June 08, 2018

Internet of Things - Data Security and User Authentication Management

Ronald Heiby

INTERNET OF THINGS - DATA SECURITY AND USER AUTHENTICATION MANAGEMENT

Introduction

The present disclosure provides systems and methods to manage user authentication and data security for "Internet of Things" (IoT) devices. Some IoT devices may have limited safeguards for ensuring that a device is communicating with a legitimate authorized user. Additionally, some IoT devices may have limited protections to ensure that data in such communications is not monitored or intercepted by unauthorized third parties. The systems and methods of the present disclosure can provide for using encryption, such as public key infrastructure (PKI) key pairs, to enable user authentication and data security for IoT devices. The systems and methods of the present disclosure can enable handling authentication and security in a manner that gives the user increased control over IoT devices as well as the data generated, used, and/or stored by the IoT devices.

Summary

According to an aspect of the present disclosure, an IoT device can be provided with a public key portion of a PKI key pair belonging to an authorized user (e.g., owner, etc.) of the IoT device. The PKI key pair of the authorized user can be used to provide user authentication and data security when connecting to and/or communicating with the IoT device, for example, from remote computing devices such as a user computing device associated with the authorized user.

Detailed Description

According to an aspect of the present disclosure, systems and methods discussed herein can provide for user authentication, security, and privacy for "Internet of Things" (IoT) devices. The systems and methods can also provide improved user control over IoT devices and the data produced and/or stored by IoT devices. In particular, the systems and methods of the present

disclosure allow for providing an IoT device with a public key portion of a PKI key pair belonging to the owner of the IoT device to provide for user authentication and data security on the IoT device. The systems and methods of the present disclosure can provide for access to and communication with the IoT device to be secured using the PKI key pair, including command/control functions, configuration functions, data retrieval, and/or other communications necessary to the function of the IoT device and/or ancillary to it. In addition, an authenticated device owner can enable the IoT device to accept one or more additional public keys corresponding to other authorized users of the IoT device, to allow the one or more other authorized users to access and/or communicate with the IoT device.

According to an example implementation of the present disclosure, an IoT device can be configured to enable user authentication and data security during initial setup of the IoT device or during configuration of an existing IoT device. During setup of an IoT device, for example, after purchase by a user and/or after a "factory reset" of the IoT device, the IoT device can be provided with a public key portion of a PKI key pair associated with the user (e.g., owner) of the IoT device. This PKI key pair associated with the user/owner can then be used to provide user authentication when connecting to the IoT device and/or provide data security of communication with the IoT device and/or data stored at the IoT device. For example, use of the PKI key pair can secure communications with the IoT device including command and/or control functions, configuration functions, data storage and/or retrieval, other communications associated with the operation of the IoT device or ancillary to it, and/or the like.

In some implementations, the user/owner can configure the IoT device to accept one or more additional public keys associated with additional users for which the owner would like to provide access to the IoT device. The user/owner can configure the IoT device such that the one or more additional users have full access (e.g., same capabilities as the owner) or such that the

one or more additional users have a restricted set of capabilities with regard to operation of the IoT device. For example, an additional user can be restricted such that the additional user cannot provide for additional public keys to be accepted by the IoT device, cannot disable and/or replace a manufacturer/service provider public key, cannot change the capabilities of other users, cannot perform other operations restricted to an owner, and/or the like. In some implementations, each additional user can be configured with a differing set of capabilities.

According to another aspect of the present disclosure, in some implementations, an IoT device may not be provided with a public key associated with a manufacturer, service provider, and/or the like pre-installed on the IoT device (e.g., prior to purchase by user). In some implementations, a current manufacturer/service provider public key can be obtained by the owner and provided to the IoT device during or after setup/configuration of the IoT device by the owner. For example, the owner may provide the IoT device with a manufacturer/service provider public key to allow for software updates and/or other administrative operations to be performed by the manufacturer/service provider.

In some implementations, the use of particular manufacturer/service provider PKI key pairs may be determined by the type of IoT device, such that some IoT devices may be provided with a standard public key associated with a manufacturer/ service provider while other IoT devices may be provided with a specific manufacturer/ service provider public key for that device (e.g., a unique key for specific device. etc.). For example, with some IoT devices (e.g., security cameras, etc.), a manufacturer/service provider may provide an additional PKI key pair for use with data and/or communication associated with the specific IoT device (e.g., security camera feed, etc.). The manufacturer/service provider can provide the additional PKI key to an owner of the IoT device (e.g., security camera, etc.). The owner can install the additional public key on the IoT device (e.g., security camera, etc.), for example, to provide for encrypting data

stream content intended to be provided to and/or stored by the manufacturer/service provider (e.g., stored on server(s) associated with the manufacturer/service provider, etc.), thereby allowing the data associated with the owner's device to remain secure. In some implementations, the data may be encrypted such that it is kept secure even from access by the manufacturer/service provider. In some implementations, the corresponding key of the key pair can be maintained by the IoT device owner, such that it can be used by the owner if the data held securely by the manufacturer/service provider needs to be retrieved.

