Technical Disclosure Commons

Defensive Publications Series

July 15, 2019

# Using Unlock Codes Associated with a User Profile to Access Applications

Saptarshi Bhattacharya

Shree Madhavapeddi

# Using Unlock Codes Associated with a User Profile to Access Applications

**Abstract:**

This publication describes systems and techniques directed to using unlock codes associated with a user profile to access applications that are available to a user device. As part of the systems and techniques, a profile manager application manages a user profile that governs access to the applications and associates an unlock code to the user profile. The user profile may be associated with a group of users or an individual user and may be configured through an interface of the user device, pre-determined based on a class of user, or retrieved from an existing account with a service provider that provides applications to the user device.

**Keywords:**

unlock password, unlock pattern, passcode, personal identification number (PIN), user profile, user group, access grant, application security, user account, authentication

**Background:**

A user device of today, such as a smart phone, is a personal device that can be shared amongst multiple users. Although the user device has evolved to become "hyper-personal" in terms of configurability (*e.g.*, user preferences, applications purchased or downloaded from an application store, settings), practices that govern access to applications are often generic.

Practices today, in general, grant access to the applications through one of several means that unlocks the user device, such as a password, a personal identification number (PIN), or facial recognition. Once access to the user device is granted, applications that are executing on the user device are accessible. Today, a user of the user device may unlock the user device and share it with a variety of persons such as a spouse, a child, a friend, or even a stranger needing to make an

urgent phone call. In unlocking the user device and granting access to the applications, the user creates a risk of an unintended use of the user device, a security risk, or a privacy risk.

Options to mitigate such risks typically are cumbersome and inefficient for the user, and require managing access to the applications at an "application-level" (*e.g.*, entering a combination of a username, a password, or a personal identification number (PIN) for an individual application once the user device is unlocked). It is desirable to develop systems and techniques which are effective at mitigating such risks while maintaining efficiencies for the user.

**Description:**

This publication describes systems and techniques directed to using unlock codes associated with a user profile to access applications that are available to a user device. As part of the systems and techniques, a profile manager application manages a user profile that governs access to the applications and associates an unlock code to the user profile. The user profile may be associated with a group of users or an individual user and may be configured through an interface of the user device, pre-determined based on a class of user, or retrieved from an existing account with a service provider that provides applications to the user device.

FIG. 1, below, illustrates accessing applications that are available to a user of the user device in accordance with one or more aspects. Although FIG. 1 illustrates the user device as a smart phone, the user device may be any device with computing capabilities and having access to multiple applications (*e.g.*, a tablet, a laptop computer, a wearable device, a desktop personal computer).

As illustrated at the left of FIG. 1, a user is inputting an unlock code through an interface of the user device. As illustrated at the right of FIG. 1, the unlock code is associated with a user

profile for a class of user (*e.g.*, "friend"). The user profile governs access to a subset of applications and features that are available to the user on the user device.

