IS YOUR WIRELESS CONNECTED DEVICE SECURE?

There are many advantages of using wireless connected devices but the modalities used are open to cybersecurity threats. In this article, Jamie Kendall, Software Engineer at Key Tech uses an example of a wireless system architecture to explain the three common cybersecurity vulnerabilities and highlights the importance of proper implementation early on in the design process to mitigate these risks.

Wireless connected systems are clearly the future of drug delivery. They allow for valuable advances in the complete care of patients, including patient compliance monitoring, improved therapy and real-time delivery diagnostics.

However, it is important to understand the current state of wireless cybersecurity before developing a connected drug delivery device system. Threats to cyber security can pose a serious risk in healthcare. Beyond fictional examples from television shows, security researchers have demonstrated in real life that attackers could remotely interrupt care, such as blocking an insulin pump or tampering with a pacemaker. Hospitals themselves have to seek to prevent attacks. The recent MedStar Health computer network attack brought a large-scale hospital's network operations to a halt.

Before examining the risks to security, we will look at the wireless modalities available.

BLUETOOTH / BLUETOOTH LOW ENERGY

While becoming extremely popular recently, Bluetooth development began in the late 1980's. Bluetooth Low Energy (LE) was first introduced in the Bluetooth specification in 2010 to target smaller and lower power devices, specifically including medical devices. Both Bluetooth and Bluetooth LE have built-in security mechanisms that protect the integrity of transmitted data. Bluetooth protocol security has evolved since its inception, with versions above 2.1 supporting multiple methods for secure encryption key exchange. Bluetooth LE was added in version 4.0 and allows for a Bluetooth connection that is slower but uses less power to operate and has similar key exchange methods as Bluetooth. A PIN is typically a short numeric code that is then converted into an encryption key of a much longer length, usually 128 bits. The most familiar method of key exchange or pairing is the PIN exchange.

> "Security researchers have demonstrated in real life that attackers could remotely interrupt care, such as blocking an insulin pump or tampering with a pacemaker."

However, a simple or even static PIN used in an embedded connected device could be brute force cracked. Even some of the latest key exchange methods cannot prevent an attacker from performing a "man-in-the-middle" attack during the key exchange portion of communication. This means that a potential attacker in proximity to the connected device and its host could pretend to be both devices and stand in the middle of communication, intercepting keys and all traffic.

WI-FI

Wireless networks, or Wi-Fi, have been around since the late 1990s. For security, the first encrypted algorithm used to secure communication was called Wired Equivalent Privacy (WEP). WEP quickly proved that it had massive security issues. While the details of the failure are not important to this discussion, the bottom line is that an attack could reveal the encryption key and decrypt all traffic without any physical manipulation of the wireless system. In addition, most networks only require the encryption key to connect, which would allow complete

Jamie Kendall
Software Engineer

Andy Rogers
Director of Business Development
E: andy@keytechinc.com

Key Tech, Inc
40 East Cross Street
Baltimore
MD 21230
United States

www.keytechinc.com

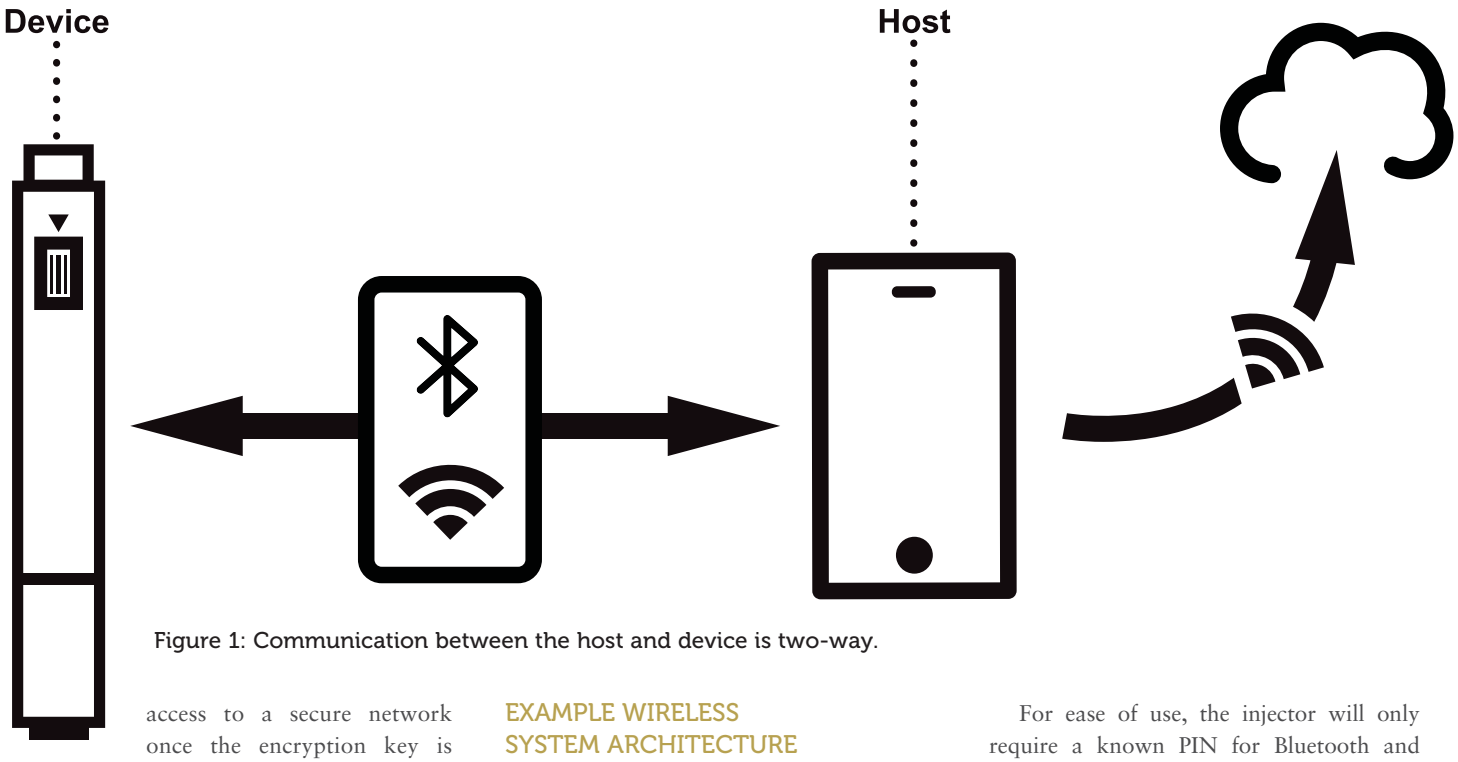

Figure 1: Communication between the host and device is two-way.

access to a secure network once the encryption key is compromised.

Newer encryption algorithms such as WPA/WPA2 are now available, but even these have weaknesses. WPA and WPA2 use AES (Advanced Encryption Standard), which is significantly better suited for Wi-Fi and doesn't have the same failings of WEP. However, for WPA key generation, most devices rely on a passphrase to generate a shared AES key. This means a plaintext passphrase is converted to a 256-bit key, using a known algorithm shared by almost all manufacturers. This step, in itself, is the biggest vulnerability, as this step allows for certain styles of attacks, to be discussed later.

EXAMPLE WIRELESS SYSTEM ARCHITECTURE

We will now explore a typical drug delivery auto injector system that uses Bluetooth or Wi-Fi communication methods to show the potential vulnerabilities in relatable scenarios.

The auto injector can be configured at the factory to either connect via Bluetooth or Wi-Fi to an application on the patient's tablet (Figure 1). In this situation, communication will be two-way – from the device to host and host to device. This will allow the tablet application to send injection results originated from the injector to a central system, as well as to set the dose that the injector will deliver remotely.

For ease of use, the injector will only require a known PIN for Bluetooth and a WPA2 passphrase when connecting in order to support a larger range of mobile devices. The pairing of the injector will remain as long as the device is used. Only on connection of a new device will a new PIN pairing procedure or passphrase be required.

This system has three common cybersecurity vulnerabilities.

Breaking Encryption

To make the auto injector system user friendly, it uses a short PIN for connection to a smart device. Unfortunately the short PIN allows for attackers using readily available and downloadable open-source

tools to try all possible PIN combinations to break the encrypted link and inspect traffic. These tools are typically used by malicious users hoping to intercept Bluetooth traffic in public places. These tools can also be aimed at a connected delivery device to capture the Bluetooth traffic for cracking offline. Passive Bluetooth collection tools also record the address of the devices and can use them as part of a cloning attack.

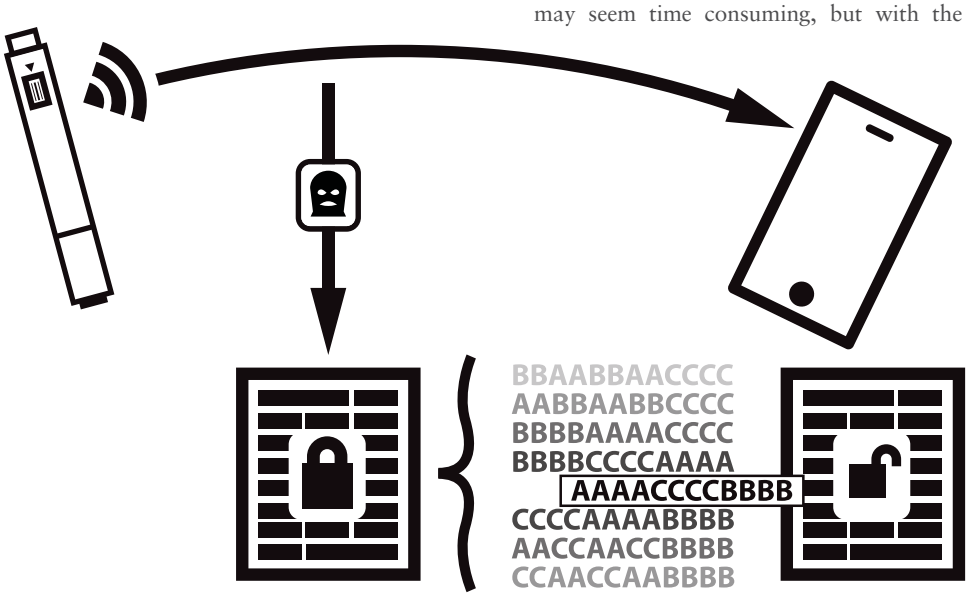

Figure 2: Using a brute force approach.

> "Careful selection and analysis of the current Wi-Fi and Bluetooth modules, as well as device hardware and software must take place early in design to prevent as much vulnerability as possible."

The Wi-Fi enabled connection can suffer a similar fate if we assume a WPA2 Wi-Fi network for data transfer. During initial connection, the host acting as a Wi-Fi Access Point manages a four-way handshake to establish a shared key, often created based on a user-provided passphrase. Capturing the information exchanged during the handshake allows an attacker to try all possible passphrase combinations.

If a simple word or short phrase was used for the passphrase, a dictionary can be used to create the pool of potential passphrase combinations and could crack the encryption relatively rapidly. Alternatively, a brute force approach can be taken for keys that are based on random numbers and characters (Figure 2). These approaches may seem time consuming, but with the advancement of dedicated hardware and cloud-based distributed cracking systems, this process can actually be performed rather quickly.

In both scenarios, broken encryption can have serious consequences. If no additional data encryption is used, all data passed between the connected delivery device and the host can be accessed by the attacker, and the device communication protocol could be reverse engineered. This would allow the attacker insight into system control as well as the potential access to private patient data, dose information and more.

The main message here is knowing that tools and attacks exist and should be factored into the system design to mitigate risk. When selecting a wireless protocol, the key exchange must be evaluated and carefully considered to reduce the likelihood of an attack like this. Longer PIN values and non-dictionary word passphrases would help mitigate the risk in general. Basing these values on the connected device's serial number, instead of a single standard key, could also help reduce the risk. It is possible to use a key generated without a passphrase to avoid the issues mentioned, but this would require more work for the user and could limit device support. If possible, using a key shared by the manufacturer with no user interaction would be best, but may not be practical for some situations.

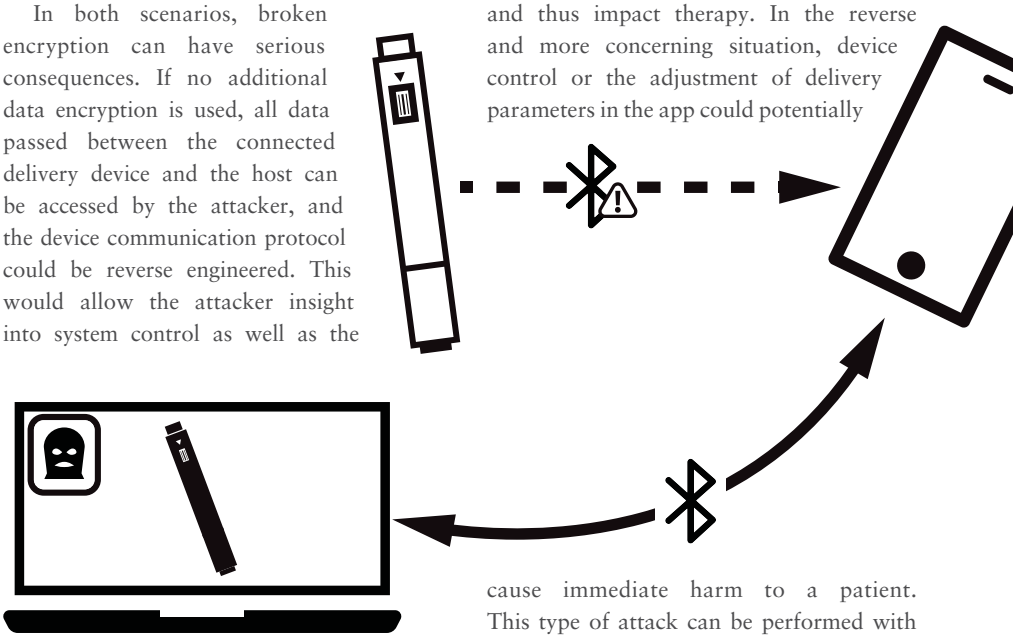

Figure 3: Device cloning.