According to another aspect of the present disclosure, in some implementations, an owner can disable and/or replace keys associated with a manufacturer/service provider, for example, to guard against the impact of a disclosure of private keys managed by the manufacturer/service provider. For example, a key associated with a manufacturer/service provider may be disabled, by an owner and/or the manufacturer/service provider, as soon as a disclosure of a corresponding private key is detected. A new key associated with the manufacturer/service provider can be provided to the owner and installed on an IoT device, for example, following appropriate verification and/or validation of the new key.

According to another aspect of the present disclosure, in some implementations, when an IoT device performs a "factory reset" or the like, all keys associated with an owner, additional users, manufacturer/service provider and/or the like, held by the IoT device can be discarded. In some implementations, an application used to communicate with and/or control an IoT device (e.g., installed/operating on a user computing device, etc.) can optionally maintain backup copies of the keys associated with the owner, additional users, manufacturer/service provider, and/or the like, as well as one or more settings previously configured for the IoT devices, for example, to provide continuity of operation in event of a device failure, device replacement, and/or the like.

According to another aspect of the present disclosure, in some implementations, private key(s) associated with an owner, additional user, and/or the like, can be stored in an encrypted form on a user computing device (e.g., smartphone, tablet, computer, etc.), associated with the owner, additional user, and/or the like, that is being used to communicate with and/or control the IoT device. In some implementations, decryption of the key can be controlled by one or more security features of the user computing device (e.g., smartphone, tablet, computer, etc.), such as for example, passwords, biometrics, and/or the like, thereby reducing a risk of attack on the IoT device by malware that may be operating on the user computing device.

As described herein, the systems and methods of the present disclosure can provide improved protection and flexibility in the face of a plethora of attack vectors, such as attacks from other machines on a local network that may have been compromised by malware, attacks from malware on the computing device intended to control the IoT device, attacks on a manufacturer's infrastructure, demands upon a manufacturer for user data, and/or the like.

Figure 1 depicts an example system 100 according to an example implementation of the present disclosure. Figure 1 illustrates one example computing system that can be used to implement the present disclosure, other computing systems can be used as well. The system 100 can comprise one or more user computing devices, such as user computing device 102, one or more IoT devices, such as IoT device 140, coupled over one or more networks, such as network 180. Additionally, in some implementations, the system 100 can include one or more remote devices (not shown), such as server computing devices operated by a manufacturer, service provider, and/or the like, that can communicate with the IoT device 140 over one or more networks to provide services associated with the IoT device 140.

The user computing device 102 can include one or more processors 104 and one or more memories 106. The one or more processors 104 can be any suitable processing device and can

be one processor or a plurality of processors that are operatively connected. The memory 106 can include one or more non-transitory computer-readable storage mediums, such as RAM, ROM, EEPROM, EPROM, flash memory devices, magnetic disks, etc., and combinations thereof. The memory 106 can store data 108 and instructions 110 which are executed by the processor 104 to cause the user computing device 102 to perform operations, including one or more of the operations disclosed herein.

According to an aspect of the present disclosure, the user computing device 102 can include an authentication/security system 112 that can implement features of the present disclosure. For example, the authentication/security system 112 can use encryption, such as through the use of PKI key pairs, to authenticate the user computing device as belonging to an authorized user associated with the IoT device 140, to secure communications between the user computing device 112 and the IoT device 140, and/or the like. The authentication/security system 112 can also provide for establishing and/or managing authentication and security for an IoT device, such as by providing for the management of key(s) of one or more PKI key pairs installed on an IoT device.

The user computing device 102 can also include one or more input/output interface(s) 114. One or more input/output interface(s) 114 can include, for example, devices for receiving information from or providing information to a user, such as through a display device, touch screen, touchpad, mouse, data entry keys, an audio output device, a microphone, haptic feedback device, etc. The user computing device 102 can also include one or more communication /network interface(s) 116 used to communicate with one or more systems or devices, including systems or devices that are remotely located from the user computing device 102.

