage of wrong domains (2 uses cases)
- available algorithmically generated domains (1 use case)

Use Case 1

Use Case 1 Details

- the case of an expired hardcoded domain
- advertising SDK
- used by ~40 Android applications, most of them are related to gaming
- contacted by more than half a million unique IP addresses daily

Distribution



Example of GET request with application

GET
/m/gdpr_sync?id=[redacted]&nv=5.5.0%2Bunity&current_consent_status=unknown&force_gdpr_applies=0&bundle=<application package>&dnt=0 HTTP/1.1
User-Agent: Mozilla/5.0 (Linux; Android 7.0; SM-G935F Build/NRD90M; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/79.0.3945.136 Mobile Safari/537.36
Accept-Language: pt-br
Host: [redacted]
Connection: Keep-Alive
Accept-Encoding: gzip

Example of POST request with application

POST /m/gdpr_sync HTTP/1.1
Accept-Language: th-th
User-Agent: Dalvik/2.1.0 (Linux; U; Android 9; FLA-LX2 Build/HUAWEIFLA-LX2)
Content-Type: application/json; charset=UTF-8
Host: [redacted]
Connection: Keep-Alive
Accept-Encoding: gzip
Content-Length: 172

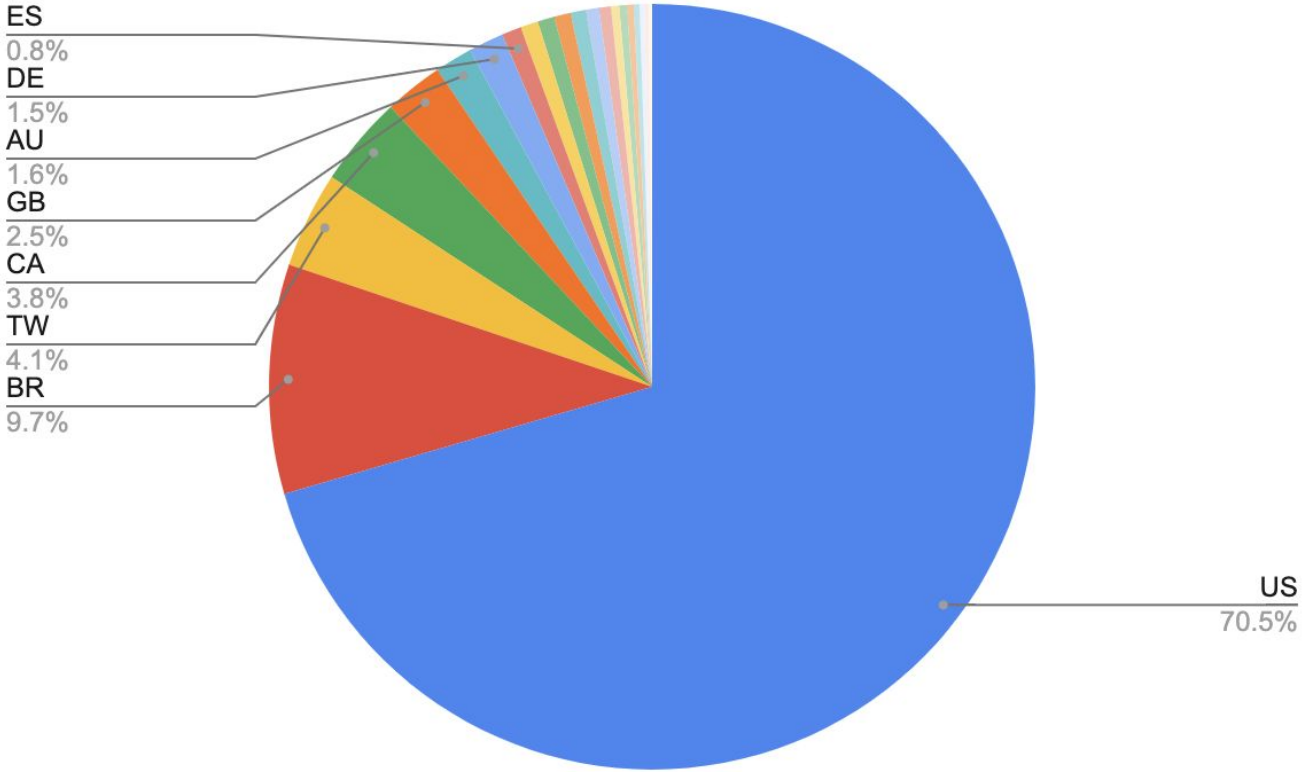

```
{
    "current_consent_status":"unknown",
    "nv":"5.5.0+unity",
    "force_gdpr_applies":"0",
    "id":"[redacted]",
    "dnt":"0",
    "bundle": <application package>
}
```

Use Case 2

Use Case 2 Details

- the case of an expired hardcoded domain
- multi-platform advertising SDK
- contacted by more than 10 million unique IP addresses daily
- ~70% of those IP addresses are located in the United States
- used by 10,000+ websites, most are related to news and social media
- used by ~2,000 Android and iOS applications, most are related to news and social media

Distribution



Example of GET request with website

GET /sync/dsp?uid=[redacted]&partner=[redacted]&zone=[redacted] HTTP/1.1
Host: [redacted]
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: image
Referer: <URL>
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8

Example of GET request with application

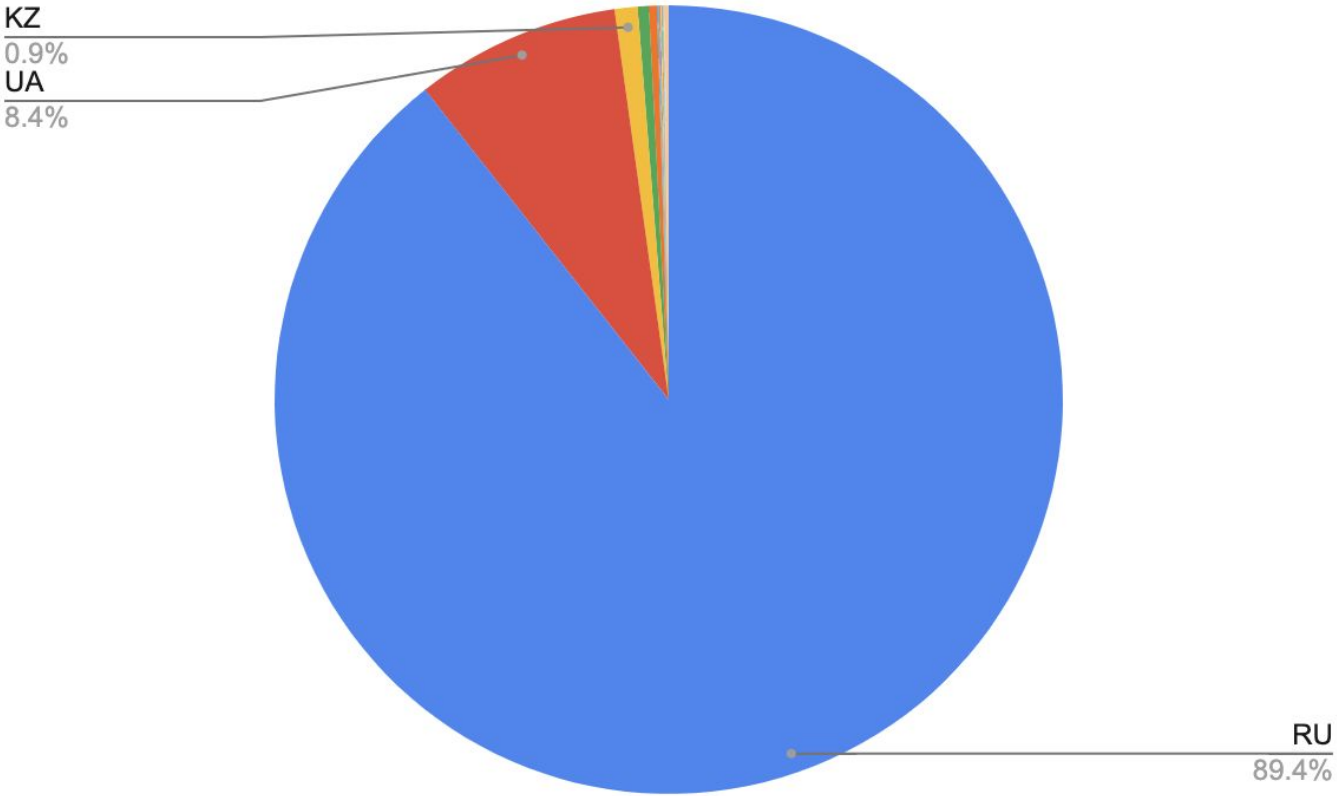
GET /sync/dsp?uid=[redacted]&partner=[redacted]&zone=[redacted] HTTP/1.1
Host: [redacted]
Connection: keep-alive
User-Agent: Mozilla/5.0 (Linux; Android 8.0.0; SM-G930V Build/R16NW; wv) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/75.0.3770.67 Mobile Safari/537.36 [FB_IAB/FB4A;FBAV/245.0.0.39.118;]
Accept: image/webp,image/apng,image/*,*/*;q=0.8
Referer: [redacted]
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
X-Requested-With: <application package>

Use Case 3

Use Case 3 Details

- unintentionally used wrong domain - advertisers bought the correct domain but distributed the SDK with the wrong domain (typo)
- browser and mobile advertising platform
- ~2.5 million unique IP addresses daily
- ~90% of IP addresses are located in Russia
- used by 20,000+ websites, most are related to gaming and movies
- used by ~1,000 different applications, most are related to social networking and browsing
- problem was fixed in a little over a week

Distribution



Example of request with website

GET /userbind?src=[redacted]&pbf=1&gi=1 HTTP/1.1

Host: [redacted]

Connection: keep-alive

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.149 Safari/537.36

Sec-Fetch-Dest: image

Accept: image/webp,image/apng,image/*,*/*;q=0.8

Sec-Fetch-Site: cross-site

Sec-Fetch-Mode: no-cors

Referer: <website>

Accept-Encoding: gzip, deflate, br

Accept-Language: ru-RU,ru;q=0.9,en-US;q=0.8,en;q=0.7

Use Case 4

Use Case 4 Details

- intentionally used wrong domain to evade syntax errors
- HTML5 advertising player
- the non-resolving domain was not meant to be contacted unless specific rare conditions were met
- received requests from half a million unique IP addresses
- problem was fixed in 2-3 days

Code before fix

```
if (xam == 1) {
    var xameleon = 'https://ssp.xameleon.io/?[redacted]&page='+referer+' and ';
} else { var xameleon = ''; }
if (buz == 1) {
    var buzzoola = 'https://exchange.buzzoola.com/adv/[redacted]/jsvpaid';
} else { var buzzoola = ''; }
var player = new Playerjs({
    id:"player",
    file:"https://www.youtube.com/embed/"+id_arr_1.rand(),
    …,
    preroll: "" + imhop + "" + ... + vhead + "" + xameleon + "" +
buzzoola + "https://321[redacted].ru"
});
```

Code after fix

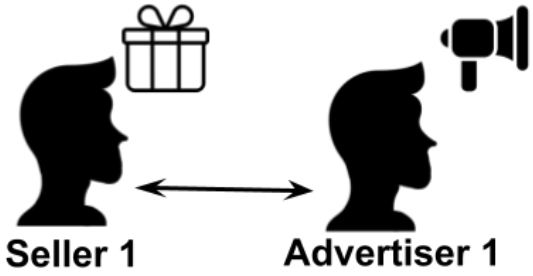
```
if (xam == 1) {
    var xameleon = 'https://ssp.xameleon.io/?[redacted]&page='+referer+' and ';
} else { var xameleon = ''; }
if (buz == 1) {
    var buzzoola = 'https://exchange.buzzoola.com/adv/[redacted]/jsvpaid';
} else { var buzzoola = ''; }
var player = new Playerjs({
    id:"player",
    file:"https://www.youtube.com/embed/"+id_arr_1.rand(),
    …,
    preroll: "" + imhop + "" + ... + vhead + "" + xameleon + "" +
buzzoola + "https://[redacted]/player/html5/media/vpaid.xml"
});
```

