

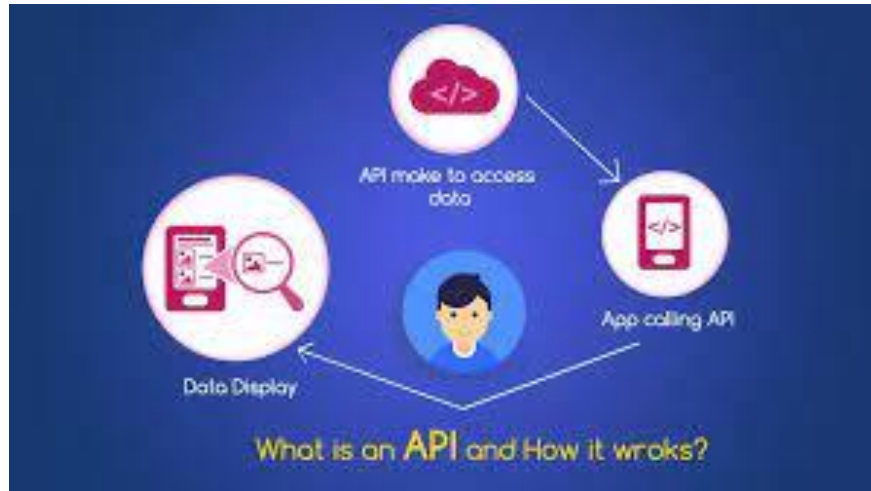
# Why Does Your Data Leak? Uncovering the Data Leakage in Cloud from Mobile Apps

*-Devin Lilaramani, Shriya Surusani, Anoop Kakkireni.*

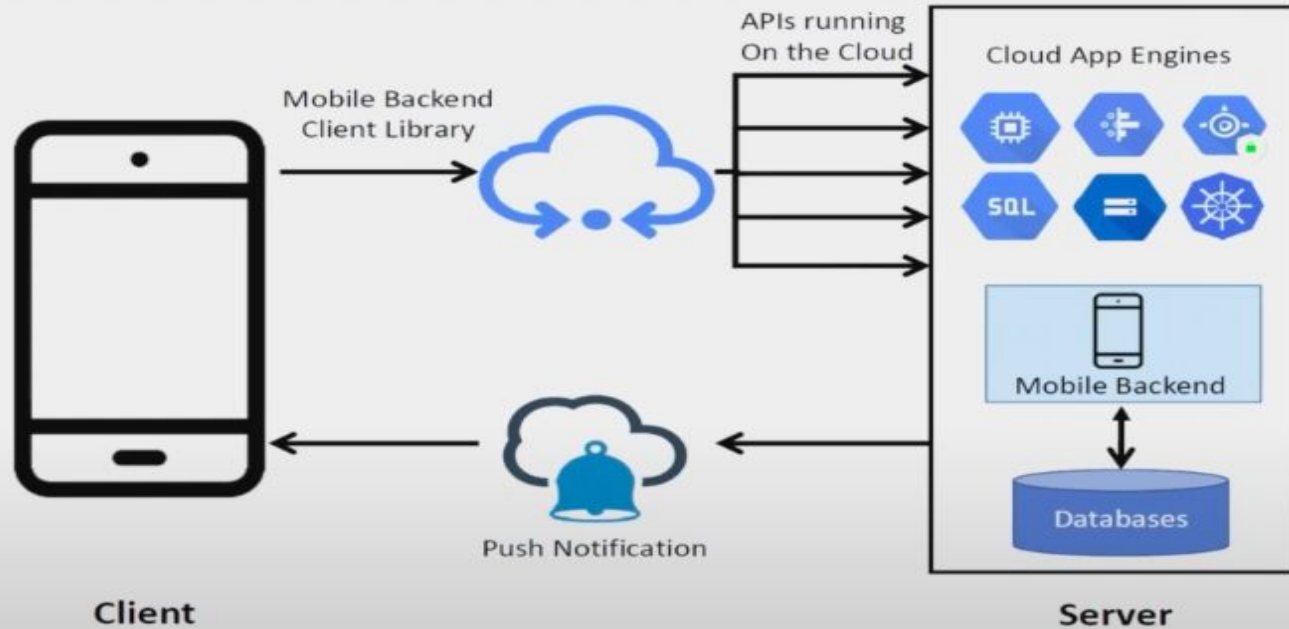
# Introduction

## What is an API?

1. Application Programming Interfaces
2. Software to Software Interfaces
3. Microservices Communication



# The Mobile Backend as a Service (mBaaS)



## How does an API Function?

An API Functions using a request verb

1. GET : To retrieve a resource
2. POST : To create a new resource
3. PUT : To edit or update an existing resource
4. DELETE : To delete a resource

