Secondary Data Sharing – Example of Mobile Push Notifications: Privacy Threats & Treatment Options

Dr. Fatbardh Veseli
Member / Rapporteur, AHWGPE, ENISA
Security Architect / Data Protection Champion, Capgemini

enisa
EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

Personal Data Sharing - Emerging Technologies
7 October 2022, Brussels, Belgium

Agenda

1

Secondary Data Sharing

Description & Use-cases

2

Mobile Push Notifications

Description & Architecture

3

Privacy Threats & Treatment Options

PETs, TETs, Arch. Patterns

4

Outlook & Summary

Characteristics of “secondary” data sharing

Data flows to **third parties**

Secondary to or as part of a primary data sharing operation

Part of software engineering or operational processes

In general, lack of transparency / awareness

Example use-cases of third party data sharing

Integrating third party services

- Mobile push notifications
- Authentication
- Sharing threat intelligence information

Outsourcing software engineering processes

- Software testing
- Migration of systems/data

Outsourcing IT operations

- Network monitoring
- Data storage, backup and restore
- Data sharing between on-premises and cloud environment

Agenda

1 **Secondary Data Sharing**

Description & Use-cases

2 **Mobile Push Notifications**

Description & Architecture

3 **Privacy Threats & Treatment Options**

PETs, TETs, Arch. Patterns

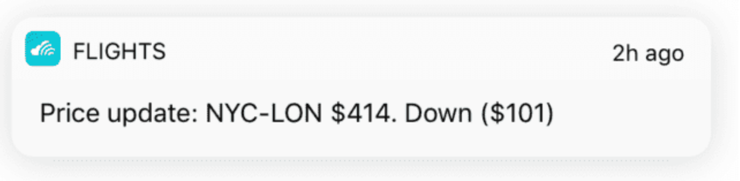
4 **Outlook & Summary**

Do you use mobile push notifications?

Do you know mobile push notifications work?

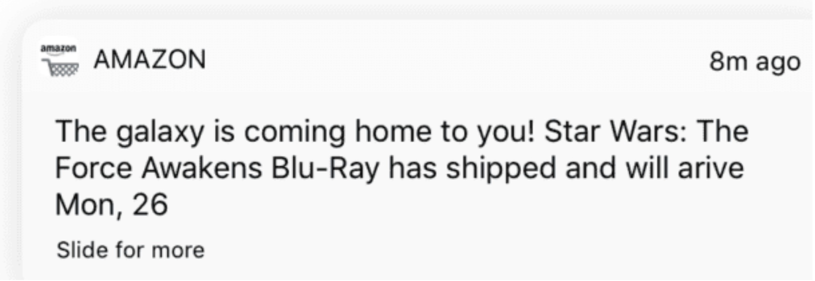
Mobile push notifications

- Notification messages pushed to the mobile users
- Message content options
  - Title
  - Content (text, emojis)
  - Icons
  - Deep links / URLs
  - Additional data



FLIGHTS 2h ago

Price update: NYC-LON $414. Down ($101)



