

API Security – a must have for network operators

Chao Yin Loong

Purpose of talk

- As network operators embrace NetOps there will be a plethora of APIs available
- Network operators increasingly automating and using APIs
- APIs by network operators need to be secure

Example

Hacker hijacks Orange Spain RIPE account to cause BGP havoc

By [Lawrence Abrams](#)



January 3, 2024



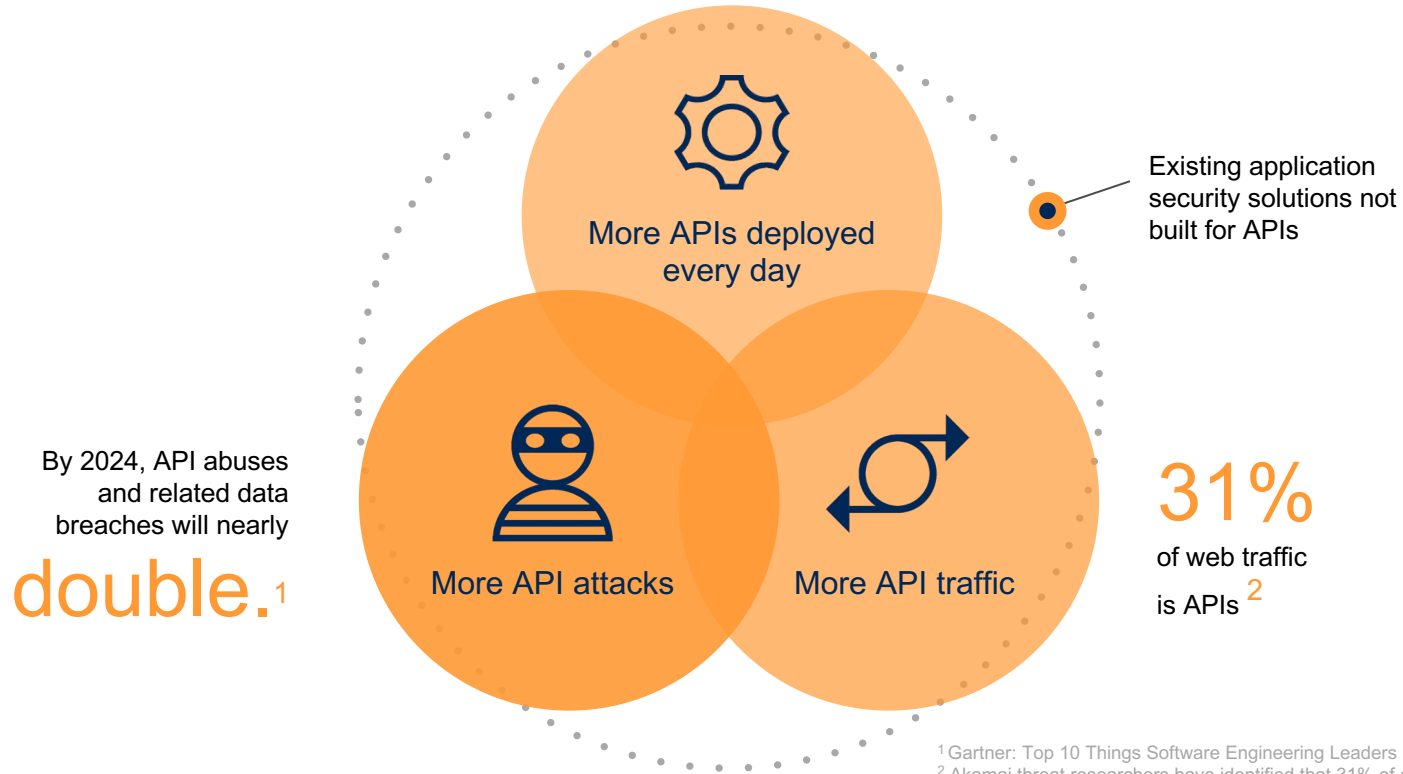
02:44 PM



0

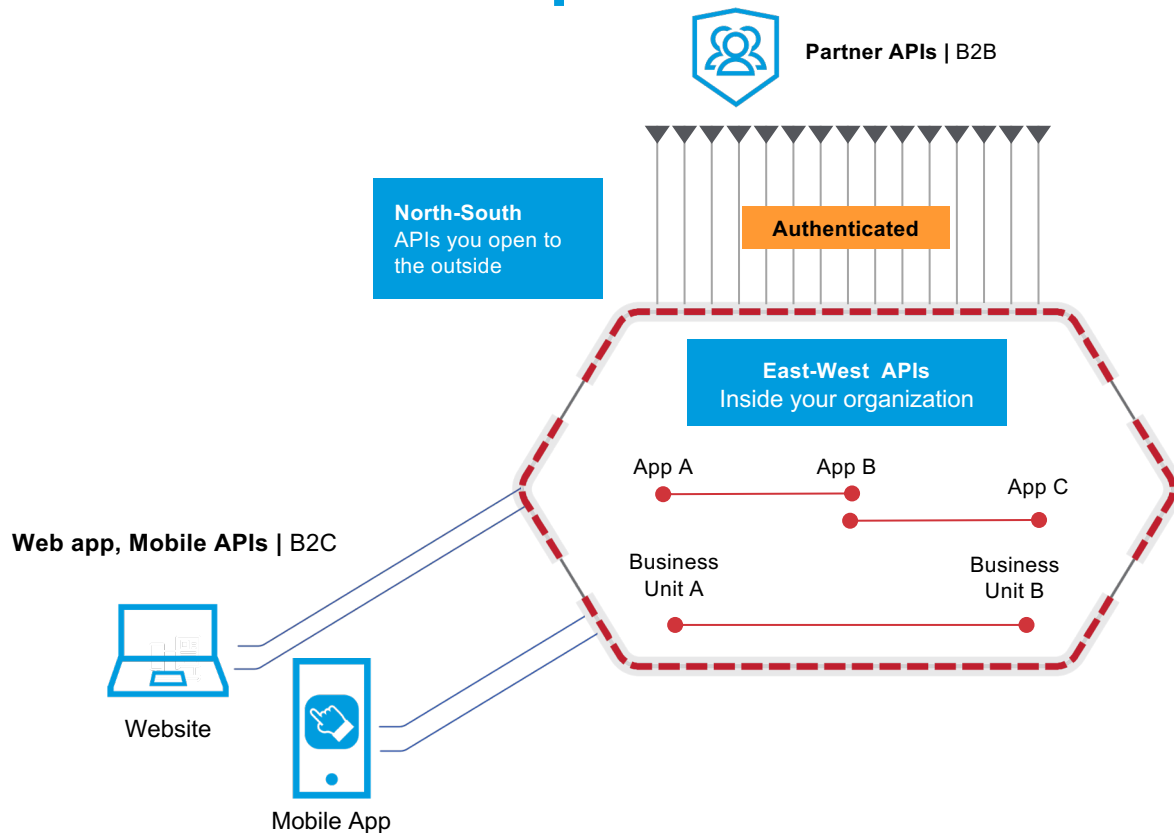
- In this case it was via a password
- Imagine if this was via an leaked API key
- Need tools to detect anomaly in the way API is used

