Technical Disclosure Commons

Defensive Publications Series

May 10, 2019

Managing Access to Location Information

Tom Price

Managing Access to Location Information

Abstract:

This publication describes systems and techniques directed to managing access to location information. A wireless-communication device, such as a smartphone, includes a sequestered location integrated circuit (IC) component that includes a location security manager application stored in memory circuitry of the sequestered location IC component. The wireless-communication device, using the sequestered location IC component, performs a technique that includes generating, from received data, a set of location information corresponding to a determined security-access level, encrypting the set of location information, and generating, for the encrypted set of location information, a security key that corresponds to the determined security-access level. The technique also includes determining that an application is allowed access to the encrypted set of location information corresponding to the determined security-access level and providing, to the application, the security key.

Keywords:

location privacy, location encryption, location access level, global positioning system (GPS) data sharing, global navigation satellite system (GNSS) data sharing, public land mobile network (PLMN) identifier sharing, universally unique identifier (UUID) sharing

Background:

Today, an application operating on a wireless-communication device may have access to data that allows the application to determine a location of a user with a high degree of accuracy. Determining the location of the user may include the application using data available to the wireless-communication device, such as global navigation satellite system (GNSS) data collected by the wireless-communication device, location data associated with a cellular base station operating near the wireless-communication device, or location data associated with a beacon or wi-fi router connected to the wireless-communication device. The application may, in realtime, cause the wireless-communication device to transmit location information associated with the determined location to a third party, such as an advertising agency or a data vendor, so that the third party might be able to develop a profile of the user. This practice, in general, generates privacy and security concerns, which are addressed by the systems and techniques described in this publication.

Description:

This publication describes systems and techniques directed to managing access to location information. A wireless-communication device, such as a smartphone, includes a sequestered location integrated circuit (IC) component that includes a location security manager application stored in memory circuitry of the sequestered location IC component. The wireless-communication device, using the sequestered location IC component, performs a technique that includes generating, from received data, a set of location information corresponding to a determined security-access level, encrypting the set of location information, and generating, for the encrypted set of location information, a security key that corresponds to the determined security-access level. The technique also includes determining that an application is allowed access to the encrypted set of location information corresponding to the determined security-access level and providing, to the application, the security key.

Fig. 1, below, illustrates an example wireless-communication device and elements of the wireless-communication device that support managing access to location information.