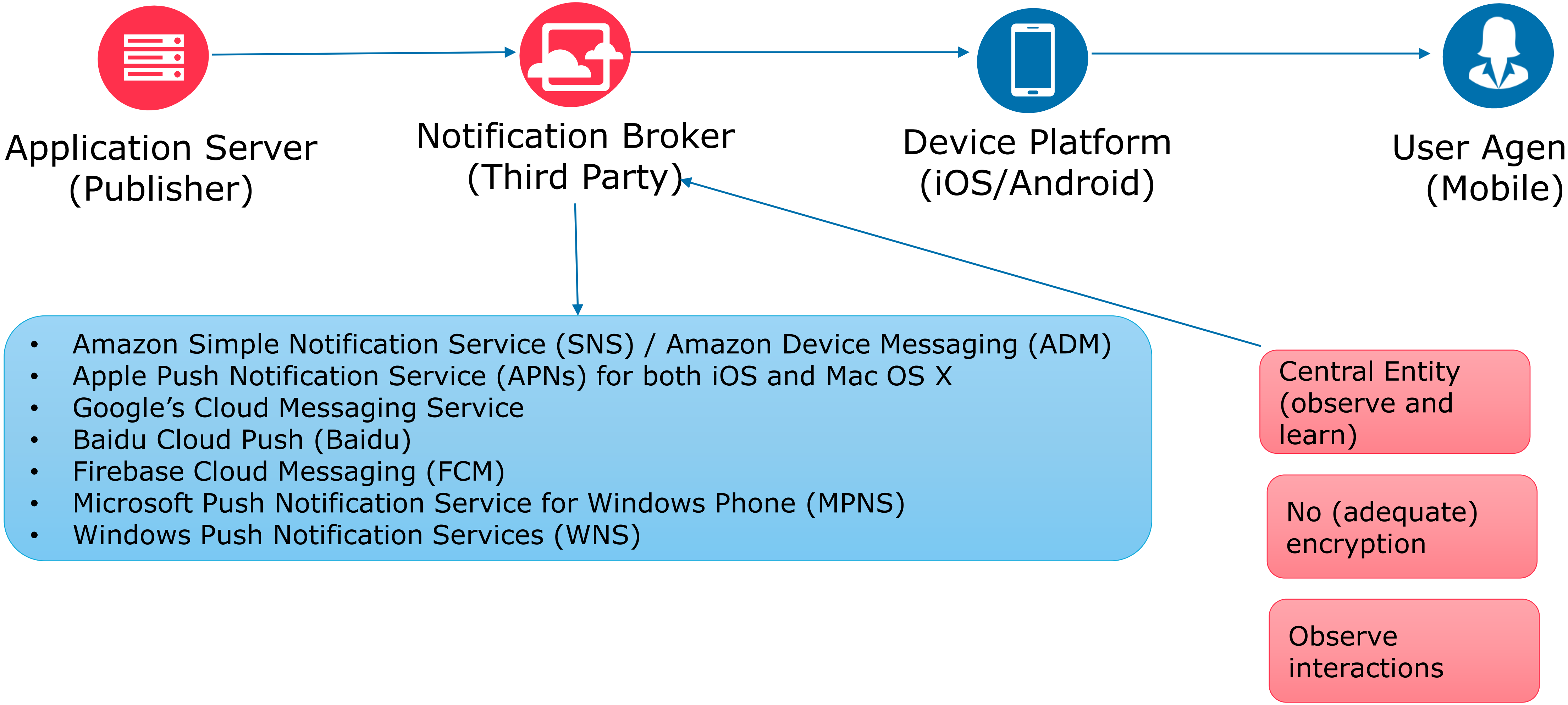
AMAZON 8m ago

The galaxy is coming home to you! Star Wars: The Force Awakens Blu-Ray has shipped and will arive Mon, 26

Slide for more

Source: Vero, https://www.getvero.com/resources/mobile-push-notifications/, last accessed 16.06.2022

Key Architecture Entities



Application Server (Publisher)

Notification Broker (Third Party)

Device Platform (iOS/Android)

User Agents (Mobile)