Device Cloning

Once encryption is broken, knowing the security key (based on a passphrase or a PIN) can lead to the next level attack with more serious consequences: device cloning. Device cloning is when the attacker uses the established key and known device address to act as an imposter in the communication architecture (Figure 3). By using the key and device address, false communication could be sent to either the host or device. From the device side, fake or incorrect dosage information could be reported to the controlling application, viewed incorrectly by users, and thus impact therapy. In the reverse and more concerning situation, device control or the adjustment of delivery parameters in the app could potentially cause immediate harm to a patient. This type of attack can be performed with common tools available today.

The most efficient way to mitigate this threat would be to require additional authentication in the device level communication protocol. A custom application layer encryption, separate from the wireless encryption, would be one way to mitigate this risk, as well as potentially adding a cipher-based digital signature to all application packets to positively identify the sender.

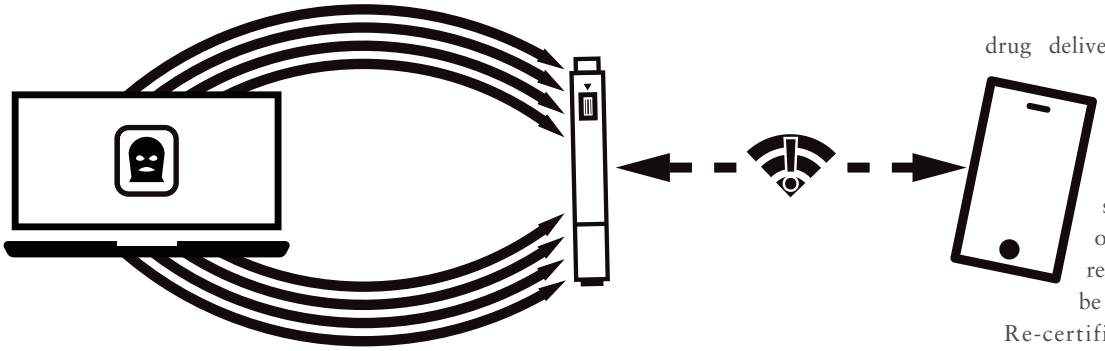

Figure 4: Denial of service blocks all legitimate communication.

Denial of Service

Another potential security risk with both example architecture configurations is the denial of service (DoS) attack. A DoS attack can take many forms, with the bottom line being reduced or non-existent communication on the device subject to attack.

In a Wi-Fi-based architecture, a de-authentication attack could effectively force the device to attempt to reconnect continuously. In the Wi-Fi protocol, a provision exists to notify clients that they have been removed from a Wi-Fi network by using the de-authentication frame. A DoS attack can take advantage of the de-authentication mechanism by broadcasting the packet with forged device addresses, causing the target device or host to attempt to reconnect repeatedly. This is done at a high enough frequency that all legitimate communication is blocked (Figure 4).

This poses clear risks for a connected delivery device. Dosage information and potentially critical or vital delivery factors could be missed. While this type of attack is hard to mitigate, a custom embedded Wi-Fi implementation stack could be modified in order to detect and/or ignore rapid de-authentication frames. This reiterates the point that connected devices need to be designed with support for the lost connection state, whether it is due to an attack or just communication failure.

SPECIAL CONSIDERATIONS FOR DRUG DELIVERY DEVICE DESIGN

Microcontrollers selected for drug delivery applications must have the processing power to handle potential security mitigations both now and in the future. The selection of a Wi-Fi or Bluetooth implementation module must be vetted for these security concerns and efficiency.

In the security world, rapid updates are usually the first line of defence against future attacks. With connected drug delivery devices, remote updates may not be feasible and could be difficult to implement. In addition to the logistics involved in rolling out new software for thousands of devices, there are also regulatory concerns that need to be addressed with a new release.

Re-certification or careful co-ordination may be required to push out a rapid update. Careful selection and analysis of the current Wi-Fi and Bluetooth modules, as well as device hardware and software, must take place early in design to prevent as much vulnerability as possible.

CONCLUSION

Wireless communication using Bluetooth, Bluetooth LE and Wi-Fi communication are all convenient and effective ways to get a drug delivery device connected to the outside world. With proper implementation and thought, the security issues discussed in this article can be mitigated. Some of the situations discussed in this article are worst-case scenarios or a combination of security concerns and potentially bad practices, but they are definitely possible using tools available today. All connected devices are potential targets, and the proximity restrictions of these connected devices should not limit the concern for advanced wireless security implementation.