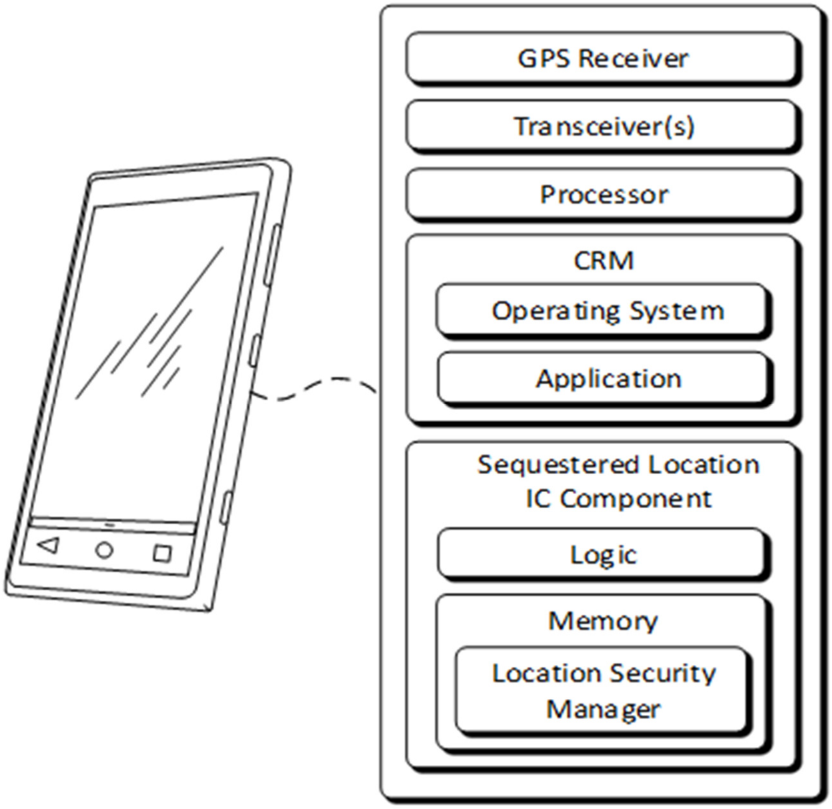

Fig. 1

As illustrated, the wireless-communication device is a smartphone. However, other wireless-communication devices (*e.g.*, a tablet, a laptop computer, a wearable device, or the like) can also support managing access to location information.

The wireless-communication device includes a global positioning system (GPS) receiver, as well as one or more transceivers (*e.g.*, fifth generation new radio (5G NR) transceiver, a Wi-Fi transceiver, and/or a Bluetooth® low-energy (BLE) transceiver). The wireless-communication device also includes a processor and a computer-readable medium (CRM). The processor may be a single core processor or a multiple core processor composed of a variety of materials, such as silicon, polysilicon, high-K dielectric, copper, and so on. The CRM may include any suitable memory or storage device such as random-access memory (RAM), static RAM (SRAM), dynamic RAM (DRAM), non-volatile RAM (NVRAM), read-only memory (ROM), or Flash memory. The CRM, in general, stores executable instructions that correspond to an operating system of the wireless-communication device and at least one application (*e.g.*, a weather application, a navigation application, a social media application, a media player application, and so on).

The wireless-communication device also includes a sequestered location integrated circuit (IC) component. The sequestered location IC component includes logic circuitry and memory circuitry, where the memory circuitry contains executable instructions of a location security manager application. In some instances, the sequestered location IC component may be a system-on-chip (SoC) component (*e.g.*, using a shared IC die that includes the logic circuitry and the memory circuitry) or a multi-chip package component (*e.g.*, using a first IC die for the logic circuitry and a second IC die for the memory circuitry). Furthermore, the sequestered location IC component has a limited interface to the processor of the wireless-communication device, restricting the ability of the application or another entity to communicate directly with the sequestered location IC component.

The sequestered location IC component, under direction of the location security manager application as executed by the logic circuitry of the sequestered location IC component, performs the operations described herein. The operations include generating, from data received by the GPS receiver and the transceivers of the wireless-communication device, multiple sets of location information. Each set of location information can correspond to a different security access-level, where each different security-access level corresponds to a different granularity of geolocation data associated with the wireless-communication device.

The operations also include encrypting each set of location information and generating a security key for each encrypted set of location information. Upon determining that an application is allowed access to an encrypted set of location information from the multiple encrypted sets of location information and corresponding to a determined security-access level, the sequestered location IC component provides, to the application via the processor, a security key that corresponds to the determined security-access level.

Fig. 2, below, illustrates example aspects of the wireless-communication device and the aforementioned operations.

