Security Best Practices for Bluetooth-Enabled Devices with Embedded Digi XBee Modules

Bluetooth in its various forms is used every day by many different types of wireless devices. For this reason, developers incorporating Bluetooth or Bluetooth Low Energy (BLE) into connected product designs must ensure these devices are secure from tampering and cyberattacks.

Digi provides Bluetooth support in Digi XBee® 3 modules. This paper provides guidance on the threats that affect Bluetooth and BLE-enabled devices as well as some best practices for securing your devices against them.

As with all devices that may be subject to either hacking or other breaches, such as unintentional configuration changes, the most important security measure is to make it difficult for your devices to be accessed by unauthorized personnel. Employ a multi-pronged approach to device security so there is no single point of failure, and to address both physical threats to devices as well as remote access.

Wireless Access Use Cases

Let's start by looking at a few scenarios in which employees managing wireless devices must be able to access them in order to configure, update or manage those devices without enabling unauthorized access. Here are some common use cases:

- A network manager with a Digi XBee 3 module embedded in a city streetlight or other inaccessible location needs to perform a factory reset on the device and still be able to configure it over the BLE interface. The customer wants to ensure they are not locked out of the device, requiring a non-BLE method of recovery.
- A field engineer needs to be able to configure the device over BLE, including resetting it to factory default.
- A technician with a mobile phone and customized application needs to configure an XBee's network settings over BLE, including most or all AT commands, to apply configuration or personalization updates during deployment, as well as to diagnose and repair the Digi XBee 3 module after initial deployment.

For more information, visit:

www.digi.com

877-912-3444 | 952-912-3444

In each of these scenarios, it is important that authorized personnel can reliably access those devices, and that only the authorized personnel be allowed to access them. In addition to the security features built into the devices, your organization should have security protocols in place such as secure password management and authentication to support the most robust security.

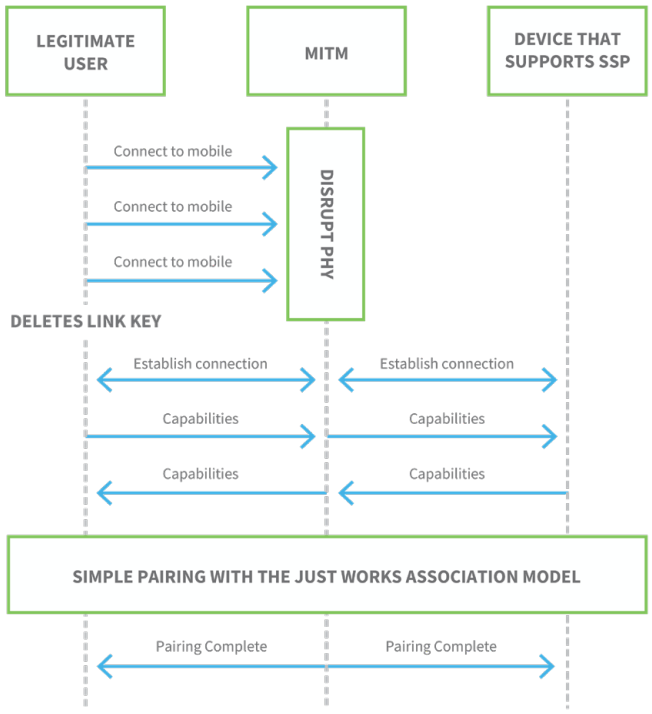
Bluetooth Security Issues During the Pairing Process

For a brief overview of Bluetooth security, see the Bluetooth Security tab in this FCC guide.

There are two main security issues with the pairing process of BLE devices:

- Passive eavesdropping
- Man in the middle (MITM)

With passive eavesdropping, there is a third device (attacker) that listens to the data being exchanged between the two devices (victims). The primary way Digi XBee modules overcome this is by securely authenticating the client device using the Secure Remote Password (SRP) algorithm, and then subsequently encrypting the data being sent over BLE using standard AES-256 encryption and the securely derived session key. SRP does not send the unique password over the air, which means a malicious actor cannot use sniffing to uncover the password.



Man in the middle (MITM) attacks happen when a third device impersonates a legitimate device and coerces the victim device(s) into connecting to the malicious device. In the diagram above, Alice and Bob are the legitimate devices and Malorie is the malicious device. When Malorie connects to Alice and Bob, Malorie can route information between the other two connected devices. Malorie can also inject false data as well as remove data before it reaches either Alice or Bob. The Digi XBee 3 module mitigates this because the devices are paired together using an SRP handshake that authenticates both ends of the communication.