The IoT device 140 can include one or more processors 142 and one or more memories 144. The one or more processors 142 can be any suitable processing device and can be one

processor or a plurality of processors that are operatively connected. The memory 144 can include one or more non-transitory computer-readable storage mediums, such as RAM, ROM, EEPROM, EPROM, flash memory devices, magnetic disks, etc., and combinations thereof. The memory 144 can store data 146 and instructions 148 which are executed by the processor 142 to cause the IoT device 140 to perform operations, for example, such as to implement operations as discussed herein. The IoT device 140 may include an authentication/security system 150 that can implement features of the present disclosure. For example, the authentication/security system 150 can store, use, and/or manage one or more public key(s) of one or more PKI key pairs associated with authorized users (e.g., an owner, other user, manufacturer, service provider, etc.) of the IoT device 140. The authentication/security system 150 can provide for using PKI key pairs to authenticate one or more remote devices (e.g., user computing devices, etc.) as belonging to an authorized user associated with the IoT device 140, to secure communications between one or more remote computing devices (e.g., user computing device 112, etc.) and the IoT device 140, and/or the like.

The IoT device 140 can also include one or more communication/network interface(s) 152 used to communicate with one or more systems or devices, including systems or devices that are remotely located from the IoT device 140, such as user computing device 102, for example. In some implementations, the IoT device 140 can also optionally include one or more input/output interface(s) 154.

Figure 2 depicts a flowchart illustrating example operations 200 for providing user authentication and data security management in accordance with aspects of the present disclosure. Although operations 200 are shown and described in a particular order for purposes of illustration and discussion, the operations are not limited to the particularly illustrated order or arrangement and certain operations can be performed in different orders or simultaneously.

The operations begin at block 202 where setup and/or configuration of an IoT device is initiated. For example, a user (e.g., owner, etc.) may be installing a new IoT device and they may desire to configure the IoT device to provide for user authentication and data security. Alternatively, a user (e.g., owner, etc.) may wish to configure an existing IoT device to provide for user authentication and data security.

At block 204, the IoT device is provided with a public key of a PKI key pair associated with the user (e.g., owner, etc.). At block 206, the IoT device is configured to enable using the PKI key pair associated with the user (e.g., owner, etc.) for user authentication to connect and/or communicate with the IoT device from a remote device (e.g., user computing device, etc.). For example, access to and communication with the IoT device can be secured using the PKI key pair, including command/control functions, configuration functions, data retrieval, and/or other communications necessary to the function of the IoT device and/or ancillary to it.

Optionally, at block 208, the IoT device can be provided with public key(s) for PKI key pair(s) associated with one or more additional users to allow additional user(s) to access, communicate with, and/or operate the IoT device. Optionally, at block 210, the IoT device can be configured to modify the capabilities of the authorized additional user(s) with regard to access and/or control by the authorized additional user(s). For example, an additional user may not be able to provide for additional public keys to be accepted, not be able to disable and/or replace a manufacturer/service provider key, and/or any other operations that may be desired to be restricted. In some implementations, the IoT device can be configured with different restrictions for each additional user.

In some implementations, the IoT device can alternatively be provided with public key(s) associated with one or more additional user(s) (e.g., block 208) and/or configured to modify the capabilities of one or more authorized additional users (e.g., block 210) at a later point in time

(e.g., separate from and after the operations of blocks 202-206). For example, after the IoT device has been configured to use the PKI key pair associated with the user (e.g., owner, etc.) and put into service, the IoT device user/owner can go back and update the IoT device configuration by providing public key(s) associated with additional user(s) to the IoT device and/or modifying the capabilities of authorized additional user(s) with respect to the IoT device. Additionally, modifying the capabilities of authorized additional user(s) can be performed separately at a later time after the IoT device has been configured with the key(s) associated with the additional user(s).

Figure 3 depicts a flowchart illustrating example operations 300 for user authentication and data security management in accordance with aspects of the present disclosure. Although operations 300 are shown and described in a particular order for purposes of illustration and discussion, the operations are not limited to the particularly illustrated order or arrangement and certain operations can be performed in different orders or simultaneously.

The operations begin at block 302 where a user (e.g., user computing device, etc.) requests to connect with an IoT device. For example, a user may wish to access an IoT device to control operation of the IoT device, retrieve data from the IoT device, and/or the like. At block 304, the IoT device performs authentication operations with the user using a PKI key associated with the user (e.g., the public key of the user stored at the IoT device, etc.).

At block 306, in response to a successful authentication of the user, the IoT device establishes communication with the user (e.g., user computing device). At block 308, the desired (e.g., authorized) operations can be performed at the IoT device by the authenticated user.