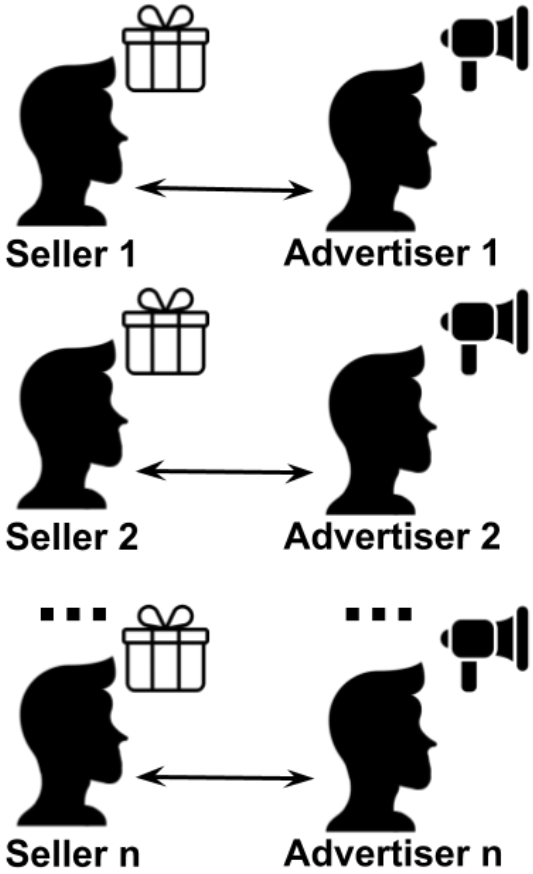
Example of request with website

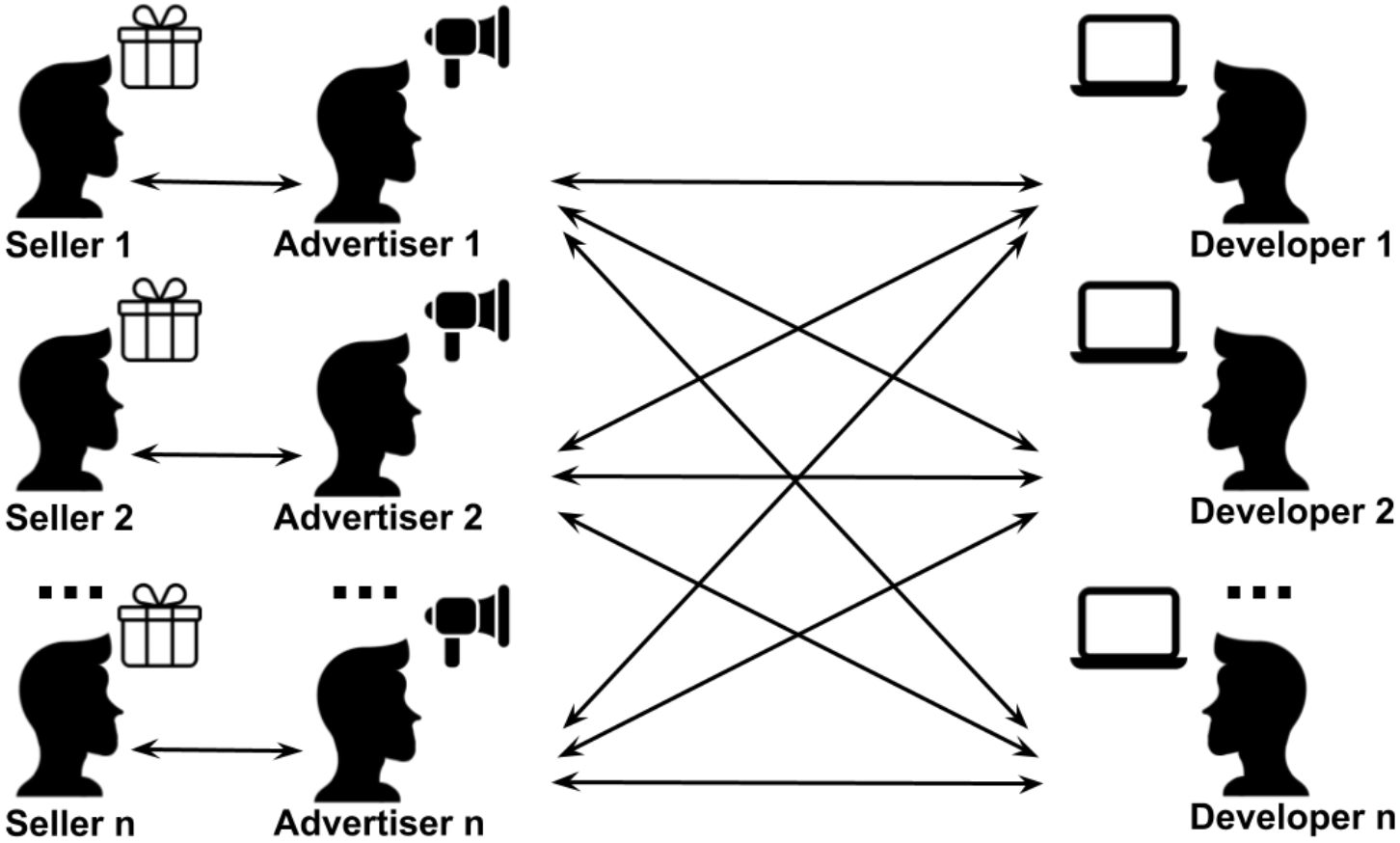
GET / HTTP/1.1
Host: [redacted]
Connection: keep-alive
Origin: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 YaBrowser/19.12.4.25 Yowser/2.5 Safari/537.36
Accept: */*
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Referer: <website>
Accept-Encoding: gzip, deflate, br
Accept-Language: ru,en;q=0.9

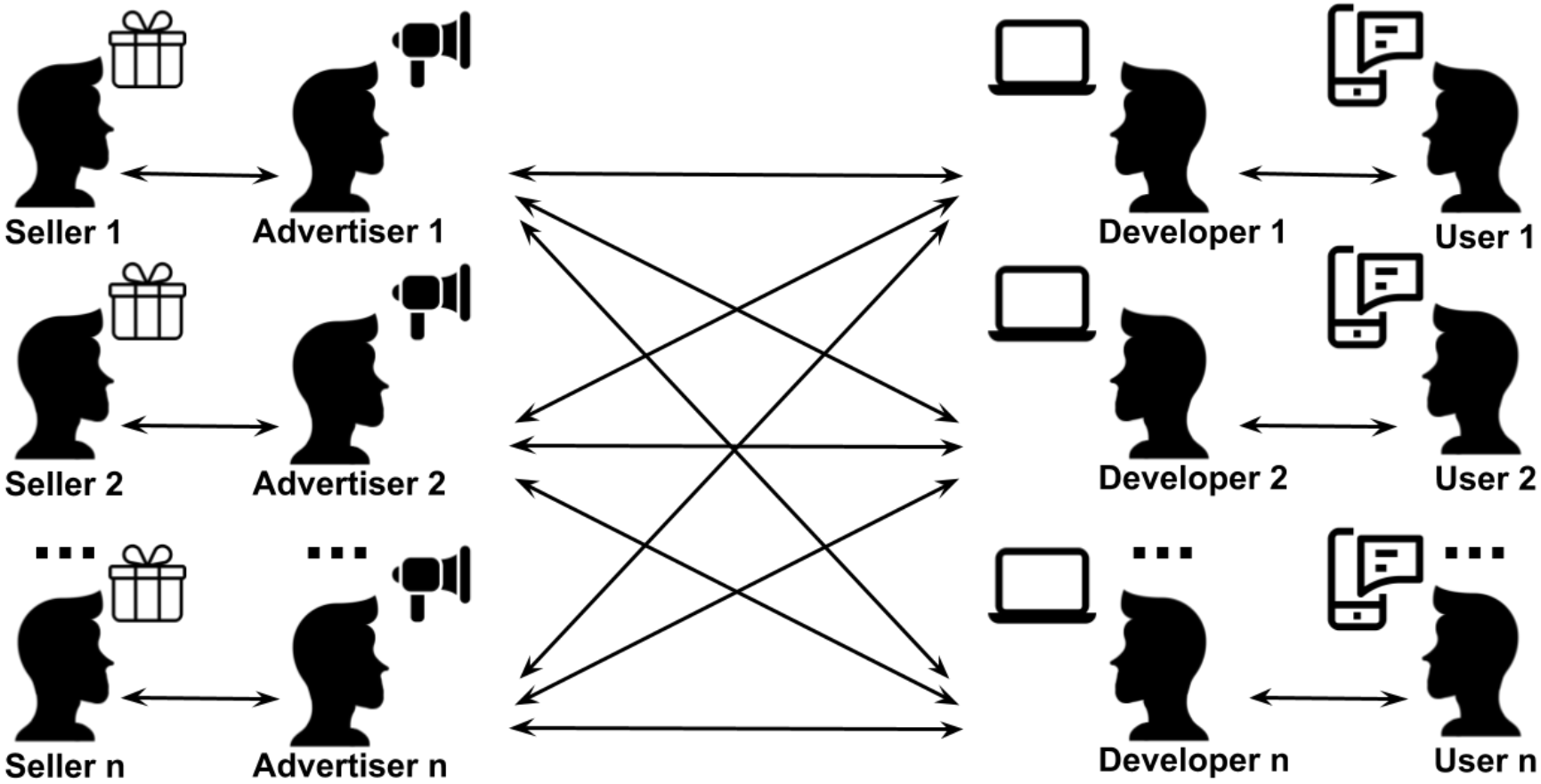
Use Case 5

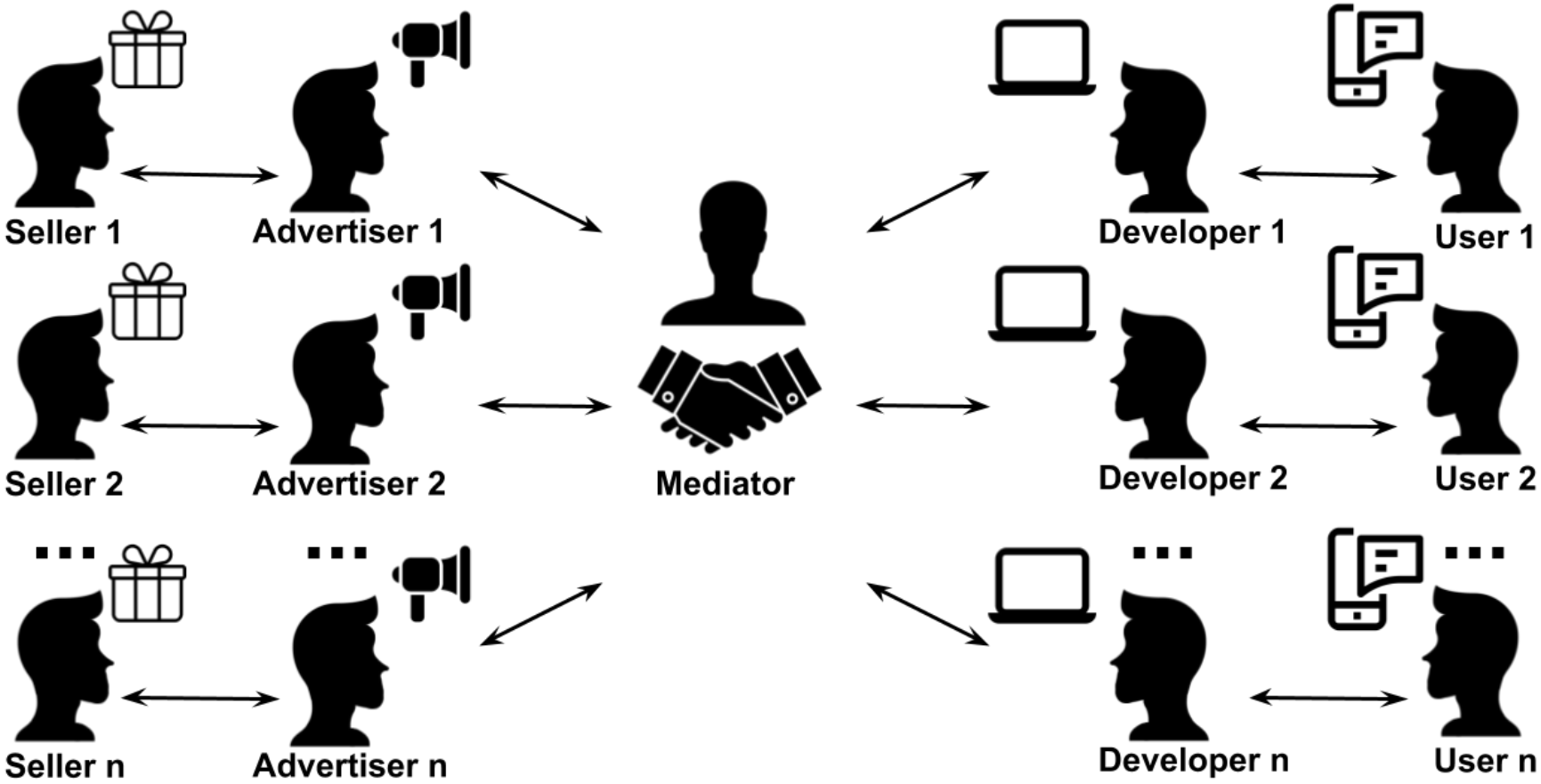
Seller 1


Seller 1
Advertiser 1


Seller 1
Advertiser 1
Seller 2
Advertiser 2
Seller n
Advertiser n


Seller 1
Advertiser 1
Developer 1
Seller 2
Advertiser 2
Developer 2
Seller n
Advertiser n
Developer n