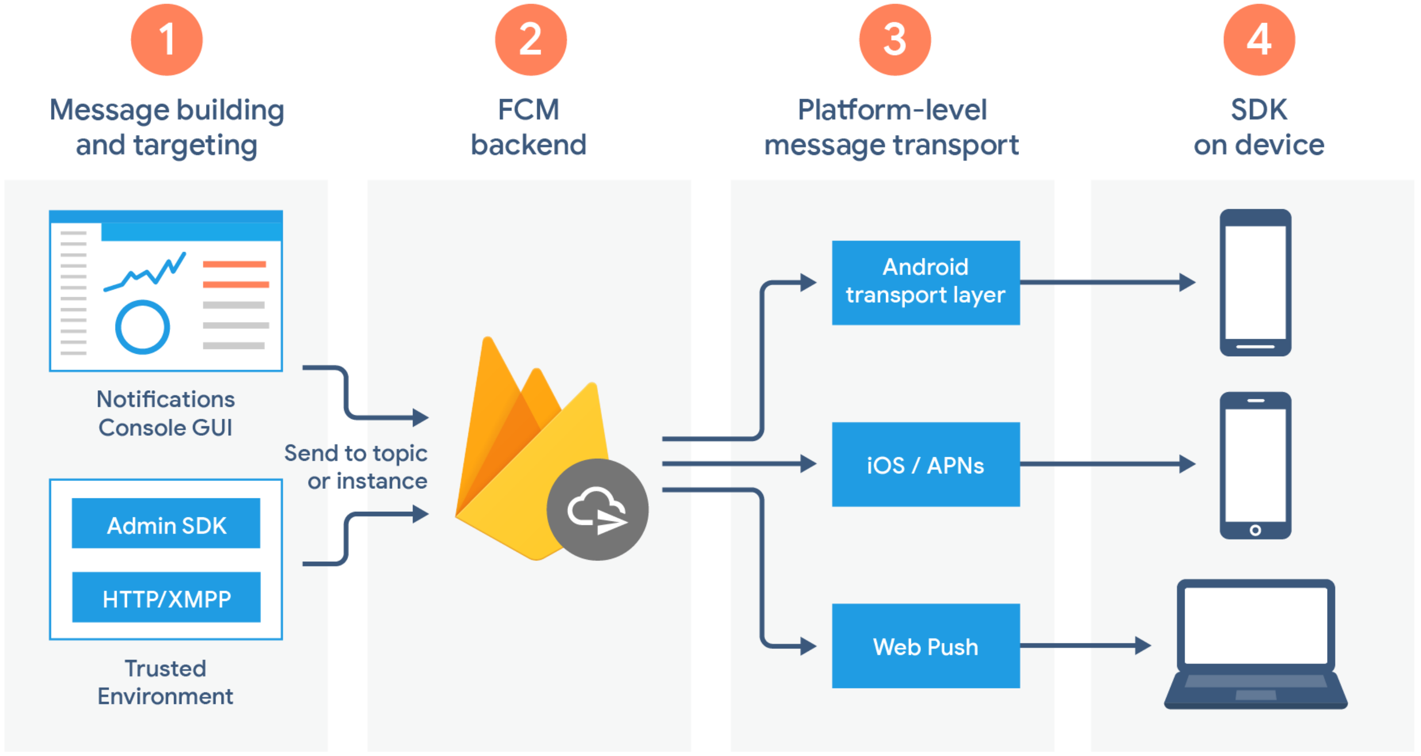
- Amazon Simple Notification Service (SNS) / Amazon Device Messaging (ADM)
- Apple Push Notification Service (APNs) for both iOS and Mac OS X
- Google’s Cloud Messaging Service
- Baidu Cloud Push (Baidu)
- Firebase Cloud Messaging (FCM)
- Microsoft Push Notification Service for Windows Phone (MPNS)
- Windows Push Notification Services (WNS)

Central Entity (observe and learn)

No (adequate) encryption

Observe interactions

Famous notification protocols: Firebase Cloud Messaging (FCM)


1
Message building and targeting
2
FCM backend
3
Platform-level message transport
4
SDK on device
Notifications Console GUI
Send to topic or instance
Admin SDK
HTTP/XMPP
Trusted Environment
Android transport layer
iOS / APNs
Web Push

Bought and operated by Google Subsidiary

Apparently "THE state of practice"

Source: FCM

Agenda

1

Secondary Data Sharing

Description & Use-cases

2

Mobile Push Notifications

Description & Architecture

3

Privacy Threats & Treatment Options

PETs, TETs, Arch. Patterns

4

Outlook & Summary

Potential privacy threats to mobile push notifications

Linkability: Observation of the interaction between the two entities (server and client) including frequency of interaction, types of messages exchanged.

