Smartphone Assisted Setup for Headless Devices

Erdi Chen

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

Recommended Citation
https://www.tdcommons.org/dpubs_series/3219

This work is licensed under a Creative Commons Attribution 4.0 License.
This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.
Smartphone Assisted Setup for Headless Devices

ABSTRACT

This disclosure describes techniques for secure setup and/or configuration for headless devices using a smartphone or other available device. A smartphone is connected to a headless device via USB and is utilized to perform setup and debug operations related to the headless device. The headless device advertises itself as an accessory device and provides a device ID and vendor ID to the smartphone. An app on the smartphone is launched with the headless device identifier as parameters. Additional communication between the headless device and the smartphone is performed over the connection using a custom protocol or encapsulated HTTP. The internet connection provided by the smartphone is utilized to fetch an authentication token from an external service that is passed to the headless device to perform authenticated setup/provisioning. The device can perform authentication with a shared secret or cryptographic signature as part of initial configuration and/or set up.

KEYWORDS

- Headless device
- Inputless device
- Internet of Things (IoT)
- Device setup
- Device configuration
- Encapsulated HTTP
- HTTP Tunnel
BACKGROUND

Headless devices such as Internet of things (IoT) devices, WiFi routers, printers, airport kiosks, etc. exclude peripherals such as display, keyboard, or other input/output devices. Many headless devices require initial setup, e.g., to connect to available WiFi or Ethernet networks to enable the devices to connect to cloud service(s) for remote device management. Troubleshooting the setup for headless devices can pose challenges due to the absence of peripheral devices for input and/or output.

Headless devices can use unencrypted data transmission for configuration. For example, WiFi routers utilize network passwords or QR codes printed on a label affixed to the device for configuration and initial setup. Broadband routers/modems use a web-based user interface when connected to an internal network. Some headless devices utilize audio encoded data transmission for configuration, some devices use Bluetooth (or other local wireless network) for initial setup, and some devices use a serial port for troubleshooting. However, these mechanisms do not typically enable the use of encryption, authentication, etc.

DESCRIPTION

A configuration process for headless devices that can enable the use of encryption and other security mechanisms can enable easy device setup without sacrificing device or user security. This disclosure describes techniques for secure set up and/or configuration for headless devices. Per techniques of this disclosure, a smartphone or other device is connected to a headless device over a USB connection and is utilized to enable users to perform setup and debug operations related to the headless device.
Fig. 1 illustrates an example of smartphone assisted headless device configuration, per techniques of this disclosure. In this illustrative example, a headless device (104) is connected to a smartphone (102) via a USB cable (106) that connects the respective USB ports. The smartphone enables a user to access the headless device to view and update configuration settings, or for other functions. The connection via a USB cable also establishes a proof of physical presence (and access to) of the headless device and thus provides physical security control for configuration of the headless device.
Fig. 2: Communication set up between smartphone and headless device

Fig. 2 illustrates an example process for smartphone assisted configuration of a headless device, e.g., an IoT device. The headless device is physically connected (210) to a smartphone (or other device) via their USB host ports using a USB cable (or other hardware connection that offers similar features). The headless device advertises itself (220) as an accessory device on the USB Connection using a communication protocol that is compatible with the smartphone.

Upon detecting the headless device, an app is launched (230) on the smartphone. Parameters for launch of the app include a device ID and vendor ID associated with the headless device. A variety of ways can be used for communication between the headless device
and the smartphone. For example, a custom protocol can be implemented (240, Option 1) to facilitate transmission of data packets between the smartphone and the headless device. Alternatively, encapsulated HTTP can be utilized (250, Option 2) to run an HTTP server on the headless device and encapsulate HTTP over accessory protocol packets. On the smartphone side, the app can create a HTTP-compatible view and feed the HTTP traffic that originates from the headless device (260).

By utilizing the communication protocols, the smartphone can act as an intermediary to enable communication between the headless device and external networks (for example, ethernet, cloud networks, etc.) for configuration, debug, etc. A vendor associated with the headless device can provide a custom app that can be installed in the smartphone. Alternatively, HTTP content can be served by different headless devices to an existing app that is already available on the smartphone in conjunction with a vendor ID/device ID pair that identifies the headless device.

An internet connection provided by the smartphone is utilized to fetch an authentication token from a cloud service that is passed to the headless device to perform authenticated setup/provisioning even when the device does not have an internet connection. The device can perform authentication with a shared secret or cryptographic signature as part of its initial configuration and/or setup. The described techniques can also be utilized in enterprise applications for multiple headless devices.

CONCLUSION

This disclosure describes techniques for secure setup and/or configuration for headless devices using a smartphone or other available device. A smartphone is connected to a headless device via USB and is utilized to perform setup and debug operations related to the headless device.
device. The headless device advertises itself as an accessory device and provides a device ID and vendor ID to the smartphone. An app on the smartphone is launched with the headless device identifier as parameters. Additional communication between the headless device and the smartphone is performed over the connection using a custom protocol or encapsulated HTTP. The internet connection provided by the smartphone is utilized to fetch an authentication token from an external service that is passed to the headless device to perform authenticated setup/provisioning. The device can perform authentication with a shared secret or cryptographic signature as part of initial configuration and/or set up.

REFERENCES