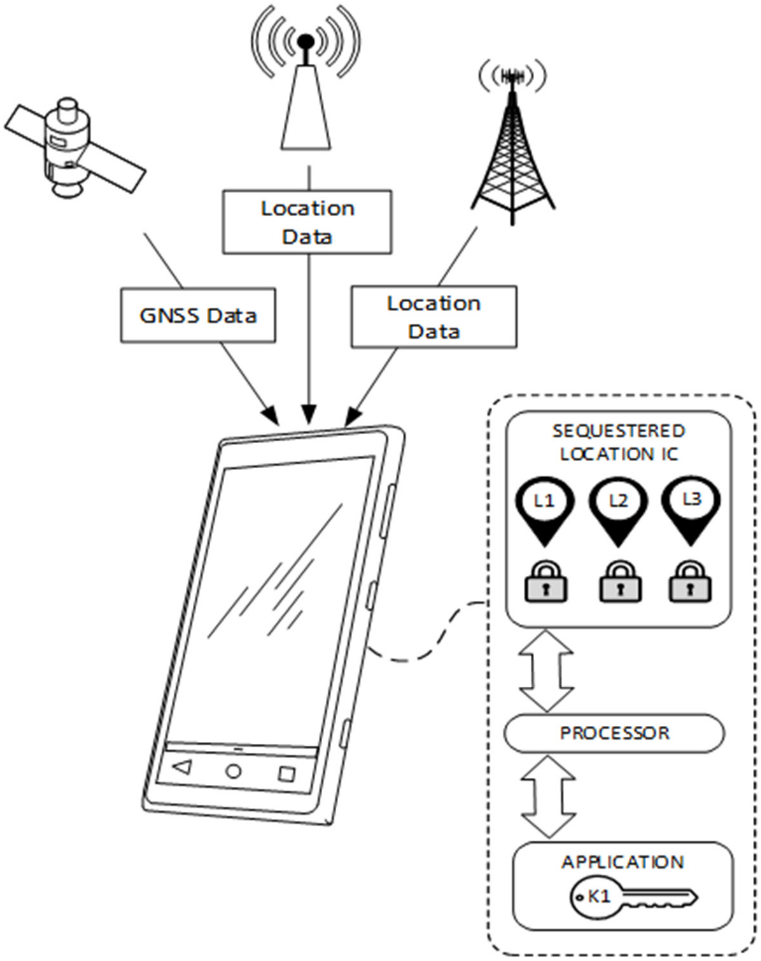

Fig. 2

As illustrated, and as an example, the wireless-communication device receives, from different access points, data that can be used to determine location information associated with the wireless-communication device. The wireless-communication device can receive one or more of GNSS data from a satellite (for computing a latitude and longitude of a geolocation of the wireless-communication device), location data from a beacon (that can be associated with a business, such as a coffee shop or a retail store at or near the location), and location data from a base station (that can be associated with a cellular service provider at or near the location). The location data received from the beacon and the base station can include, for example, respective GNSS data that the beacon and base station receive from the satellite, respective computed geolocations of the beacon and base station, or identifiers that are associated with the beacon and base station (*e.g.*, a universally unique identifier (UUID) or a public land mobile network (PLMN) identifier) that the wireless-communication device can use to reference location information. The wireless-communication device can use one or more of the received data to generate location information associated with the wireless-communication device.

The processor of the wireless-communication device (*e.g.*, the processor executing the instructions of the operating system in the CRM) works in combination with the logic circuitry of the sequestered location IC component (*e.g.*, the logic circuitry of the sequestered location IC component executing the instructions of the location security manager application) to secure the location information. The sequestered location IC component then generates different sets of location information corresponding to different security-access levels (*e.g.*, sets L1-L3) and encrypts the different sets of location information. For each set of encrypted location information, the sequestered location IC component also generates a security key.

In the illustrated example, the sequestered location IC component determines that an application is allowed access to a set of location information corresponding to a security access-level of “L1” and provides, to the application via the processor, a corresponding key (*e.g.*, the corresponding security key “K1”). In some instances, determining that the application is allowed access to a set of location information corresponding to a particular security-access level may be a result of the user selecting the application for access to the particular security-access level through an interface of the wireless-communication device (*e.g.*, an interface generated under direction of the location-security manager application), while in other instances determining that the application is allowed access to the particular security-access level may be associated with a default setting of the wireless-communication device’s operating system.

Figure 3, below, illustrates examples of different sets of location information corresponding to different security-access levels.