Seller 1
Advertiser 1
Seller 2
Advertiser 2
Seller n
Advertiser n
Developer 1
User 1
Developer 2
User 2
Developer n
User n


Seller 1
Advertiser 1
Developer 1
User 1
Seller 2
Advertiser 2
Mediator
Developer 2
User 2
Seller n
Advertiser n
Developer n
User n

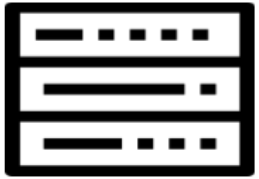
Use Case Details

- multi-platform mobile advertising mediator
- integrates 70+ advertising providers
- uses a Domain Generation Algorithm as fallback for hardcoded domain, which generates:
  - 1 domain daily
  - 1 domain monthly
  - 1 domain yearly

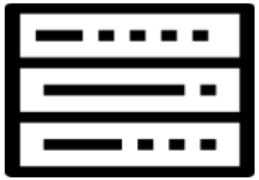
Communication flow

- hardcoded domain: accessible
- generated domains: not important

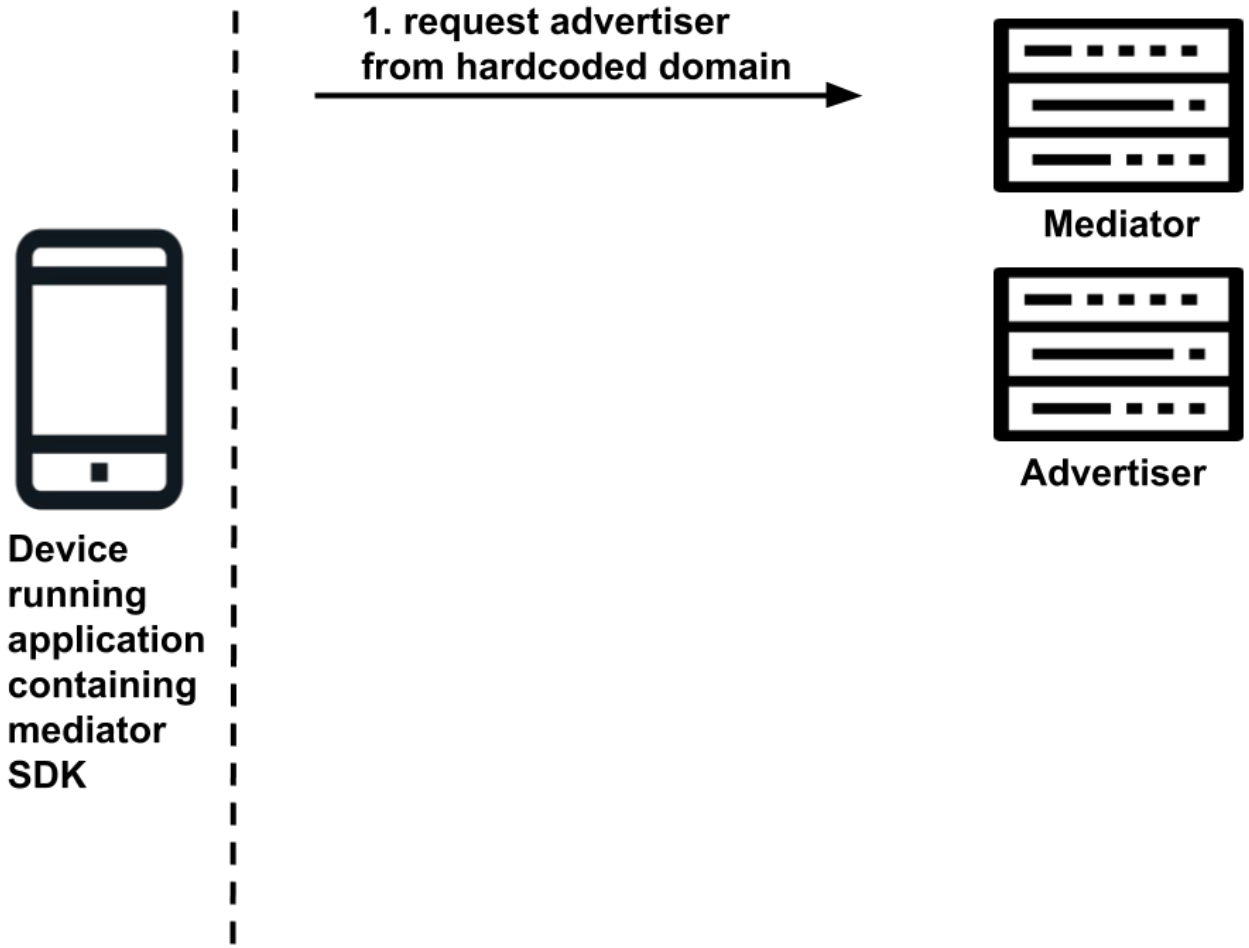
Device running application containing mediator SDK