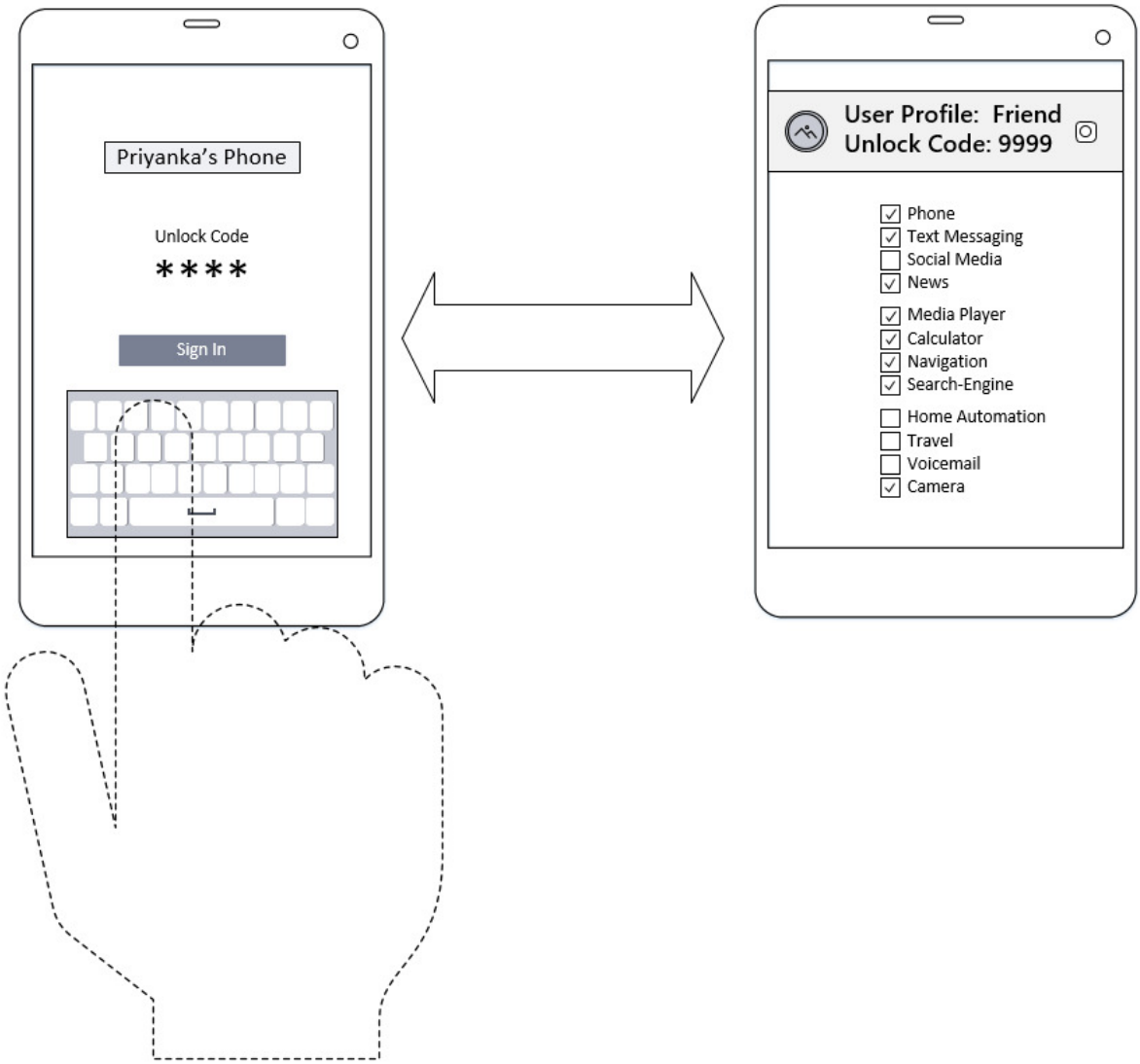


**FIG. 1**

The user profile may be configured through an interface of the user device, pre-determined based on a class of user, or retrieved from an account that grants access to applications that are available to the user device. In some instances, the applications may be stored and executed by

the user device, while in other instances the applications may be offered through a service provider (*e.g.*, a cloud-computing service, an internet-service).

FIG. 2, below, illustrates an example user device and elements of the user device that support accessing applications that are available to a user of the user device in accordance with one or more aspects.