# Introduction

## What is an API?

Standard GET Response:

**GET** [https://developer.nrel.gov/api/alt-fuel-stations/v1/nearest.json?api\\_key=XXXXXXXXXX&location=Clemson+SC](https://developer.nrel.gov/api/alt-fuel-stations/v1/nearest.json?api_key=XXXXXXXXXX&location=Clemson+SC)

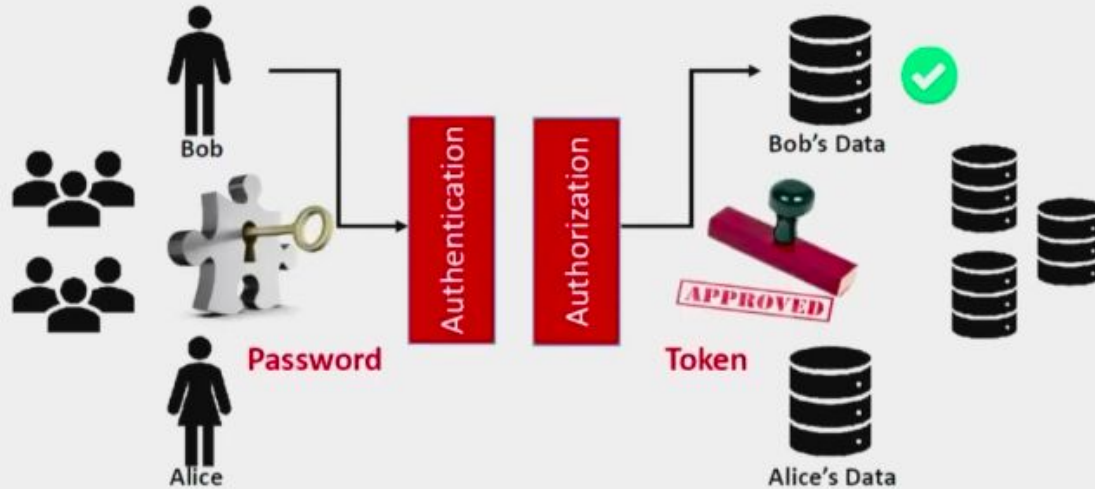
*IF exists : HTTP Response 200(OK)*

*IF Doesn't exist: HTTP Response 404(Not Found)*

## Security in APIs

- As Data flows through the API, Security is of the utmost importance to prevent data leakage.
- API are obvious entry points for attackers to break into the system
- Handling requests to resources that aren't allowed.
- Field-Level access control : What should be visible to which user?
- Using Postman to verify the results of the vulnerabilities.

# Data Leakage as an Access Control Problem



## mBaas Cloud Providers

aws



Firebase



Azure



# Crawling the Web

Using scrapy for finding the most used apps and then extracting the apk files of those apps.

```
(base) PS C:\Users\sshri> scrapy shell
2022-03-13 15:06:05 [scrapy.utils.log] INFO: Scrapy 2.6.1 started (bot: scrapybot)
2022-03-13 15:06:05 [scrapy.utils.log] INFO: Versions: lxml 4.6.3.0, libxml2 2.9.10, cssselect 1.1.0, parsel 1.6.0, w
b 1.22.0, Twisted 22.2.0, Python 3.8.8 (default, Apr 13 2021, 15:00:03) [MSC v.1916 64 bit (AMD64)], pyOpenSSL 20.0.1
penSSL 1.1.1k 25 Mar 2021), cryptography 3.4.7, Platform Windows-10-10.0.22000-SP0
2022-03-13 15:06:05 [scrapy.crawler] INFO: Overridden settings:
{'DUPEFILTER_CLASS': 'scrapy.dupefilters.BaseDupeFilter',
 'LOGSTATS_INTERVAL': 0}
2022-03-13 15:06:05 [scrapy.utils.log] DEBUG: Using reactor: twisted.internet.selectreactor.SelectReactor
2022-03-13 15:06:05 [scrapy.extensions.telnet] INFO: Telnet Password: 68d6410e50cd3856
2022-03-13 15:06:05 [scrapy.middleware] INFO: Enabled extensions:
['scrapy.extensions.corestats.CoreStats',
 'scrapy.extensions.telnet.TelnetConsole']
2022-03-13 15:06:05 [scrapy.crawler] INFO: Crawling enabled
In [2]: fetch("com.cardinalblue.piccollage.google_66410_apps.evovi.com.apk")
2022-03-13 15:44:48 [scrapy.core.engine] DEBUG: Crawled (200) <GET file:///C:/Users/sshri/com.cardinalblue.piccollage.g
ogle_66410_apps.evovi.com.apk> (referer: None)
In [3]:
```

