December 2021

Globally Non-Deterministic, Locally Deterministic Unique Identifier to Enable Local Tracking of a Connected Wi-Fi Access Point

Chinmay Dhodapkar

Globally Non-Deterministic, Locally Deterministic Unique Identifier to Enable Local Tracking of a Connected Wi-Fi Access Point

Abstract:

This publication describes methods of preserving user privacy through the prevention of Wi-Fi location tracking by generating a unique identifier (UID) for a Wi-Fi access point (AP) on a per-computing device basis (e.g., a first UID is generated for use by a first computing device, a second UID is generated for use by a second computing device). The generated UIDs are locally deterministic (unique to a specific computing device), but globally non-deterministic (different UIDs are generated for different computing devices).

Keywords:

Audio call quality, location permission, location tracking, privacy, network switching, phone service, voice call quality, VoIP, VoLTE, wireless, Wi-Fi, access point, identity

Background:

Wi-Fi location tracking is a process of using the characteristics of nearby Wi-Fi and other wireless access points (APs) to determine the geolocation of a computing device. These characteristics may include identity information (e.g., device address, Basic Service Set Identifier (BSSID), Media Access Control (MAC) address) for the AP. For example, an application installed on a computing device, which has access to AP identity information, may be able to utilize a public Wi-Fi AP location database to determine the geolocation of the computing device, potentially raising privacy concerns. In such an example, Wi-Fi AP identity information can be logged over

time from multiple users' computing devices that connect to it, allowing for a correlation between the AP identity information and location information.

One way of addressing such privacy concerns is to utilize application permissions on the computing device that prevent an application from accessing AP identity information unless the user has granted the application permission for such access. While an effective solution, application permissions can make it difficult for applications to access and utilize AP identity information in ways that do not cause privacy concerns (e.g., where the application is not utilizing the identity information to determine a location).

Description:

This publication describes methods of preserving user privacy through the prevention of Wi-Fi location tracking by generating a unique identifier (UID) for a Wi-Fi AP on a per-computing device basis (e.g., a first UID is generated for use by a first computing device, a second UID is generated for use by a second computing device). The generated UIDs are locally deterministic (unique to a specific computing device), but globally non-deterministic (different UIDs are generated for different computing devices). By generating a locally deterministic, but globally non-deterministic UID for an AP on a per-computing device basis, for utilization by applications installed on a computing device, such applications can be provided with AP identity information without raising Wi-Fi location tracking concerns.

An example application that will be mentioned throughout this publication is an Internet Protocol Multimedia Subsystem-calling (IMS-calling) application that provides users with voice calling over 4G/LTE, 5G, and Wi-Fi. Currently, at least on some wireless computing devices (e.g., smartphone, tablet), the decision to use Wi-Fi for voice calling is based on the Received Signal

Strength Indicator (RSSI). However, a strong RSSI does not necessarily guarantee good voice call quality. For example, the AP could be serviced by an Internet Service Provider (ISP) with low data rates and accessed by many wireless computing devices simultaneously, like a coffee shop's Wi-Fi. The IMS-calling application may track and associate Wi-Fi voice call quality over time with a specific AP. If the application determines that the AP has consistently poor voice call quality, even though it has a strong RSSI, the application can avoid connecting to that AP in the future. Due to privacy concerns, any application (e.g., IMS-calling application) that is interested in tracking a Wi-Fi AP over time but is not interested in location information, must still be granted location permission.

The problem of how to disclose a UID for a Wi-Fi AP to an application on a computing device without exposing sensitive information that can be used for location tracking is solved by generating a locally deterministic (the same UID is generated every time the computing device application utilizes the AP), but globally non-deterministic (different computing devices do not generate identical UID for the same AP) UID for an AP and providing the UID to applications.

An example process for generating a locally deterministic, but globally non-deterministic UID for an AP is illustrated in Fig. 1. In Fig. 1, a computing device deterministically generates a private key, potentially based on a unique identifier for that device (e.g., device ID, International Mobile Equipment Identity (IMEI), serial number, Federal Communications Commission (FCC) ID), during bootup and stores it in a local, secure keystore or similar storage medium. An application (e.g., IMS-calling application) requests the UID of a Wi-Fi AP to which the computing device is wirelessly connected. A first one-way hash is generated based on the private key and the unique identity for the application (e.g., application package name, application ID). A second one-way hash is then generated based on the first one-way hash and the identity information (e.g.,

MAC address, BSSID) of the Wi-Fi AP. This second hash is the locally deterministic, but globally non-deterministic UID, which can be used as fake identity information by an application to identify and/or track a wireless AP over time. Optionally, the process could further include providing the UID to the application, for example, via an application programming interface (API) provided by an operating system (OS) or another framework.

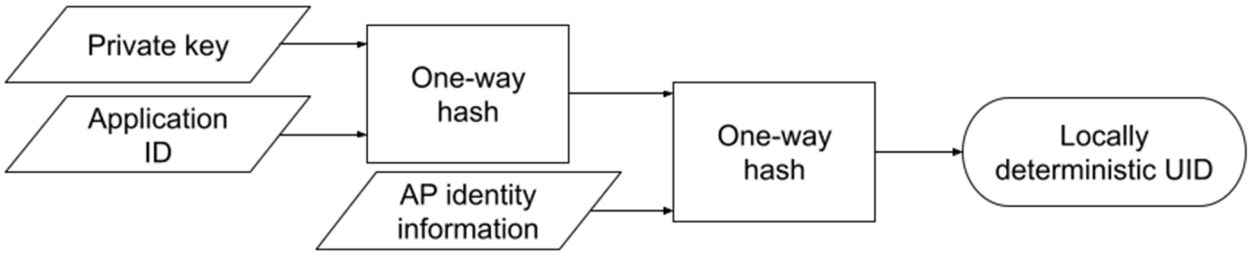

Fig. 1. Flowchart detailing the generation of a locally deterministic UID.

Through the utilization of this process, even if the application leaks the UID to a network server, the server will not be able to correlate it with other UIDs coming from the same application and same Wi-Fi AP. This is because the UID is based on the private key for a specific computing device (i.e., no two computing devices will have the same UID). For example, two computing devices connect to the same Wi-Fi AP using the same application. The UID for the AP with respect to each computing device remains unique because each computing device has its own private key (e.g., device ID, IMEI, FCC ID). Although both computing devices connected to the same AP using the same application, the UIDs from each device are different, so any server with access to both UIDs cannot correlate them to the same AP. Using a process like the one described above allows an application, like the IMS-calling application, to track Wi-Fi APs in order to determine their voice call quality over time without exposing the user's location information to the application. In this way, computing device applications can be provided with AP identity information in a way that avoids the privacy concerns of Wi-Fi location tracking.

References:

[1] Patent Publication: US20180041512A1. Notification Framework for Access Point Controllers. Priority Date: August 3, 2016.

[2] Patent Publication: CN107094293A. Device and Method for Acquiring Real MAC Address of WiFi Terminal. Priority Date: June 27, 2017.

[3] Patent Publication: US20090257361A1. Methods and Apparatus for Determining Communication Link Quality. Priority Date: September 28, 2006.

[4] Patent Publication: US20200226623A1. Method and System for Customer Assistance in a Retail Store. Priority Date: July 19, 2013.

[5] "Companion Device Pairing." Android Developers. Accessed November 15, 2021. https://developer.android.com/guide/topics/connectivity/companion-device-pairing.