Journal of Diabetes Science and Technology
2020, Vol. 14(6) 1111–1115
© 2019 Diabetes Technology Society
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/1932296819864416
journals.sagepub.com/home/dst
SAGE

Bluetooth Wireless Technology Cybersecurity and Diabetes Technology Devices

William Saltzstein, B.S.E.E

Abstract

Medical devices have transitioned from hospital into the home and consumer environments and have been shown to provide for mobility and quality-of-life improvements for chronic conditions such as diabetes. It is important to collect sensor and usage data while remotely connected in real time. The protection of these data is commonly called "cybersecurity." Bluetooth® wireless technology (Bluetooth is a registered trademark of the Bluetooth Special Interest Group, Inc.) is commonly used for low-cost medical devices to provide connections to other medical devices as well as compute and display devices such as smartphones. This paper provides a review of its use with respect to diabetes devices with a particular focus on cybersecurity.

Keywords

Bluetooth, cybersecurity, glucose monitoring, insulin pump

Introduction

Medical devices have made the transition from hospital into the home and consumer environments. The devices have demonstrated the capability to provide for mobility and quality-of-life improvements in the care of chronic conditions such as diabetes.

Home and wearable medical devices not only provide diagnostic information and sensor data, but also deliver therapies and medication. It has become increasingly important to collect the sensor and usage data, often while connected remotely and in some cases in real time.

The protection of data generated, stored, and transmitted between computing devices is commonly called "cybersecurity": the state of protection against unauthorized or unintended use or abuse of data.

Bluetooth wireless technology is commonly used for low-cost medical devices to provide connections to other devices and to compute and display devices such as smartphones. This paper provides a review of its use with respect to diabetes devices with a particular focus on cybersecurity.

System Architecture

The "Internet of Things" is a commonly used term for systems that utilize devices in communication with the cloud. An out-of-hospital wearable medical system architecture utilizes similar constructs with medical device components in a "Medical Internet of Things," as shown in Figure 1.

Many devices such as insulin pumps and glucose measurement devices are designed with Bluetooth wireless technology for connectivity to each other or to a gateway. Bluetooth wireless technology provides for the transfer of glucose meter values to smartphone apps used for trends and alerts to the user and their caregivers. Bluetooth is used to connect the glucose measurement devices to each other and to the smartphone for calibration. Finally, Bluetooth is also used for the connection to an insulin pump for data used in closed-loop operation.

Data storage and access capabilities are provided by cloud computing platforms such as Microsoft Azure and Amazon Web Services. These platforms may also host Electronic Health Records and artificial intelligence components to provide automatic data interpretation and trending.

Bluetooth Wireless Technology

Bluetooth wireless technology today includes two variants: classic Bluetooth and Bluetooth low energy (BLE). Classic Bluetooth was introduced 20 years ago to provide audio communications and data. Most smartphones and computers

Code Blue Communications, Inc. dba, Code Blue Consulting, Ashland, OR, USA

Corresponding Author:
William Saltzstein, B.S.E.E, Code Blue Consulting, Inc., 164 Clear Creek Drive, #201, Ashland, OR 97520, USA.
Email: billsalt@consultcodeblue.com