Secure Remote Password in Digi XBee 3 Modules

Digi XBee 3 modules mitigate the two above attack paths as well as the two attack case studies below, by using the SRP algorithm. The client authenticates to the Digi XBee 3 module by implementing the Secure Remote Password protocol to prove cryptographically that it knows the password that generated the SRP salt and verifier values stored on the XBee. (See the $S, $V, $W, $X and $Y AT commands in the documentation for your module.) Subsequent communication over the BLE API interface is encrypted using a shared session key.

The shared session key is derived from two random numbers. One is generated by the client and the other

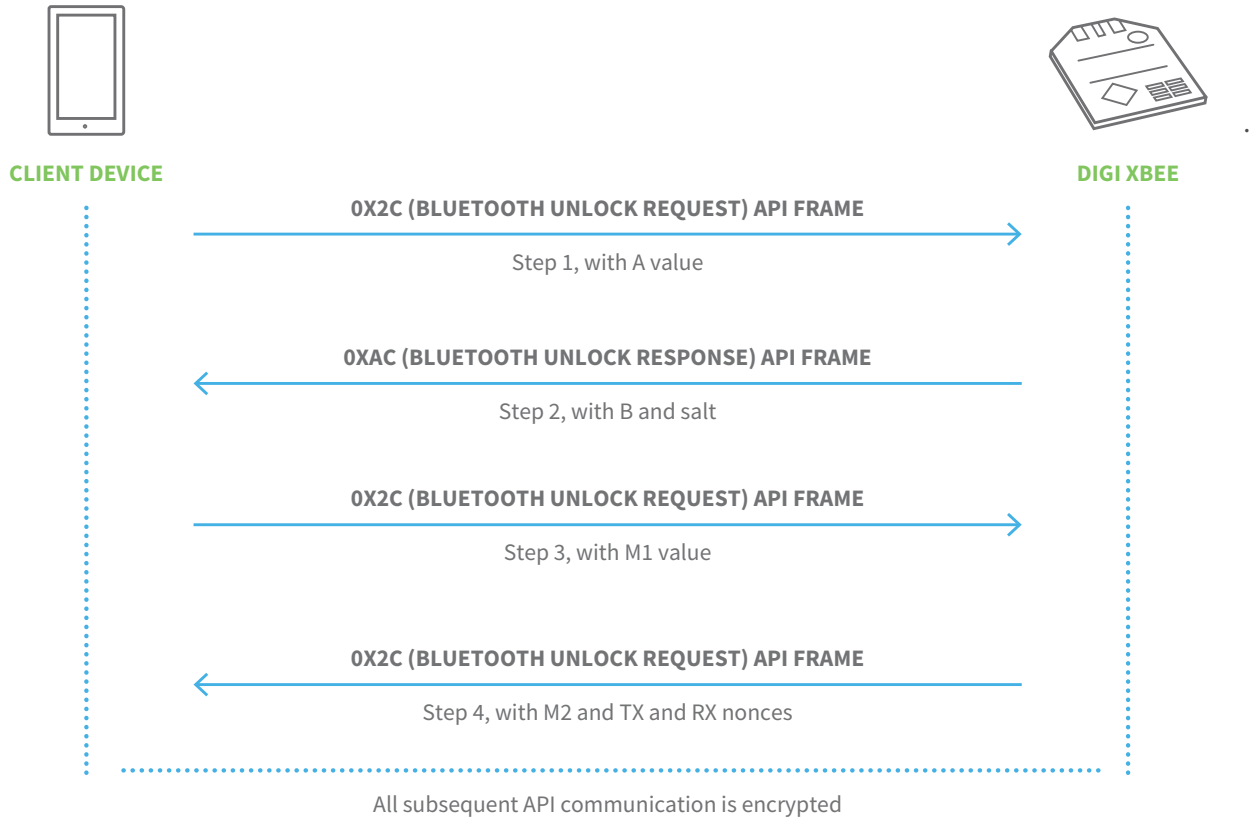
one is generated by the Digi XBee 3 module. Each login attempt generates a unique session key. The values M1 and M2, sent between the client and the XBee in the diagram below provide authentication challenges between the two sides attempting to establish secure communication. These values are cryptographic hashes of the shared session key. Once each side validates the authentication challenge presented to the other one, communication can proceed using the mutually derived shared session key*.

The SRP salt is a random 32-bit number that — when hashed cryptographically with a secure password — ensures the security of Digi XBee 3 module BLE communications. The AT command $S is used in conjunction with the $V, $W, $X, and $Y verifiers.

A cryptographic calculation using the salt and verifiers authenticates the client for the BLE API service without storing the secret password on the XBee 3 module.