# Applications in our dataset

```
C:\Users\sshri\Desktop\Tool>cd api_key_detector
```

```
C:\Users\sshri\Desktop\Tool\api_key_detector>ls
```

Boilr.apk	Gardine.apk	LeafPic.apk	Paseo.apk	Trekarta.apk	WaniDoku.apk
Calendula.apk	Gen_authtoken.py	Metronome.apk	PoetAssistant.apk	TriPeaks.apk	Yokatta.apk
FediPhoto-Lineage.apk	JitsiMeet.apk	Nonocross.apk	SimplySolid.apk	ValueSetAnalysis.java	

```
C:\Users\sshri\Desktop\Tool\api_key_detector>
```

# Reverse engineered the files

For checking the vulnerable code.

```
/* renamed from: d */
private static int m15766d() {
    SecureRandom secureRandom = new SecureRandom();
    byte[] bArr = new byte[4];
    byte b = 0;
    while (b == 0) {
        secureRandom.nextBytes(bArr);
        b = ((bArr[0] & byte.MAX_VALUE) << Ascii.CAN) | ((bArr[1] & 255) << Ascii.DLE) | ((bArr[2] & 255) << 8) | (bArr[3] & 255);
    }
    return b;
}

public static KeysetManager withEmptyKeyset() {
    return new KeysetManager(Keyset.newBuilder());
}

public static KeysetManager withKeysetHandle(KeysetHandle keysetHandle) {
    return new KeysetManager((Keyset.Builder) keysetHandle.m09033ff().toBuilder());
}

@Deprecated
public synchronized KeysetManager add(KeyTemplate keyTemplate) throws GeneralSecurityException {
    addNewKey(keyTemplate, false);
    return this;
}
```

```
KeyProvider23() {
}

public synchronized Key retrieveKey(String str) throws KeyNotFoundException {
    Key key;
    try {
        KeyStore instance = KeyStore.getInstance(ANDROID_KEY_STORE_NAME);
        instance.load((KeyStore.LoadStoreParameter) null);
        if (instance.containsAlias(str)) {
            Log log = Logger;
            log.debug("AndroidKeyStore contains keyAlias " + str);
            logger.debug("loading the encryption key from Android KeyStore.");
            key = instance.getKey(str, (char[]) null);
            if (key == null) {
                throw new KeyNotFoundException("Key is null even though the keyAlias: " + str + " is present in " + ANDROID_KEY_STORE_NAME);
            }
        } else {
            throw new KeyNotFoundException("AndroidKeyStore does not contain the keyAlias: " + str);
        }
    } catch (Exception e) {
        throw new KeyNotFoundException("Error occurred while accessing AndroidKeyStore to retrieve the key for keyAlias: " + str, e);
    }
    return key;
}
```

# Checking any false positives

- Ran the tool against the dataset.
- Confirmed that no false positives exist while scanning for the cloud providers in the apps.
- Results were confirmed by cross checking it which our results found after reverse engineering the files.