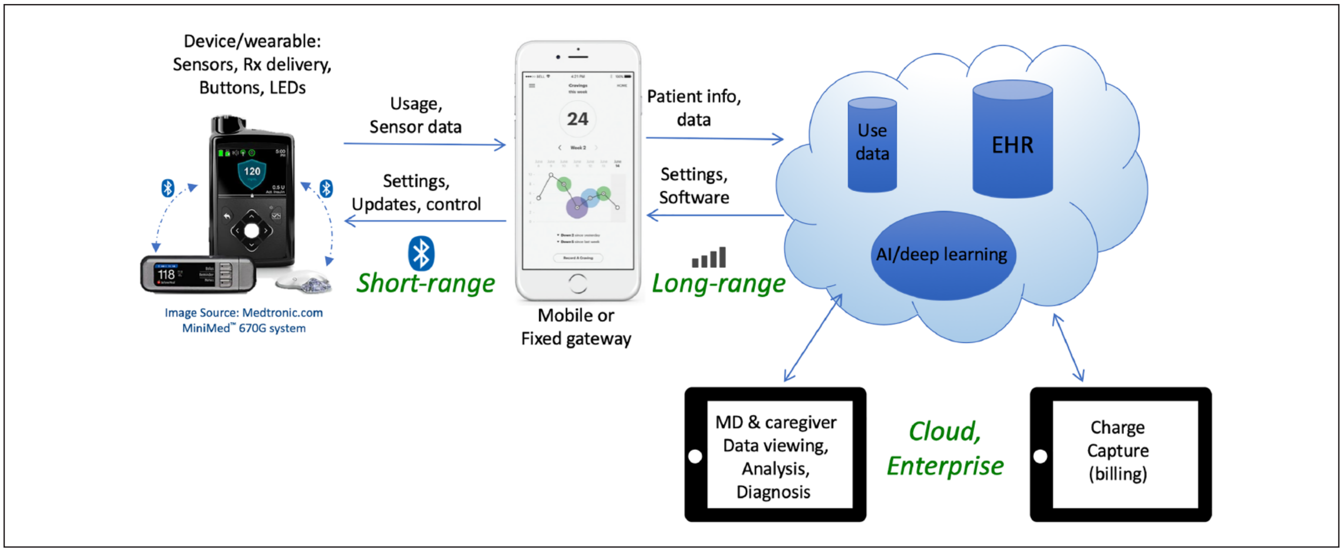

Figure 1. The Medical Internet of Things architecture.

Table 1. Bluetooth Features.

Feature	Classic Bluetooth	BLE
Introduced	Bluetooth 1.0: 1999	Bluetooth 4.0: 2011
Power	Runs for days on AAA batteries	Runs for months on coin cell battery
Data rate (throughput)	700 kbps-2.1 Mbps	100 kbps-800 kbps
Required software stack components	Dozens	Generic access profile, Generic attribute profile, and security manager
Specification versions	Version 1.0 and beyond	Version 4.0 and beyond
Connection type	Streaming	Periodic
Operating frequency	2.40-2.485 GHz	2.40-2.485 GHz
Coexistence and robustness	FHSS, AFH, error detection, forward error correction, data retransmission	FHSS, AFH, error detection, data retransmission
Encryption	SAFER+ 128-bit	AES 128-bit
Channels	79	40
Network topology	Star (piconet or scatternet)	Star, beacon, mesh
Devices in network	8 (1 master, 7 slaves)	Thousands
Audio	Yes	Limited
Standard serial port emulation profile	Yes	No
Maximum output power	20 dBm (100 mW) with power control, 10 dBm otherwise	10 dBm (10 mW) through Bluetooth 4.2, 20 dBm in Bluetooth 5

Abbreviations: AFH, adaptive frequency hopping; FHSS, Frequency Hopping Spread Spectrum.

are dual mode (supporting both classic and BLE), but many devices such as headsets, blood pressure meters, and glucometers only support one.

Many of the newer devices today utilize BLE for lower cost and improved battery life. A brief feature comparison of the two variants is shown in Table 1.

This paper will focus on systems that use BLE, since it is best suited to mobile and wearable diabetes technology devices. The technology provides for periodic data connections and reasonable data rates. BLE's lower data rate and transmission implementation allow for very low power operation, enabling devices using BLE to operate from a single coin cell battery for months or even years.

BLE is currently used in many types of medical devices that have been approved and cleared by the FDA, including those listed below. Several of these devices also have interoperable standardized "profiles" defined and maintained by the Bluetooth Special Interest Group, as indicated by the "*."