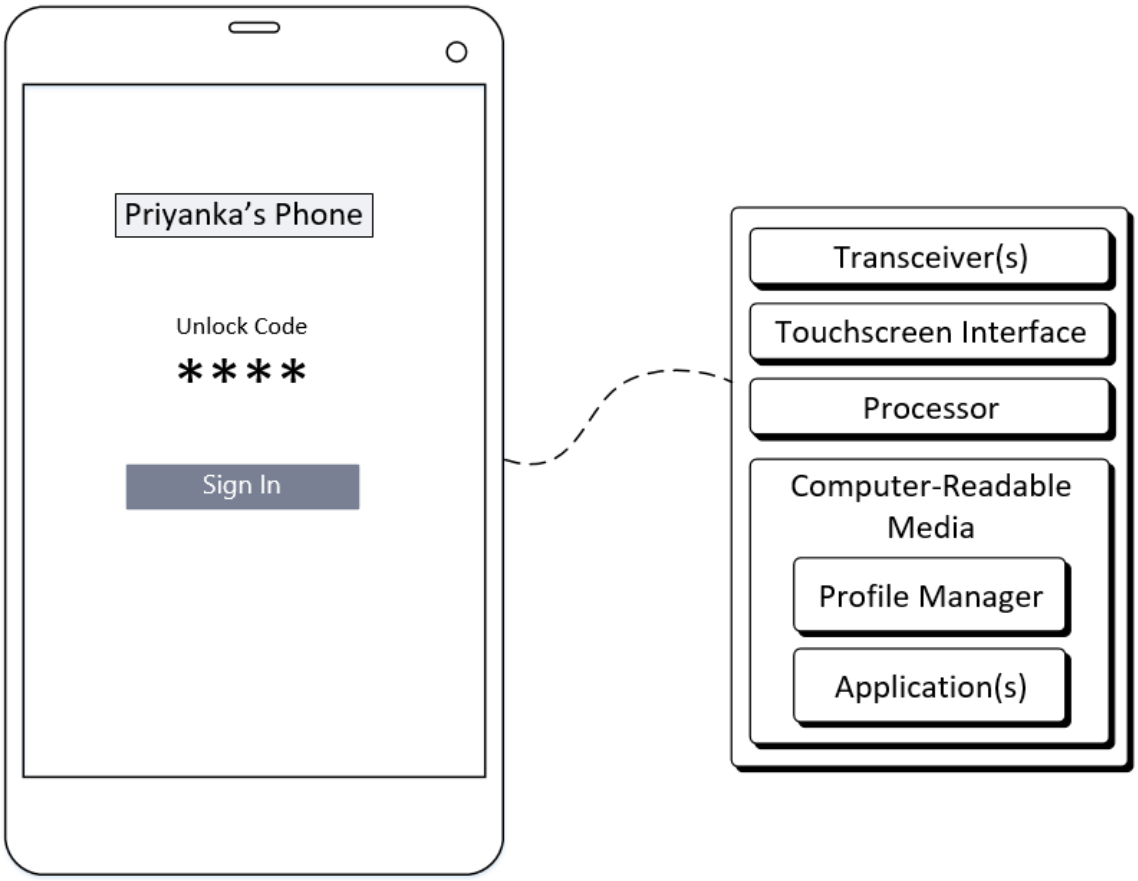


**Fig. 2**

The user device includes one or more transceivers for wirelessly communicating with networks through which the user device can access applications, download applications, or retrieve user profiles. The transceivers might include, for example, a wireless local area network (WLAN) transceiver, a fourth-generation long term evolution (4G LTE) transceiver, a fifth-generation new

radio (5G NR) transceiver, and so on. The user device also includes a touchscreen interface that can visibly render output and/or receive input, such as a Light Emitting Diode (LED) display or a Liquid Crystal Display (LCD) with touchscreen capabilities. The user device further includes a processor that performs basic logic to implement features of using an unlock code to grant access to applications available to a user device. The processor may be a single-core processor or a multiple-core processor composed of a variety of materials.

In addition, the user device includes a computer-readable medium (CRM) storing a profile manager application and one or more other applications (*e.g.*, a phone application, a text messaging application, a social media application, 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. While the profile manager application is illustrated as stored within the CRM, other implementations can include any combination of firmware, hardware, and/or software.