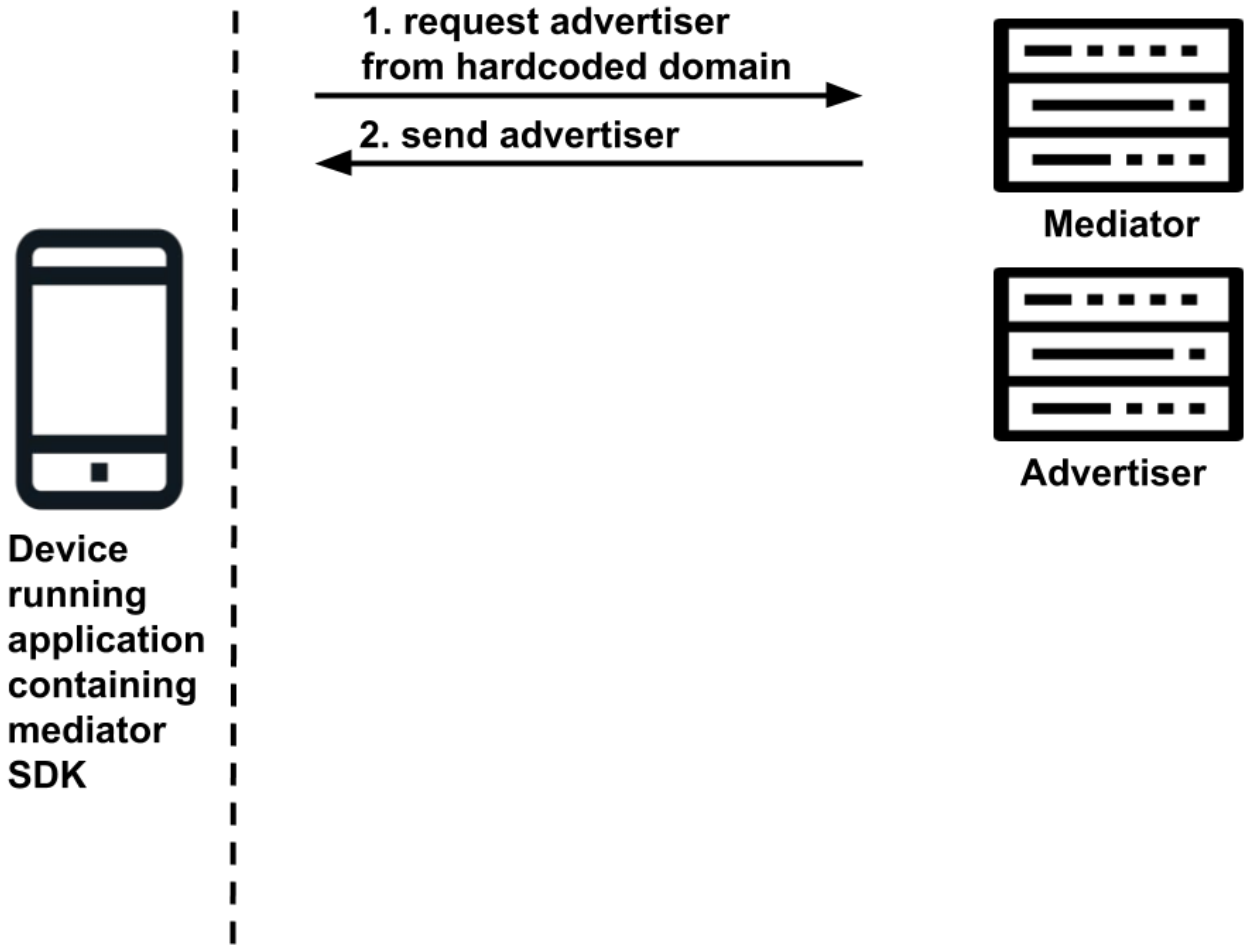


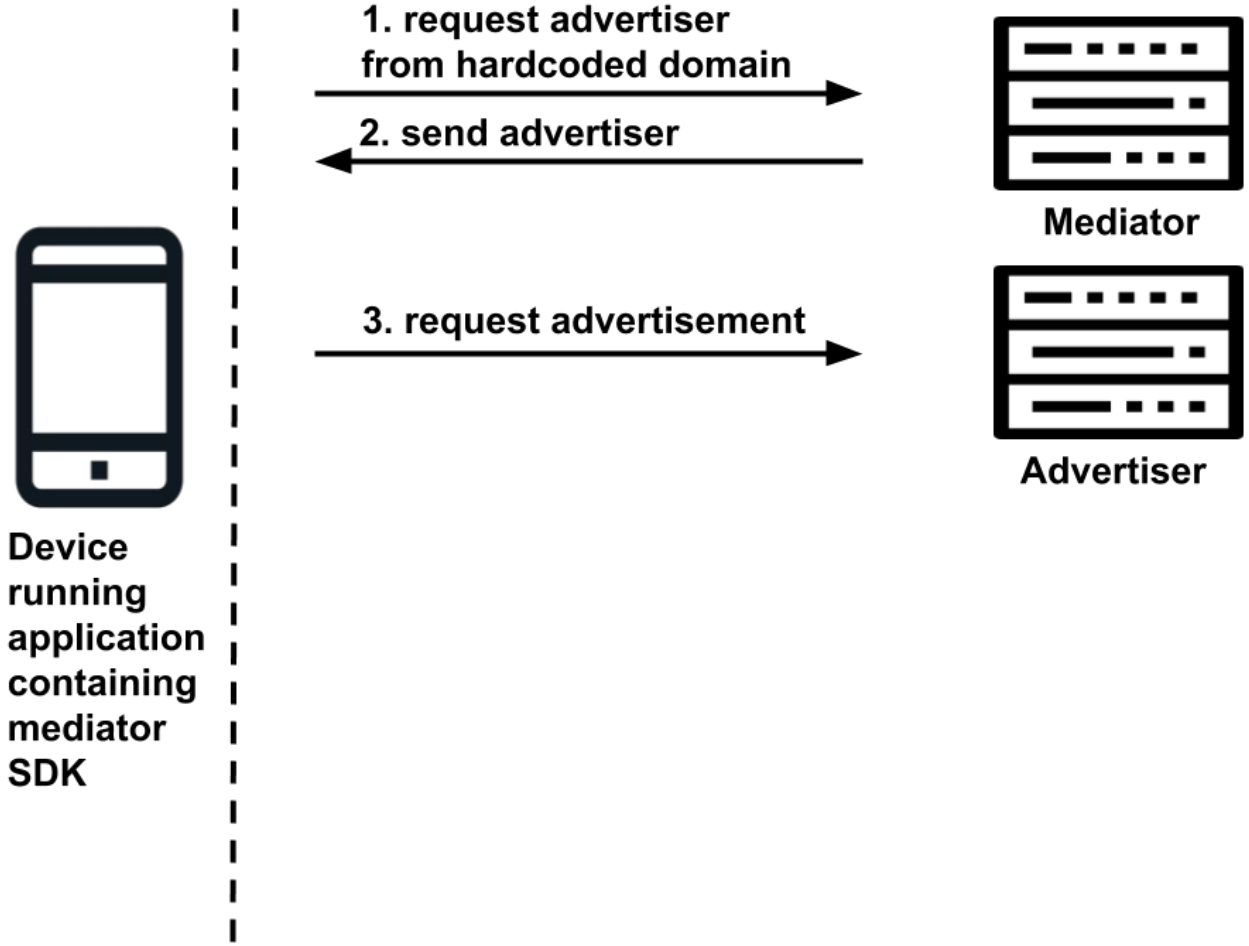
Mediator

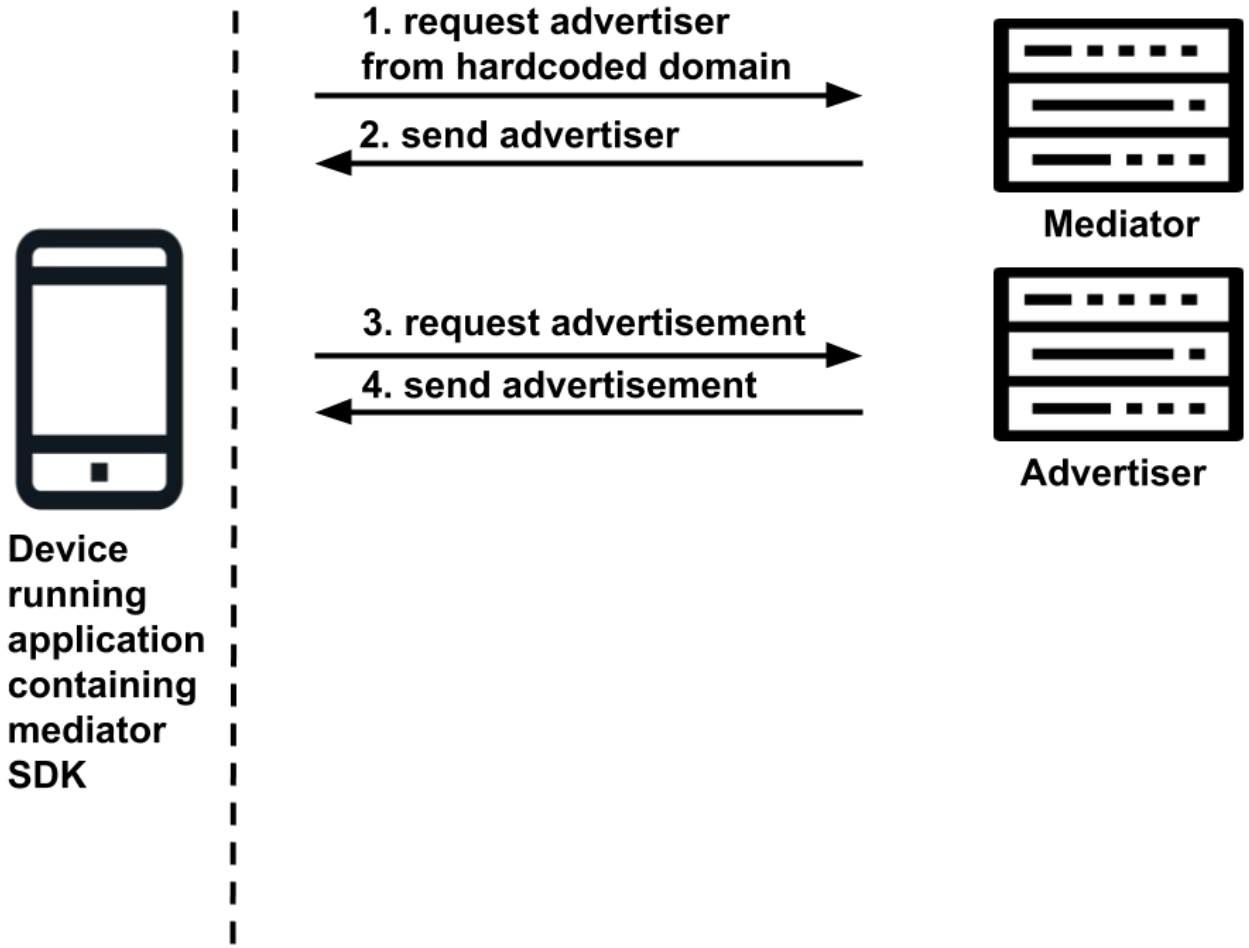


Advertiser


1. request advertiser
from hardcoded domain
Mediator
Advertiser
Device
running
application
containing
mediator
SDK

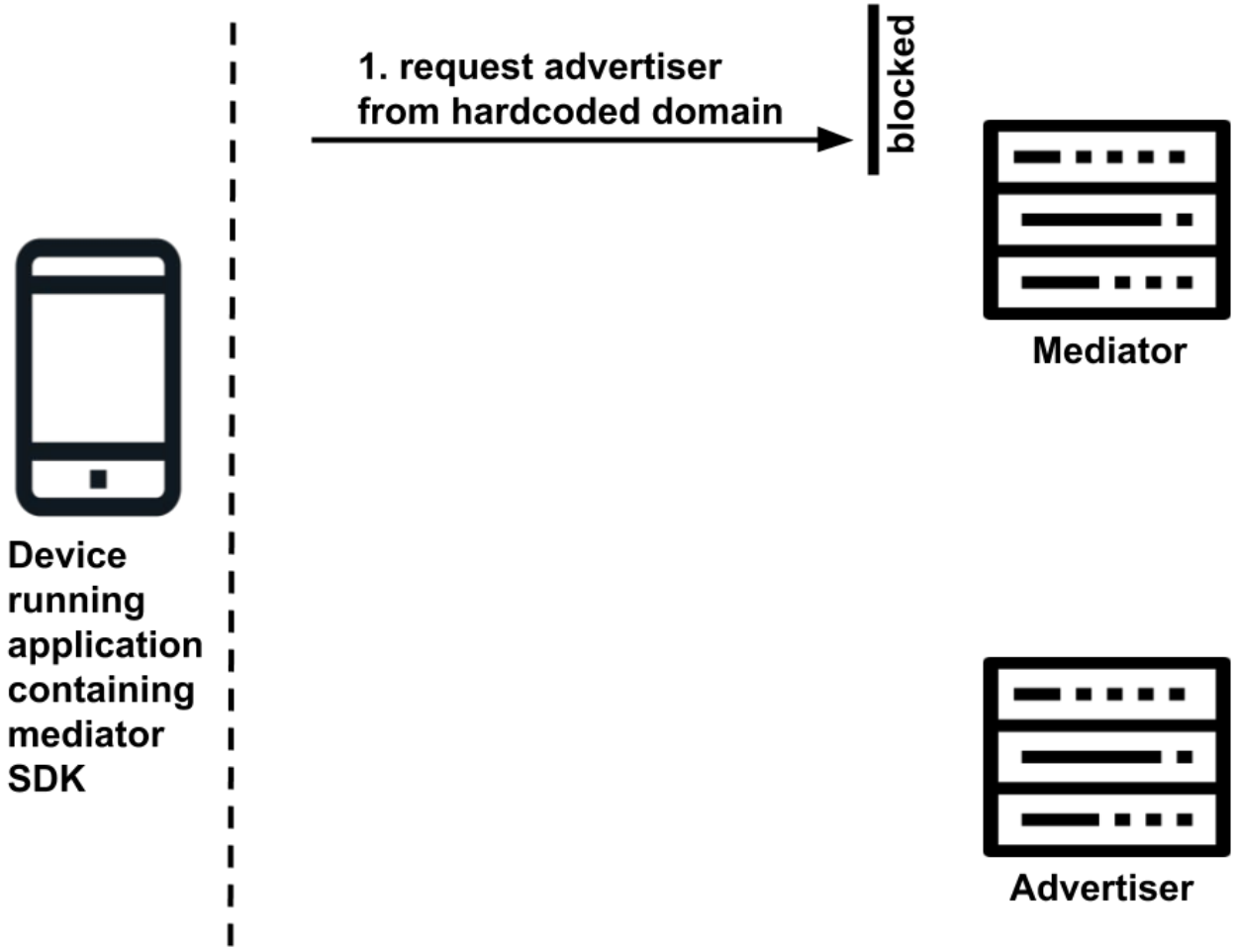

1. request advertiser
from hardcoded domain
2. send advertiser
Mediator
Advertiser
Device
running
application
containing
mediator
SDK

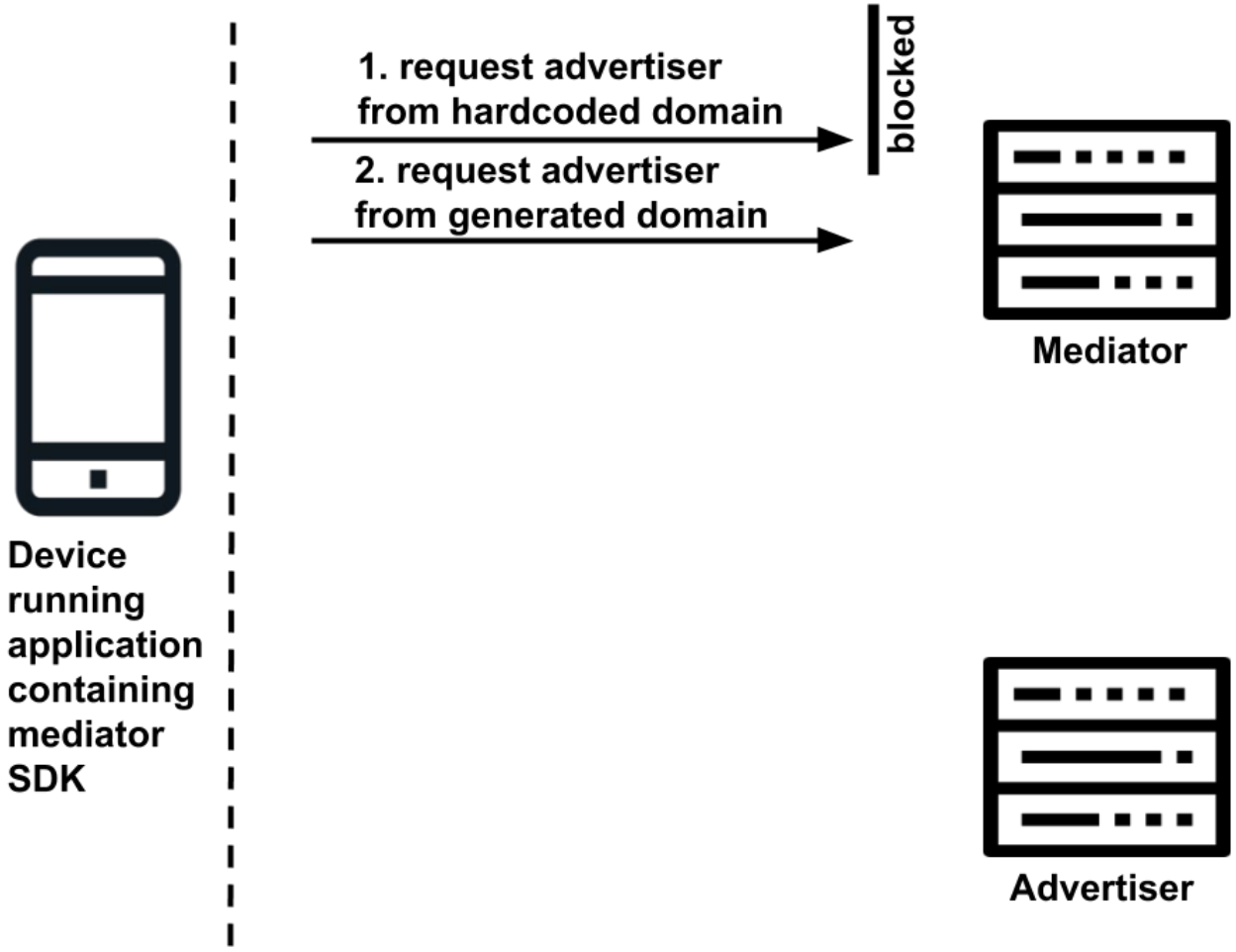

1. request advertiser
from hardcoded domain
2. send advertiser
Mediator
3. request advertisement
Advertiser
Device
running
application
containing
mediator
SDK