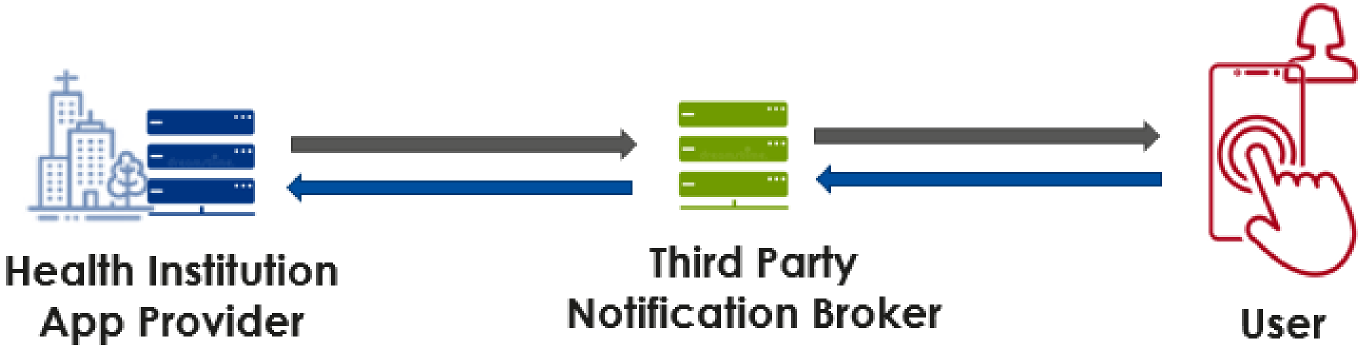
Identifiability: Messages can identify the user

Disclosure: the content of the messages being pushed may be disclosed, thus violating the confidentiality of the notification.

Unawareness: potential unawareness of the user, but also developers / architects

Non-compliance: potentially lack of compliance, e.g. regarding consent, transparency, data flow documentation, data subject rights, etc.

Use case: Mobile Push Notifications in eHealth scenario



Health Institution App Provider

Third Party Notification Broker

User

„Here are the results of your medical examination"

„Please upload test results from your cardiology visit"

„Here I upload additional examination results after my surgery"

Risk treatment options

Risk avoidance

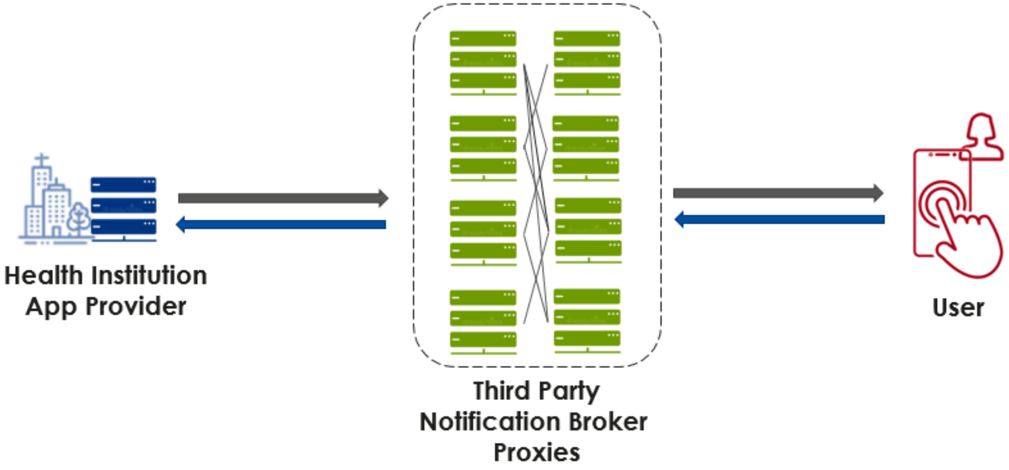
- Do not use push notifications
- Use „local“ (pull) notifications proactively

Risk Modification

- E2E Encryption
- Anonymous Notification Protocols (PETs)
- Transparency Enhancing Technologies (TETs)
- Architectural Patterns
- Own Notification Service

Anonymous Notification Protocols (PETs)