- *Blood pressure
- *Blood Glucose Meter
- *Continuous Glucose Meter

- *Pulse oximeter
- *Thermometer
- *Weight scale
- Insulin pump
- Cardiac implant
- Neural implant
- Electrocardiogram
- Prosthetics

BLE allows for thousands of connected devices to one "central," but practical resource constraints of devices typically limit connections to five to ten. All of the devices in a network can be connected at the same time, and many networks can coexist in the same space without noticeable performance degradation.

BLE can also broadcast data without a connection using its advertising capability to function as "beacons" used for location or to broadcast data.

Cybersecurity

While this paper focuses on the BLE wireless interface commonly used to connect mobile medical devices, many of the cybersecurity concepts discussed for BLE also apply to other wireless interfaces.

People and devices used to intercept and interject data are commonly called "bad actors" by cybersecurity experts. These actors target "assets" of value that may be stored on and exchanged between devices including patient information, medical device data, and credit cards.

Data assets have varying value, both to a bad actor and the intended user. A single glucose measurement value intercepted from a device is of very low value without any context or patient information. However, if that glucose measurement is used to determine insulin dosage and a bad actor is able to substitute data, the result could be harmful to the user. Additionally all patient information including name, diagnosis, and treatment must be secured to meet HIPAA requirements.

The designers of the devices and system must analyze the value of the assets and implement appropriate cybersecurity solutions for the complete system that includes the devices. It is also important to recognize that data assets increase in value stored or transmitted in combination.

Bluetooth and Cybersecurity

BLE uses a Frequency Hopping Spread Spectrum (FHSS) radio based on a method originally developed for the US Navy in the Second World War to defeat interception and prevent jamming. Today's available technology provides relatively easy methods to intercept FHSS transmissions unless additional preventative cybersecurity measures are provided, such as those provided by BLE.

BLE includes several features that can be used to implement good cybersecurity measures. *Bluetooth cybersecurity features in BLE must be appropriately designed and implemented by the device manufacturer and system developers; they cannot be enabled by the user.*

The two key cybersecurity methods provided by BLE for cybersecurity allow for *authentication* and *encryption*. Authentication is the process of making certain that the connecting device is exactly what it appears to be. In human terms, a phone call may come in with a caller ID that matches a number you might know, but until the call is answered and the voice recognized and few private questions are answered it cannot be known whether the caller is authentic.

Encryption is the process of coding data so that it is unreadable without the use of specialized algorithms combined with key data.

Authentication and encryption work together: A connection must be authenticated *and* encrypted to be truly secure.

Authentication and encryption are set up during the initial connection for BLE devices, a process called "pairing." A central device "scans" to discover peripheral devices that are "advertising." The user or app then selects the desired advertising device. The BLE Security Manager module then conducts pairing and key distribution utilizing the Security Manager Protocol (SMP) and the devices authenticate each other (if enabled) and encryption keys are exchanged (if enabled).

The central and peripheral devices can optionally store the pairing information using SMP in an operation called "bonding," enabling devices to remember pairing information if/when the devices are disconnected and later reconnected.

Different levels of authentication are provided by the BLE specification to allow for varying needs of the system; these levels are called "modes." These modes allow different methods to authenticate and then encrypt depending on the user interface components available on the devices. The best authentication possible should be used to protect the assets.

It can be challenging to implement appropriate security measures to match the value of the assets and maintain a good user experience. Implementing cybersecurity for Bluetooth can often involve additional user interaction and user interface features (display, light emitting diodes, and buttons), and these interactions can adversely affect usability if not carefully implemented.

Risk Analysis Process and Resources

Medical device and system developers must submit a cybersecurity analysis as part of the FDA process for medical devices in the United States. This includes an analysis of potential cybersecurity issues, their severity, and appropriate mitigations for the device and system to prevent cybersecurity hazards.

The National Institute of Standards and Technology (NIST) provides important resources for cybersecurity, including a cybersecurity framework[1] for entire organizations to provide an overall framework for instituting cybersecurity policies and practices:

- Identify
  - Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- Protect
  - Develop and implement the appropriate safeguards.
- Detect
  - Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- Respond
  - Develop and implement the appropriate activities to take action.
- Recover
  - Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

NIST also provides a valuable document[2] that addresses the use of BLE wireless and provides recommendations regarding usage and specification revision concerns as summarized below.

- Use the strongest Bluetooth security mode that is available for their Bluetooth devices.
- Address Bluetooth wireless technology in their security policies and change default settings of Bluetooth devices to reflect the policies.
- Ensure that Bluetooth users are made aware of their security-related responsibilities regarding Bluetooth use.
- Use Bluetooth revision 4.2 or later (this author recommends 5.0 or later).

Bluetooth's Particular Risks and Mitigations

Pairing and Bonding

In some scenarios an eavesdropping device may be able to intercept key information and then use this to decrypt communications (a "man-in-the-middle" attack). The latest revisions of the BLE specification (5.0 and later) have addressed flaws and increased protection during the pairing process. While the strongest modes of Bluetooth security virtually eliminate this risk, they may affect usability.

Developers can utilize good practices in the design of devices that include the following:

- Utilize the highest security mode possible.
- Limit the time that devices are in the advertising and pairing states.
- Lower the radio power to limit the range of the signal.
- Use out-of-band techniques (including near field communications).

Advertising

BLE devices advertise when they are available to connect. The advertisement can be easily seen by a scanning device (smartphone) used by a bad actor. It is important for privacy that the advertised data not be humanly readable since that could identify a person to the device. For example, advertising "Glucometer_xyz" in clear text could be used to identify a person with diabetes nearby, so a unique name that is not easily readable and identifiable should be used.

Authentication and Encryption

It is very important to understand that BLE authentication and encryption are *optional* features supported by the specification. Medical device and system designers must enable use the security modes appropriate with the value of the data assets.

Bluetooth and Software Revisions

Though sometimes overlooked, all BLE products (even if they use a module) must go through an approval process that assures compatibility that generates an approval listing (see www.bluetooth.com for listings). While somewhat difficult to decipher, these listings show the version and optional specification features (including security features) that are implemented and tested.

Device operating software and the BLE specification are periodically updated, and these updates often include bug fixes associated with compatibility and cybersecurity. Manufacturers need to provide methods to make sure that the devices that they depend upon are updated with the latest revisions of software.

Smartphone Apps

There is an additional risk associated with apps on smartphone operating system platforms from malicious apps installed inadvertently by the end user, and this is a risk for all smartphone communications technologies. While authentication and encryption create a secure connection between the devices, these methods do not provide a secure connection between the application software on the smartphone and the device. In some cases, other apps running on the platform may be able to use the connection and provide a cybersecurity breach.

Developers should add app-level authentication to mitigate this risk, and users of the devices should be cautioned to use apps from reliable sources only. Note that work is currently underway to provide this app-level authentication as an optional BLE feature.

Conclusion

Bluetooth wireless technology is currently used in many different types of medical devices including those for patients with diabetes. BLE provides key communications capabilities between devices in the system and an interface to the cloud and caregivers.

The BLE technology provides many features to implement good cybersecurity. Developers and manufacturers must appropriately implement these features and the most recent specification revision in order to implement systems that are secure for their users.

Declaration of Conflicting Interests

The author(s) declared the following potential conflicts of interest with respect to the research, authorship, and/or publication of this article: The author is the president and principal of Code Blue Communications, Inc., which does business as Code Blue Consulting. Code Blue provides consulting services for clients in the medical device field, including services in the business of diabetes technology.

William Saltzstein is a full-time employee of Code Blue. Code Blue is an adopter member of the Bluetooth Special Interest Group.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was funded by Code Blue Consulting.

ORCID iD

William Saltzstein https://orcid.org/0000-0002-5519-2420

References

1. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf. Published April 16, 2018. Accessed July 9, 2019.
2. Padgette J, Bahr J, Batra M, et al. Guide to Bluetooth Security, SP800-121 Rev.1 (May 2012). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf. Accessed July 9, 2019.