In general, the profile manager application, when executed by the processor, can direct the user device to perform a variety of operations directed to using unlock codes associated with a user profile to access applications that are available to the user device. Such operations may include receiving, through the touchscreen interface, inputs that correspond to the unlock code or other inputs that configure a user profile (*e.g.*, assign a name to a user profile, identify one or more users that might be in a "group" user profile, toggle applications that may be accessed, assign an unlock code to a user profile). In some instances, the user profile may correspond to a class of user, such as a "friend," "stranger," "spouse," "child," or "group." The user profile may, in other instances, correspond to an individual user.

The profile manager application when executed by the processor may also direct the user device to wirelessly communicate, using the transceiver, with a service provider that provides applications to the user device. In some instances, wirelessly communicating with the service provider may include retrieving the user profile from an existing account with the service provider. In an instance where the user profile is configured by the user of the user device (*e.g.*, not retrieved from the service provider), the profile manager application may direct the user device to wirelessly communicate the user profile (or portions of the data contained within the user profile) to the service provider so that the service provider might be able to aggregate data across multiple users to tailor a provided application to a user profile or type of user.

The profile manager application may, in some instances, store the user profile. The profile manager application may also implement a layer of security, such as a password that prevents a user (other than an owner of the user device) from accessing the user profile. The user profile manager application may also include a machine-learned model, where the machined-learned model is trained using machine-learning techniques. Such a machine-learned model may assist configuring the user profile based on historic use or access to the applications that are stored in the CRM of the user device or accessed through the service provider.

A first example scenario of using unlock codes to access applications that are available through the user device includes a friend of the user needing to make a call. Based on a "friend" user profile associated with an unlock code of "9999" (*e.g.,* the "friend" user profile may be pre-configured by the user or retrieved from a service provider), the user may input "9999" to the touchscreen display of the user device (*e.g.*, the screen may be "locked" from a timeout condition). The user device quickly loads a "friend" user profile that allows access to the phone application but prohibits access to other applications (*e.g.*, a social media application, a home automation

application, a voicemail application). The user may hand over the user device to the friend with confidence that allowed access to applications available to the user device is appropriate for the scenario.

A second example scenario of using unlock codes to access applications that are available through the user device includes a child wanting to use the user device for entertainment. Based on a "child" user profile associated with an unlock code of "1111," the user may input "1111" to the touchscreen display of the user device. The user device quickly loads a "child" user profile that allows access to a select group of gaming applications but prohibits access to other applications (*e.g.*, a media player application or other gaming applications may not be appropriate for the child).

A third example scenario of using unlock to access applications that are available through the user device includes a spouse wanting to use the user device to send a message using a social media application. Based on a "spouse" user profile associated with an unlock code of "8888," the user may input "8888" to the touchscreen display of the user device. Even though the owner of the user device does not have access to the spouse's social media application, the user device quickly loads a "spouse" user profile that the spouse has authorized in a social media account and logs the spouse into the social media application using the spouse's credentials.

The aforementioned systems and techniques are modifiable to accommodate mechanisms other than the use of the unlock code as described above. For example, as opposed to the unlock code, biometrics (facial recognition, audio recognition, fingerprint recognition) may be associated with a user profile to access applications that are available to the user device. Furthermore, in addition to governing access to applications, the aforementioned systems and techniques are also

modifiable to govern and disable types of notifications (*e.g.*, haptic notifications, audible notifications).

Further to the descriptions 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), 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.

**References:**

[1] US 20130333020 A1, Method and Apparatus for Unlocking an Electronic Device that Allows for Profile Selection, Assignee/Applicant Google Technology Holdings LLC, filed June 8, 2012.

[2] US 20150324564 A1, Dynamic Activation of User Profiles Based on Biometric Identification, Assignee/Applicant: Qualcomm Incorporated, Date of Filing May 7, 2014.

[3] How to Create Multiple User Accounts/Guest Mode on Android – Hide Apps, Photo, & Contact, Rudy Labs, November 25, 2017. https://www.youtube.com/watch?v=ygHBYw-OfzI.

[4] Add Members to Your Family Group, Microsoft Corporation, March 29, 2019. https://support.microsoft.com/en-in/help/12417/microsoft-account-add-members-to-family.