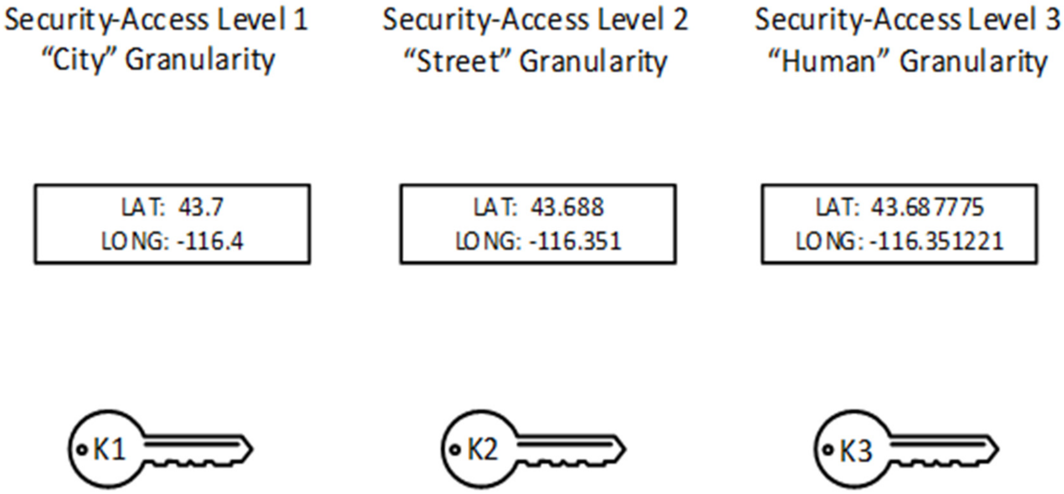

Fig. 3

As illustrated at the left of Fig. 3, a first set of location information is associated with an example security-access level 1. As illustrated, geolocation information (*e.g.*, latitude data and longitude data as computed by the sequestered location IC component) is at a granularity that corresponds to a "city" granularity (*e.g.*, a precision of 0.1 decimal degrees for the latitude data and the longitude data corresponds to an accuracy of 10(+) km at the equator). This first set of location information might be suitable, for example, for a weather application that is stored or executing on the wireless-communication device. In such an instance, the weather application can access an encrypted version of the first set of location information using a security key "K1" (as provided by the sequestered location IC component).

As illustrated in the middle of Fig. 3, a second set of location information is associated with an example security-access level 2. As illustrated, geolocation information (*e.g.*, latitude data and longitude data as computed by the sequestered location IC component) is at a granularity that corresponds to a "street" granularity (*e.g.*, a precision of 0.001 decimal degrees for the latitude data and the longitude data corresponds to an accuracy of 100(+) m at the equator). This second set of location information might be suitable, for example, for a navigation application that is stored or executing on the wireless-communication device. In such an instance, the navigation application can access an encrypted version of the second set of location information with the security key "K2" (as provided by the sequestered location IC component).

As illustrated at the right of Fig. 3, a third set of location information is associated with an example security-access level 3. As illustrated, geolocation information (*e.g.*, latitude data and the longitude data as computed by the sequestered location IC component) is at a granularity that corresponds to a "human" granularity (*e.g.*, a precision of 0.000001 decimal degrees for the latitude data and the longitude data corresponds to an accuracy of 100(+) mm at the equator). This third set of location information might be suitable, for example, for an emergency location service that is stored or executing on the wireless-communication device. In such an instance, the emergency location service can access an encrypted version of the third set of location information with the security key “K3” (as provided by the sequestered location IC component).

In some instances, the sets of location information can include identifiers that might be associated with an access point or network to which the wireless-communication device is connected. For example, the sets of location information might include a public mobile land network (PLMN) identifier associated with a base station or a universally unique identifier (UUID) associated with a beacon. The identifiers may, in some instances, identify a context of a location (such as a UUID of a beacon associated with a retail store).

In some instances, a security key may also include “time box” limitations for access to the encrypted set of location information. For example, the security key K1 (*e.g.*, the security key K1 of example Fig. 3) may provide the application (*e.g.*, the weather application) access to the first set of encrypted location information for a single occurrence or for a time period of 48 hours.

In some instances, generating the sets of location information can also include “fuzzing” data within the sets of location information. An example of fuzzing may include the sequestered location IC component applying offsets to either the latitude data or the longitude data. In such instances, the sequestered location IC component can include random number generator circuitry to support the fuzzing techniques.

