March 20, 2017

A Simplified Method For Securing Bluetooth Communication

Van Tu

Follow this and additional works at: http://www.tdcommons.org/dpubs_series

Recommended Citation
http://www.tdcommons.org/dpubs_series/429
A SIMPLIFIED METHOD FOR SECURING BLUETOOTH COMMUNICATION

ABSTRACT

Disclosed herein is a simplified Bluetooth communication mechanism that is secure and enables configuration of the security settings when paired with another Bluetooth device. Once paired, the system prompts the user to select either a normal or a secure access mode. The normal mode allows access to normal as well as sensitive or personal data available in the phone, while the secure access mode restricts access to sensitive data. Data access requests are handled by the system to permit access based on the security mode settings. This mechanism provides a single toggle that prevents personal data being synced to any publicly shared device. The system further allows the user to change mode of access as required. A typical use would be pairing a mobile phone with a rented car to leverage the car's audio system for improved sound quality of a GPS app running on the phone.

BACKGROUND

It is common for any Bluetooth enabled device, such as a car, to request access to personal data when paired with a mobile phone. Mobile phones and other similar devices typically have security mechanisms to help restrict access to personal and other sensitive data, which is usually implemented via granular permissions. Access to personal data is acceptable when the pairing is done with trusted devices but it is not recommended when pairing with temporary and publicly shared devices such as a rental car. The reason behind this being that the data synced to the temporary and publicly shared device may not be stored in a secure fashion and could be accessed by other users of the device. While mobile phones and other similar devices typically have security mechanisms to help restrict access to personal and other sensitive data, this is usually implemented via granular permissions that can be confusing to some users and complex to change when incorrectly configured.

DESCRIPTION
Disclosed here are a system and method of a Bluetooth pairing process that provides a simplified workflow for configuring the security settings of a mobile device when being paired with another Bluetooth device. The system presents the user with a sequence of prompts regarding the access granted to the Bluetooth device with respect to sensitive data such as contacts, message data, etc. FIG.1 illustrates the method of selecting Bluetooth pairing mode.

To begin with, a Bluetooth pairing process is initiated by the user between her phone and a shared device. Once the pairing is completed, the system prompts the user to select the pairing mode. The user can choose either a normal mode, or secure access mode. In normal mode, the user would be subjected to the usual phone settings allowing her to decide what data should be shared and made available to the paired Bluetooth device. Requests for that data would be granted or denied according to the configuration specified by the user. In secure access mode sensitive data stored on the phone is restricted. In an extreme case, the system may restrict the Bluetooth device to receiving data that is sent by the mobile phone with no ability to request data. On any further request made by the device to access phone data via Bluetooth, the phone grants access only if the user had selected the normal access mode, but prohibits access to any personal and other sensitive data if the user had chosen secure access mode. The system may provide the user the option of changing the chosen access mode, if desired.
An example use case is as follows:

1. The user initiates the Bluetooth pairing process between her phone and a shared device (e.g. a rental car).
2. The Bluetooth pairing process proceeds as usual.
3. After the pairing process is complete but before any data is exchanged between the devices, the user is prompted on her phone if the newly paired device should be paired in normal or "rental" mode.
4. If the user responds indicating pairing should be completed in normal mode then the phone will configure security settings as per its usual workflow.
5. Any further request made by the Bluetooth device regarding access to data in the phone is verified and accepted if the user has granted permission via the usual phone
settings. Such a request is denied if the user has selected secure/rental access mode, or if configured via the usual phone settings.

An example of phone data access by the device would be the pairing of the mobile phone with the car to leverage the car's audio system to improve the sound quality of a GPS app running on the phone.

The system and method illustrated provide a single toggle that prevents personal data being synced to any publicly shared device. The method illustrated also provides a simplified and clear workflow for securing communication with temporary and/or shared devices, thereby minimizing errors in the configuration of security policies that could leave personal and other sensitive information vulnerable to being viewed or stolen by others.