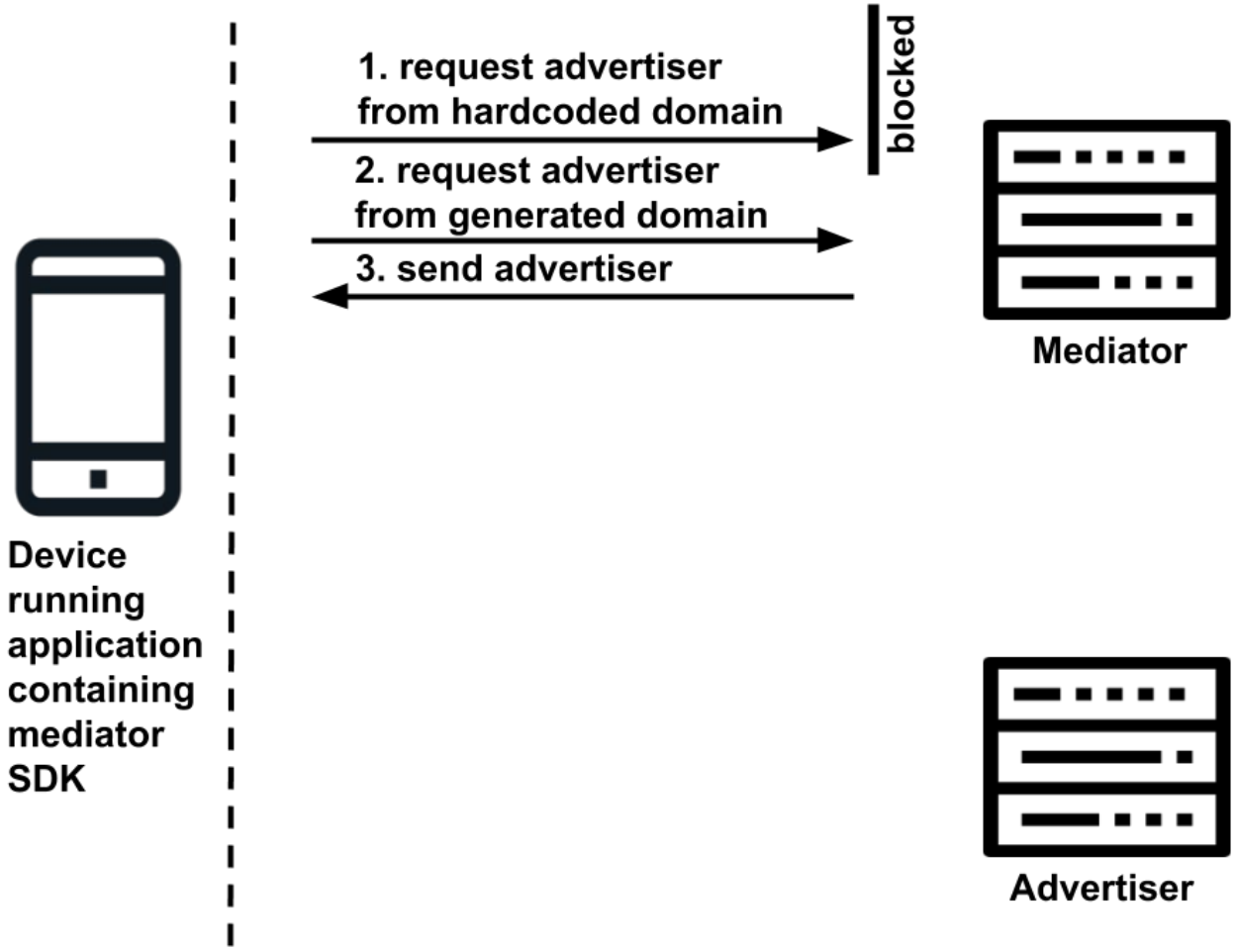

1. request advertiser
from hardcoded domain
2. send advertiser
Mediator
3. request advertisement
4. send advertisement
Advertiser
Device
running
application
containing
mediator
SDK

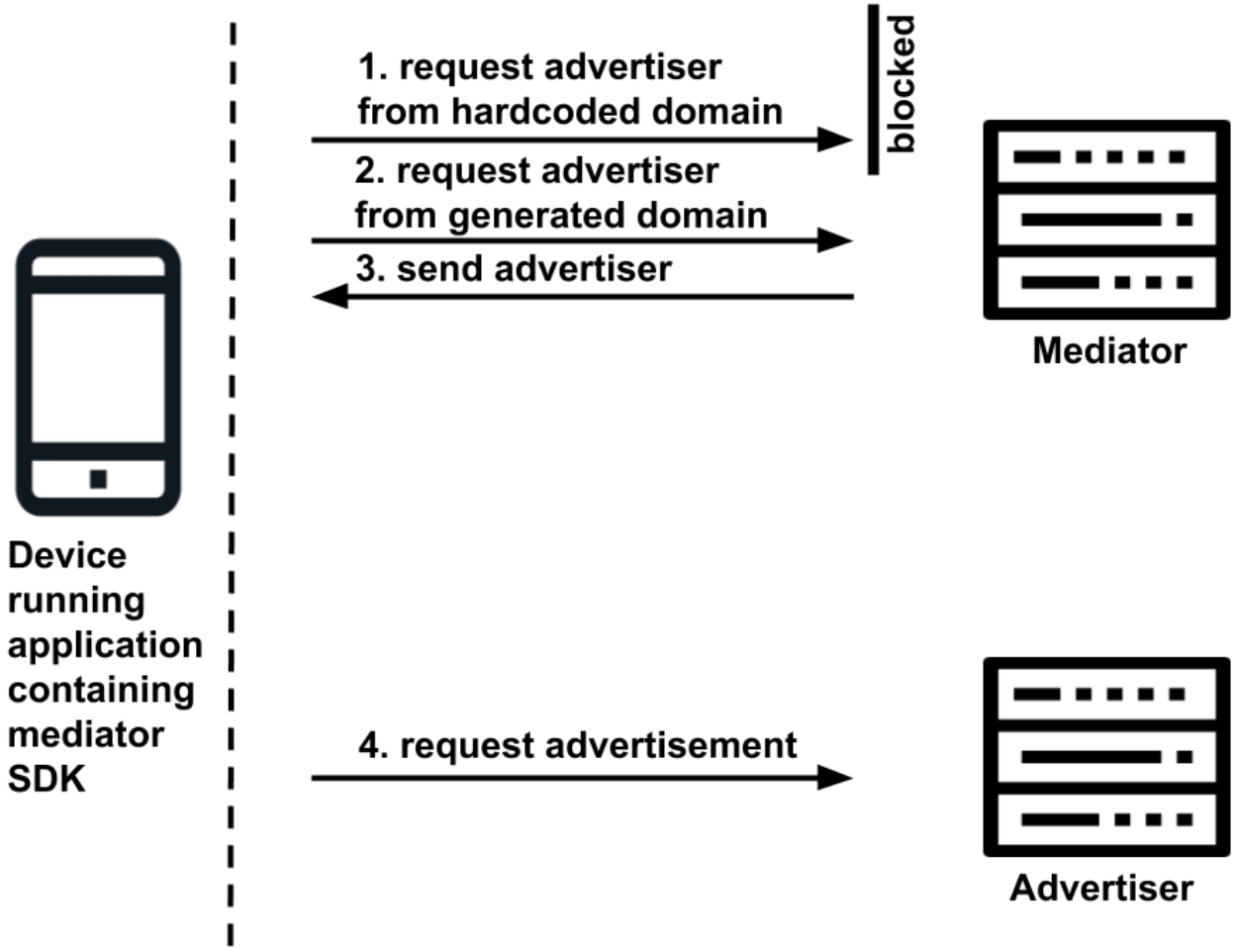
Communication flow

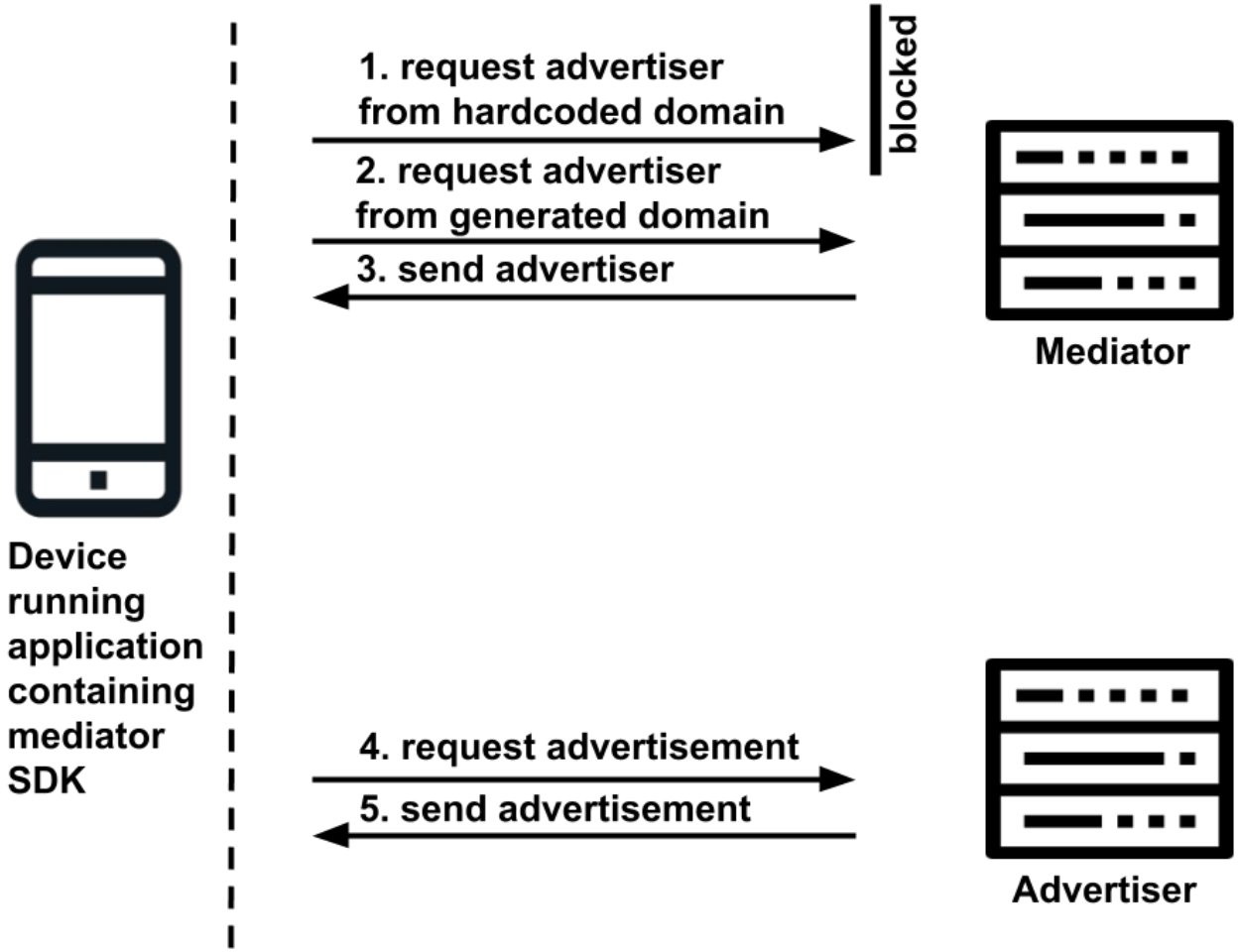
- hardcoded domain: unreachable
- generated domains: belong to the mediator


1. request advertiser
from hardcoded domain
blocked
Mediator
Device
running
application
containing
mediator
SDK
Advertiser


1. request advertiser
from hardcoded domain
blocked
2. request advertiser
from generated domain
Mediator
Device
running
application
containing
mediator
SDK
Advertiser