The API Security Environment

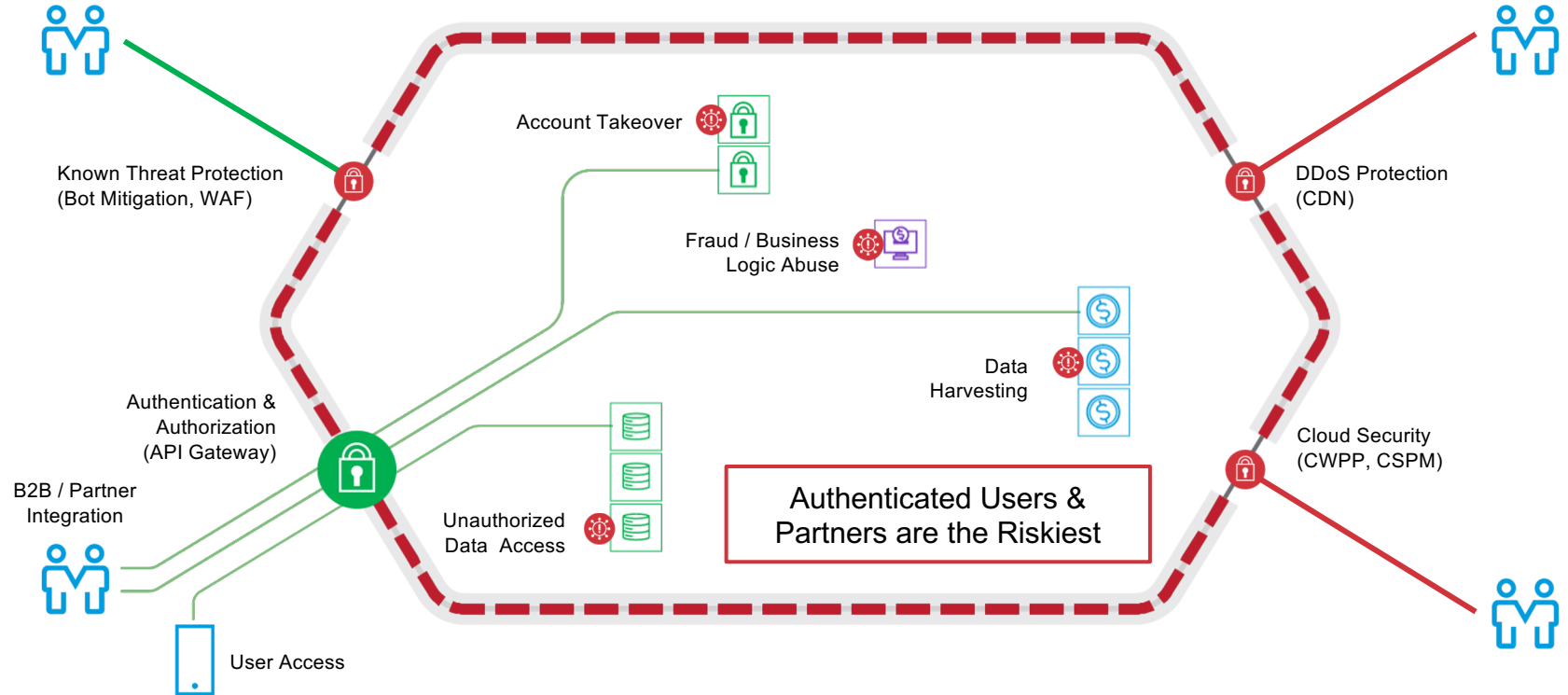


¹ Gartner: Top 10 Things Software Engineering Leaders Need to Know About APIs
² Akamai threat researchers have identified that 31% of all traffic protected by Akamai is API traffic

What is your API landscape?



API Abuse Can Happen Beyond WAAP



Real world examples : Large mobile network operator Data Breach

- 1.API used during testing got exposed.
- 2.API had no Authentication or Authorization mechanisms.
- 3.API had no rate-limiting that allowed attackers to send a large number of requests to retrieve data.
- 4.Customer IDs were stored in a weak format instead of the UUID mechanism, which allowed attackers to easily guess and request millions of records.

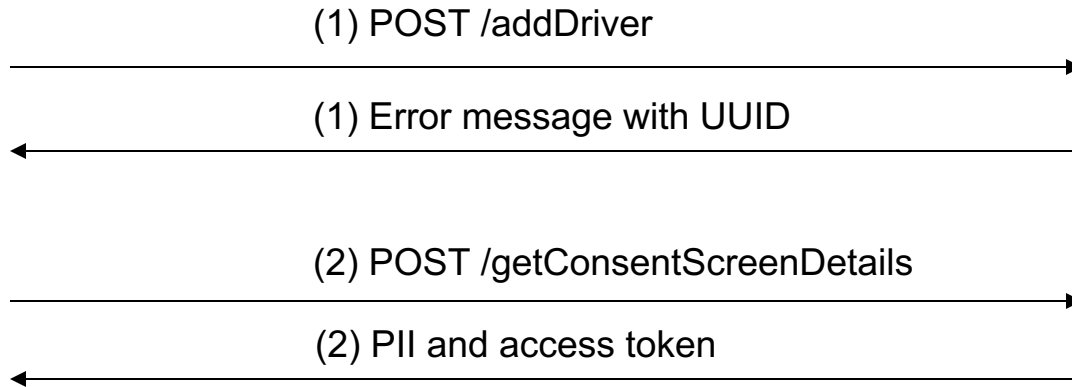
Hypothetical example: Abusing RIR API



1. Various RIR provides API interface
2. API compromised by malicious users through various means
3. Without any system to immediately detect anomalous usage, hackers can misconfigure BGP routing and RPKI configuration and cause havoc

Real world examples : Uber: Account Takeover

- How I could Have hacked your Uber Account (Anand Prakash, 2019)
- Anand got from a phone number/email address to full account takeover
- The vulnerabilities were quickly fixed by Uber



Real world examples : Uber: Account Takeover

```
POST /p3/fleet-manager/_rpc?rpc=addDriverV2 HTTP/1.1
Host: partners.uber.com
{"nationalPhoneNumber": "99999xxxx" "countryCode": "1"}
```

(1)

```
Response:
{"status": "failure" "data": {"code": 1009, "message": "Driver 4
0xx5e-xxxx-b01a-xxxx not found"}}
```

```
POST /marketplace/_rpc?rpc=getConsentScreenDetails HTTP/1.1
Host: bonjour.uber.com
Connection: close
Content-Length: 67
Accept: application/json
Origin: https://bonjour.uber.com
x-csrf-token: xxxxx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_3)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.103
Safari/537.36
DNT: 1
Content-Type: application/json
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: xxxxx
{"language": "en", "userId": "xxxx-776-4xxxx1bd-861a-837xxx604ce"}
```

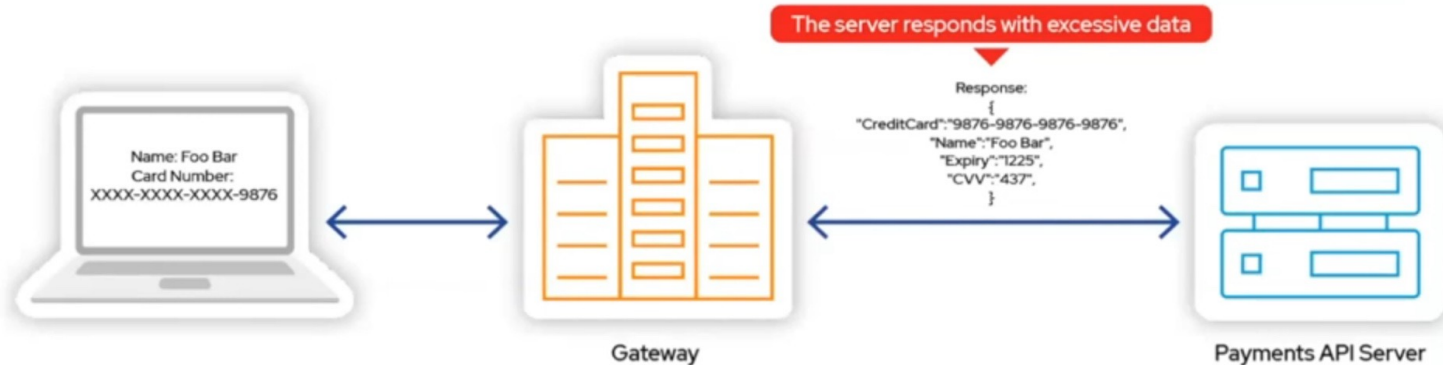
(2)

```
{
  "status": "success",
  "data": {
    "data": {
      "language": "en",
      "userId": "xxxxxxie",
      "getUser": {
        "uid": "cxxxxx5f7371e",
        "firstname": "Maxxxx",
        "lastname": "XXXX",
        "role": "PARTNER",
        "languageId": 1,
        "countryId": 77,
        "mobile": null,
        "mobileToken": 1234,
        "mobileCountryId": 77,
        "mobileCountryCode": "+91",
        "hasAmbiguousMobileCountry": false,
        "lastConfirmedMobileCountryId": 77,
        "email": "xxxx@gmail.com",
        "emailToken": "xxxxxxx",
        "hasConfirmedMobile": "no",
        "hasOptedInSemaMarketing": false,
        "hasConfirmedEmail": true,
        "gratuity": 0.3,
        "nickname": "abc",
        "gmail.com": "BBBBB",
        "banned": false,
        "cardio": false,
        "token": "b008ec414baxxxxx",
        "fraudScore": 0,
        "inviteId": null,
        "pictureUrl": "xxxxx.jpeg",
        "recentFareSplitterUids": ["xxx"],
        "lastSelectedPaymentProfileId": "xxxxxx",
        "lastSelectedPaymentProfileGoogLewalletUids": null,
        "inviteCode": {
          "promotionCodeId": "xxxxx",
          "promotionCodeUids": "xxxxx",
          "promotionCode": "anishas185",
          "createdAt": {
            "type": "Buffer",
            "data": [0, 0, 1, 76, 2, 21, 215, 101]
          },
          "updatedAt": {
            "type": "Buffer",
            "data": [0, 0, 1, 76, 65, 211, 61, 9]
          },
          "driverInfo": {
            "contactInfo": "9999999999",
            "contactInfoCountryCode": "+91",
            "driverLicense": "None",
            "firstDriverFrId": null,
            "iphone": null,
            "partnerUserId": "xxxxxxx",
            "receiveSms": true,
            "twilioNumber": null,
            "twilioNumberFormatted": null,
            "cityKnowledgeScore": 0,
            "createdAt": {
              "type": "Buffer",
              "data": [0, 0, 1, 84, 21, 124, 80, 52]
            },
            "updatedAt": {
              "type": "Buffer",
              "data": [0, 0, 1, 80, 152, 77, 41, 77]
            },
            "deletedAt": null,
            "driverStatus": "APPLIED",
            "driverFlowType": "UBERX",
            "statusLocks": null,
            "contactInfoCountryIso2Code": "KR",
            "driverEngagement": null,
            "courierEngagement": null,
            "partnerInfo": {
              "address": "xxxxxxx",
              "territoryId": "xxxxxx",
              "company": "None",
              "address2": "None",
              "cityId": 130,
              "cityName": "None",
              "firstPartnerFrId": null,
              "preferredCollectionPaymentProfileId": null,
              "iphone": "",
              "phoneCountryCode": "+91",
              "state": "None",
              "vatNumber": "None",
              "zipCode": "None",
              "createdAt": {
                "type": "Buffer",
                "data": [0, 0, 1, 84, 21, 124, 80, 52]
              },
              "updatedAt": {
                "type": "Buffer",
                "data": [0, 0, 1, 181, 30, 177, 80, 137]
              },
              "deletedAt": null,
              "fleetTypes": [],
              "fleetServices": [],
              "isFleet": true,
              "analytics": {
                "signupLat": 133.28741199,
                "signupLng": 1117.1111,
                "signupTerritoryId": "xxxxx",
                "signupPromoId": null,
                "signupForm": "iphone",
                "signupSessionId": "xxxxxxx",
                "signupAppVersion": "2.84.1",
                "signupAttributionMethod": null,
                "createdAt": {
                  "type": "Buffer",
                  "data": [0, 0, 1, 76, 2, 21, 219, 11]
                },
                "updatedAt": {
                  "type": "Buffer",
                  "data": [0, 0, 1, 76, 2, 21, 219, 11]
                },
                "signupCityId": 130,
                "signupDeviceId": null,
                "signupReferralId": null,
                "signupPromoCode": null,
                "signupPromoCodeUids": null,
                "signupPromoUids": null,
                "signupMethod": "REGULAR",
                "createdAt": {
                  "type": "Buffer",
                  "data": [0, 0, 1, 76, 2, 21, 215, 153]
                },
                "updatedAt": {
                  "type": "Buffer",
                  "data": [0, 0, 1, 182, 81, 35, 153, 135]
                },
                "deletedAt": null,
                "tenancy": "uber/production",
                "mobileConfirmationStatus": "MOBILE_NO_CONFIRMED",
                "nationalId": null,
                "nationalIdType": null,
                "merchantLocation": null,
                "lastConfirmedMobile": "xxxxxxx",
                "requestedDeletionAt": null,
                "dateOfBirth": "xxxxxx",
                "userTypes": null,
                "preferredName": "xxxxxxx",
                "freightInfo": null,
                "tempPictureUrl": null,
                "identityVerified": null,
                "paymentIntentType": null,
                "riderEngagement": null,
                "identityId": null,
                "gender": "Inferred",
                "genderId": null,
                "genderDocumented": null,
                "riderEligible": null,
                "defaultPaymentProfileByProduct": null,
                "loginEligibility": null,
                "getDisclosureVersionUids": "",
                "getLocaleCopy": null
              }
            }
          }
        }
      }
    }
  }
}
```

Real world examples : Uber: Account Takeover

API3:2019 – Excessive data exposure

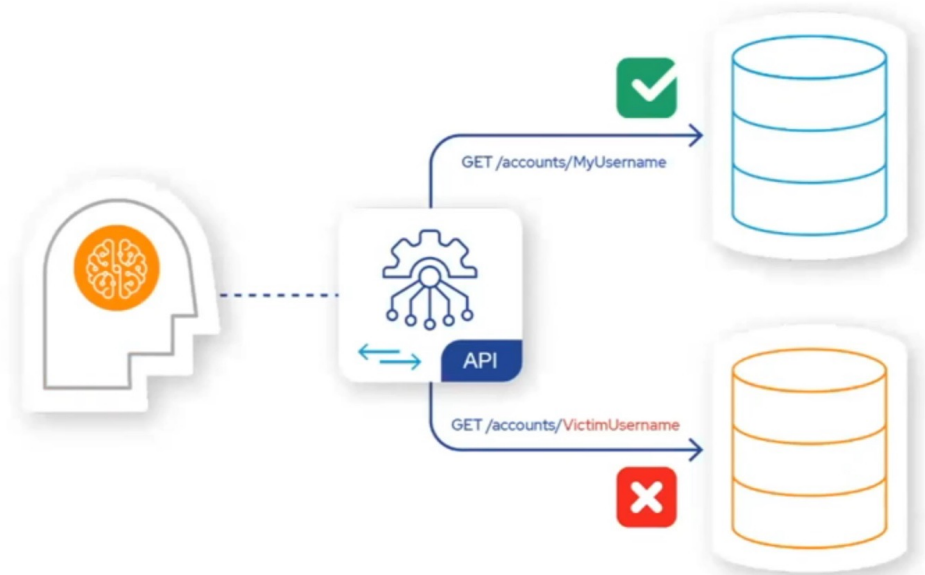
- The APIs exposed much more data than required to operate



Real world examples : Uber: Account Takeover

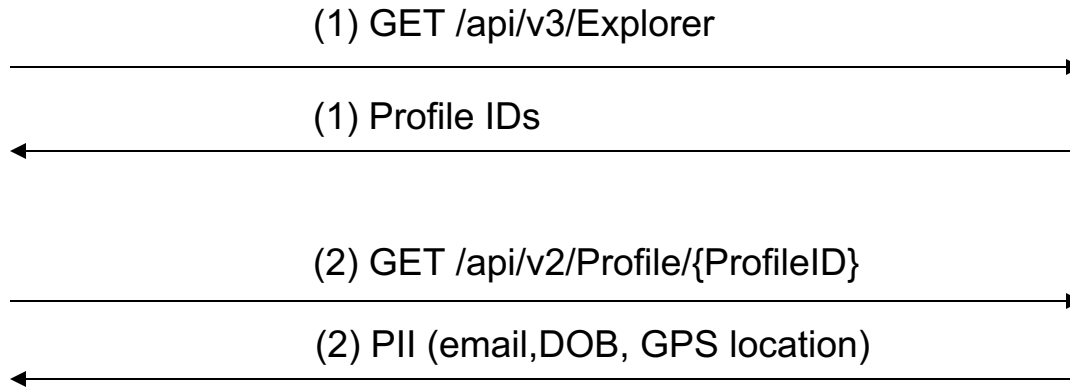
API:2019 – **B**roken **O**bject Level **A**uthorization

- Users can access resources that are not owned by them



Real world examples : Scoolio: Data Exposure

- Scoolio – German student app
- API exposed PII and more for any user in the platform



Real world examples : Scoolio Vulnerability

/api/v3/Profile/{ProfileID}

```
{
  "profileId": "26dad47a-8354-45f6-960e-ef05b58a6536",
  "schoolId": "85ce1b51-7da3-4bff-bb29-87d0553ae719",
  "clLvl": 9,
  "clExt": "B",
  "isAmbassador": false,
  "nickName": "MariaMaier2005",
  "slogan": "🇪🇺🇩🇪",
  "emojiCount": "2",
  "userFilesIds": [],
  "profileImageId": "154bf0cd-2c53-4a6e-8590-c5879086373c",
  "explorerImageId": "f49b8c4f-76a8-40bd-8716-458fd4cf4080",
  "dayOfBirth": "2005-10-01T00:00:00Z",
  "emailConfirmed": true,
  "blocked": false
}
```

/api/v2/Profile/{ProfileID}

```
{
  "profileId": "26dad47a-8354-45f6-960e-ef05b58a6536",
  "schoolId": "85ce1b51-7da3-4bff-bb29-87d0553ae719",
  "clLvl": 9,
  "clExt": "B",
  "email": "mariamaiercool2005@gmail.com",
  "parentsEmail": "dannyroller@gmail.com",
  "parentsAcceptedConditionsDate": "2021-03-12T13:23:33",
  "acceptedConditionsDate": "2021-03-12T11:13:12",
  "slogan": "🇪🇺🇩🇪",
  "imgIds": [
    "006642e8-4ec2-4b8d-9077-4d6f7a5a7c2d"
  ],
  "position": {
    "lon": 13.7491207,
    "lat": 51.0716188,
    "updatedAt": "2021-10-22T05:09:31Z"
  },
  "nickName": "MariaMaier2005",
  "dayOfBirth": "2005-10-01T00:00:00Z",
  "isAmbassador": false,
  "emojiCount": "2",
  "userFilesIds": [
  ],
  "profileImageId": "154bf0cd-2c53-4a6e-8590-c5879086373c",
  "explorerImageId": "f49b8c4f-76a8-40bd-8716-458fd4cf4080",
  "emailConfirmed": true,
  "blocked": false
}
```

Real world examples : Coinbase

coinbase



The screenshot shows a ZDNET article header with navigation icons (globe, search, user, menu). Below the header is a breadcrumb trail: Home / Finance / Blockchain. The main headline reads: "Coinbase pays out largest bug bounty ever for trading interface flaw". A sub-headline states: "The researcher who discovered the issue was paid \$250,000."



Tree of Alpha @Tree_of_Alpha · Feb 19

I just used 0.0243 ETH to sell 0.0243 BTC on the BTC-USD pair, a pair I do not have access to, without holding any BTC.

Hoping this is a UI bug, I check the fills on the order, and they match the API: those trades really happened, on the live order book.

What happened:

- User scraped API calls from web UI
- Identified 4 key parameters for any Coinbase transaction
- Manipulated the parameters via API calls
- Sold crypto they DID NOT own

**OWASP API #1
Broken Object Level
Authorization**

Real world examples : Coinbase

coinbase

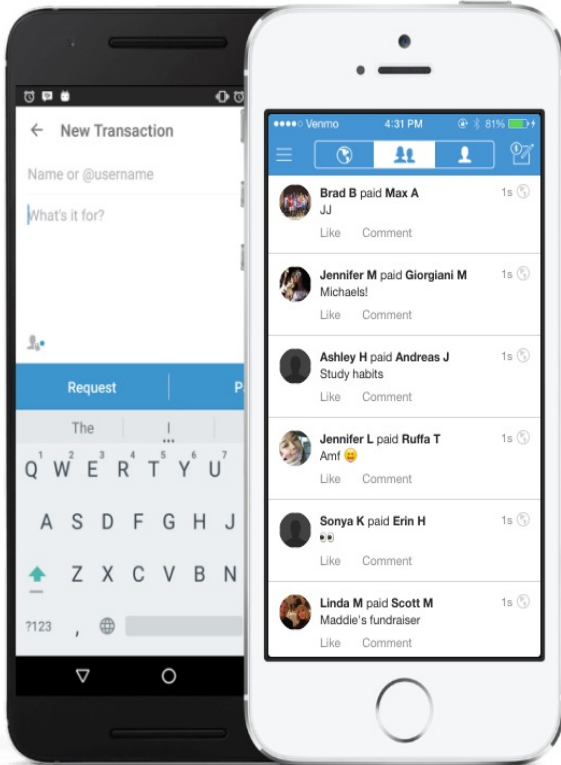
▼ Request Payload [view source](#)

```
{client_order_id: "274fce73-edd3-4fc5-b2a3-86290cd70698", product_id: "ETH-EUR", side: "SELL",...}
  client_order_id: "274fce73-edd3-4fc5-b2a3-86290cd70698"
  order_configuration: {limitLimitGtc: {baseSize: "0.02433012", limitPrice: "3000", postOnly: false}}
    limitLimitGtc: {baseSize: "0.02433012", limitPrice: "3000", postOnly: false}
      baseSize: "0.02433012"
      limitPrice: "3000"
      postOnly: false

  product_id: "ETH-EUR"
  side: "SELL"
  source_account_id: "74f5810e-bda4-5277-ba28-90cb98798984"
  target_account_id: "e64ba5fc-7db3-5e04-81ee-cedfd4fb2543"
```

2/11/22 18:33:14	BTC-USD	Limit	Sell	\$43,597.24	0.02433012 BTC	100.00%	\$1,060.73	Filled
------------------	---------	-------	------	-------------	----------------	---------	------------	--------

Real world examples : Venmo



```
⌵  Preserve log  Disable cache  Offline No throttling
Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other
x Headers Preview Response Cookies Timing
▼ {paging: {next: "https://venmo.com/api/v5/public?until=1477360149",...},...}
  ▶ 0: {payment_id: 288477882, permalink: "/story/580eba1723e064eac0d48825", via: "", action_links: {},...}
  ▶ 1: {payment_id: 288477883, permalink: "/story/580eba1723e064eac0d48828", via: "", action_links: {},...}
  ▶ 2: {payment_id: 288477887, permalink: "/story/580eba1723e064eac0d48834", via: "", action_links: {},...}
  ▼ 3: {payment_id: 288477891, permalink: "/story/580eba1823e064eac0d4883b", via: "", action_links: {},...}
    action_links: {}
    ▶ actor: {username: "Olivia-Topolski", picture: "https://s3.amazonaws.com/venmo/no-image.gif",...}
      audience: "public"
      comments: []
      created_time: "2016-10-25T01:49:11Z"
      ▶ likes: {count: 0, data: []}
        mentions: []
        message: "YAY!!"
        payment_id: 288477891
        permalink: "/story/580eba1823e064eac0d4883b"
        story_id: "580eba1823e064eac0d4883b"
      ▶ transactions: [{, ...}]
        type: "payment"
        updated_time: "2016-10-25T01:49:11Z"
        via: ""
    ▶ 4: {payment_id: 288477890, permalink: "/story/580eba1823e064eac0d4883c", via: "", action_links: {},...}
    ▶ 5: {payment_id: 288477870, permalink: "/story/580eba1623e064eac0d487f5", via: "", action_links: {},...}
    ▶ 6: {payment_id: 288477871, permalink: "/story/580eba1623e064eac0d487f8", via: "", action_links: {},...}
    ▶ 7: {payment_id: 288477872, permalink: "/story/580eba1623e064eac0d487f9", via: "", action_links: {},...}
```

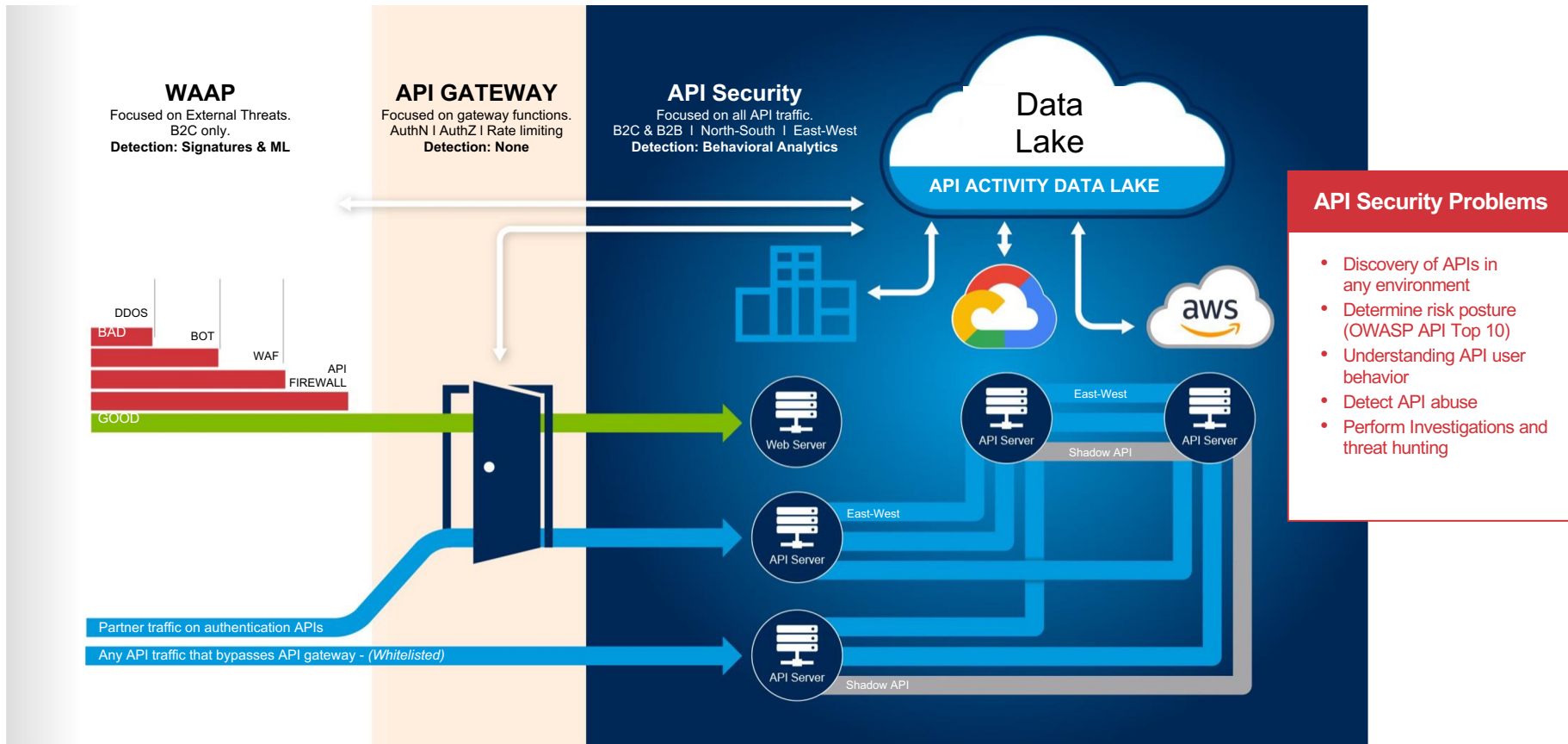
Real world examples : Venmo

<https://venmo.com/api/v5/public?since=1476921600&until=1476921660&limit=1000000>

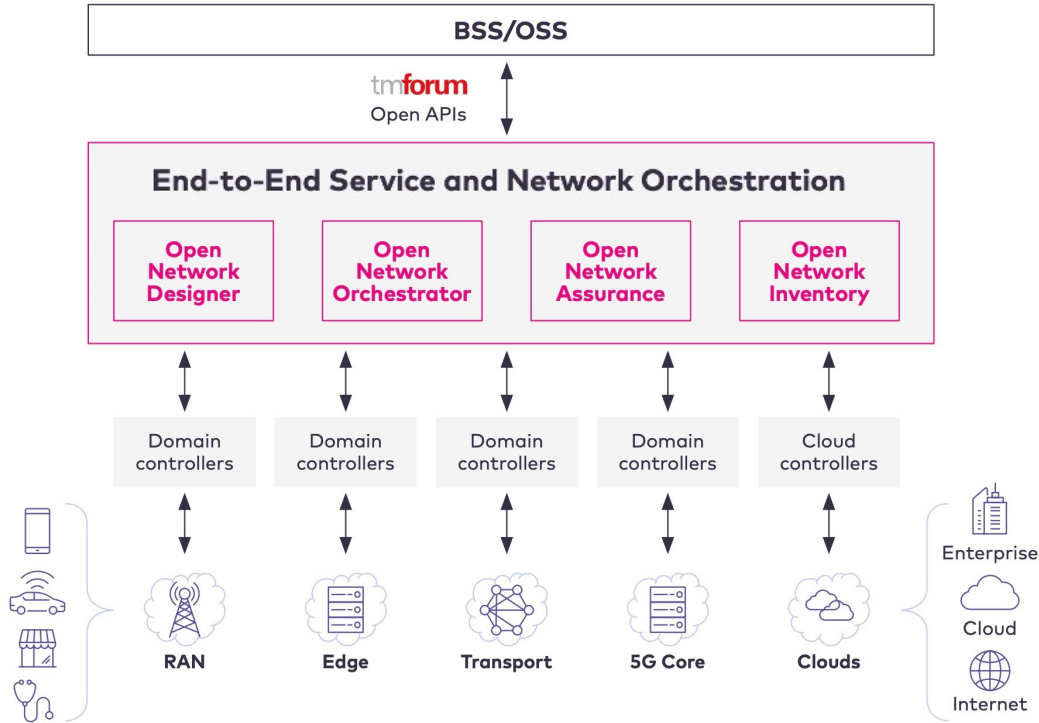
Researches found there was 2 other undocumented query params since and limit that can be added to scrape much more data

```
{
  payment_id: 2038598177,
  permalink: "/story/5cf5379e7addfb4bc7a43016",
  via: "",
  action_links: {},
  transactions: [
    {
      target: {
        username: "Lindsay-Pelley",
        picture: "https://s3.amazonaws.com/venmo/no-image.gif",
        is_business: false,
        name: "Lindsay Pelley",
        firstname: "Lindsay",
        lastname: "Pelley",
        cancelled: false,
        date_created: "2016-10-05T15:29:07",
        external_id: "2054482061950976570",
        id: "14515489"
      }
    }
  ],
  story_id: "5cf5379e7addfb4bc7a43016",
  comments: [],
  updated_time: "2019-06-03T15:07:10Z",
  audience: "public",
  actor: {
    username: "r_pelley",
    picture: "https://venmopics.appspot.com/u/v1/m/82e7cc5a-fab2-4764-bd4f-f26e637da0bc",
    is_business: false,
    name: "robert pelley",
    firstname: "robert",
    lastname: "pelley",
    cancelled: false,
    date_created: "2017-01-18T14:16:36",
    external_id: "2130547014893568807",
    id: "17515985"
  },
  created_time: "2019-06-03T15:07:10Z",
  mentions: [],
  message: "👉👉",
  type: "payment",
  likes: {
    count: 0,
    data: []
  }
}
```

Why you need API Security even if u have WAF & API Gateway ?