Figure 4, below, illustrates example operations performed by the wireless-communication device including the sequestered location IC component. In some instances, the sequence of the example operations may be re-ordered. Also, in some instances, the operations or portions of the operations may be performed by an entity other than the wireless-communication device (*e.g.*, an access point or a cloud-based security service). Additionally, and in some instances, the operations may be associated with an application that is not stored on the wireless-communication device but is executing remote from the wireless-communication device (*e.g.*, a cloud-based application).

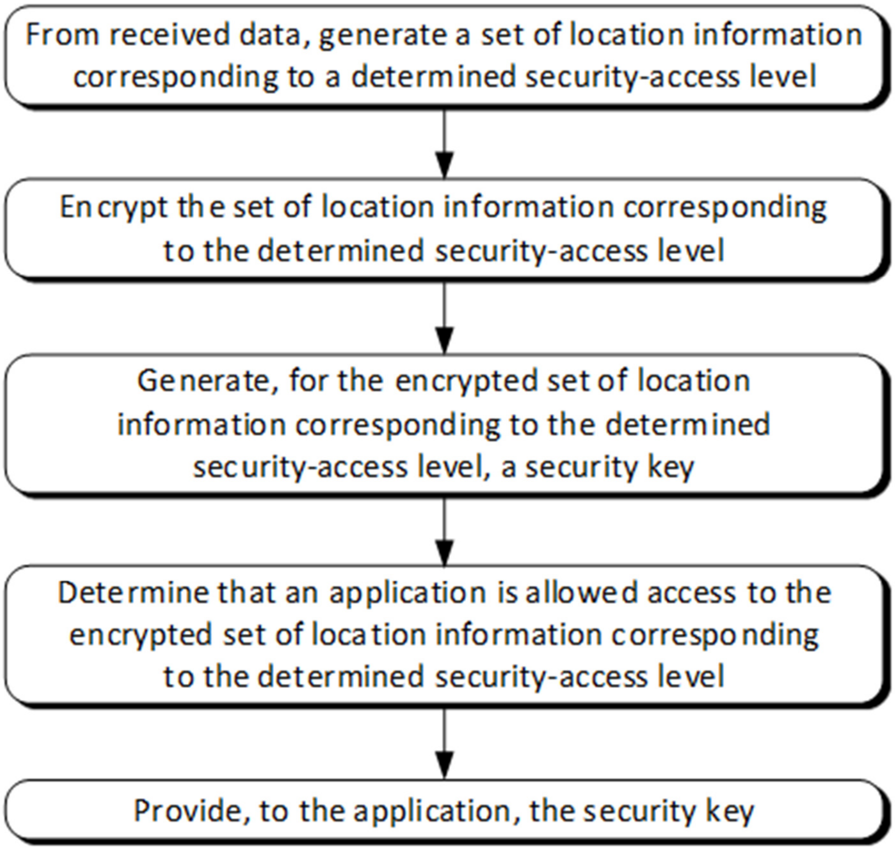
From received data, generate a set of location information corresponding to a determined security-access level
Encrypt the set of location information corresponding to the determined security-access level
Generate, for the encrypted set of location information corresponding to the determined security-access level, a security key
Determine that an application is allowed access to the encrypted set of location information corresponding to the determined security-access level
Provide, to the application, the security key

Fig. 4

Further to the systems and the techniques directed to managing access to location information, as described above, a user may be provided with controls allowing the user to make an election as to both if and when systems, programs or features described herein may enable collection of user information (*e.g.*, information about a user’s social network, social actions or activities, profession, a user's preferences, or a user’s current location), and if the user is sent content or communications from a server. In addition, certain data may be treated in one or more ways before it is stored or used, so that personally identifiable information is removed. For example, a user's identity may be treated so that no personally identifiable information can be determined for the user, or a user's geographic location may be generalized where location information is obtained (such as to a city, ZIP code, or state level), so that a particular location of a user cannot be determined. Thus, the user may have control over what information is collected about the user, how that information is used, and what information is provided to the user.

In conclusion, managing access to location information, using techniques and systems as described above, addresses privacy and security concerns associated with an application accessing location information available on a wireless-communication device. The wireless-communication device, using the sequestered location IC component, prevents unintended access to the location information by an application or other entity.