Technical Article

How Bluetooth® 4.2 Can Help Enable Product Security

With the release of the new *Bluetooth*® low energy software development kit (SDK), BLE-Stack 2.2 software, TI is offering a completely new level of security as indicated in the **Bluetooth 4.2 Core Specification**. But what exactly do these security improvements mean, and why are they being rolled out now?

There are two independent security upgrades that come with Bluetooth 4.2:

1. Secure pairing
2. Privacy

Secure pairing

Pairing is the process of setting up a connection between two Bluetooth devices that need to exchange information through some form of defined relationship. In many cases, this information is of little value to other parties who might be within receiving range of the RF packets being exchanged over the connection. But as Bluetooth moves from the smartphone ecosystem to the Internet of Things (IoT), where home and building automation as well as automotive and medical/health applications require the transfer of information that could lead to serious consequences if intercepted or altered by attackers, it becomes vital to offer a secure connection where the confidentiality and the integrity of the data is ensured by adherence to a common standard. This is what Bluetooth 4.2 brings to the table.

Securely encrypting the packets transmitted between two devices in a connection is quite straightforward as long as they both share a secret key. AES-CCM is the encryption technique used in both Bluetooth 4.2 and earlier standards. But this technique does not provide a way for two devices that are being paired by their owner to exchange a secret key that cannot be read by passive eavesdroppers several meters away. This is the big improvement in Bluetooth 4.2, where the Elliptic Curve Diffie-Hellman (ECDH) key agreement protocol is introduced. ECDH is today's gold standard in key agreement schemes, and allows two parties with no previously shared information to establish a secret key that is known to them only. Sniffers who have observed the exchanged packets will not be able to "guess" the shared key. This is made possible by the asymmetric key properties of Elliptic Curve Cryptography (ECC), which allows both parties to have one public key and one private key. A packet encrypted by device 1's private key and device 2's public key can only be decrypted by device 2, using device 2's private key and device 1's public key. Device 2 will then know that the packet could only have come from device 1, and could not have been read by anyone else. The same method is used to transmit from device 2 to 1, using device 2's private key and device 1's public key. This is still an anonymous exchange and does not prove the identity of device 1 or 2. Identity proof, if needed, can be added at the application level by letting device 1 and 2 exchange certificates that prove their identity based on their public keys.

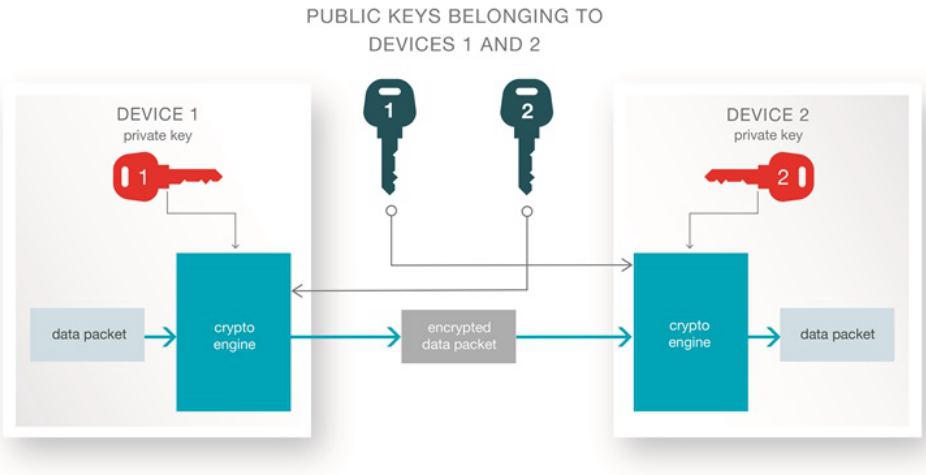

Figure 1. Device 1 sends an authenticated and private message to device 2. Only device 2 can read it, and only device 1 could have sent it, as it needs device 2's private key to be decrypted, and was encrypted using device 1's private key

Privacy

In order to enable pairing with new devices, Bluetooth low energy peripherals will send out connectable advertisements with regular intervals. If they stop transmitting advertisements, they will never be able to establish a new connection again, so this activity is continued throughout the lifetime of the device. These advertisements contain the information a scanning central (e.g. a smartphone) needs to initiate a pairing process with that peripheral. That includes the Bluetooth Device address (BD address), which uniquely identifies that peripheral. This makes it very simple to track peripheral devices and log their position. Passive observers need only to listen for advertising peripherals, log the BD addresses and forward them to a data processing center that receives BD addresses from many observers. In this way, peripherals can be tracked anywhere an organization has set up observers. And since more and more of these peripherals are constantly worn by their owners, it is effectively the owner who is tracked and not just the peripheral. For retail chains, this can help them analyze how customers move around in their stores or even between stores. This collection and use of information is in most cases harmless, but the ease with which this type of tracking can be set up means that there are many organizations that will be capable of doing it, as they do not need to be particularly resourceful or technologically advanced.

This problem is solved with the privacy enhancements in Bluetooth 4.2 and the solution is quite simple: The Bluetooth 4.2 peripheral devices regularly choose a new and random BD address to use in their advertisements. Only after a connection is set up with a trusted master, is the peripheral device's real BD address disclosed. Observers wanting to track advertising Bluetooth 4.2 peripherals will have no way of resolving the real BD address based on the randomly chosen advertising address and tracking the random address will only last until the device choses a new one.

Summary

Bluetooth 4.2, as implemented in TI's BLE-Stack 2.2, offers significantly improved security and privacy, allowing Bluetooth developers to deploy devices that can enter secure connections without being intercepted or tracked by observers. To incorporate these security enhancements into your Bluetooth product, check out TI's SimpleLink™ Bluetooth low energy CC2640 wireless microcontroller (MCU).

Where to Go Next?

- Learn more about the CC2640 wireless MCU.
- Download the new BLE-Stack 2.2 here.
- Read more about BLE-Stack 2.2 in our latest blog post.
- Order the Bluetooth low energy LaunchPad™ development kit.
- Check out our online training with SimpleLink Academy.
- Got a question? Ask our experts.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265