Best In Class Bluetooth

A Perspective

January 3, 2023

Overview

Afero believes that IoT products should be simple and easy to use, have fast and frustration free onboarding, and be secure end-to-end from the factory, to the end product, to the cloud, and to the mobile app. To accomplish this, Afero has invented many solutions to solve these problems. Through this effort, Afero has created a patented suite of technologies using Bluetooth Low Energy (BLE) to enable the simple and fast onboarding and setup of new IoT products. This whitepaper describes how Afero-powered products use Bluetooth Low Energy (BLE) for secure, rapid, and pain free setup and onboarding.

The traditional use of Bluetooth technologies has resulted in significant problems and issues for end users, which in turn has resulted in significant customer support calls and product returns. These problems are due to the complexities of Bluetooth pairing and the way most IoT products handle the setup and configuration of new devices. The table below is a quick overview of some of the main issues surrounding Bluetooth in IoT products, with additional details down below.

Issues	Problem Statements	Afero's Solution
Pairing	Traditional Bluetooth pairing causes confusion and problems for the average non-technical user. When it does not work, it is nearly impossible to troubleshoot and fix. In addition, pairing is device specific and not portable.	Afero-powered products do not need or use traditional Bluetooth pairing. In addition Afero-powered products are tied to a user's account and can follow the user regardless of the device they use.
Onboarding	Getting devices connected to the network and to a user's account is called onboarding. This the cause of most issues and end user frustration. Devices without screens and keyboards (e.g., lights, fans, switches, etc) can be very challenging to set up. To get most IoT products onboarded requires the user to first Bluetooth pair the device to their phone and then go	Afero-powered products do not need or use traditional Bluetooth pairing. They also do not require users to connect directly to the device. Meaning, the device does not create its own WiFi network that the user has to connect to. Afero's unique technology streamlines all of this complexity.

	through a process to connect their phone to the device’s WiFi access point (SoftAP). During this process the user needs to push the WiFi credentials through this connection, but this uses the WiFi networks that the phone can see, not what the end device can see. This can cause a lot of problems for end users. Once that is done, the end user can disconnect from the device’s WiFi access point and rejoin their normal WiFi network, after which they can attempt to connect back to the device to finish the process of configuring. But this is only possible if everything above worked correctly. If not, it is really challenging to troubleshoot and fix. It usually results in users going through a factory reset and starting all over. So many things can go wrong during this process and end users have no way of understanding how to make it work.	Once the end user scans the QR code the device is automatically added to the user's account and can instantly be configured and used. Another key point with Afero-powered products is they use the WiFi networks that they can see, not what the user’s phone can see. This greatly simplifies the onboarding experience for users.
Security	The Bluetooth Low Energy (BLE) stack has had multiple security vulnerabilities in their key exchange mechanisms and pairing mechanism (e.g., KNOB atack, BLESA, etc).	Because of the way Afero uses BLE, Afero-powered products are immune to these sorts of attacks.
Privacy	The Bluetooth encryption layer is well documented as being not very secure.	Afero-powered products do not use the Bluetooth encryption layer, but rather use a full enterprise grade encryption stack, see down below.

BLE the Afero Way

In 2014 Afero recognized there were serious problems with the security, privacy, and onboarding of IoT devices. Afero also discovered significant problems with using traditional Bluetooth pairing mechanisms and devices running versions of SoftAP. These issues have caused a lot of problems for end users and have hindered the adoption of IoT products and the goal of smart and connected homes. Afero set out to change this, not by simply combining various opensource technologies, but rather by innovating and creating new world class technologies. The Afero ecosystem and architecture is backed by 93 patents and millions of successfully deployed and active devices.

Encrypted Sessions

All Afero-powered products use mutually authenticated end-to-end encryption when connecting to the Internet. Each time a device connects to the internet it uses a unique session key that is established through strong internet standard cryptographic primitives like elliptical curve Diffie-Hellman (ECDH). The traffic is then encrypted with that unique session key using AES-GCM. This gives devices and their traffic perfect forward secrecy (PFS). These sessions are similar to a point-2-point VPN and can be established over non TCP/IP protocols and communication channels. This allows Afero products to work seamlessly over Bluetooth Low Energy (BLE) as well as WiFi.

Bluetooth Pairing

Afero-powered products do not use or need traditional Bluetooth pairing or the weak Bluetooth encryption layer. All traffic is encrypted, but uses strong encryption as described above.

This technology is made possible through an Afero proprietary BLE Profile that sits on top of the standard BLE GATT (Generic ATTribute) layer of the BLE communication stack. This BLE Profile allows the Afero system to securely identify and connect with Afero-powered BLE products without needing to use traditional Bluetooth pairing.

Problems with Bluetooth pairing are a common source of user frustration and customer support calls. With millions of Afero-powered products in existence today, Afero has the data to demonstrate that Afero's approach results in a tenfold (10x) decrease in customer support calls/product returns.

Onboarding and Setup

All Afero-powered products use Bluetooth Low Energy (BLE) with proprietary Bluetooth profiles to simplify and speed up the connectivity, setup, and onboarding of new devices. This provides significant value over competing IoT solutions. This design makes Afero-powered products immune to traditional customer Bluetooth pairing problems, weak Bluetooth encryption, and Bluetooth man-in-the-middle vulnerabilities.

WiFi Setup

If a device needs WiFi connectivity, Afero-powered products can use the BLE layer between the user's phone or computer to negotiate and set up the WiFi connections on the device. Doing it this way ensures that the WiFi network selected (SSID and BSSID) are ones that the product can actually see, not what the user’s phone or computer can see. This is a huge advantage compared to other IoT based products on the market today and reduces a lot of post installation customer support calls.

Any Internet Connection

All Afero-powered products are able to tunnel encrypted traffic through any internet connection that is available to them. This includes WiFi connections and BLE via the user’s device (e.g., phone, tablet, computer, etc).

Direct to Device Connection and Failover

Afero-powered products with more than one communication stack (e.g., WiFi + BLE) can automatically reroute traffic over any network connection that is available. This networking design is especially useful in situations where a WiFi enabled device is no longer able to talk to the WiFi network (passphrase has changed, WiFi access point is down, internet router is down, etc). This ensures that the user can continue to access and control their devices, even if WiFi is down. When a network connection problem like this occurs the user will see a notification on their phone, at this point they simply need to come into range of the BLE device and the product will automatically connect to the internet through the user’s phone. All of this happens seamlessly and without compromising security or data privacy. This proprietary and patented technology is called Afero BLE Failover.

Conclusion

Afero-powered products do not suffer from the problems that impact most IoT products when using Bluetooth technologies. Because of this innovation, Afero-powered products have greatly improved the experience for end users and have helped Afero customers see a 10x decrease in customer support calls and product returns.

Author
Bret Jordan CISSP - Afero

Disclaimer

The content contained in this document is correct as of January 2023 and represents the status quo at the time it was written. The Afero security policies, procedures, systems, and solutions may change going forward as we strive to continuity improve the protections for our customers.