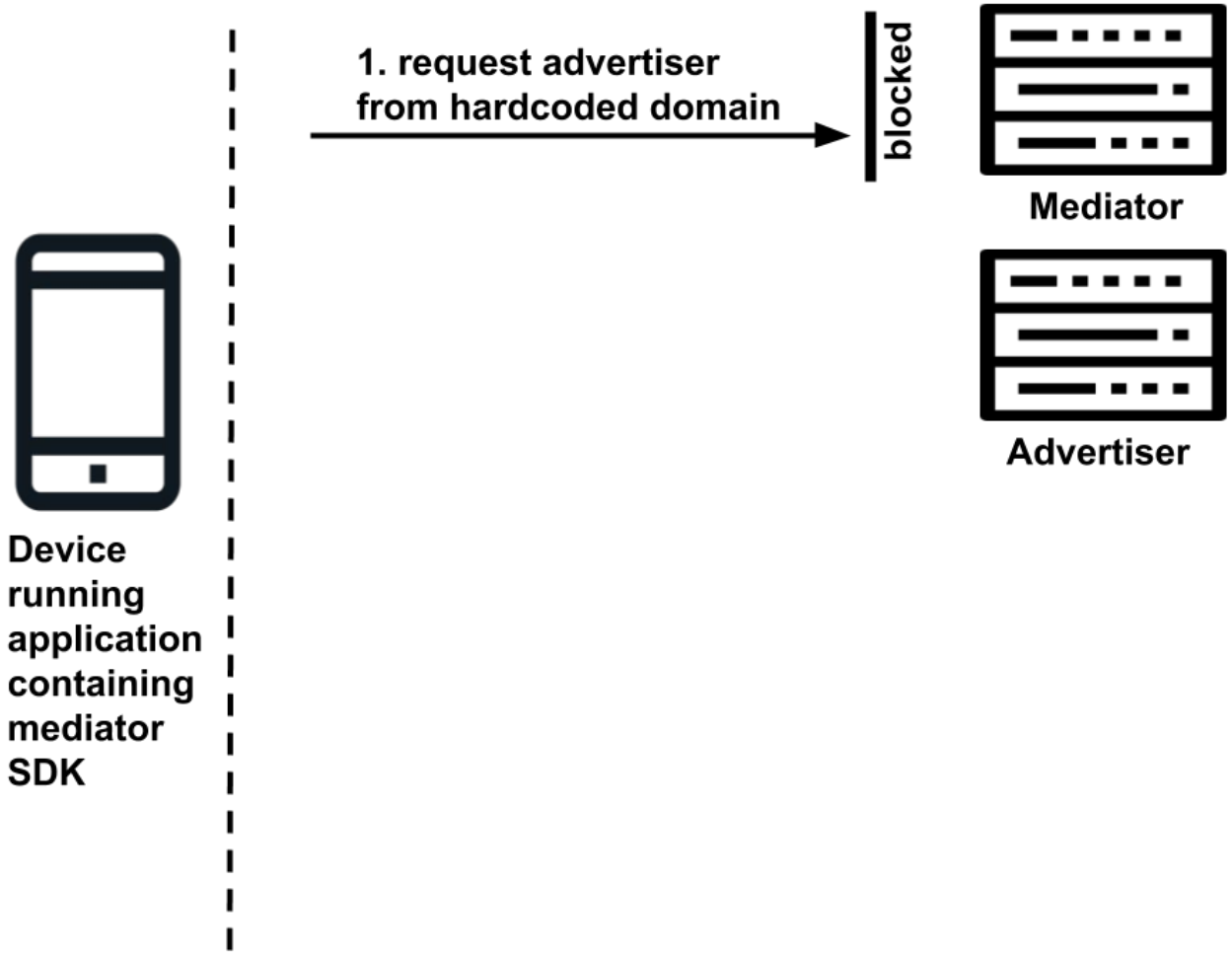

1. request advertiser
from hardcoded domain
blocked
2. request advertiser
from generated domain
3. send advertiser
Mediator
Device
running
application
containing
mediator
SDK
Advertiser

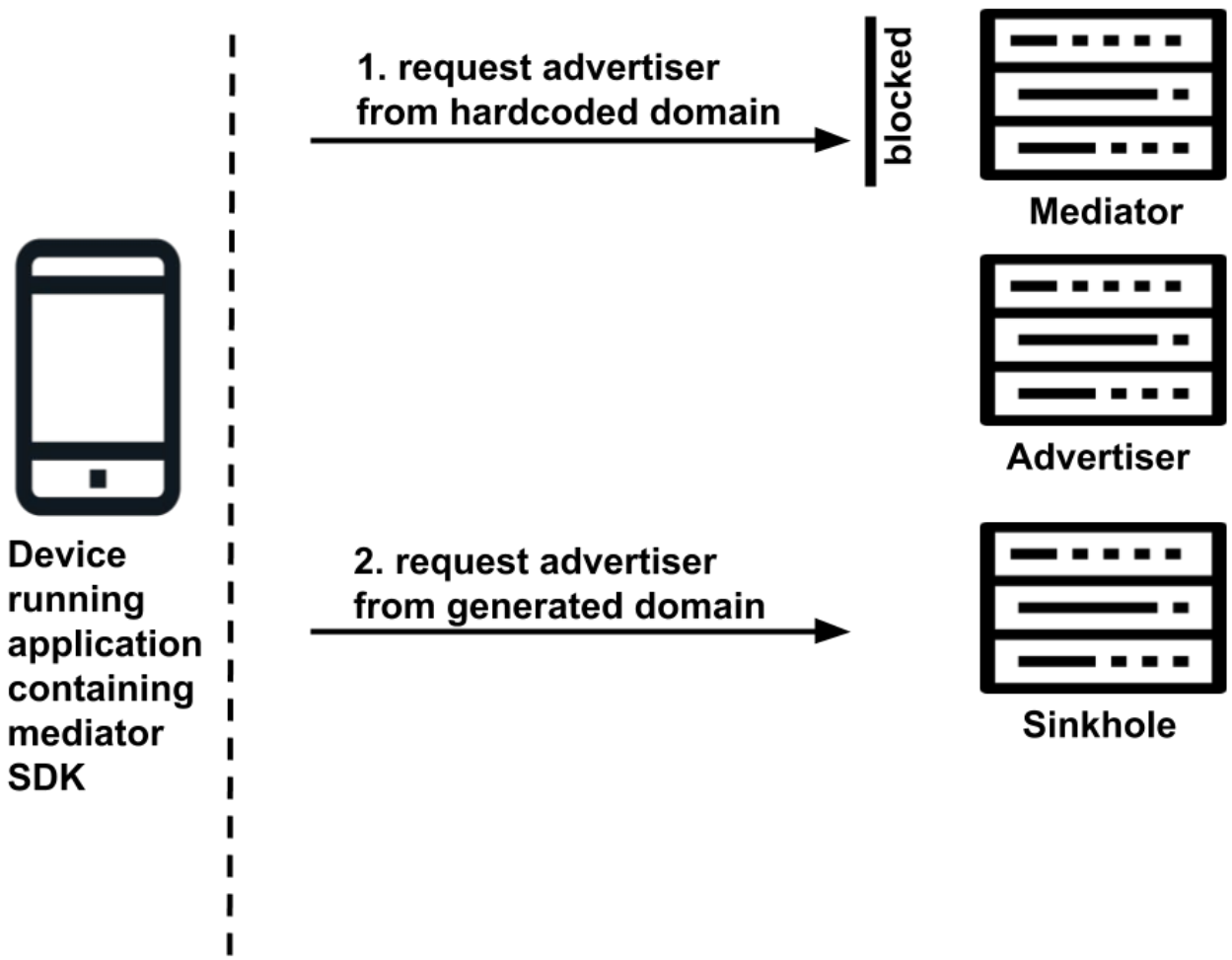

1. request advertiser
from hardcoded domain
blocked
2. request advertiser
from generated domain
3. send advertiser
Mediator
Device
running
application
containing
mediator
SDK
4. request advertisement
Advertiser


1. request advertiser
from hardcoded domain
blocked
2. request advertiser
from generated domain
3. send advertiser
Mediator
Device
running
application
containing
mediator
SDK
4. request advertisement
5. send advertisement
Advertiser

Communication flow

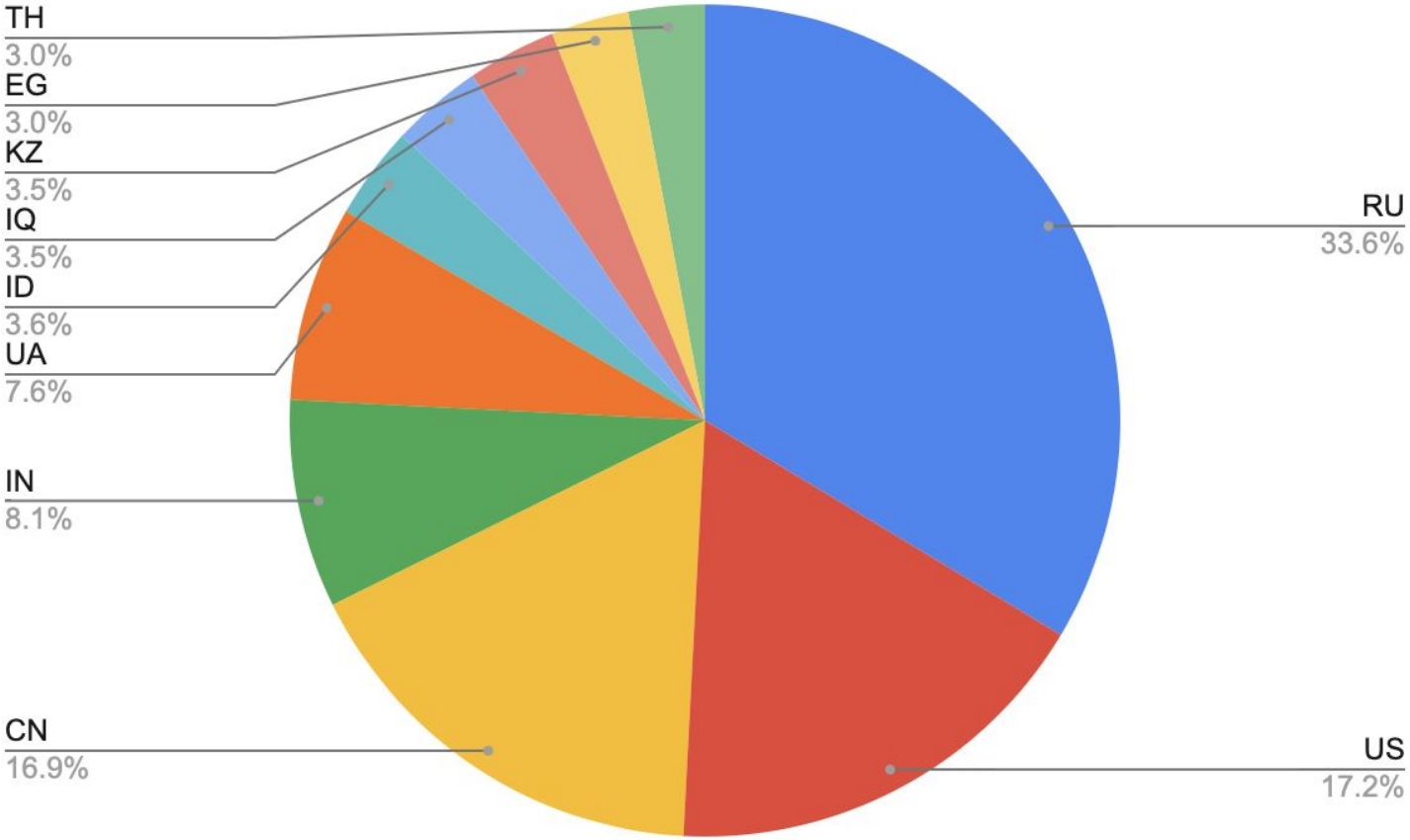
- hardcoded domain: unreachable
- generated domains: sinkholed


1. request advertiser
from hardcoded domain
blocked
Mediator
Advertiser
Device
running
application
containing
mediator
SDK


1. request advertiser
from hardcoded domain
blocked
Mediator
Advertiser
Device
running
application
containing
mediator
SDK
2. request advertiser
from generated domain
Sinkhole

Distribution

contacted by tens of thousands of devices



Example of request

POST /get HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 13_4_1 like Mac OS X) AppleWebKit/609.1.20 (KHTML, like Gecko) Mobile/17E262 DManager/27
Accept-Language: fr-FR;q=1, ar-FR;q=0.9, en-FR;q=0.8
Accept-Encoding: gzip, deflate, br
Content-Type: text/plain
Connection: keep-alive
Content-Length: 1064
Accept: */*

<body>

Information about devices

Hardware characteristics:

- device manufacturer, type, and model
- height, width and pixel ratio of the display
- the total and the available RAM
- percentage of battery

Software characteristics:

- platform (android or ios)
- operating system version
- SDK version
- whether the device is rooted or not

Information about users

- language
- time zone
- local time
- gender
- age
- relation
- occupation
- smoking
- alcohol

Information about advertisements

- type of advertisement
- whether advertising tracking is enabled
- number of shown advertisements
- number of advertisements fully watched
- number of clicks