# Extracted Keys

```
C:\Users\sshri\Desktop\Tool\api_key_detector>javac ValueSetAnalysis.java
```

```
C:\Users\sshri\Desktop\Tool\api_key_detector>java ValueSetAnalysis
```

```
0.06817095,0.00014711,0.00681442,ISSN8yYzHk84Y6PfMd_1BvhNCBzgfQxcSP5bx--ZMil0Qmkh/VU2bBUpYulVyxgwh5nY5s
0.06817095,0.00014711,0.00681442,c487ba1b6d536aec1f3e48bffbe3532c1f78b1a2
0.06817095,0.00014711,0.00681442,e1d0c9ce505b1822d97a34ade0107d241d82ec74fd522e4963e602c
0.06817095,0.00014711,0.00681442,oxBmfms2SrMeEB5iaQUFR7VCnLYFxNY3jLHPGYXmd7fe81e4f62df3e
0.06817095,0.00014711,0.00681442,AuhXCurI1rloe8xbkzHpXnZQ3D993ibcHXaCJsc56_70Sm1vTYgeXH0uo/BbXz-tnClC85
0.06817095,0.00014711,0.00681442,075b4a0782c168c8c197691365e8a6c65ed13d410fd10a68a2068ba
0.06817095,0.00014711,0.00681442,NHxD9JJoV24aI5sDmZo/Kbex7Fa6d8eJz7DBSRI0g
0.06817095,0.00014711,0.00681442,dfdf3928dd6d77c62d290162ccdb61bbfda041ddfb6d70bed45eef6
0.06817095,0.00014711,0.00681442,0ad60a37fb035d1d9c1c0094c1a558848a156cb167c33a36d6e2cff
0.06817095,0.00014711,0.00681442,0cdcU07Pn00FAHuDdZcwQDfAHMnARUT7CRIWJ9m
0.06817095,0.00014711,0.00681442,eyJ0eXAI0iJKV1QilC0hbGciliJIUzI1NiJ9.eyJlbwFpbCI6ImFkb2
0.06817095,0.00014711,0.00681442,zS/3eq7qguYNawW83NmFY7fIcCkqw_kPwOn8lZVyboxNK_VsIh7Q7Xw93cZw4GLAUBJs4l
0.06817095,0.00014711,0.00681442,KFsukQJ8FpgQu9u8qiga0qqDDydNh5K5o9vzQM6JpJwvBaD7mPgp7RW5ZLZQer6GDr_QtQ
0.06817095,0.00014711,0.00681442,YfPlv0e6pzN9h3Ceq0s02J/dra747RxXP0xyNcJG
0.06817095,0.00014711,0.00681442,Led8vxbES1fs1Lv_0jYl0-y1lsCi07W0sutuHd0JgUbcVbur/Bl0aMZ-w0vXSikmQwMKfF
```

```
C:\Users\sshri\Desktop\Tool\api_key_detector>
```

# Querying with the cloud providers endpoint

- Using the extracted key, one of the Get request made to AWS.
- This shows that there are no Misconfigured AWS Authorization Rules.

← → ↻ [ec2.amazonaws.com/?Action=RunInstances&ImageId=ami-2bb65342&MaxCount=3&MinCount=1&Placement.AvailabilityZone=us-east-1a&Monitoring.Enabled=true&Version=2016-11-15...](https://ec2.amazonaws.com/?Action=RunInstances&ImageId=ami-2bb65342&MaxCount=3&MinCount=1&Placement.AvailabilityZone=us-east-1a&Monitoring.Enabled=true&Version=2016-11-15...) ↗ ☆

This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
▼<Response>
  ▼<Errors>
    ▼<Error>
      <Code>AuthFailure</Code>
      <Message>AWS was not able to validate the provided access credentials</Message>
    </Error>
  </Errors>
  <RequestID>4f108d06-118b-4f80-b366-810cd7094c9b</RequestID>
</Response>
```



# Querying to AWS database using the key

- Get request made to AWS simple DB.
- This shows that this is the root key that was present in the mobile apk. The attacker can easily extract this. Thus, causing data leakage.