Figures

Figure 1

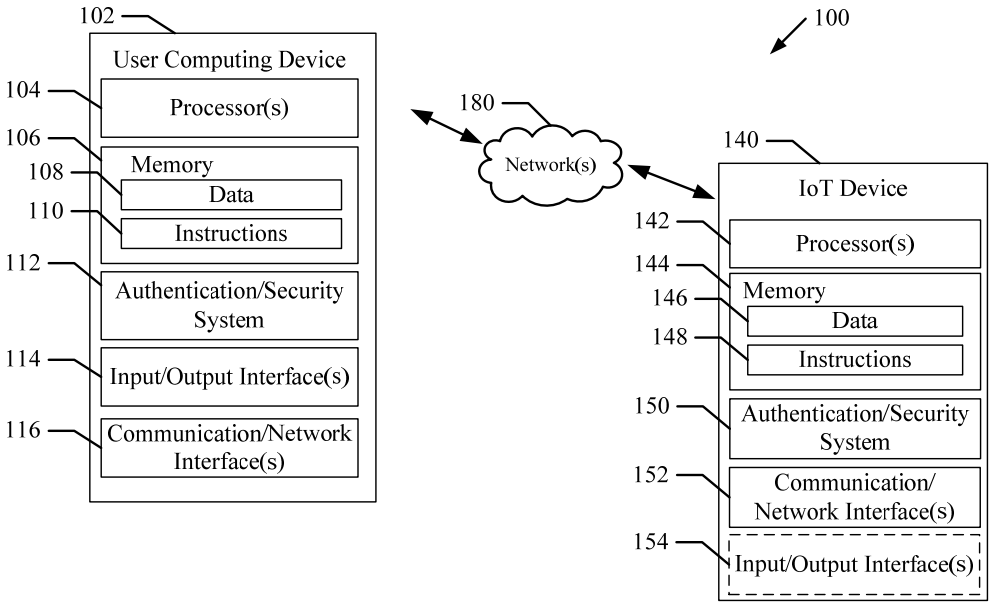


Figure 2

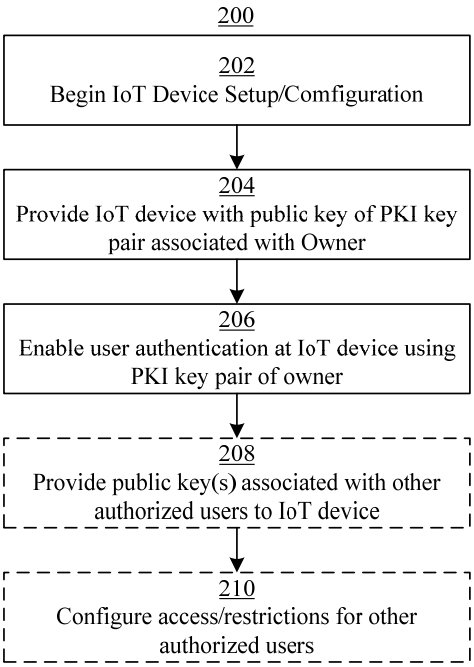
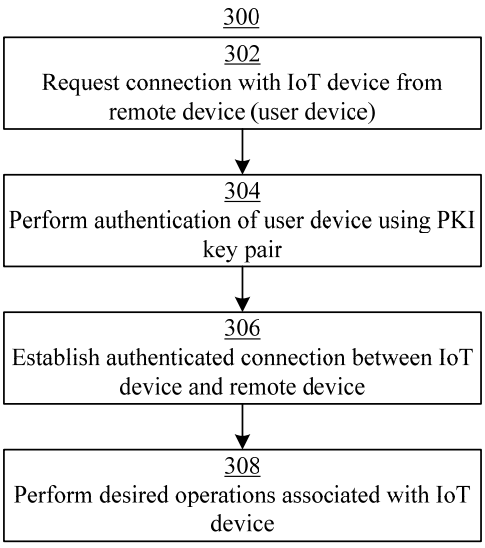


Figure 3



Abstract

The present disclosure describes systems and methods that provide for managing user authentication and data security for “Internet of Things” (IoT) devices. More particularly, the present disclosure provides for providing an IoT device with a public key portion of a PKI key pair belonging to an authorized user (e.g., owner, etc.) of the IoT device. The PKI key pair of the authorized user can be used to provide user authentication and data security when connecting to and/or communicating with the IoT device. The systems and methods of the present disclosure can provide for improved user control over IoT devices and the data generated, used, and/or stored by IoT devices.