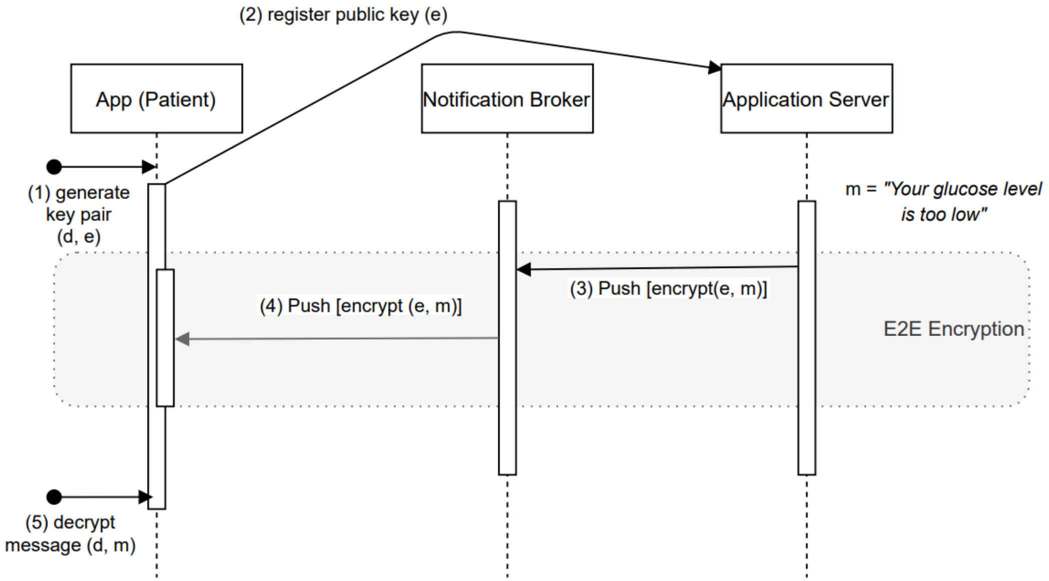
- Chain of proxies (mixes) rather than a central notification server
  - Random node chain
  - Encrypted communication between nodes
- Example: AnNotify*
  - **unlinkability** between the subscriber and publisher
  - **untraceability** of push notifications to a subscriber, and
  - **broadcast privacy**, hiding the fact of whether a subscriber is subscribed to a notification or not.



*Piotrowska, A., Hayes, J., Gelernter, N., Danezis, G.: AnNotify: A Private Notification Service., IACR eprint (2016)

End-to-End (E2E) Encryption

- The pushed messages are often not encrypted (adequately)
- E2E Encryption solves the disclosure problem
  - May still reveal private information
  - Other privacy risks remain (e.g. metadata are still available)
- Work already happening in this regard
  - e.g. Project Capillary (https://github.com/google/capillary)
  - Often platform specific (e.g. Java / Android)
  - W3C Push Working Draft (https://www.w3.org/TR/push-api/)



(2) register public key (e)
App (Patient)
Notification Broker
Application Server
(1) generate key pair (d, e)
m = "Your glucose level is too low"
(3) Push [encrypt(e, m)]
(4) Push [encrypt (e, m)]
E2E Encryption
(5) decrypt message (d, m)

*

Architectural Patterns

- Apply the „Need to push“ strategy
  - Push message without payload
  - Pull the payload from the server directly (without the notification broker)

Transparency Enhancing Technologies (TET)

- Privacy tools in the CI/CD Pipeline
  - Transparency Enhancing Technologies (TETs)
  - „Privacy as Code“
  - “DevPrivOps”?
- Systematically declare & report
  - Privacy policies
  - Data flows
- Enhance transparency & compliance
- Examples:
  - Fidesctl (https://ethyca.github.io/fides/1.8.4/),
  - TIRA*

*Grünewald, P. Wille, F. Pallas, M. C. Borges and M. -R. Ulbricht, "TIRA: An OpenAPI Extension and Toolbox for GDPR Transparency in RESTful Architectures," 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2021, pp. 312-319, doi: 10.1109/EuroSPW54576.2021.00039

Agenda

1

Secondary Data Sharing

Description & Use-cases

2

Mobile Push Notifications

Description & Architecture

3

Privacy Threats & Treatment Options

PETs, TETs, Arch. Patterns

4

Outlook & Summary

Potentially relevant factors for the choice of the push notification service provider

- Ease of integration & maintenance

Interoperability

Scalability

Usability aspects

- Battery drain
- Delays

“Use whatever everyone else is using”

Outlook & Conclusion

- „Secondary‟ data sharing common in many applications / use cases
- Mobile push notifications as an example
- Measures potentialy generalizable (as strategies)
- Privacy Engineering to
    - Raise awareness about problems (both users and developers / architects)
    - Identify and Develop alternative Patterns and Technologies
- PETs

Thank you!

Contact: fatbardh.veseli@capgemini.com