```
- Hotels", "impression_id": "000b000000825c088d3f8743a2bea22ef931f92969", "expansion": {}, "tags": [{"id": 4295, "name": "Hotels & Motels", "primary": true}, {"id": 4302, "name": "Family-Friendly Hotels", "primary": false}, {"id": 4303, "name": "Tourist Hotels", "primary": false}, {"id": 4306, "name": "Weekend Getaway Hotels", "primary": false}, {"id": 4305, "name": "Luxury Hotels", "primary": false}, {"id": 4307, "name": "Pet-Friendly", "primary": false}, {"id": 12643, "name": "Pet-Friendly", "primary": false}, {"id": 12644, "name": "Private Bath", "primary": false}, {"id": 12646, "name": "Room Service", "primary": false}, {"id": 12641, "name": "Meeting Center", "primary": false}, {"id": 12642, "name": "Online Reservations", "primary": false}, {"id": 11349, "name": "Discover Accepted", "primary": false}, {"id": 12638, "name": "Hotel Spa", "primary": false}, {"id": 12639, "name": "Hotel Dining", "primary": false}, {"id": 12636, "name": "Hotel Dining", "primary": false}, {"id": 12637, "name": "Hotel Pool", "primary": false}, {"id": 12635, "name": "Hotel Bar", "primary": false}, {"id": 12633, "name": "Hotels", "primary": false}, {"id": 4299, "name": "Budget Hotels", "primary": false}, {"id": 11361, "name": "Mastercard Accepted", "primary": false}, {"id": 4287, "name": "Lodging", "primary": false}, {"id": 11382, "name": "Visa Accepted", "primary": false}, {"id": 11333, "name": "American Express Accepted", "primary": false}, {"id": 4300, "name": "Business Hotels", "primary": false}], "public_id": "holiday-inn-boston-at-boston", "business_operation_status": 1, "scorecard": "0", "votes": 0, "awards": [], "has_menu": false, "politanName": "Boston, MA Metro", {"id": 4730635, "featured": false, "name": "The Lenox Hotel", "city": "Boston", "state": "MA", "postal_code": "02116", "neighborhood": "Back Bay East", "latitude": 42.349218, "longitude": -71.079376, "phone_number": "6174214970", "rating": 0.0, "profile": "http://www.citysearch.com/profile/4730635/boston_ma/the_lenox_hotel.html", "has_reviews": true, "user_review_count": 0, "sample_categories": "Hotels & Motels, Family-Friendly Hotels, Tourist Hotels, Weekend Getaway Hotels", "impression_id": "000b0000000215c3406ecb49a29de6247d8", [{"id": 4295, "name": "Hotels & Motels", "primary": true}, {"id": 4302, "name": "Family-Friendly Hotels", "primary": false}, {"id": 4303, "name": "Tourist Hotels", "primary": false}, {"id": 4306, "name": "Hotels", "primary": false}, {"id": 4305, "name": "Luxury Hotels", "primary": false}, {"id": 12636, "name": "Hotel Dining", "primary": false}, {"id": 3997, "name": "Health Clubs & Gyms", "primary": false}, {"id": 12645, "name": "Romantic", "primary": false}, {"id": 11375, "name": "Shop Online", "primary": false}, {"id": 4298, "name": "Boutique Hotels", "primary": false}, {"id": 4299, "name": "Budget Hotels", "primary": false}, {"id": 11361, "name": "Mastercard Accepted", "primary": false}, {"id": 11349, "name": "Discover Accepted", "primary": false}, {"id": 4287, "name": "Lodging", "primary": false}, {"id": 1697, "name": "Lodging", "primary": false}, {"id": 11382, "name": "Visa Accepted", "primary": false}, {"id": 11333, "name": "American Express Accepted", "primary": false}, {"id": 4300, "name": "Business Hotels", "primary": false}], "public_id": "holiday-inn-boston-at-boston", "business_operation_status": 1, "scorecard": "0", "votes": 0, "awards": [], "has_menu": false, "politanName": "Boston, MA Metro", {"id": 4716325, "featured": false, "name": "Omni Parker House Hotel"}]
```

# Results of our analysis

Name	Cloud Service Used	App Description and Functionality	Privacy Sensitive
Yokatta	AWS	Flashcards based language learning app	✗
Simply Solid	AWS	Pick a solid color as your homescreen background color	✓
Boilr	AWS	Android app which monitors Bitcoin, cryptocurrencies, cryptoassets, futures and options, triggering price alarms	✗
Metronome	AWS	Professional tool to help all musicians play with flawless accuracy	✗
TriPeaks	AWS	Classic solitaire puzzle game	✓

Apps that use AWS as their backend service



# Results of our analysis

Name	Cloud Service Used	App Description and Functionality	Privacy Sensitive
Calendula	Firebase	Manage your medical prescriptions through a simple and intuitive interface	✗
WaniDoku	Firebase	Japanes leaning app	✗
Poet Assistant	Firebase	A set of offline tools to help with writing poems	✗
Nonocross	Firebase	Simple number puzzle game based around grids	✓
Paseo	Firebase	Step counting app	✗

Apps that use Google  
Firebase as their backend  
service

# Results of our analysis

Name	Cloud Service Used	App Description and Functionality	Privacy Sensitive
FediPhoto-Lineage	Azure	Quickly post photos	✗
Trekarta	Azure	Designed for hiking, geocaching, off-roading, cycling, boating and all other outdoor activities	✓
LeafPic	Azure	A fluid, material-designed alternative gallery	✗
Gardine	Azure	A minimalistic one-touch app switcher	✓
Jitsi Meet	Azure	Instant video conferences efficiently adapting to your scale	✗

Apps that use Microsoft Azure as their backend service



Thankyou (: