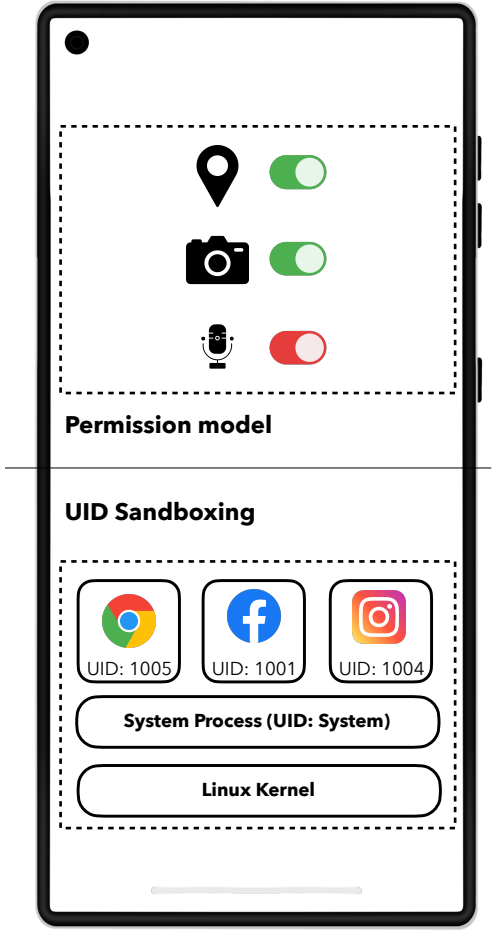
Covert Web-to-App Tracking via Localhost on Android

Breaking Cross-Context Isolation through an Unmediated Loopback Channel

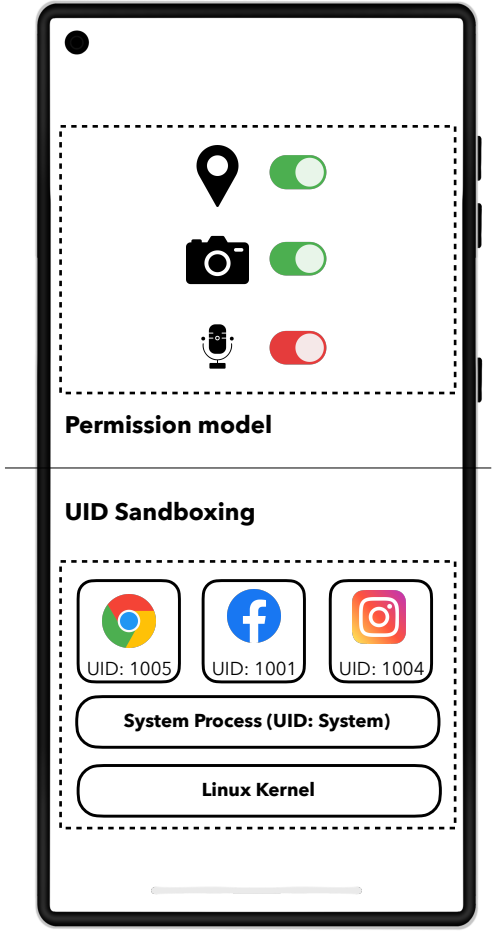
Aniketh Girish, Gunes Acar, Narseo Vallina-Rodriguez, Nipuna Weerasekara, Tim Vlummens

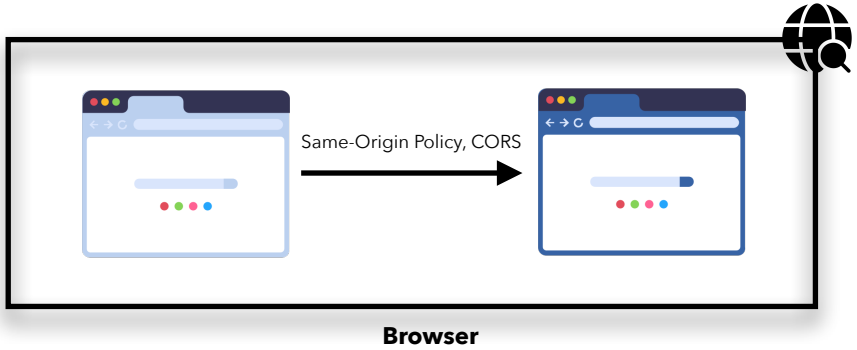
PEARG, IETF
July 25, 2025
Madrid, Spain

Modern Platforms Enforce Contextual Isolation

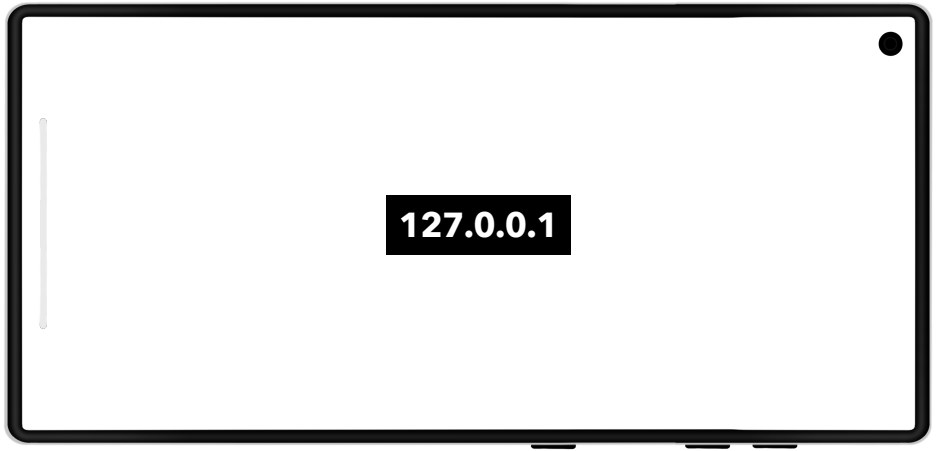


Modern Platforms Enforce Contextual Isolation





Localhost: A Quiet Cross-Context Channel

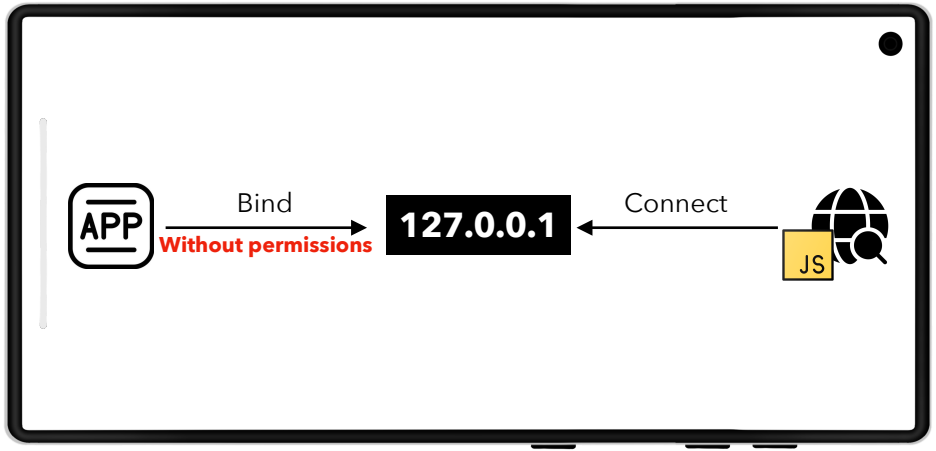


Localhost: A Quiet Cross-Context Channel

- Apps can bind to 127.0.0.1 without permissions.

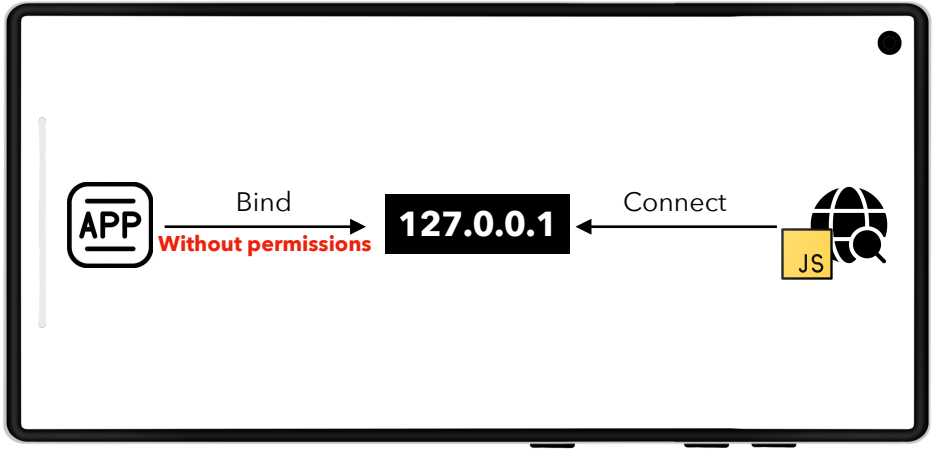
Localhost: A Quiet Cross-Context Channel

- Apps can bind to 127.0.0.1 without permissions.
- Browsers allow web JS to initiate connections to localhost.



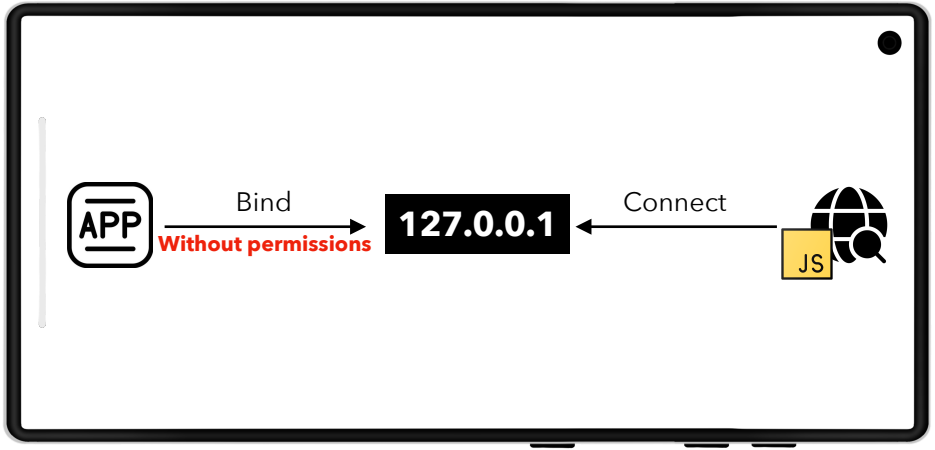
Localhost: A Quiet Cross-Context Channel

- Apps can bind to 127.0.0.1 without permissions.
- Browsers allow web JS to initiate connections to localhost.
- Legitimate purposes: used for testing, debugging, P2P fallback.



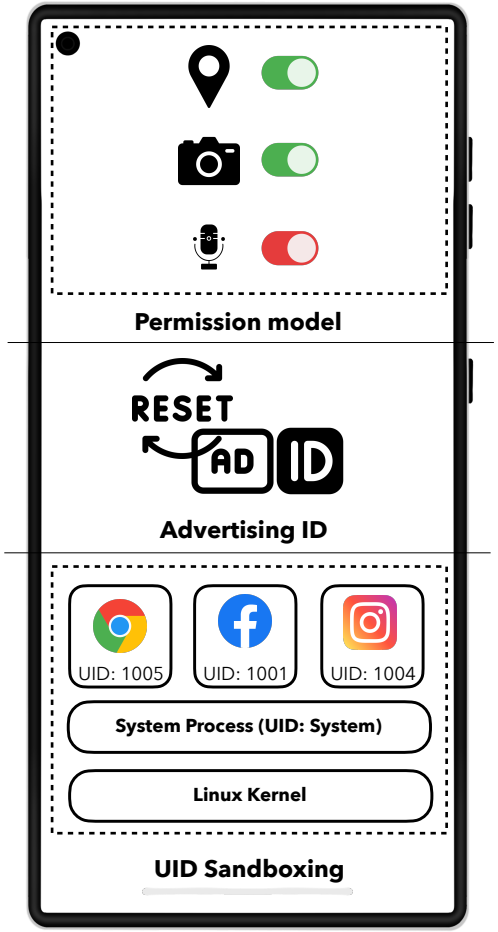
Localhost: A Quiet Cross-Context Channel

- Apps can bind to 127.0.0.1 without permissions.
- Browsers allow web JS to initiate connections to localhost.
- Legitimate purposes: used for testing, debugging, P2P fallback.

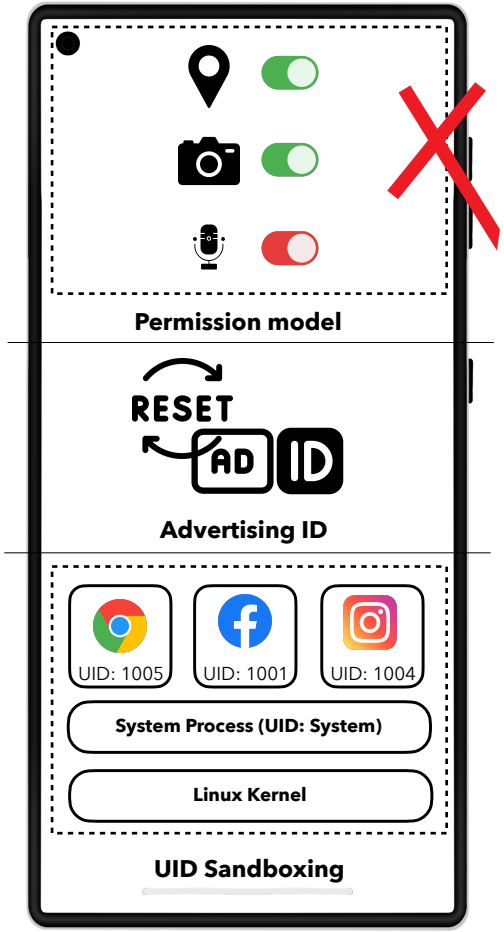


Any app can listen. Any website can send. And the user sees none of it.

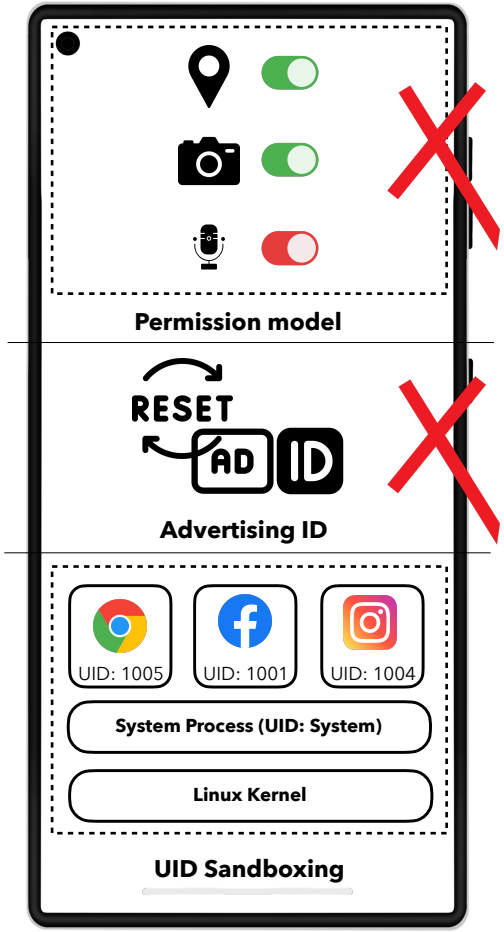
Existing Defenses are Ineffective



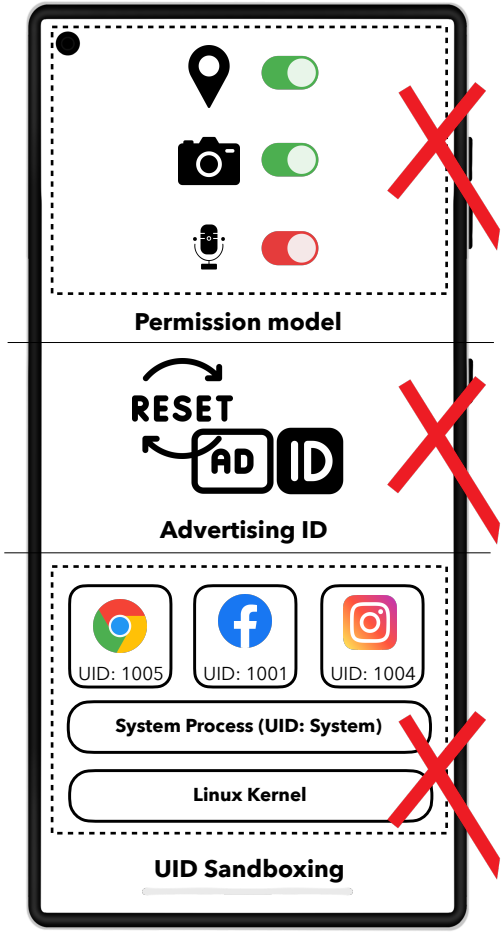
Existing Defenses are Ineffective



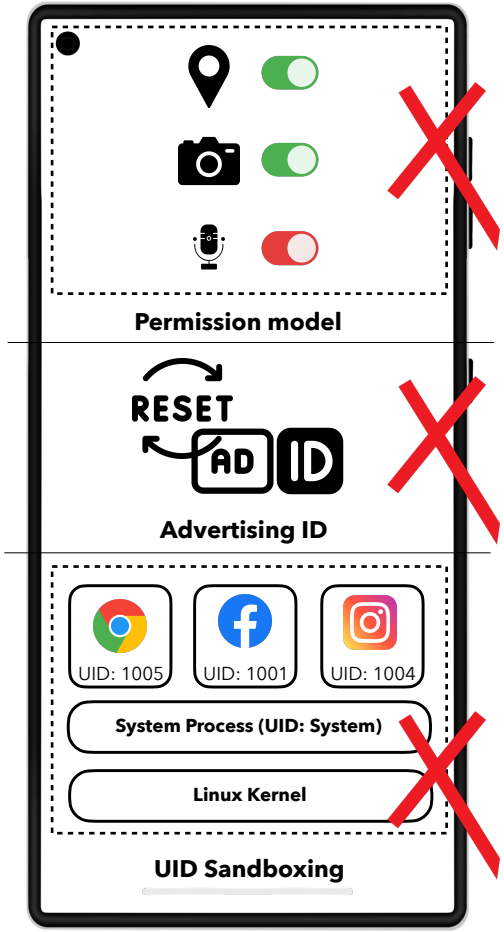
Existing Defenses are Ineffective

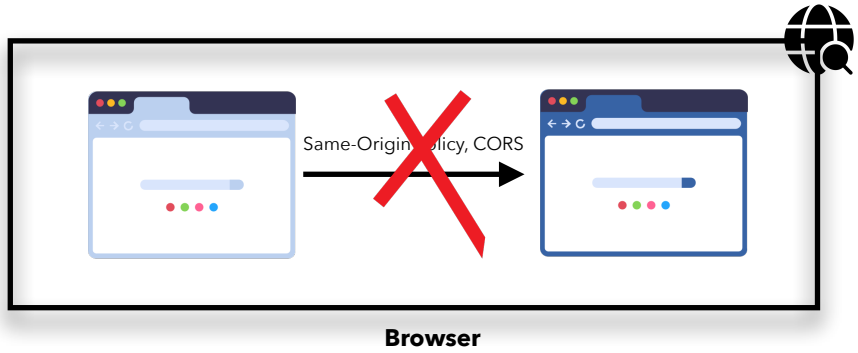


Existing Defenses are Ineffective

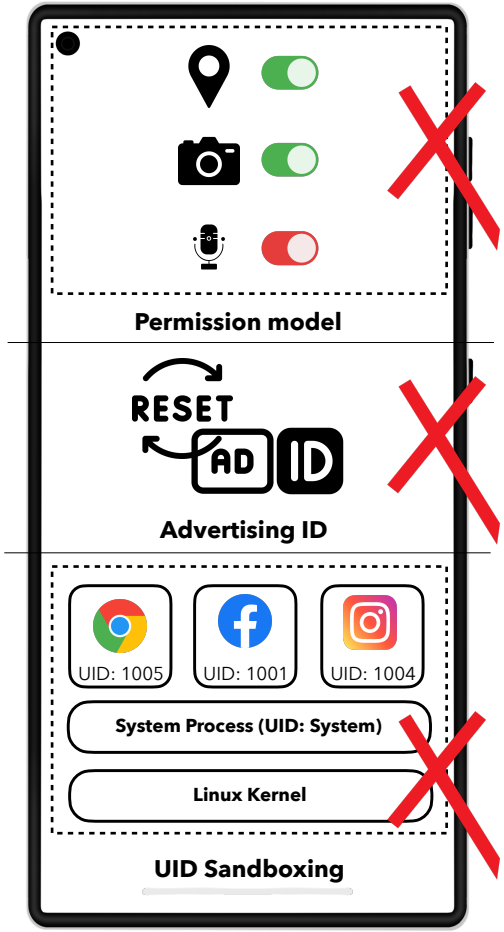


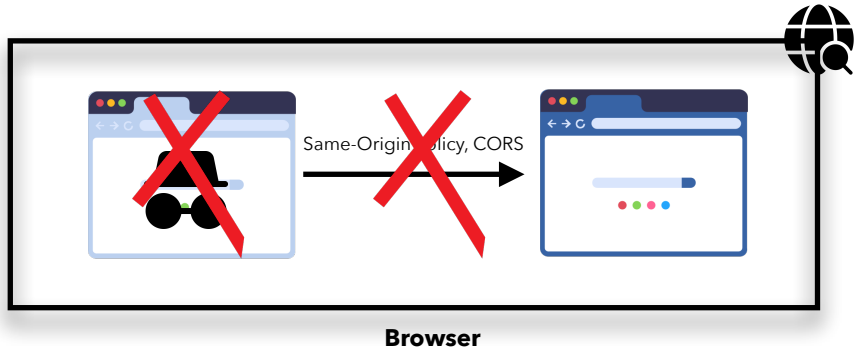
Existing Defenses are Ineffective



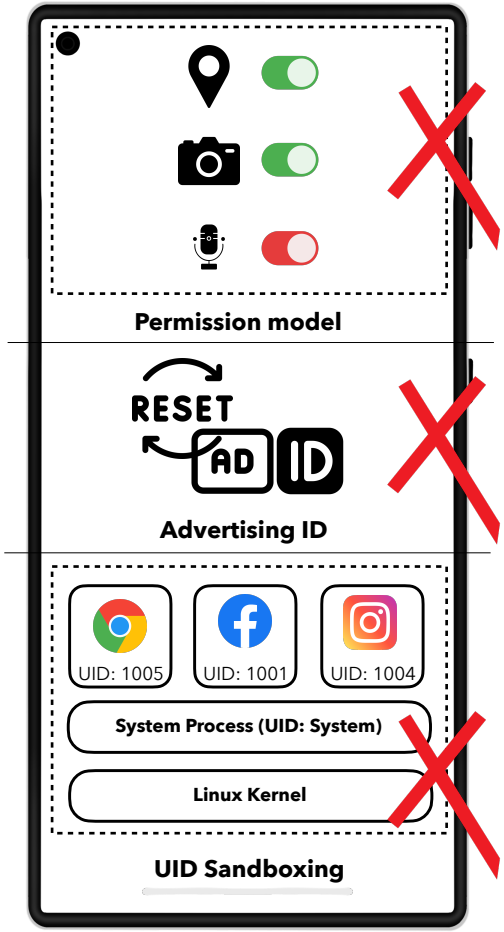


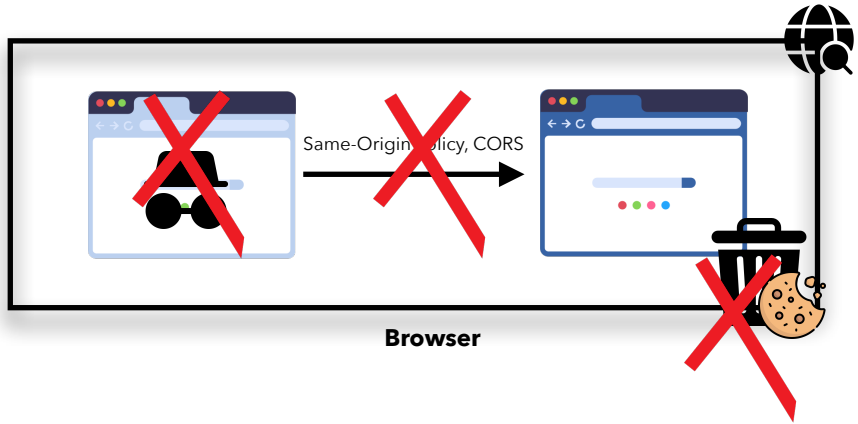
Existing Defenses are Ineffective



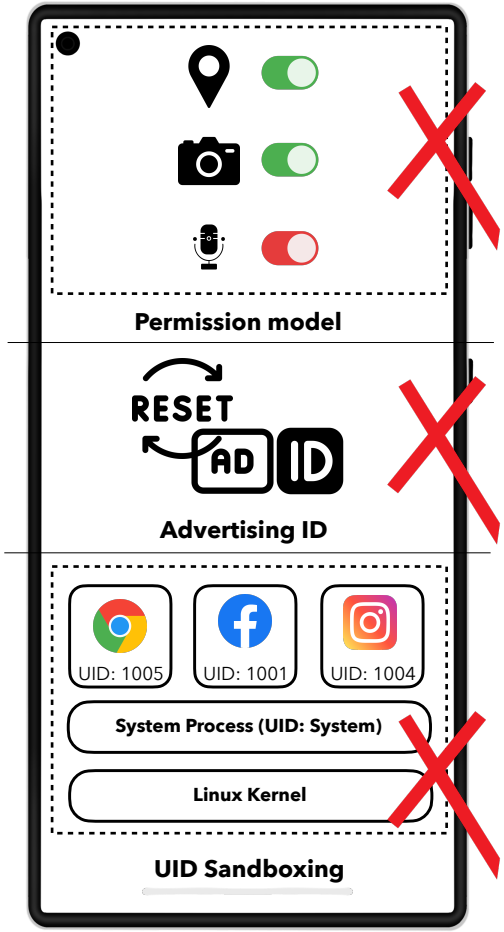


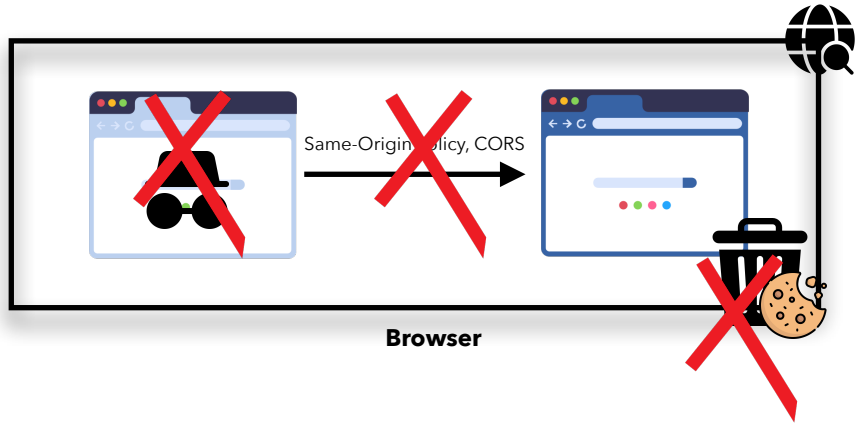
Existing Defenses are Ineffective



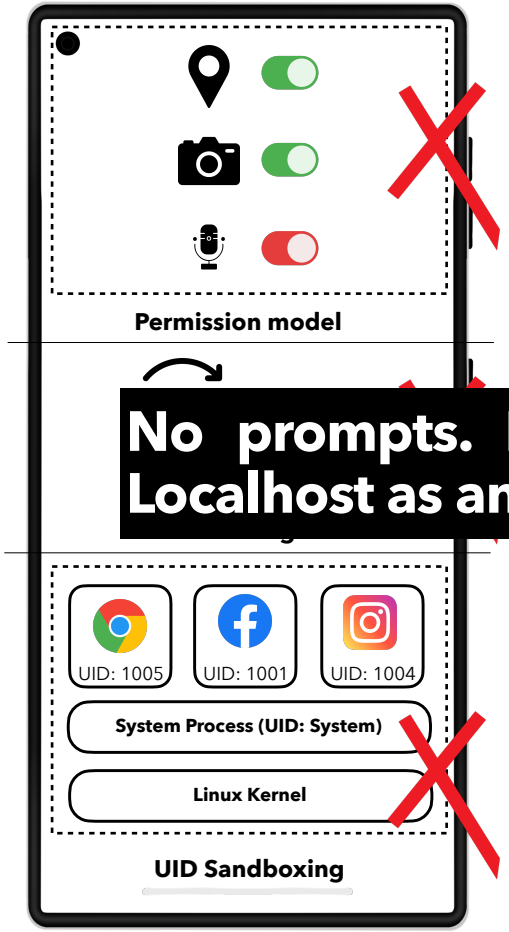


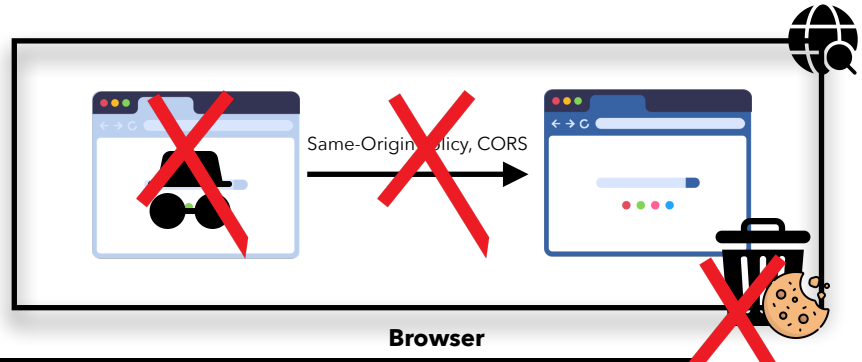
Existing Defenses are Ineffective





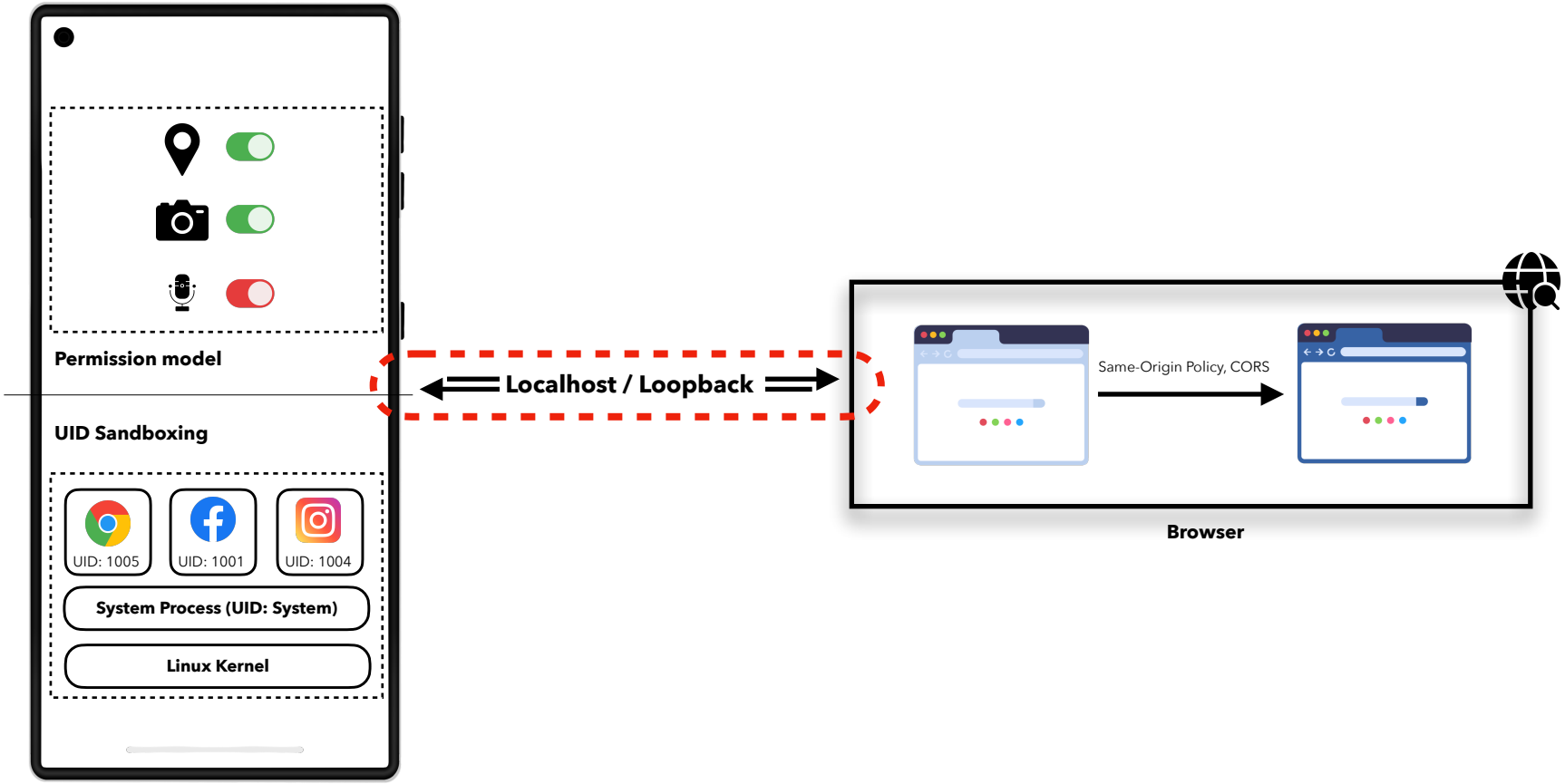
Existing Defenses are Ineffective



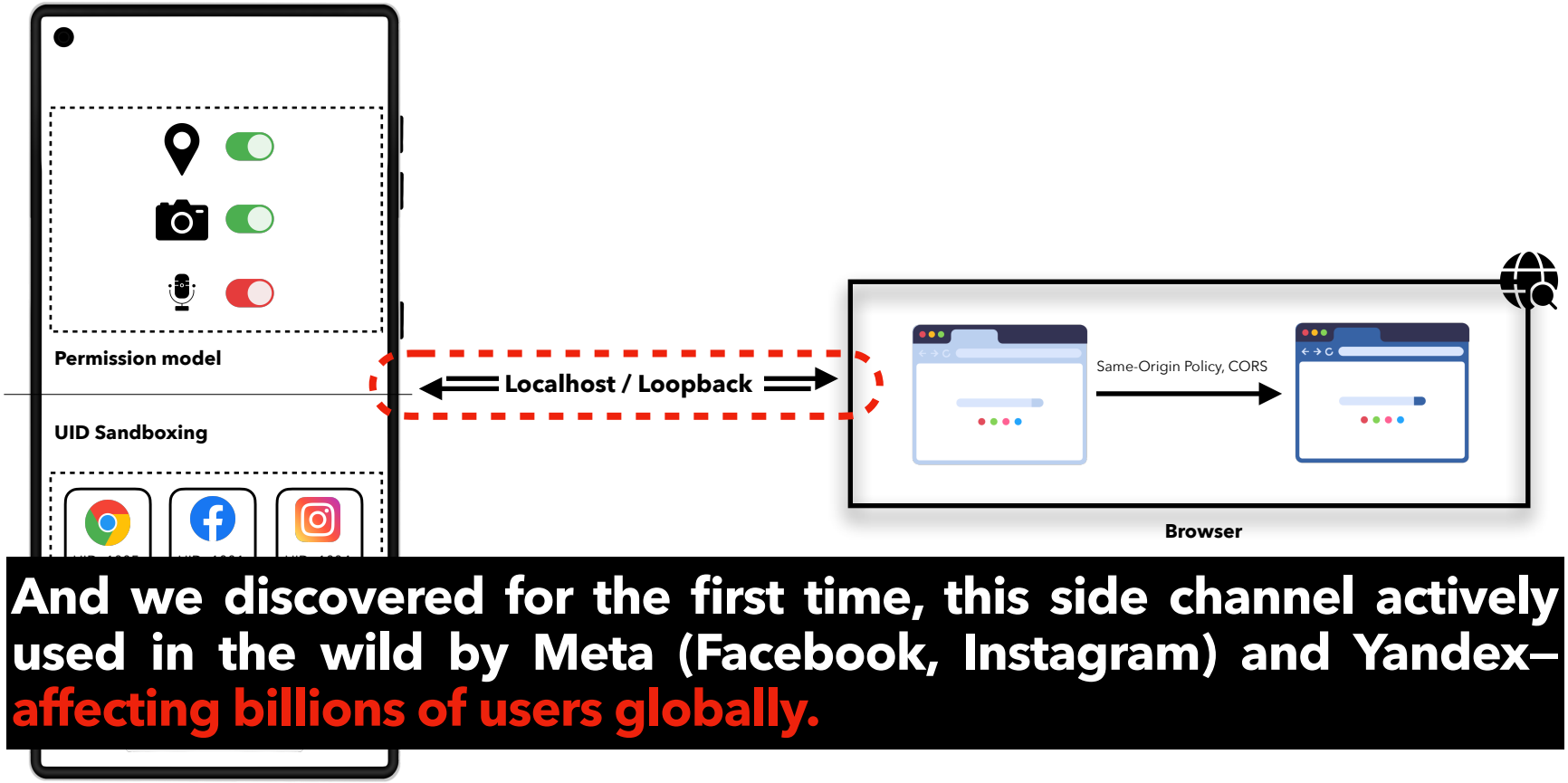


No prompts. No permissions. No protection.
Localhost as an attack vector bypasses them all.

Do Sites Use Localhost to Communicate with Mobile Apps?



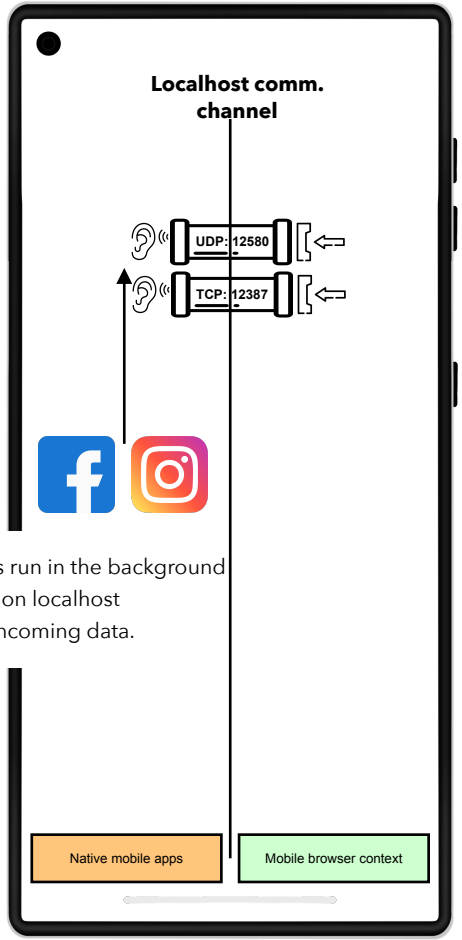
Do Sites Use Localhost to Communicate with Mobile Apps?



And we discovered for the first time, this side channel actively used in the wild by Meta (Facebook, Instagram) and Yandex–affecting billions of users globally.

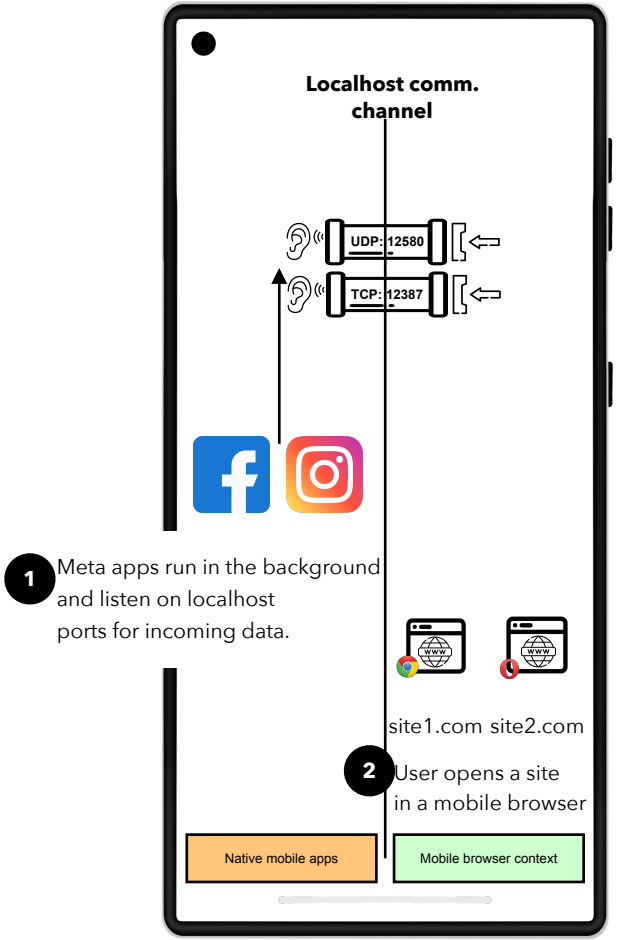
Meta’s Side Channel

Technical Details

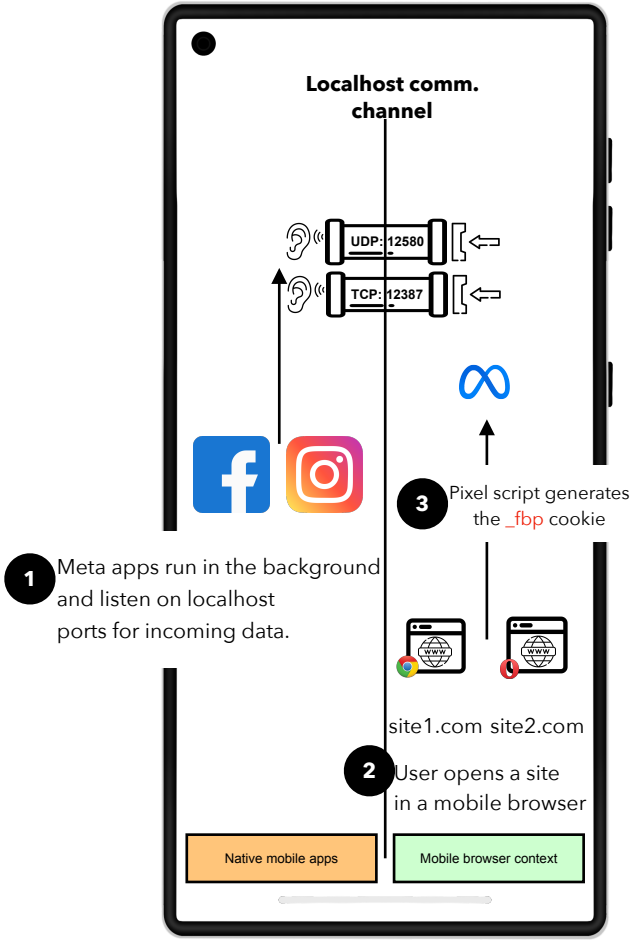


1 Meta apps run in the background and listen on localhost ports for incoming data.

Technical Details

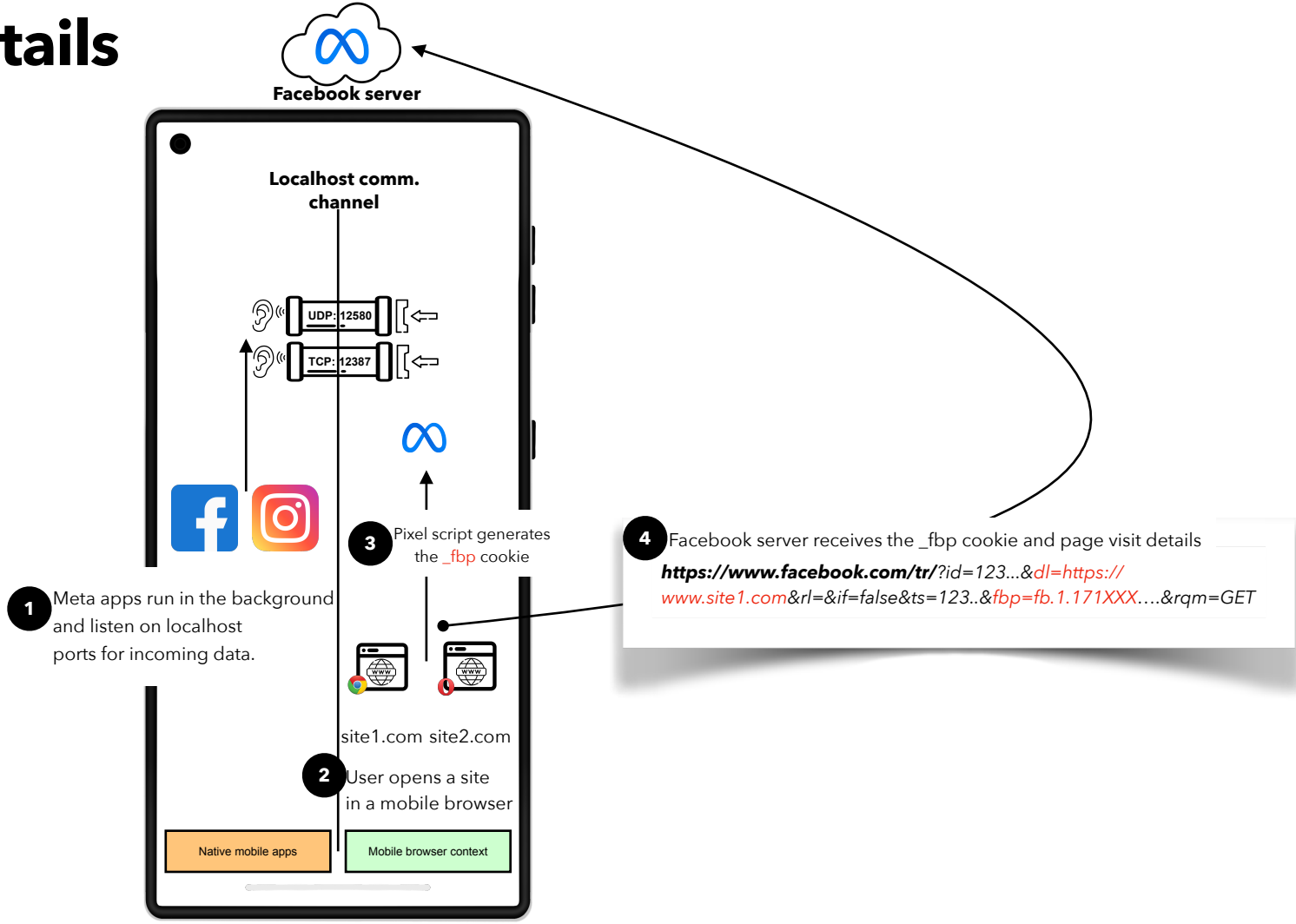


Technical Details

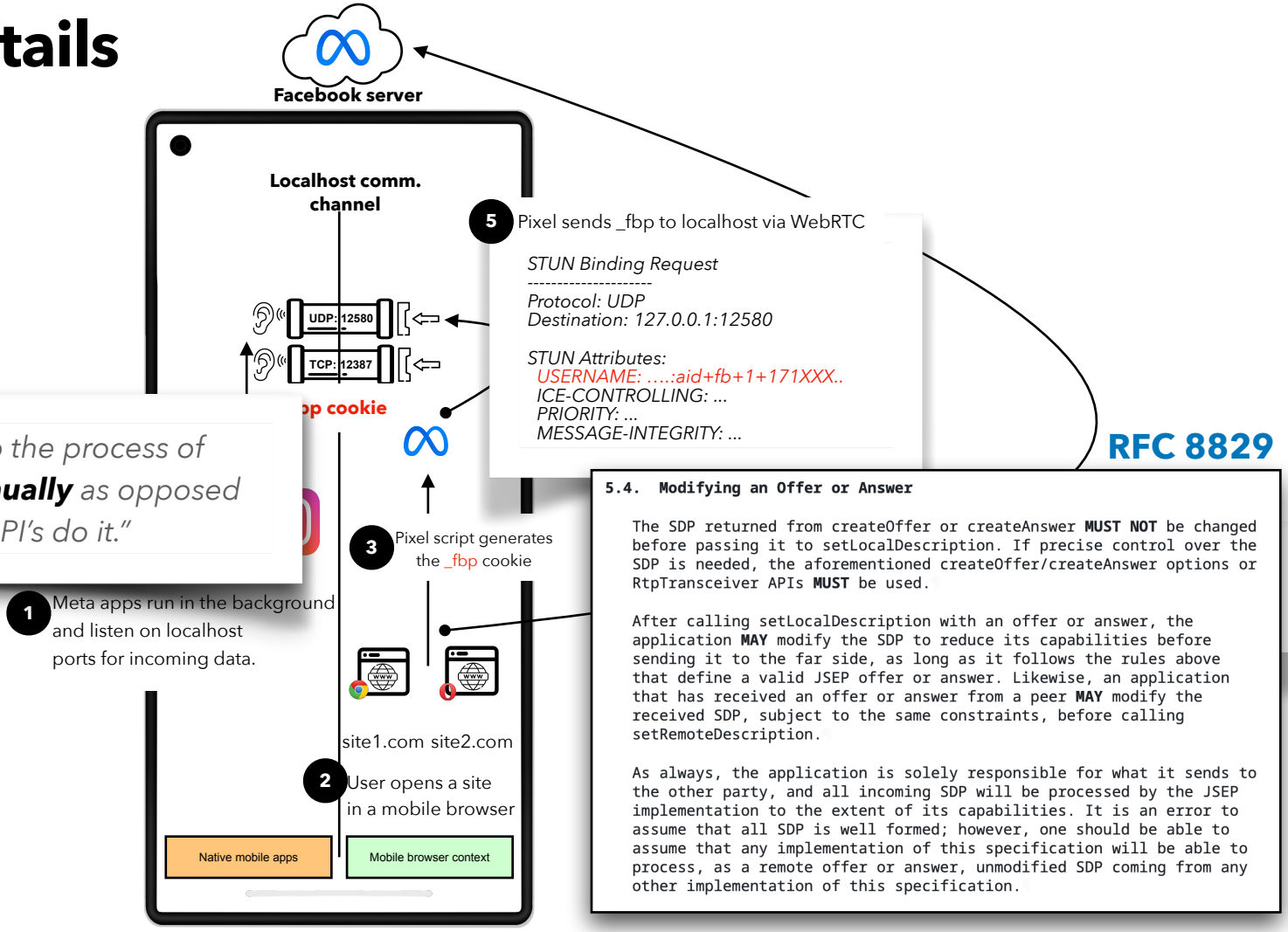


*"When the Meta Pixel is installed on a website, and the Pixel uses **first-party cookies**, the Pixel automatically saves a **unique identifier** to an _fbp cookie **for the website domain** if one does not already exist."*

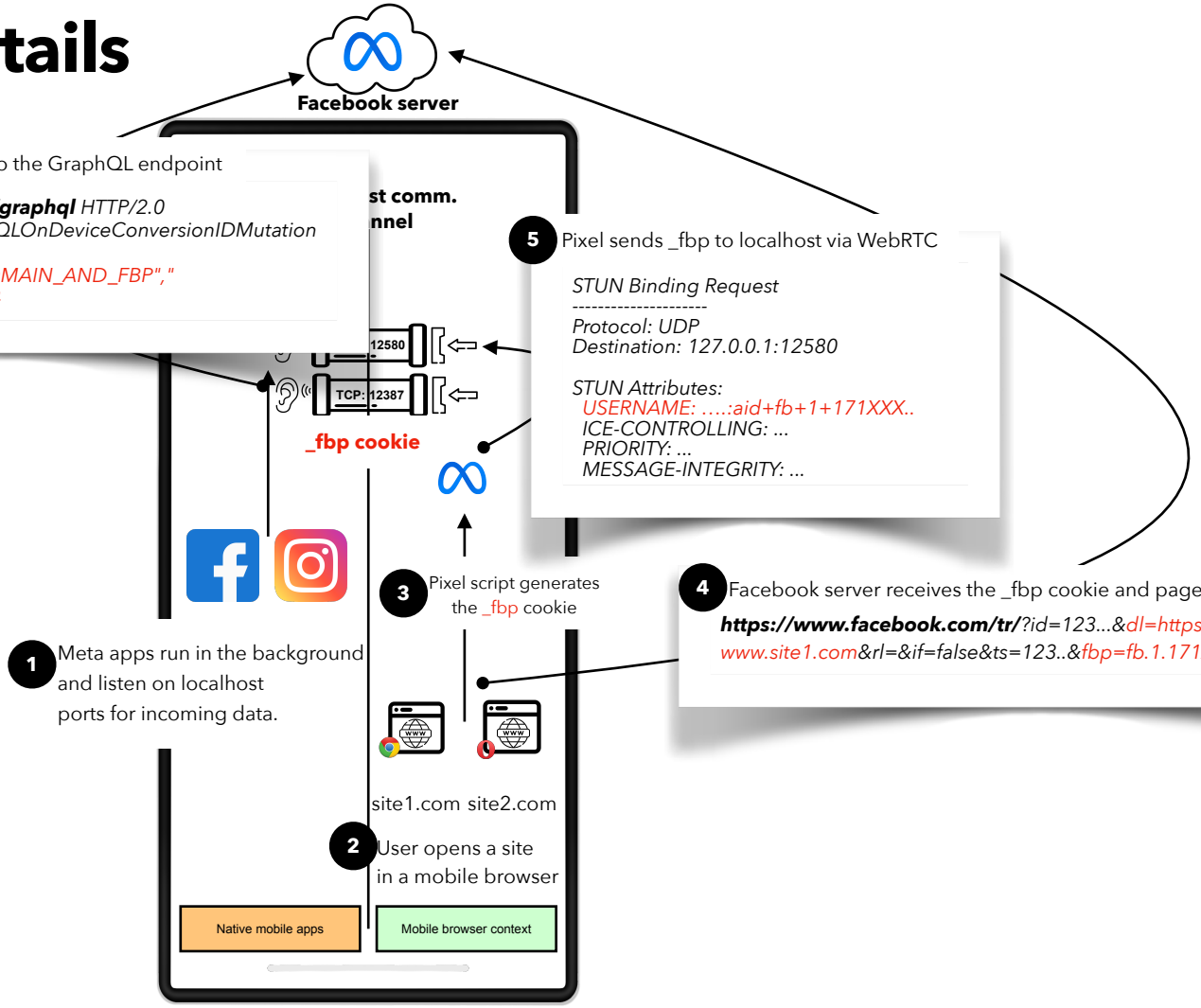
Technical Details



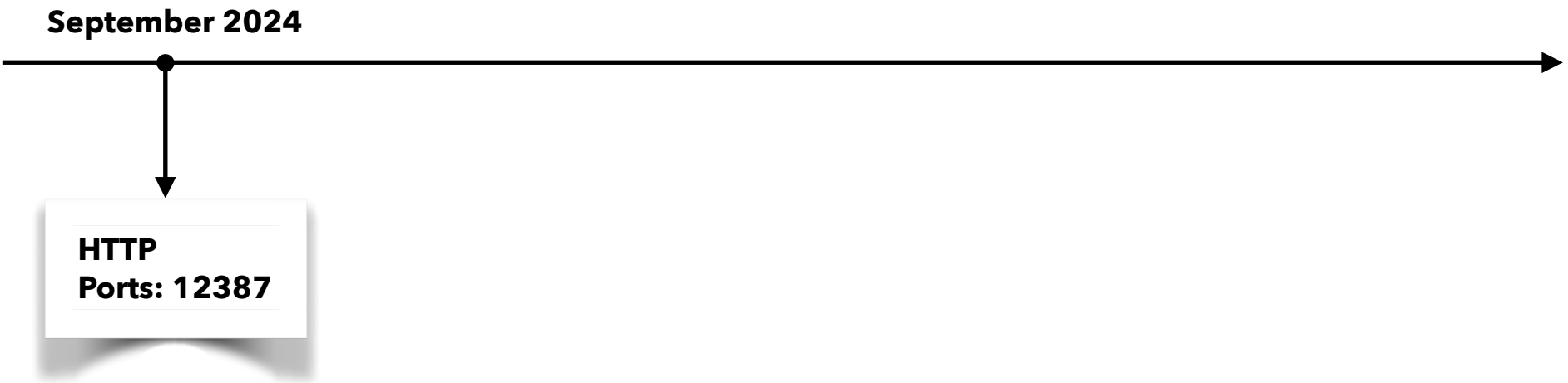
Technical Details



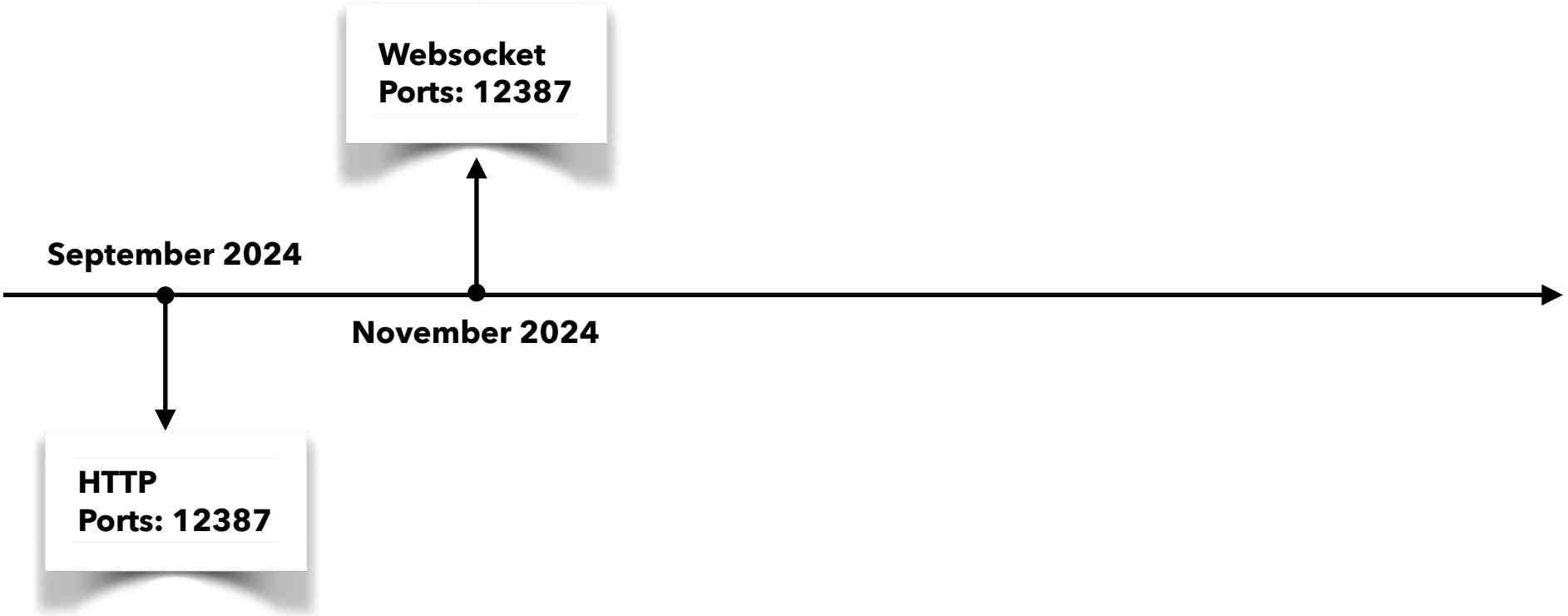
Technical Details



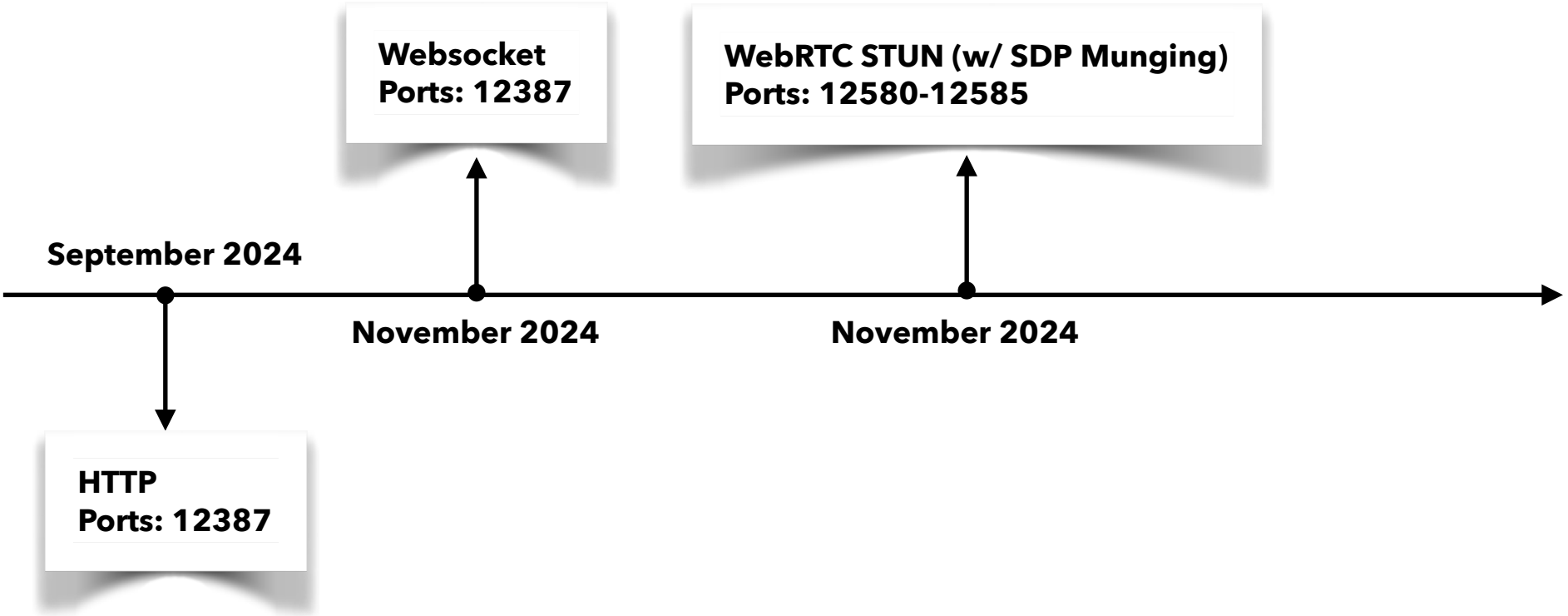
Meta’s Side Channel: Behaviour Across Time



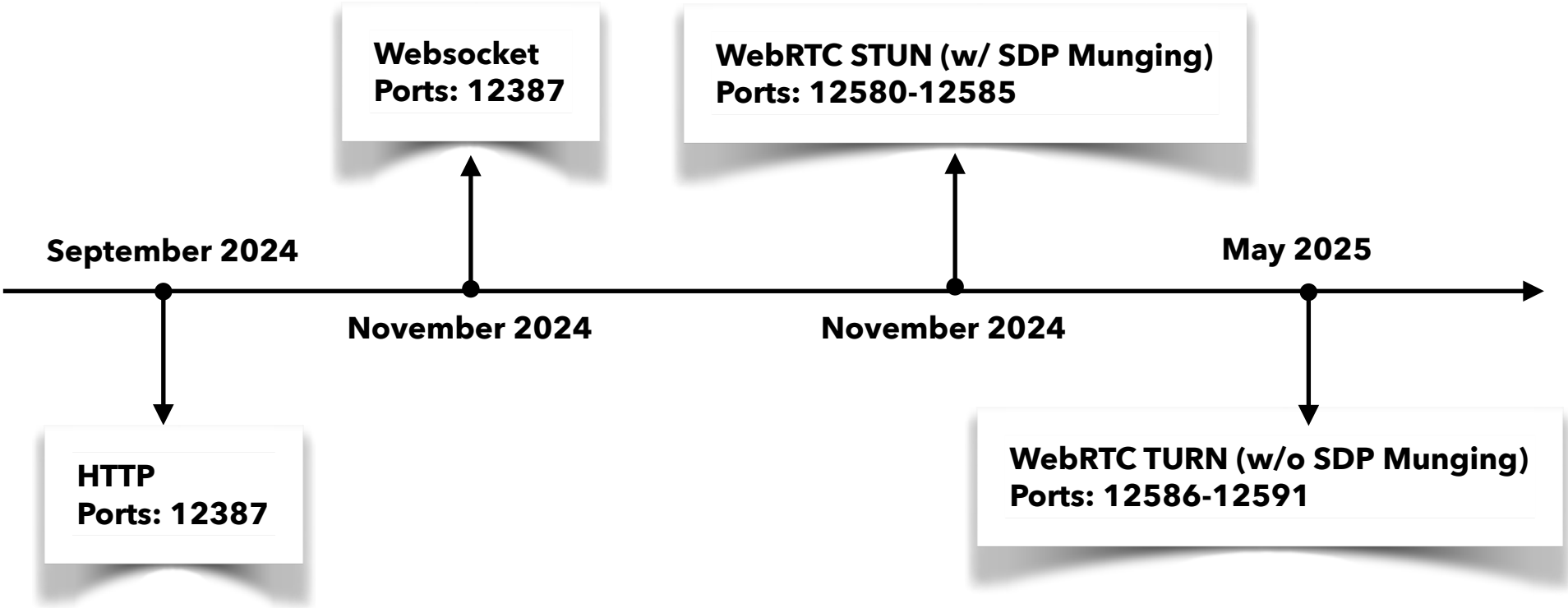
Meta’s Side Channel: Behaviour Across Time



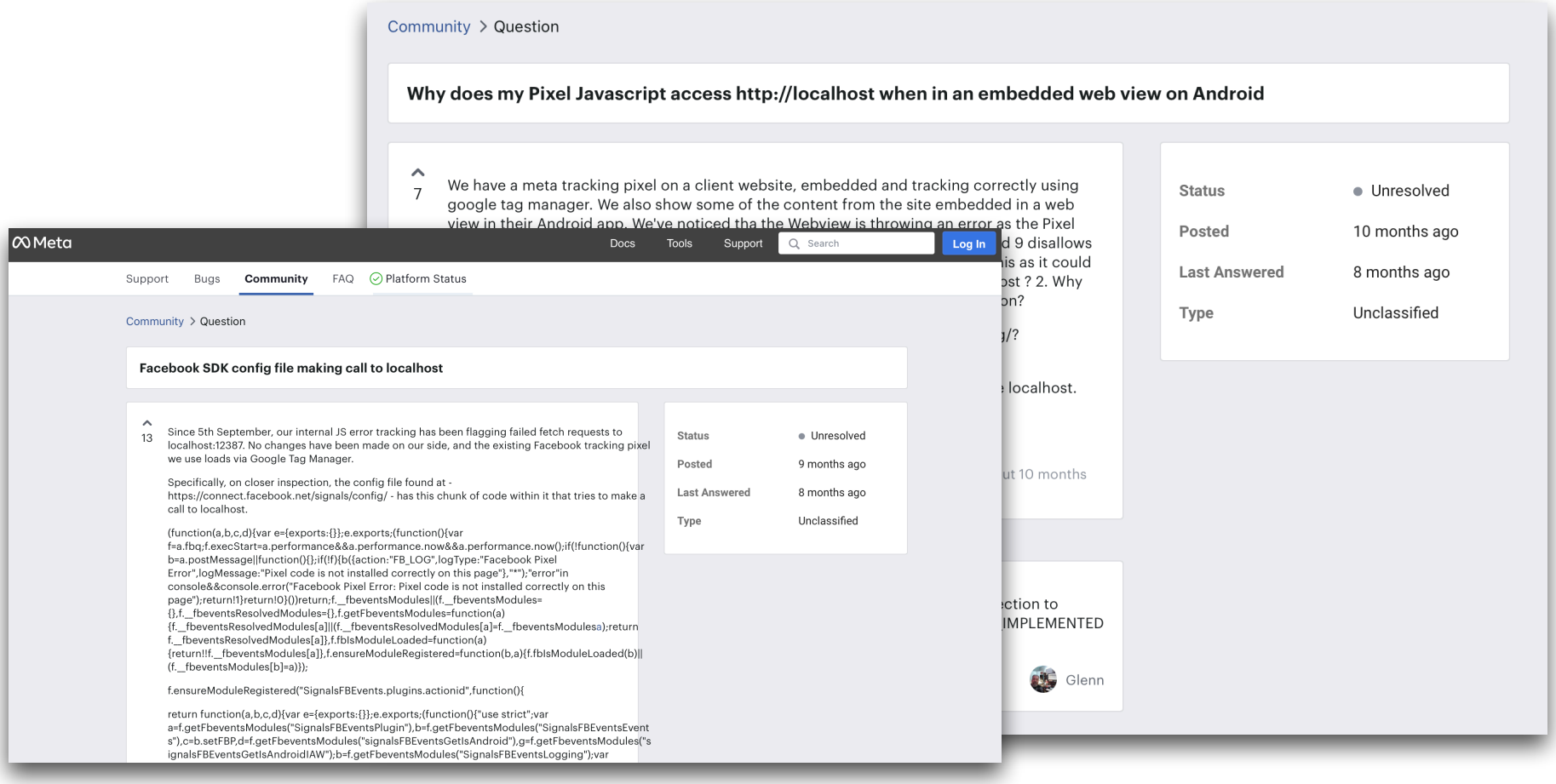
Meta's Side Channel: Behaviour Across Time



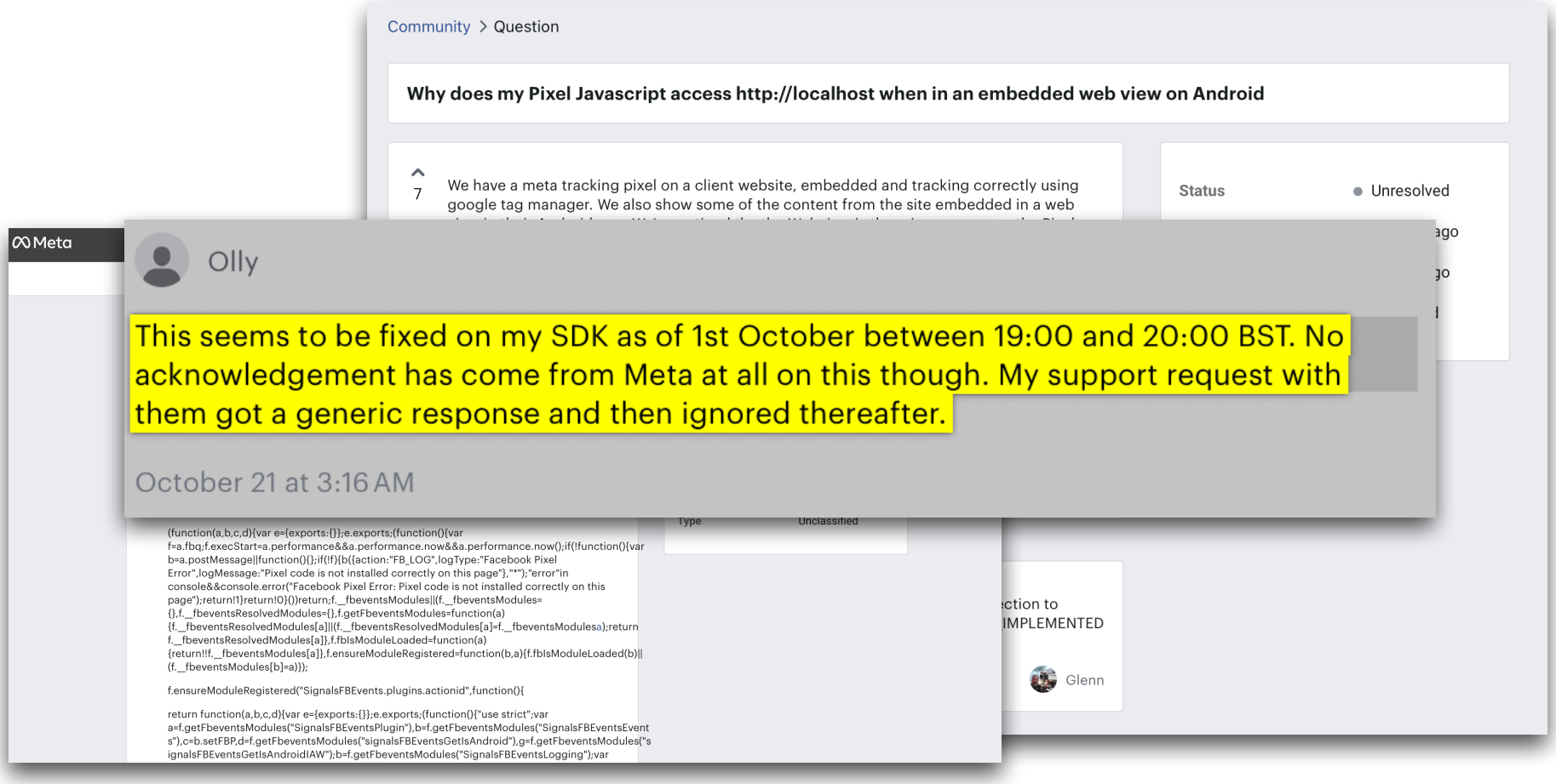
Meta's Side Channel: Behaviour Across Time



Were Website Owners Even Aware?

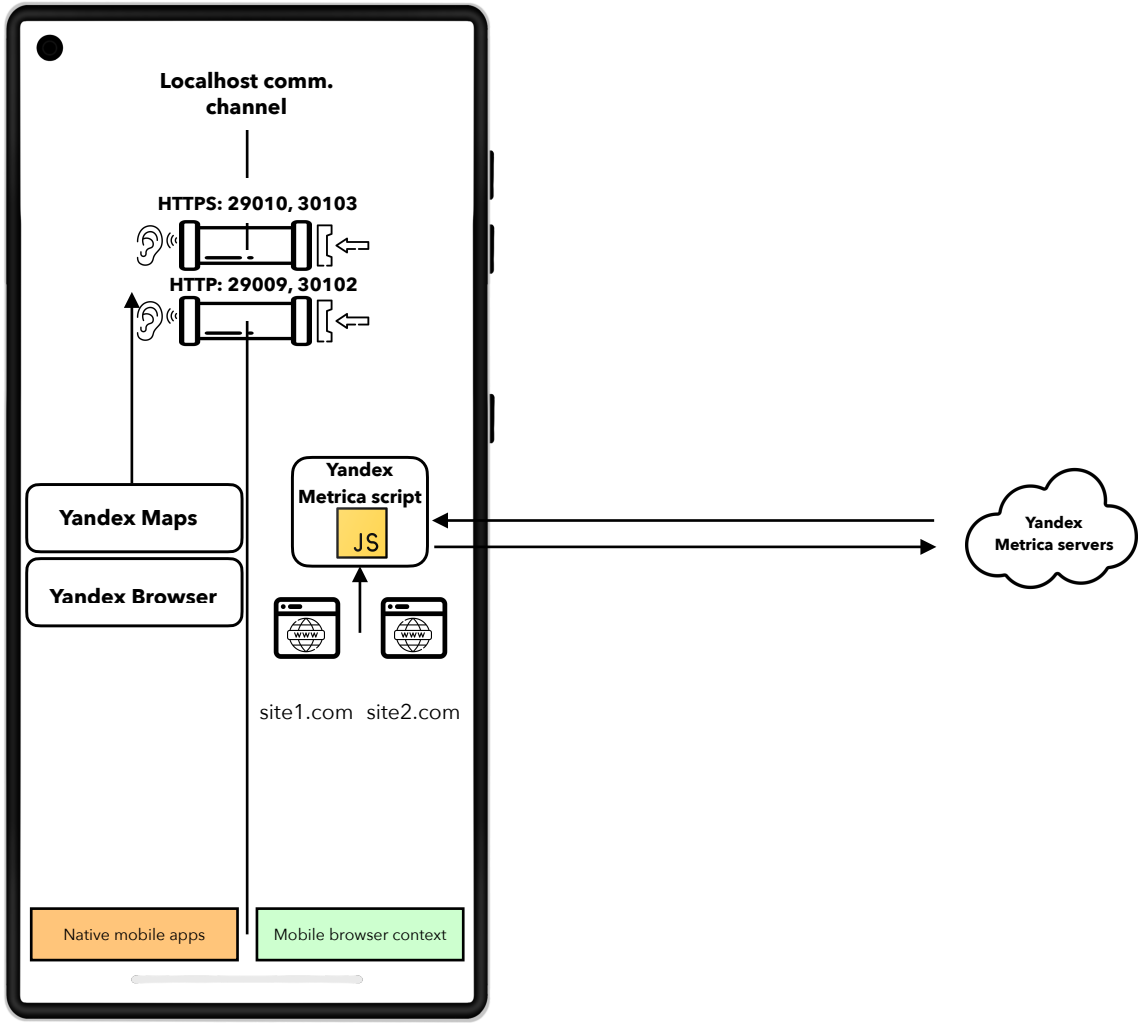


Were Website Owners Even Aware?

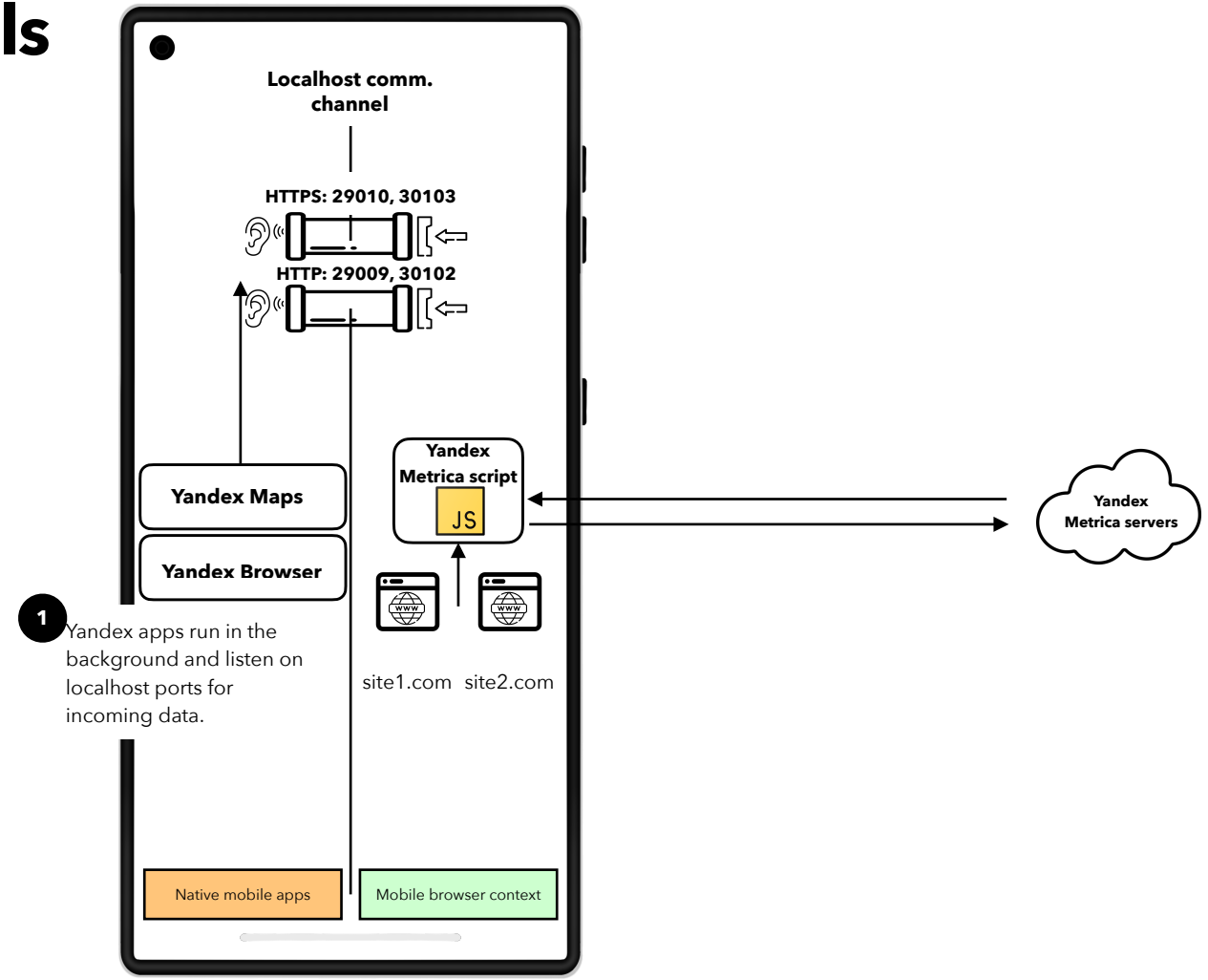


Yandex's Side Channel

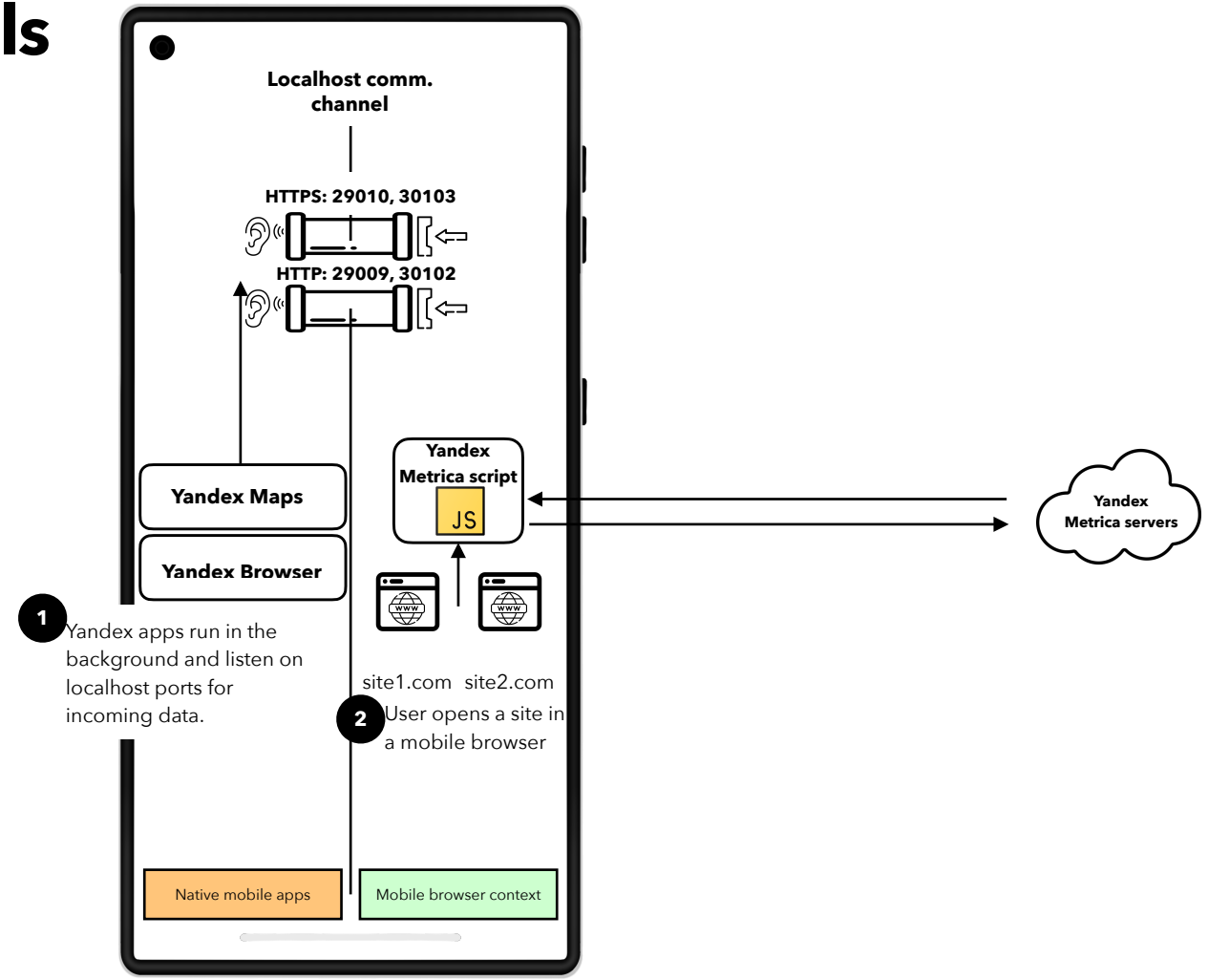
Technical Details



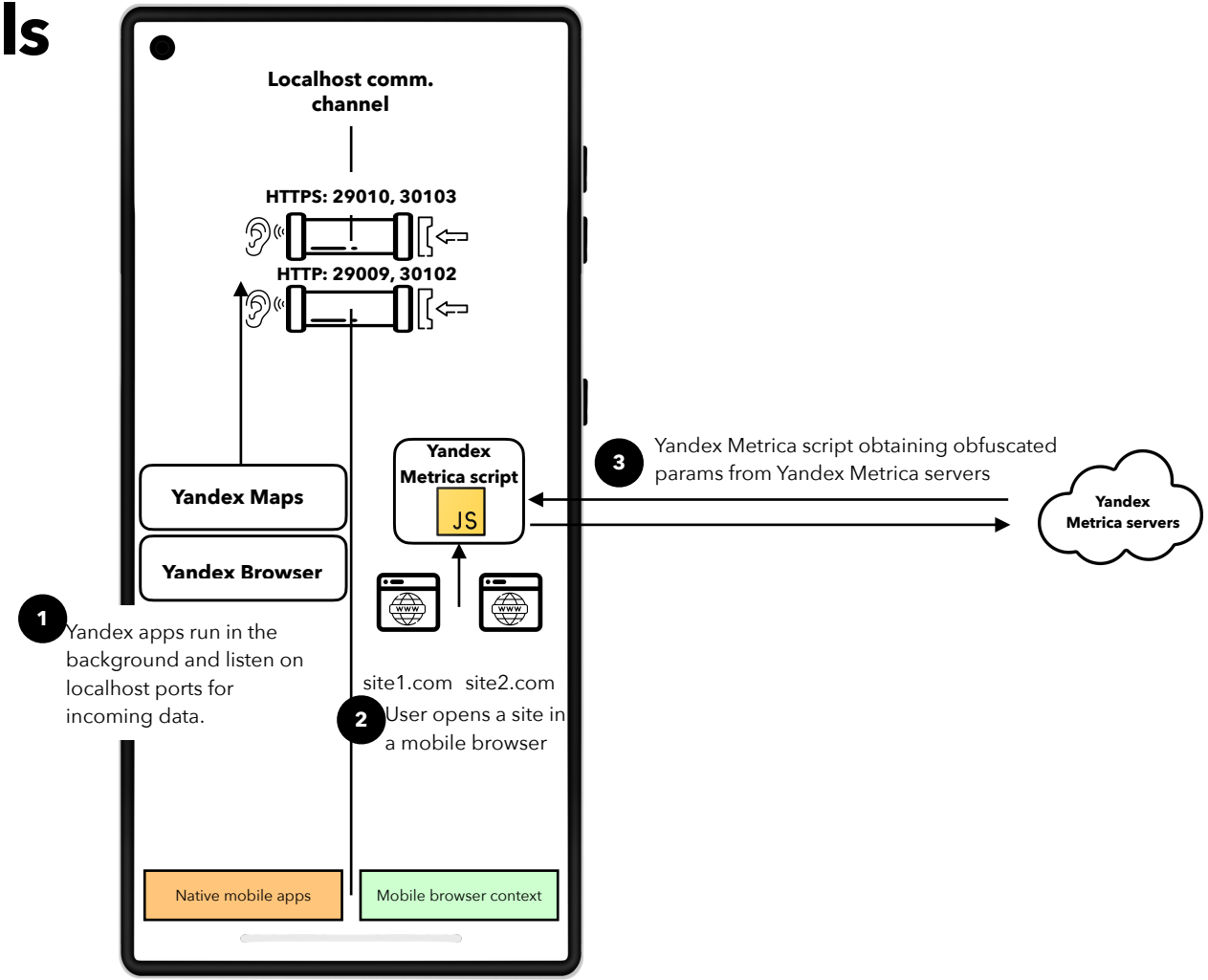
Technical Details



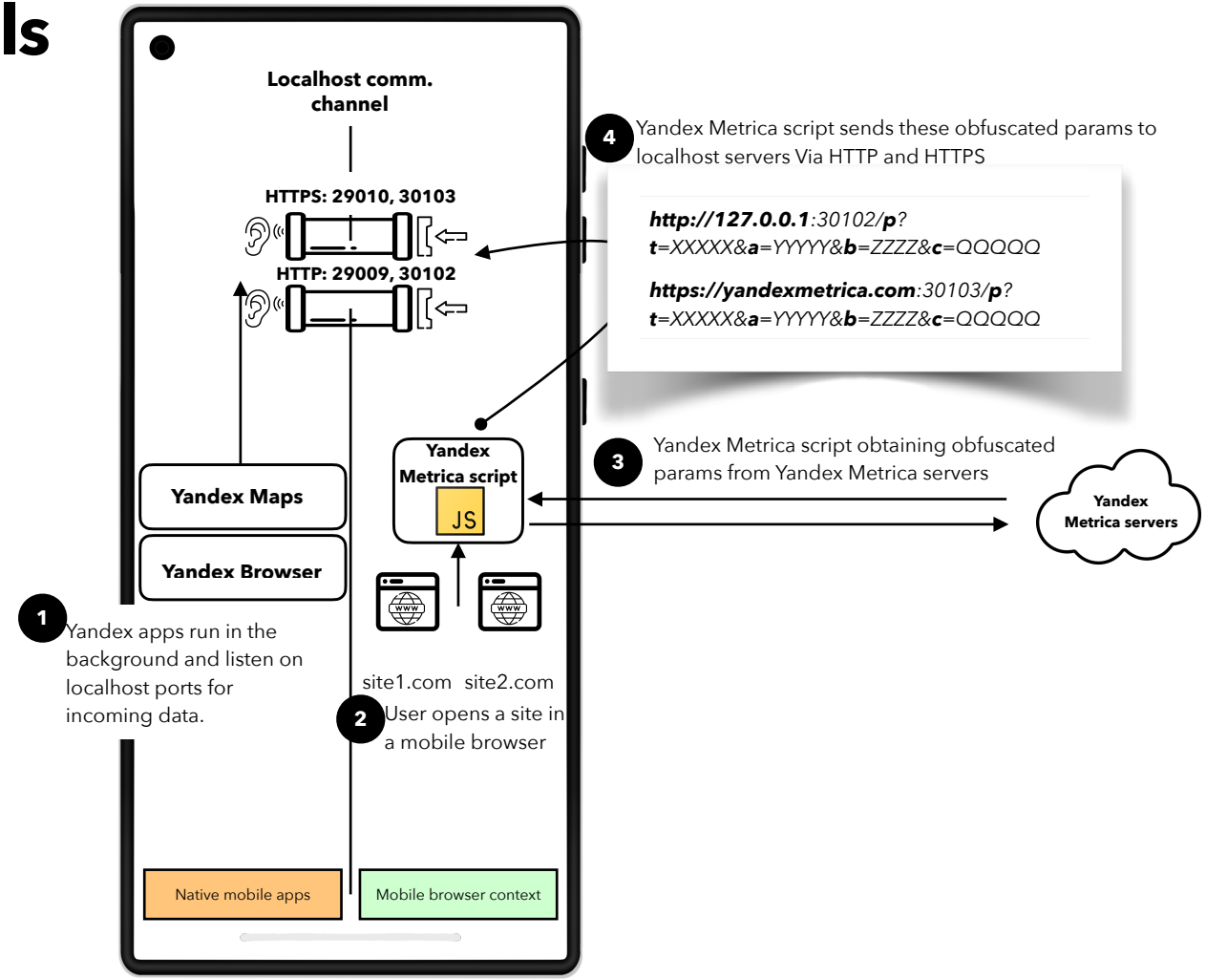
Technical Details



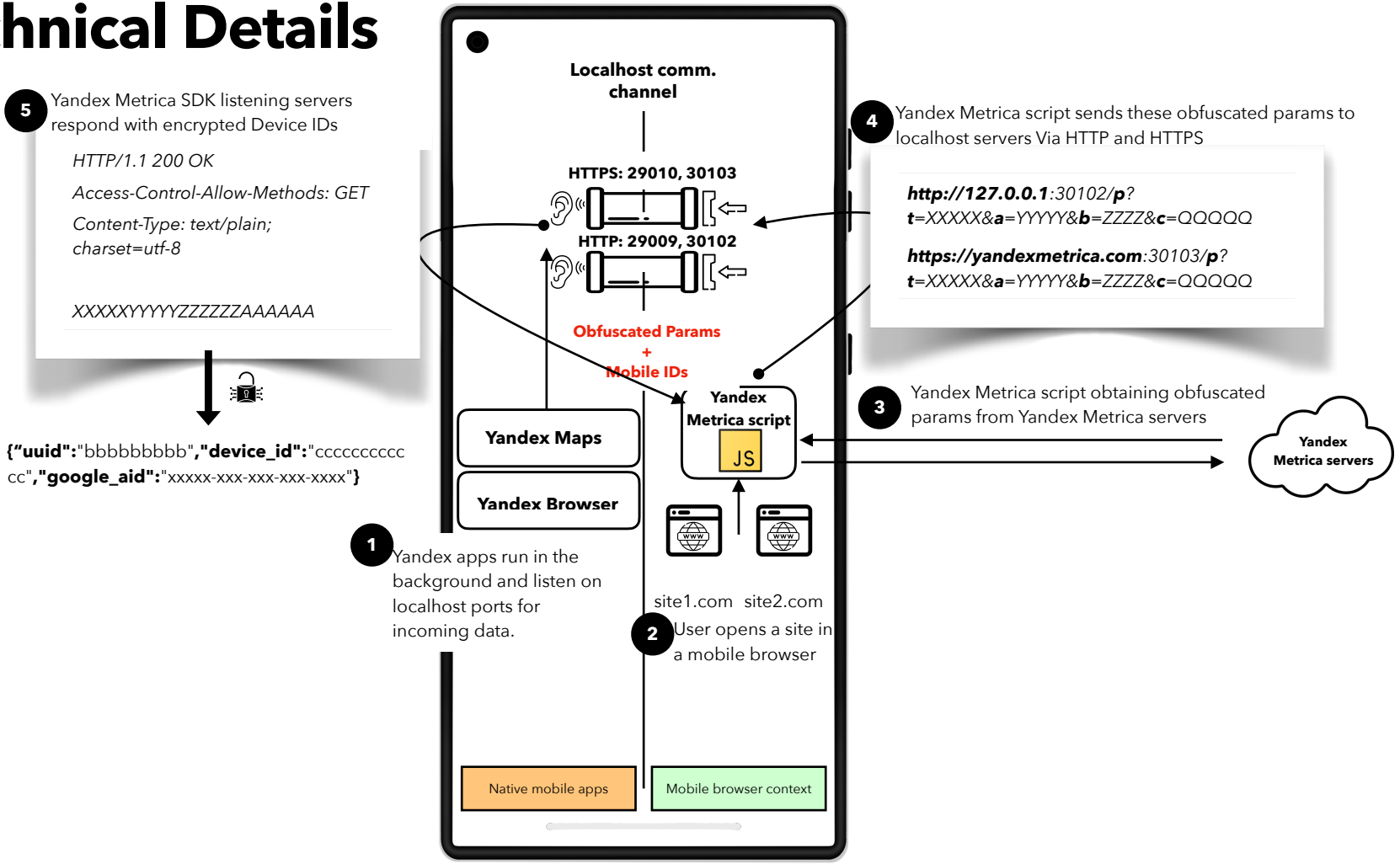
Technical Details



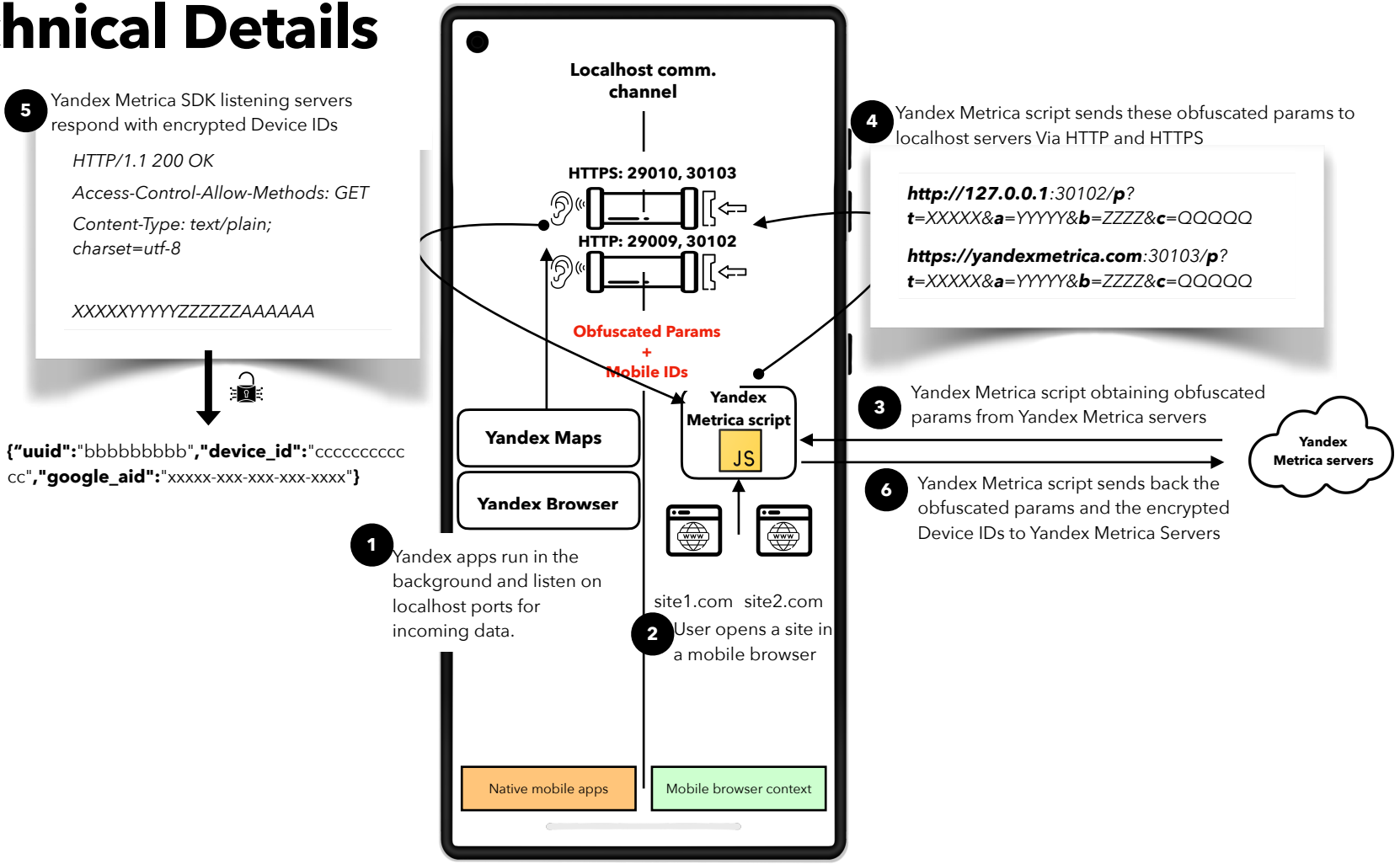
Technical Details



Technical Details



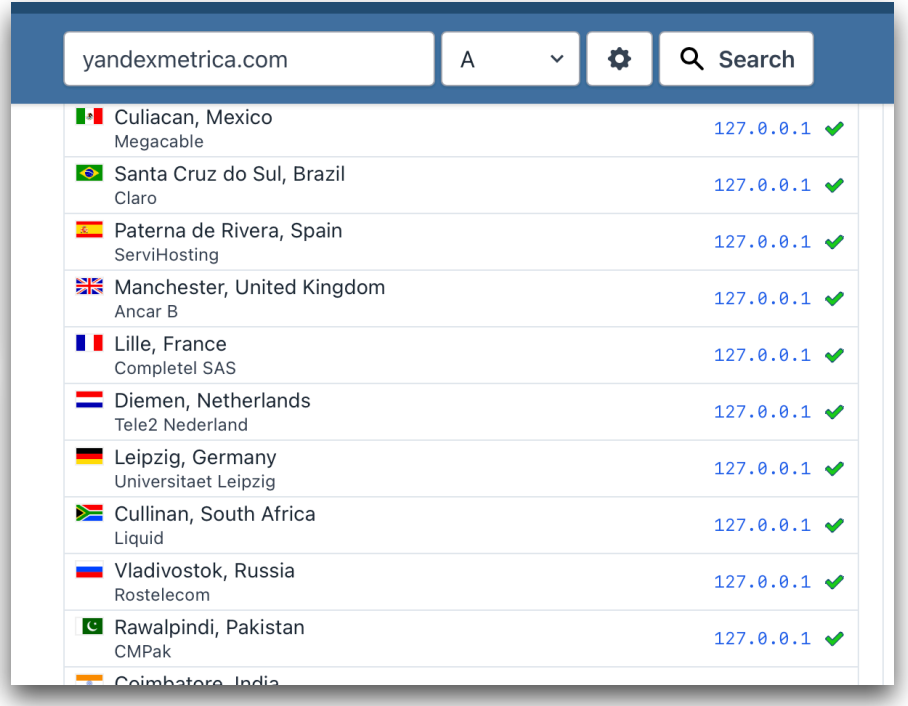
Technical Details



Technical Details: Domain Name Points to Localhost

```
www.milliyet.com.tr outbound to 127.0.0.1:30102 not encrypted

GET /p?t=UV|L7,!"T[rwe&D_>ZIb\aW#98Y.PC6k&a=O8ej58gw+
XCJg[redacted]XBQKn8FjQeBC8YuC&b=YT+
Cyq2SzbgTX0dxeohWGr[redacted]VbPC/Nj&c=7[redacted]7 HTTP/1.1^M

www.milliyet.com.tr outbound to 127.0.0.1:29009 not encrypted

GET /p?t=UV|L7,!"T[rwe&D_>ZIb\aW#98Y.PC6k&a=O8ej58gw+
XCJg[redacted]XBQKn8FjQeBC8YuC&b=YT+
Cyq2SzbgTX0dxeohWGr[redacted]VbPC/Nj&c=7[redacted]7 HTTP/1.1^M
```

```
www.milliyet.com.tr outbound to yandexmetrica.com:30103 encrypted

GET /p?t=UV|L7,!"T[rwe&D_>ZIb\aW#98Y.PC6k&a=O8ej58gw+
XCJg[redacted]XBQKn8FjQeBC8YuC&b=YT+
Cyq2SzbgTX0dxeohWGr[redacted]VbPC/Nj&c=7[redacted]7 HTTP/1.1^M

www.milliyet.com.tr outbound to yandexmetrica.com:29010 encrypted

GET /p?t=UV|L7,!"T[rwe&D_>ZIb\aW#98Y.PC6k&a=O8ej58gw+
XCJg[redacted]XBQKn8FjQeBC8YuC&b=YT+
Cyq2SzbgTX0dxeohWGr[redacted]VbPC/Nj&c=7[redacted]7 HTTP/1.1^M
```

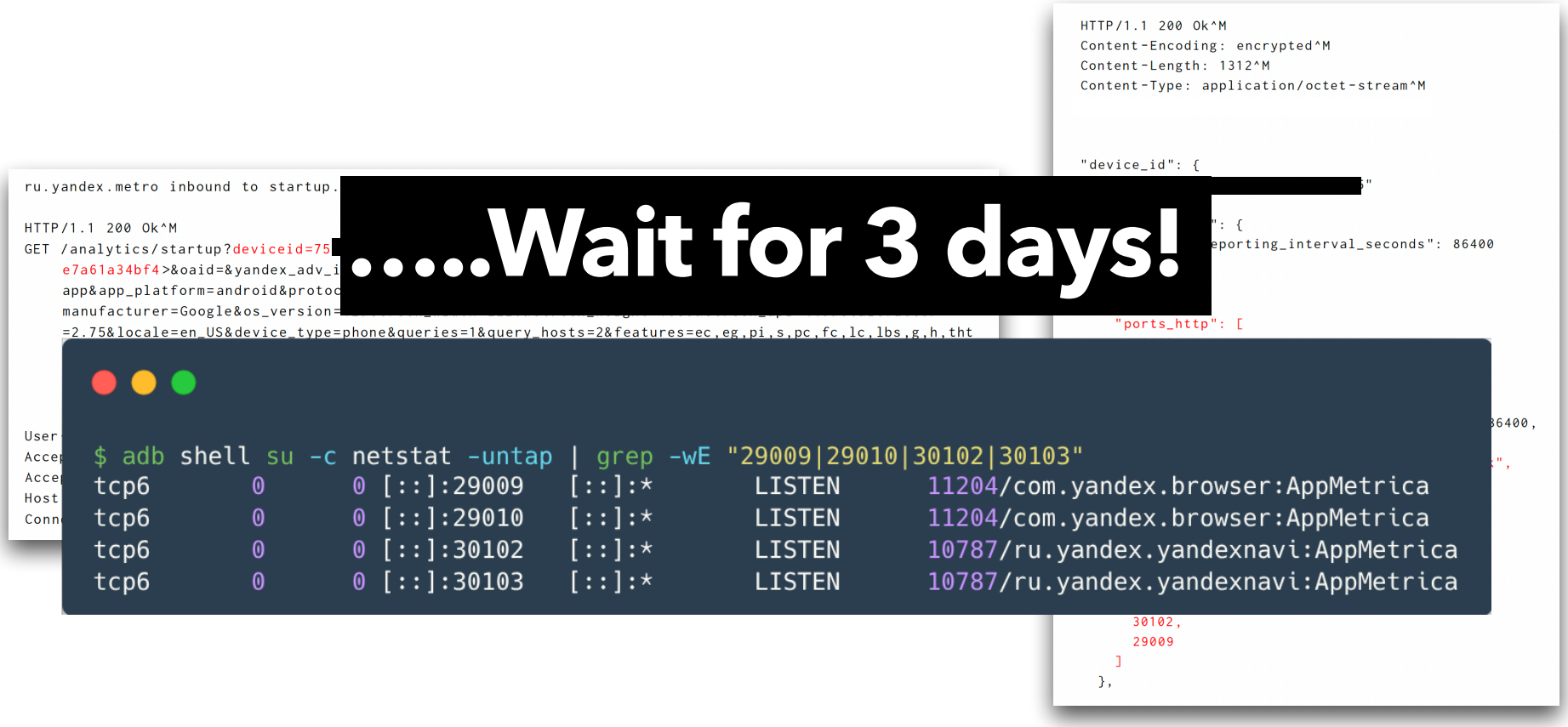


Technical Details: Delayed Activation

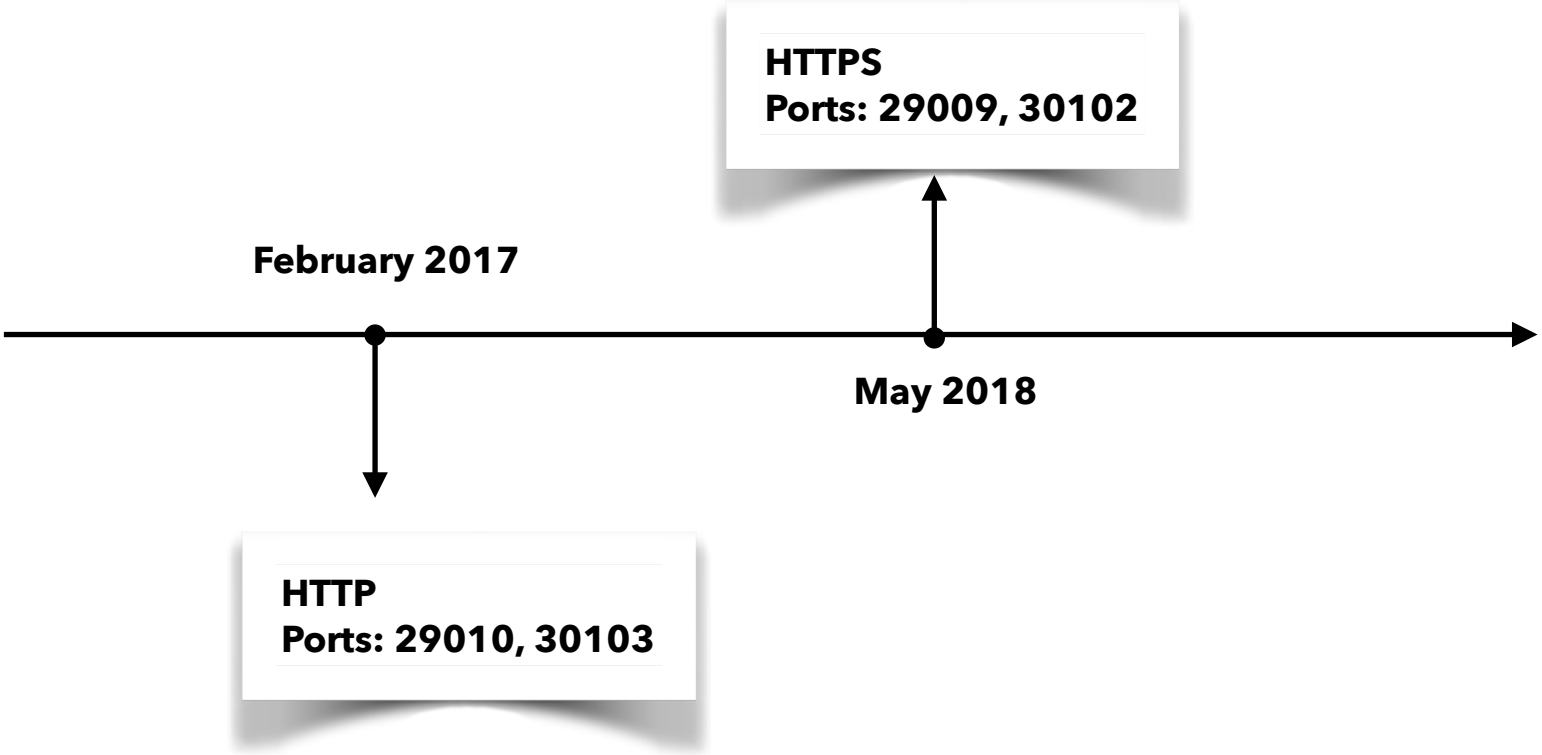
```
ru.yandex.metro inbound to startup.mobile.yandex.net:443

HTTP/1.1 200 Ok^M
GET /analytics/startup?deviceid=75[redacted]de&adv_id=d01143[redacted]
    e7a61a34bf4>&oaid=&yandex_adv_id=&app_set_id=753[redacted]52ede&app_set_id_scope=
    app&app_platform=android&protocol_version=2&analytics_sdk_version_name=5.2.1&model=AOSP on sargo&
    manufacturer=Google&os_version=12&screen_width=2220&screen_height=1080&screen_dpi=440&scalefactor
    =2.75&locale=en_US&device_type=phone&queries=1&query_hosts=2&features=ec,eg,pi,s,pc,fc,lc,lbs,g,h,tht
    ,wa,wc,ca,si,sl,ilc,gplc,up,ucfb,ues,ures,cai,caico,sp&s=1&app_id=ru.yandex.metro&lc=1&app_debuggable
    =0&sl=1&country_init=es&uuid=e6[redacted]5e&time=1&requests=1&stat_sending=1&
    permissions=1&ilc=1&up=1&ucfb=1&ues=1&ures=1&rp=1&tht=1&cc=1&mak=1&d=1&pc=1&app_system_flag=0&aic=1&
    at=1&ec=1&eg=1&su=1 HTTP/1.1^M
User-Agent: com.yandex.mobile.metrica.sdk/5.2.1.45002274 (Google AOSP on sargo; Android 12)^M
Accept-Encoding: encrypted^M
Accept: application/json^M
Host: startup.mobile.yandex.net^M
Connection: Keep-Alive^M
```

```
HTTP/1.1 200 Ok^M
Content-Encoding: encrypted^M
Content-Length: 1312^M
Content-Type: application/octet-stream^M



"device_id": {
    "hash": "18[redacted]"
  },
  "stat_sending": {
    "disabled_reporting_interval_seconds": 86400
  },
  ....
  "socket": {
    "ports_http": [
      30102,
      29009
    ],
    "launch_delay_seconds": 0,
    "min_successful_request_interval_seconds": 86400,
    "min_failed_request_interval_seconds": 3600,
    "token": "UV|L7,!\"T[rwe&D_>ZIb\\aW#98Y.PC6k",
    "first_delay_seconds": 259200,
    "ports_https": [
      30103,
      29010
    ],
    "seconds_to_live": 86400,
    "ports": [
      30102,
      29009
    ]
  },
```

Technical Details: Delayed Activation

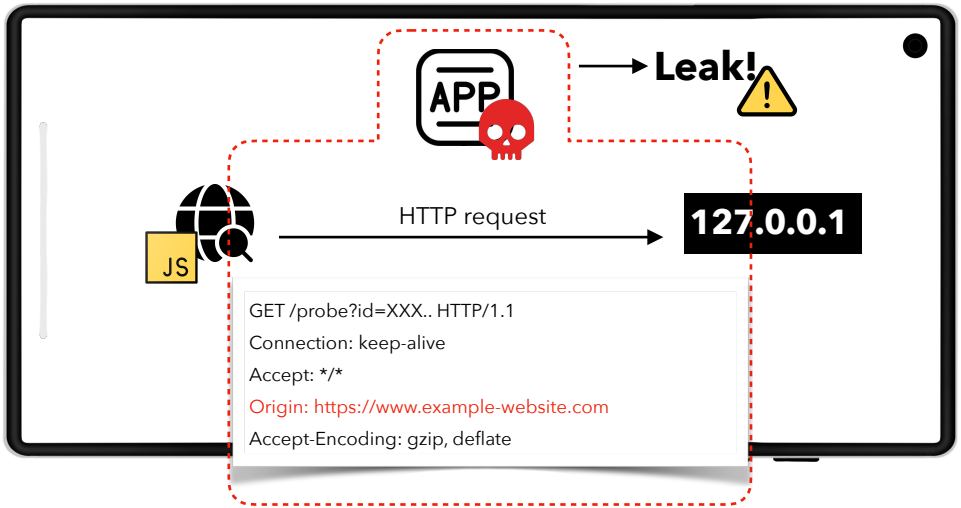


Yandex's Side Channel: Behaviour Across Time



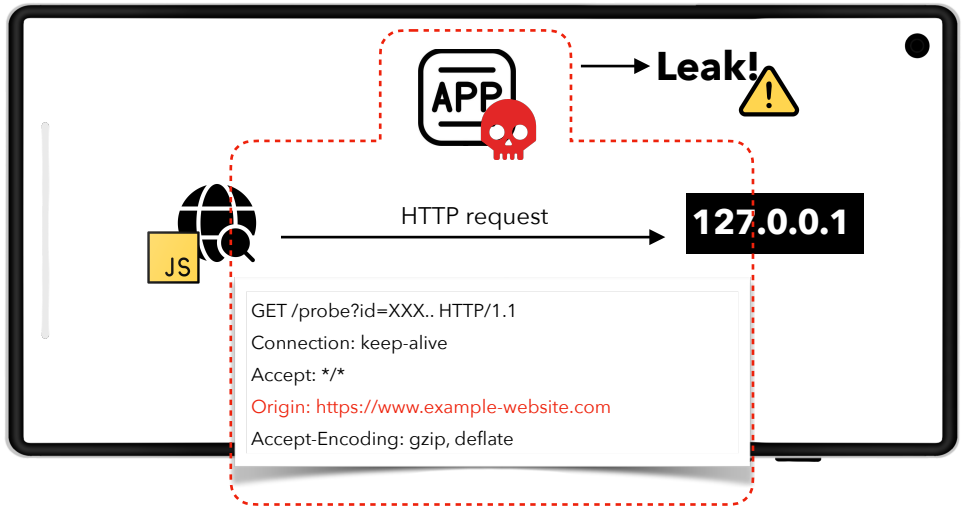
Browsing History Leak

- Malicious apps can intercept HTTP/ WebSocket based localhost requests
- Origin headers reveal web browsing activity



Browsing History Leak

- Malicious apps can intercept HTTP/ WebSocket based localhost requests
- Origin headers reveal web browsing activity



Affected – even in **private mode**

Minimally exposed

Unaffected

Affected Sites – Real-World Scale of Abuse

Meta → 11 Million

Yandex → 1 Million

Affected Sites – Real-World Scale of Abuse

🇺🇸 United States (New York vantage point)

- Meta Pixel:
  - 17,223 sites with tracker
  - 13,468 sites (78.2%) initiate localhost before consent
- Yandex Metrica:
  - 1,312 sites with tracker
  - 1,095 sites (83.5%) initiate localhost before consent

Affected Sites – Real-World Scale of Abuse

🇺🇸 United States (New York vantage point)

- Meta Pixel:
  - 17,223 sites with tracker
  - 13,468 sites (78.2%) initiate localhost before consent
- Yandex Metrica:
  - 1,312 sites with tracker
  - 1,095 sites (83.5%) initiate localhost before consent

🇪🇺 Europe (Frankfurt vantage point)

- Meta Pixel:
  - 15,677 sites with tracker
  - 11,890 sites (75.8%) initiate localhost before consent
- Yandex Metrica:
  - 1,260 sites with tracker
  - 1,064 sites (84.4%) initiate localhost before consent

Affected Sites – Real-World Scale of Abuse

These results suggest that localhost abuse is not only real—it's global, widespread, and potentially without meaningful user awareness or control.

🇺🇸 Un

-
  - 17,223 sites with tracker
  - 13,468 sites (78.2%) initiate localhost before consent
- Yandex Metrica:
  - 1,312 sites with tracker
  - 1,095 sites (83.5%) initiate localhost before consent

-
  - 15,677 sites with tracker
  - 11,890 sites (75.8%) initiate localhost before consent
- Yandex Metrica:
  - 1,260 sites with tracker
  - 1,064 sites (84.4%) initiate localhost before consent

Responsible Disclosure & Platform Mitigations

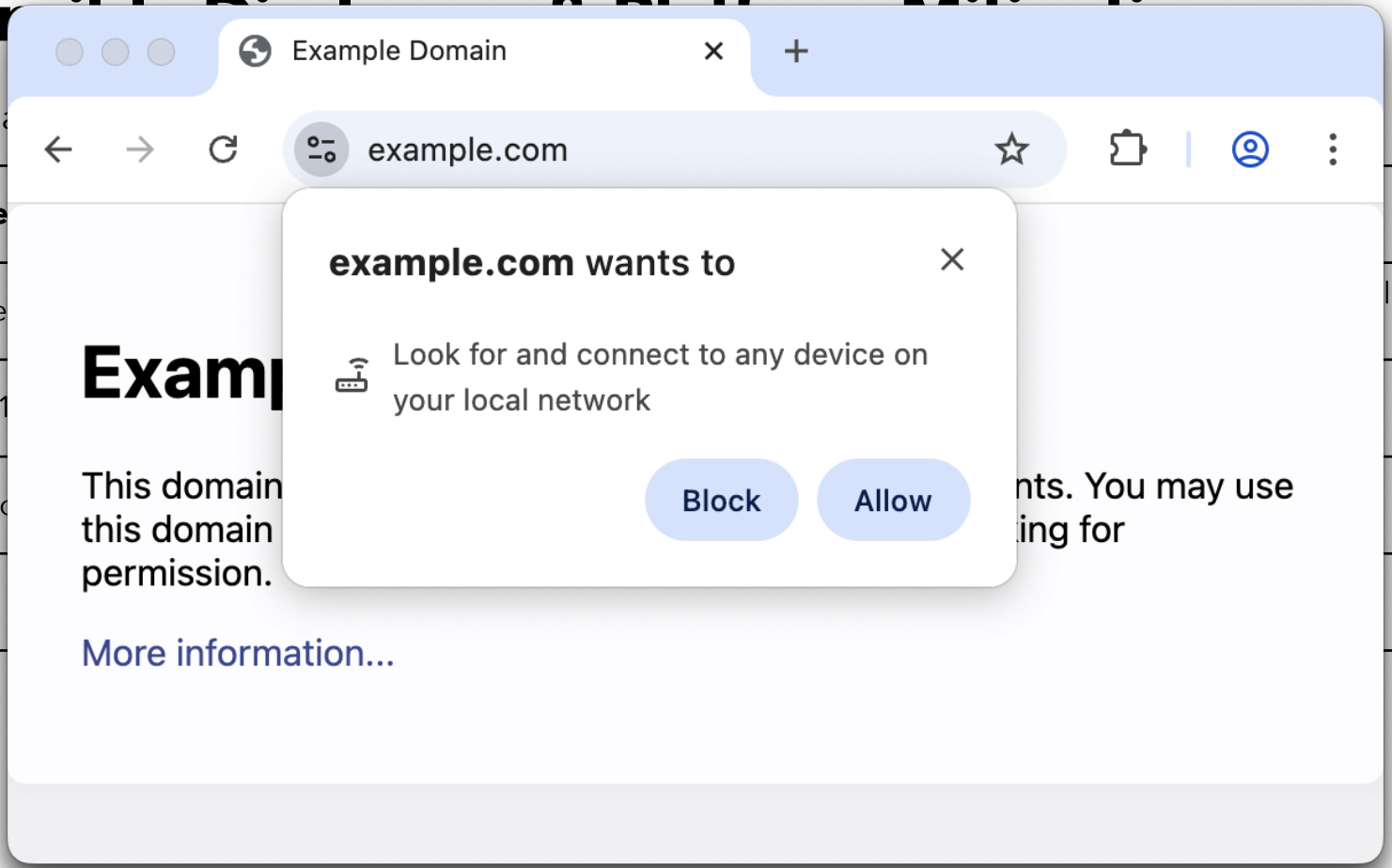
- Coordinated disclosure led to rapid mitigations by Chrome, Firefox, DuckDuckGo, Brave

Browser	Yandex Affected	FB Affected	Mitigations
Chrome 136	✅	✅	Chrome 137 blocks abused ports + SDP munging / Local Network Access (LNA)
Firefox 138	✅	❌	Port blocking in version 139
DuckDuckGo	⚠️ Minimal	❌	Blocklist amended
Brave	❌	❌	Blocklist + localhost user prompts since 2022

Respor

- Coordina

Browse			
Chrome			l Network
Firefox 1			
DuckDuc			
Brave			



Responsible Disclosure & Platform Mitigations

- Coordinated disclosure led to rapid mitigations by Chrome, Firefox, DuckDuckGo, Brave

Browser	Yandex Affected	FB Affected	Mitigations
Chrome 136	✅	✅	Chrome 137 blocks abused ports + SDP munging / Local Network Access (LNA)
Firefox 138	✅	❌	Port blocking in version 139
DuckDuckGo	⚠️ Minimal	❌	Blocklist amended
Brave	❌	❌	Blocklist + localhost user prompts since 2022

Responsible Disclosure & Platform Mitigations

- Coordinated disclosure led to rapid mitigations by Chrome, Firefox, DuckDuckGo, Brave

Browser	Yandex Affected	FB Affected	Mitigations
Chrome 136	✅	✅	Chrome 137 blocks abused ports + SDP munging / Local Network Access (LNA)
Firefox 138	✅	❌	Port blocking in version 139
DuckDuckGo	⚠️ Minimal	❌	Blocklist amended
Brave	❌	❌	Blocklist + localhost user prompts since 2022

Platform-level issues remain unresolved.
No user prompts, weak IPC policies.

Platform Scope: Android Only?

Platform Scope: Android Only?

Confirmed: Only Android was affected in our real-world tests

→ Meta and Yandex scripts targeted Android apps and browsers

Platform Scope: Android Only?

Confirmed: Only Android was affected in our real-world tests

→ Meta and Yandex scripts targeted Android apps and browsers

No abuse detected on iOS

→ Despite similar localhost access being technically possible

Platform Scope: Android Only?

Confirmed: Only Android was affected in our real-world tests

→ Meta and Yandex scripts targeted Android apps and browsers

No abuse detected on iOS

→ Despite similar localhost access being technically possible

iOS differences:

→ Background execution + stricter platform controls

Platform Scope: Android Only?

Confirmed: Only Android was affected in our real-world tests

→ Meta and Yandex scripts targeted Android apps and browsers

No abuse detected on iOS

→ Despite similar localhost access being technically possible

iOS differences:

→ Background execution + stricter platform controls

Other surfaces like desktop browsers or smart TVs may also be at risk

→ But *not yet investigated*

Media Impact

ars TECHNICA AI BIZ & IT CARS CULTURE GAMING HEALTH POLICY SCIENCE SECURITY SPACE TECH FORUM SUBSCRIBE SIGN IN

THE SPY WHO TRACKED ME

Meta and Yandex are de-anonymizing Android users' web browsing identifiers

Abuse allows M

DAN GOODIN – 3 JUN 2025

sky news 17 Jul 26° 20° Watch Live

Home UK Politics World US Money Science, Climate & Tech Ents & Arts Programmes Puzzles More

Meta found 'covertly tracking' Android users through Instagram and Facebook

Google says Meta and search engine company Yandex used Android capabilities "in unintended ways that blatantly violate our security and privacy principles".

Mickey Carroll
Science and technology reporter

Wednesday 4 June 2025 16:45, UK

The Washington Post
Democracy Dies in Darkness

Help Desk | Tech in Your Life | Your Data and Privacy | Internet Access | What's New | Ethical Issues | Ask a Question

Meta found a new way to violate your privacy. Here's what you can do.

Even hardened digital privacy veterans said they were stunned by Meta's tactics.

June 6, 2025

5 min Summary 465

EL PAÍS

Tecnología

TU TECNOLOGÍA · CIBERSEGURIDAD · PRIVACIDAD · INTELIGENCIA ARTIFICIAL · INTERNET · GRANDES TECNOLÓGICAS · ÚLTIMAS NOTICIAS

PRIVACIDAD EN INTERNET >

Este es el método oculto con el que Meta rastrea sin permiso la navegación en móviles (también en modo incógnito o con VPN)

Un grupo de investigadores descubre el sistema que usan las apps de Instagram y Facebook desde septiembre de 2024 para reunir el historial web de cada usuario en sus dispositivos Android

Media Impact

ars TECHNICA AI BIZ & IT CARS CULTURE GAMING HEALTH POLICY SCIENCE SECURITY SPACE TECH FORUM SUBSCRIBE SIGN IN

THE SPY WHO TRACKED ME

Meta and Yandex are de-anonymizing Android users' web browsing identifiers

Abuse allows M

sky news 17 Jul 26° 20° Watch Live

EL PAÍS

Tecnología

TU TECNOLOGÍA · CIBERSEGURIDAD · PRIVACIDAD · INTELIGENCIA ARTIFICIAL · INTERNET · GRANDES TECNOLÓGICAS · ÚLTIMAS NOTICIAS

PRIVACIDAD EN INTERNET >

Este es el método oculto con el que Meta rastrea sin permiso la navegación en móviles (también en modo incógnito o con VPN)

Un grupo de investigadores descubre el sistema que usan las apps de Instagram y

"The developers [Meta & Yandex] in this report are using capabilities present in many browsers across iOS and Android in unintended ways that blatantly violate our security and privacy principles" – Google Representative

The Washington Post
Democracy Dies in Darkness

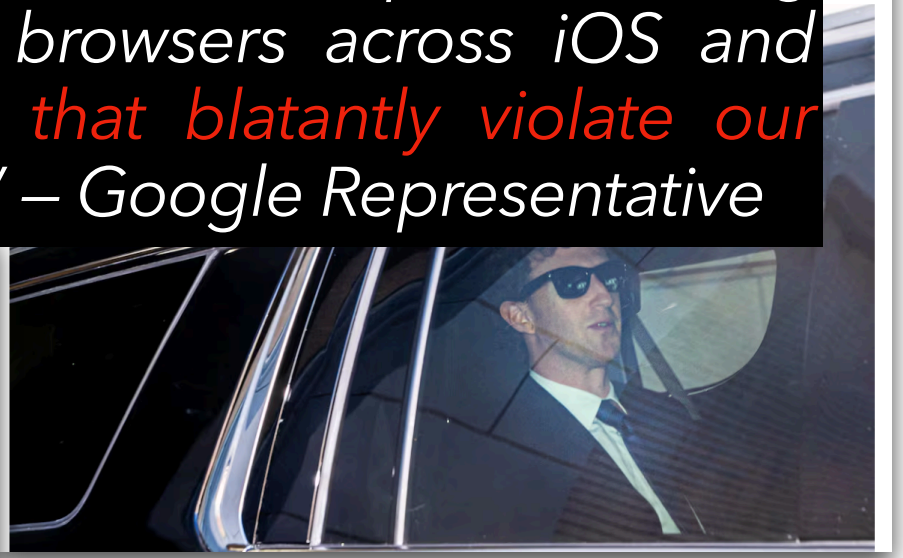
Help Desk | Tech in Your Life | Your Data and Privacy | Internet Access | What's New | Ethical Issues | Ask a Question

Meta found a new way to violate your privacy. Here's what you can do.

Even hardened digital privacy veterans said they were stunned by Meta's tactics.

June 6, 2025

5 min Summary 465



Conclusion

Android's isolation guarantees are incomplete

→ Localhost allows covert cross-process communication with no user visibility.

We reveal the first real-world deployment of covert web & app identity linkage

→ Meta & Yandex bridged cookies to AAIDs and logged-in identities silently—impacting billions.

Platform assumptions must be re-evaluated

→ "No permission = no access" breaks when localhost is in the middle.

Existing defenses are ineffective

→ Sandboxing, incognito mode, and permission models offer no meaningful protection

Fixes are partial—attack surface remains

→ Addressing this requires platform-centric solutions: deeper sandbox enforcement, consent-aware networking, and web-to-app auditing.

Thank you!

Aniketh Girish
aniketh.girish@networks.imdea.org

SCAN ME

Disclosure website