Information about applications

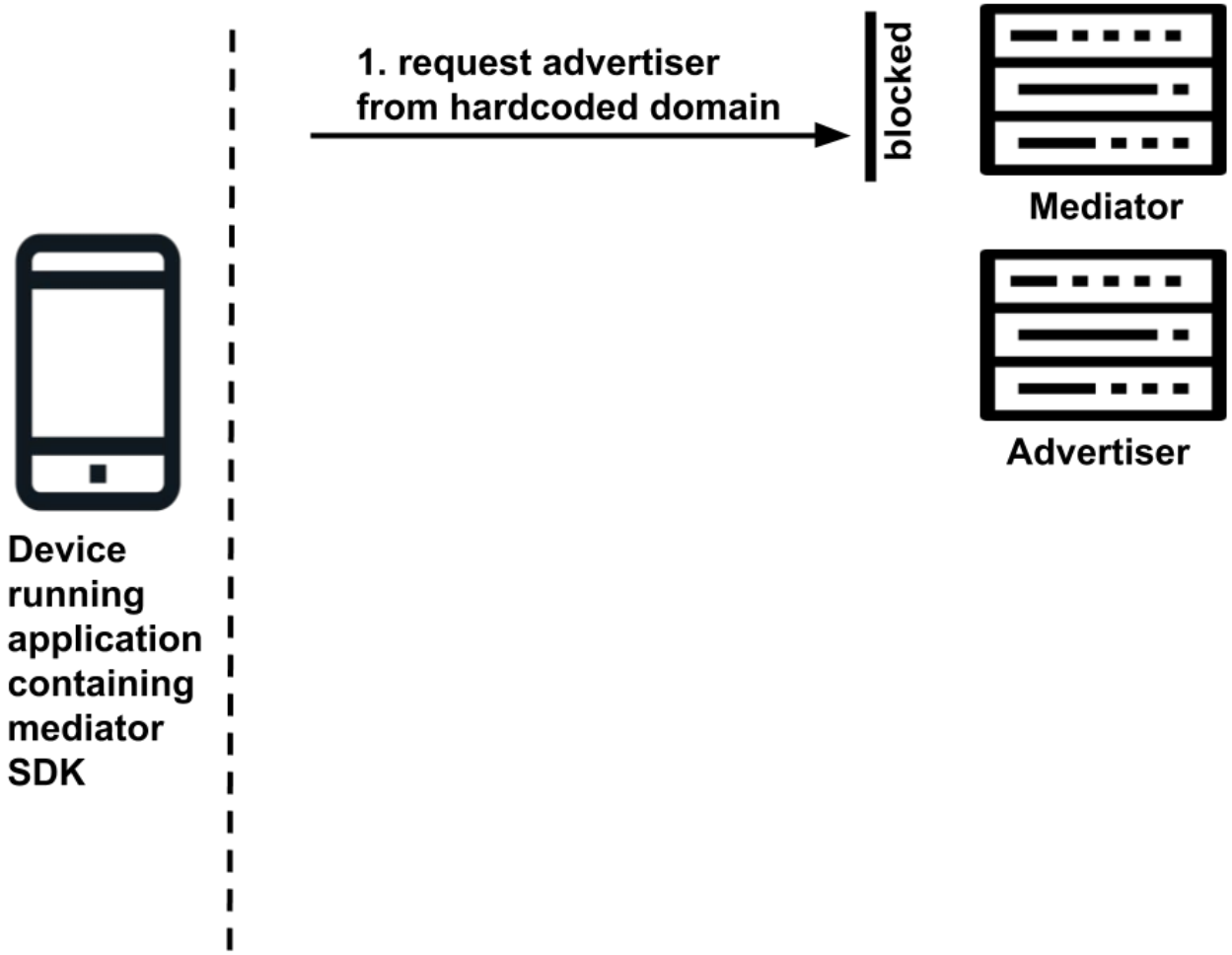
- list of enabled advertisers
- install time
- uptime
- app key
- package name
- package version

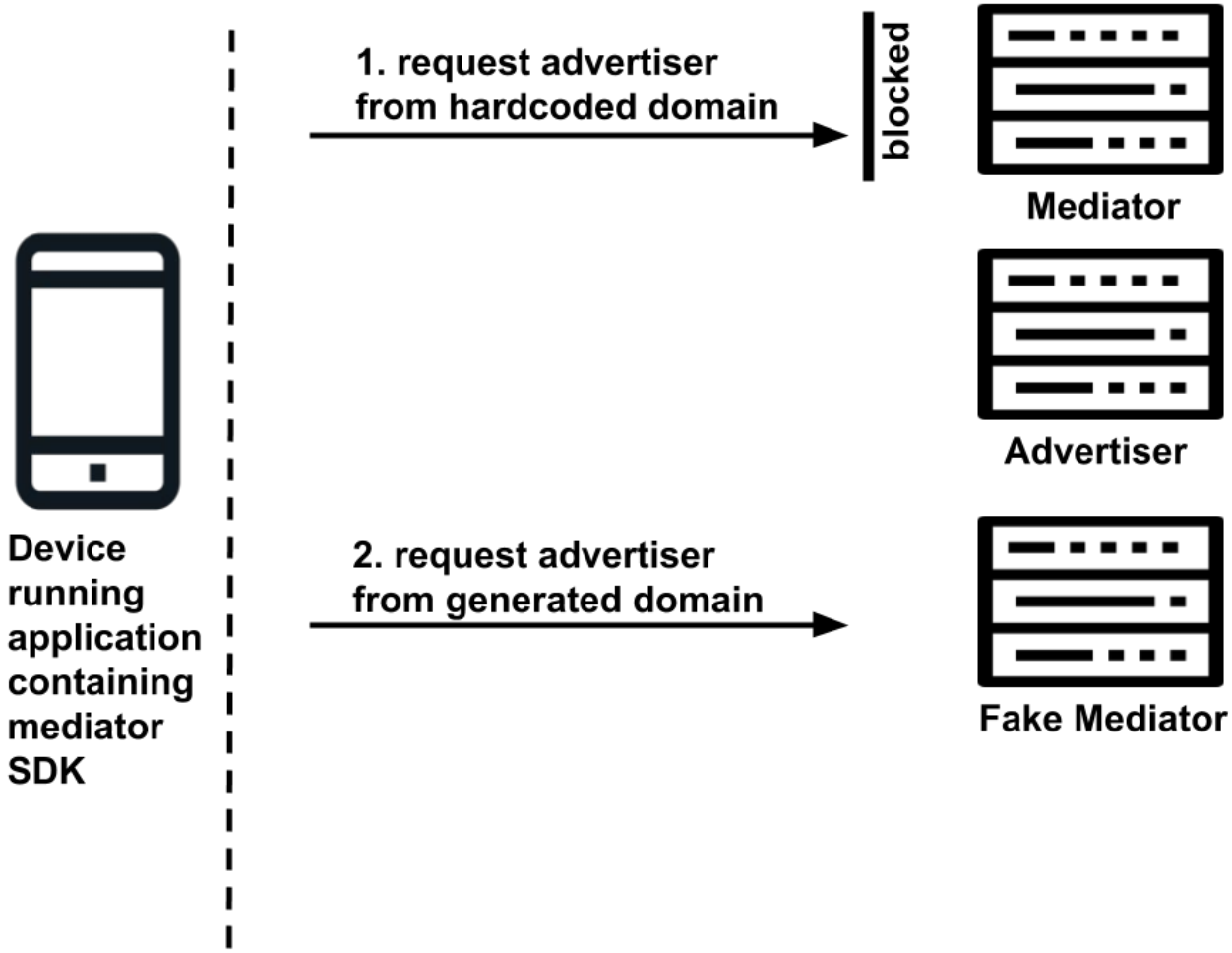
Applications

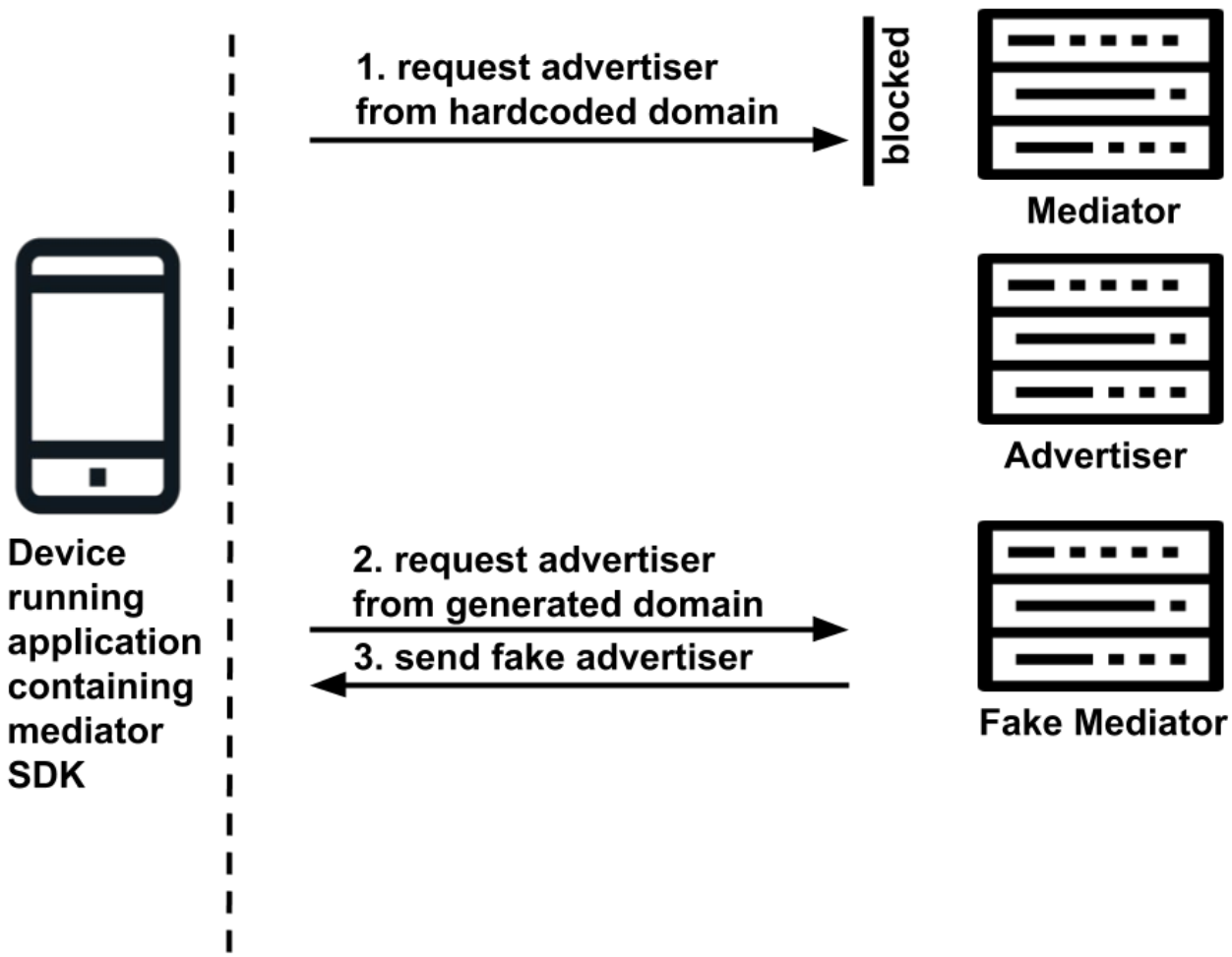
- used in ~2000 applications
- in top 10 applications sorted by number of received requests:
  - 1 application has almost one million installs
  - 1 application has almost half a million installs
  - 4 applications have a quarter of a million installs