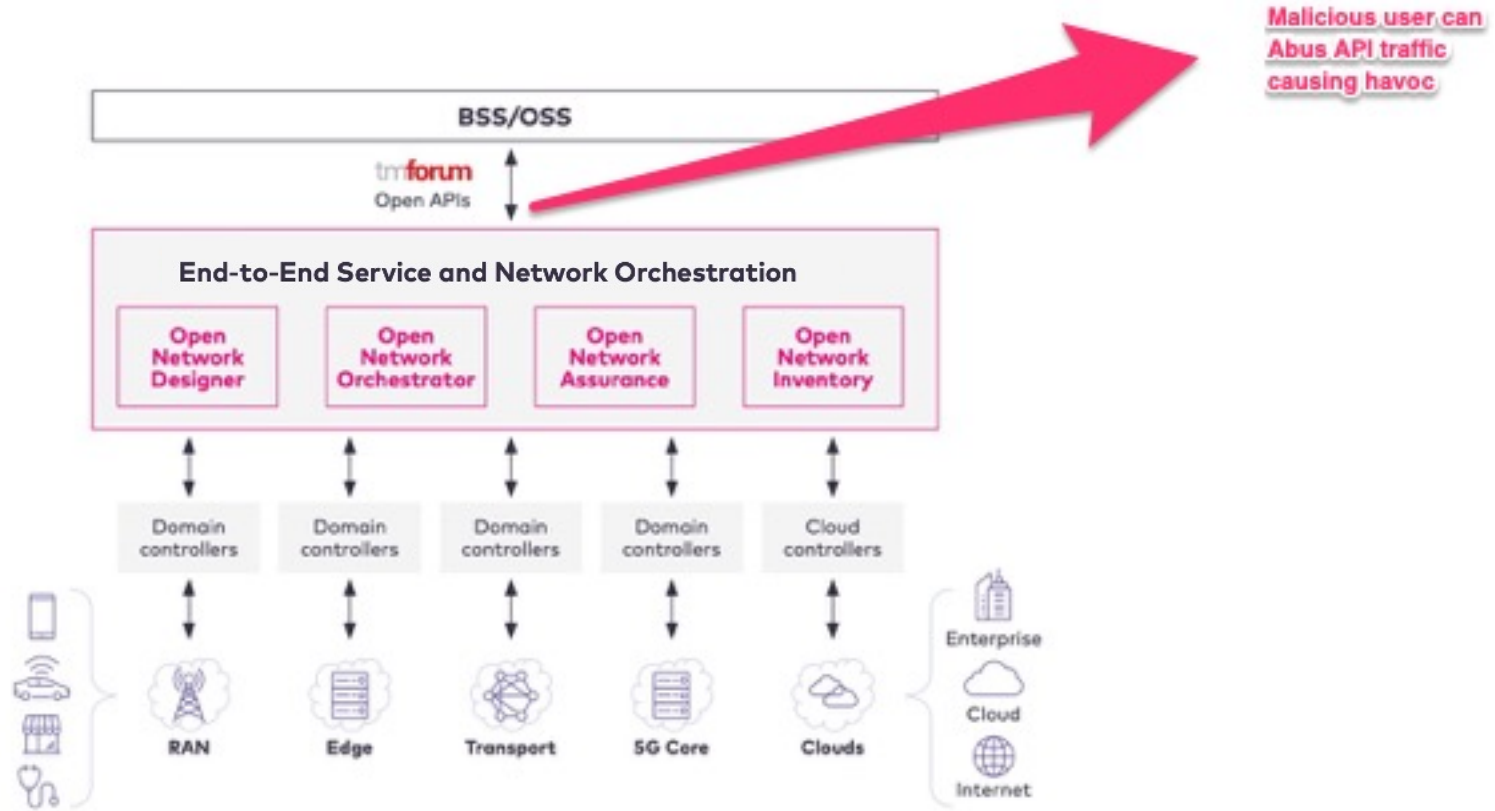


Use case Network Orchestration (NetOps) by operators

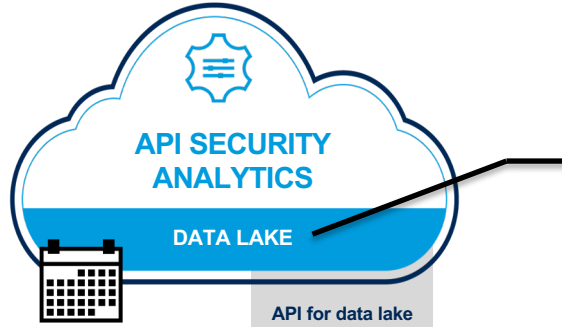


- Networks vendors using TMForum Open APIs
- Open APIs can be abuse through low and slow logical attacks

Use case Network Orchestration (NetOps) by operators

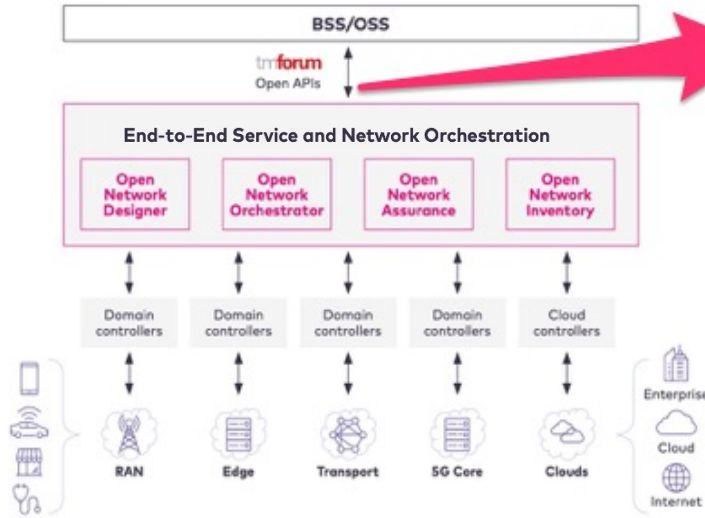


Use case Network Orchestration (NetOps) by operators



Tokenized API activity data

Behavior of users of API is monitored for any abuses



Reference architecture for monitoring API Behavior, enables alerting on any abuse

Summary

- Network operators are increasingly using API across the organization
- Security should be a main consideration
- This talk highlights the potential abuse that could happen
- A potential architecture for API Security has been proposed

Q&A