The Digi XBee 3 module uses the BLE Unlock API frame to authenticate a connection on the Bluetooth interface and to unlock the processing of AT command frames. The unlock process is a combination of the SRP algorithm using the RFC5054 1024-bit group and the SHA-256 hash algorithm.

When this process completes, each side will have a shared session key, which is used to communicate in an encrypted fashion with the peer. The Modem Status — 0x8A with the status code 0x32 (Bluetooth Connected) — is sent through the UART. When the connection is terminated, a Modem Status Frame with the status code for 0x33 (Bluetooth Disconnected) is sent through the UART.



*Note: The authentication is only mutual if the verifier on the server is kept secret. Passwords on the XBee are never stored and are never transmitted over the air, which provides an excellent layer of protection. However, as discussed, a multi-pronged approach to security is important to prevent physical access or other brute force hacking methods by unauthorized users. An important best practice for Digi XBee modules is to turn off Bluetooth after initial configuration. Additionally, follow industry best practices for password management and prevent physical access to devices by unauthorized personnel.

For more information, visit:

www.digi.com

877-912-3444 | 952-912-3444

BLE Attack Case Studies and Mitigations

The following examples illustrate the range of attack types designed to exploit Bluetooth vulnerabilities, and how XBee 3 modules are designed to mitigate these risks.

BLE Proximity Authentication Example: A BLE proximity authentication vulnerability was discovered by NCC Group researchers that could be used to unlock cars, smart locks, company building access systems, mobile phones, laptops, and other devices, according to a report from NCC Group.

The BLE vulnerability is "not a traditional bug that can be fixed with a simple software patch, nor an error in the Bluetooth specification." Many devices use BLE proximity authentication. This vulnerability has been known for years, but existing devices came with detectable levels of latency and are not capable of connections that apply link-layer encryption.

A malicious actor can use this power attack to convince a Bluetooth device that the malicious actor is close to the device, when in fact they may be hundreds of miles away. This attack can still happen if the vendor has taken defensive mitigations and implemented latency bounding. It can be performed in seconds and can be repeated almost endlessly. Even if a malicious actor were to be in proximity of the Digi XBee 3 module, the malicious actor would have to have the correct M1 value. If a malicious actor is in possession of M1, they would still be unable to participate in the secured session unless they had also gained possession of or derived the key and state established throughout the SRP session.

BLE Spoofing Attacks: BLE Spoofing Attacks (BLESA) were found by a team of academic researchers from Purdue, as described in their paper. This attack arises from authentication issues when a device is trying to reconnect. When this attack is successful, it allows a malicious actor to connect to a device and send spoofed data to it. To get this spoofed data, the malicious actor must find a server that a BLE-enabled device is connected to and pair with it to obtain its attributes.

SRP prevents spoofing attacks since meaningful communication can only be had with the device after the client has been authenticated. Otherwise, the XBee will reject the communication with the client.

Additional Considerations: Cybersecurity is not a "set it and forget it" practice, but instead requires ongoing maintenance as new threats emerge.

Firmware updates are the best practice to mitigate vulnerabilities. Digi XBee 3 modules can be upgraded to combat new vulnerabilities and stay ahead of attackers. Our products are designed for quick, over-the-air firmware upgrades as new threats are identified in the industry.

Digi is highly tuned to industry best practices and emerging threats. Visit our Security Center for additional information, or to sign up for our RSS feed and receive security alerts.

Conclusion: Bluetooth is instrumental in our day-to-day lives and in a growing range of enterprise and industrial applications. The consequence of Bluetooth popularity raises the importance of security because there are many ways to attack a Bluetooth or BLE-enabled device and steal sensitive information which require proactive measures. While Bluetooth Low Energy is the "new" Bluetooth and is more secure, there are still ways to get into the devices. Overall, whether a device uses classic Bluetooth or BLE, security features need to be incorporated into Bluetooth-enabled devices to protect businesses and property.

Explore the Digi XBee Ecosystem

Digi XBee® is a complete ecosystem of communication modules for development of wireless products across the vast range of verticals utilizing connected technologies and the Internet of Things today. Browse the XBee Ecosystem, which supports multiple wireless protocols — from mesh networking to cellular connectivity to LoRaWAN — and offers a full suite of tools and development kits for OEMs and independent developers. Prototype, test, develop and get your product to market quickly with Digi XBee. And if you need support anywhere along the way, Digi Wireless Design Services can help.

Contact us to learn more about Digi Solutions

For more information, visit:

www.digi.com

877-912-3444 | 952-912-3444

A4/1022
91004582