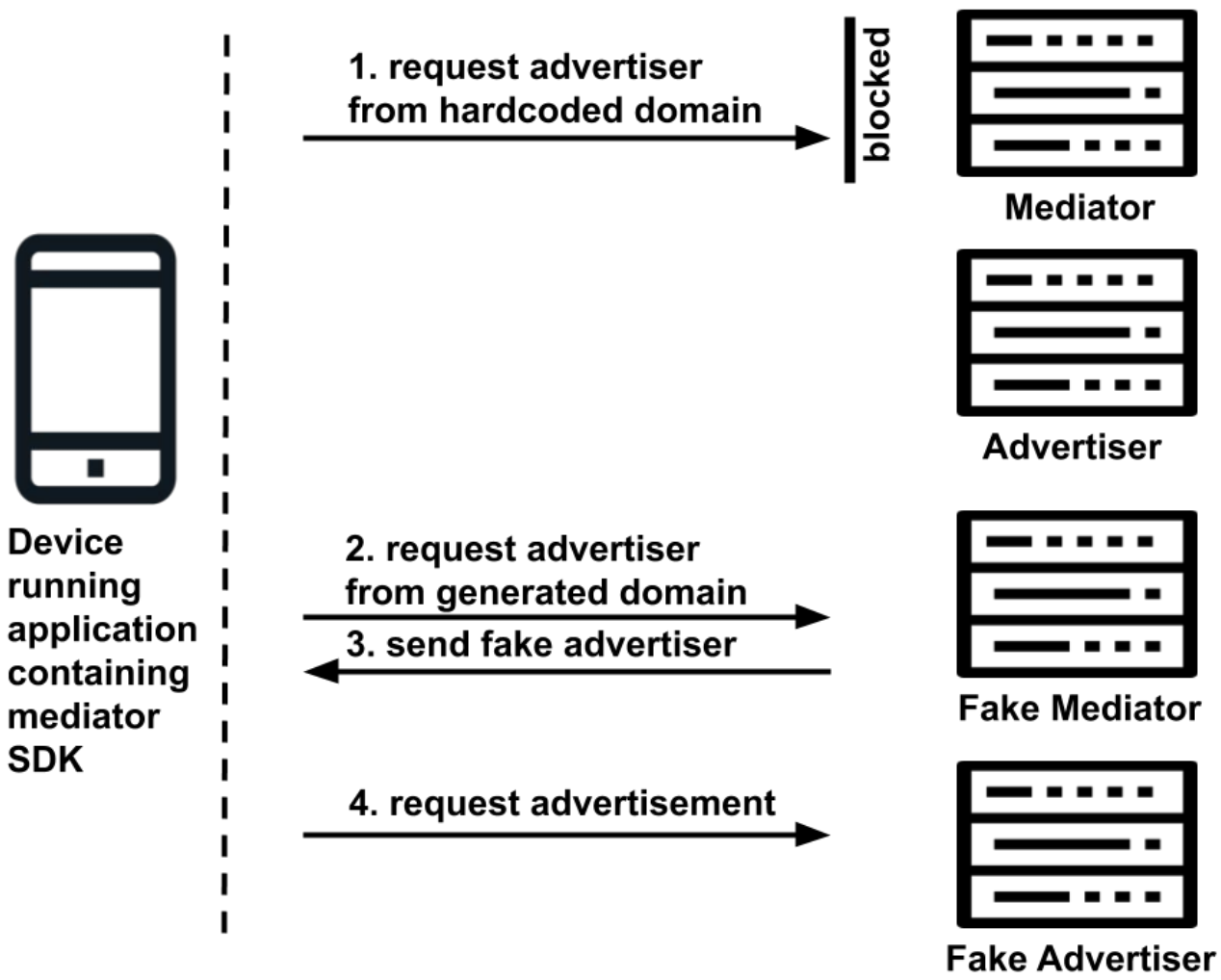
Communication flow

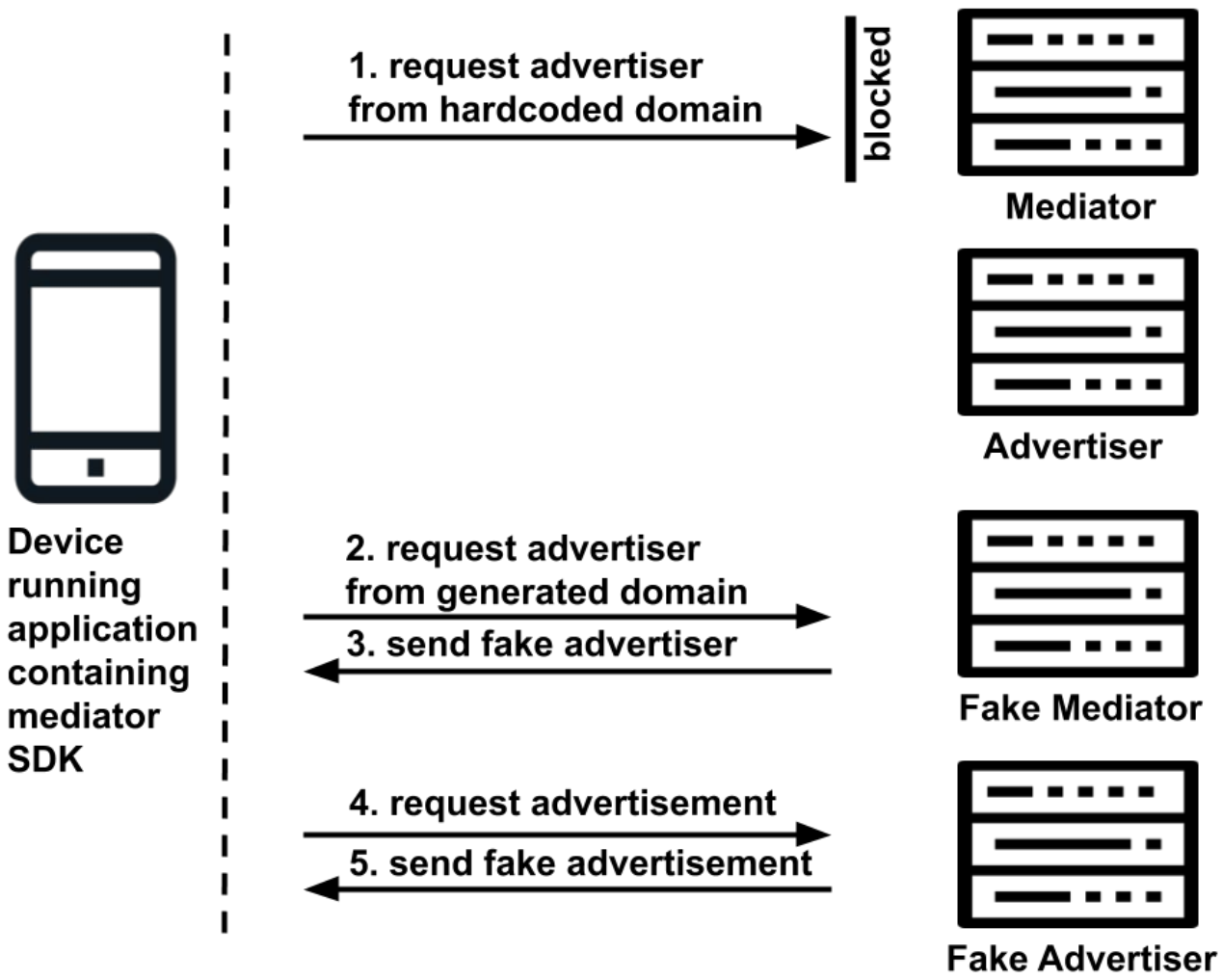
- hardcoded domain: unreachable
- generated domain: belongs to a malicious third party

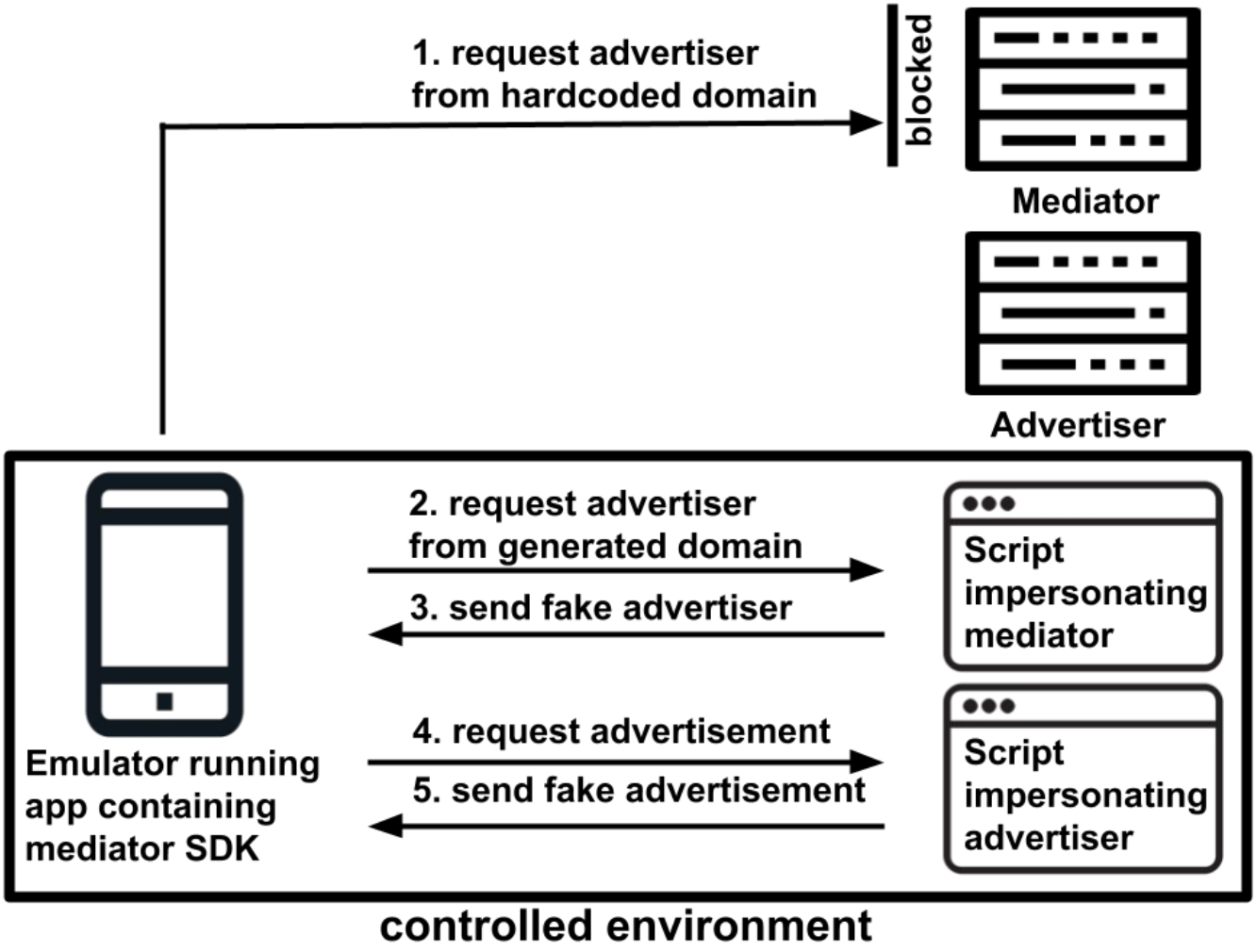

1. request advertiser
from hardcoded domain
blocked
Mediator
Advertiser
Device
running
application
containing
mediator
SDK


1. request advertiser
from hardcoded domain
blocked
Mediator
Advertiser
Device
running
application
containing
mediator
SDK
2. request advertiser
from generated domain
Fake Mediator


1. request advertiser
from hardcoded domain
blocked
Mediator
Advertiser
Device
running
application
containing
mediator
SDK
2. request advertiser
from generated domain
3. send fake advertiser
Fake Mediator


1. request advertiser
from hardcoded domain
blocked
Mediator
Advertiser
Device
running
application
containing
mediator
SDK
2. request advertiser
from generated domain
3. send fake advertiser
Fake Mediator
4. request advertisement
Fake Advertiser


1. request advertiser
from hardcoded domain
blocked
Mediator
Advertiser
Device
running
application
containing
mediator
SDK
2. request advertiser
from generated domain
3. send fake advertiser
Fake Mediator
4. request advertisement
5. send fake advertisement
Fake Advertiser


1. request advertiser
from hardcoded domain
blocked
Mediator
Advertiser
2. request advertiser
from generated domain
3. send fake advertiser
Script
impersonating
mediator
4. request advertisement
5. send fake advertisement
Script
impersonating
advertiser
Emulator running
app containing
mediator SDK
controlled environment

Demo

Possible Attacks

- impersonate mediator and provide specially crafted ads
- gather information about users and advertisers using the mediator and sell it on underground markets

Comparison of use cases

Use case	Applications / Websites	Unique IPs per day	Platform	Fixed
Use case 1 (hardcoded domain)	~40	~500 000	Android	no
Use case 2 (hardcoded domain)	~10 000 websites, ~20 000 apps	>10 000 000	Android, iOS	no
Use case 3 (wrong domain)	~20 000 websites, ~1 000 apps	~2 500 000	mobile, browser	yes
Use case 4 (wrong domain)	unknown	~500 000	HTML5 player	yes
Use case 5 (DGA)	~2 000 apps	min ~60 000	mobile	no

Conclusion

Attackers can easily sinkhole advertising infrastructure in order to create an infection vector targeting advertiser’s user base.