
Key Points

- Continuous development of Bluetooth technology is rapidly increasing the use of Bluetooth-enabled devices. New uses of Bluetooth, such as mesh networking, will increase the ubiquity of this technology.

- Bluetooth devices are vulnerable to typical wireless networking threats, such as denial-of-service (DoS), eavesdropping, and man-in-the-middle (MITM) attacks. In addition, the technology is vulnerable to specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications.

- Individuals and organizations should maintain an ongoing awareness of the Bluetooth technology they are using to minimize vulnerabilities. National Security Agency (NSA) recommendations for individuals using Bluetooth mitigate many risks.

Introduction

Bluetooth technology is rapidly becoming ubiquitous. As the world begins to rely more heavily on cellular data and Internet connectivity for communication and information sharing, concerns over connection access and security are becoming more prevalent. Emerging technology seeks to provide essential data services, even if no cellular or Internet connection (Wi-Fi or hard-wired) is available or desired. Mobile applications (apps), such as FireChat, are gaining in popularity because of their ability to send and receive messages without a cellular or Internet connection. Protesters in Hong Kong are reportedly using FireChat to send messages covertly to circumvent the government firewall.

Similarly, Iraqi citizens also flocked to the FireChat app after the Iraqi government’s near-total blockage of the Internet and its content. Apps such as FireChat are made possible by Bluetooth technology, a technology that has been around for over a decade, but only recently reemerged as a priority for technology companies.

From wearable technologies—such as Fitbits and Google Glass—to automobiles, manufacturers are incorporating Bluetooth capability into modern devices at a greater rate. Bluetooth’s emerging pervasiveness presents unique implications for the future.
Benefits of Bluetooth Technology

(U) Making a device Bluetooth-ready is attractive for many reasons. Bluetooth technology is inexpensive and uses minimal power and limited physical space within the device. Most importantly, Bluetooth presents a wireless solution for connecting devices, which makes the technology more portable and more accessible than its predecessors. Enabling Bluetooth allows for simple sharing of documents, music, contacts, or any other type of data. For example, users can synchronize data from wearable technologies—such as fitness trackers—to their smartphones, which allows automatic and instantaneous updates to their fitness data.

(U) Every device on the Internet is assigned an Internet Protocol (IP) address for identification and location purposes. As of February 2011, all of the more than 4 billion IP addresses available in IPv4—the current communications protocol—were used. A new protocol, IPv6, was developed to prevent IP address exhaustion. IPv6 uses a 128-bit address and the number of available IPv6 addresses is so large that every person on earth could each own more than one billion IPv6 addresses.†

(U) Fitbits are wireless devices that users wear to track health data, to include activity level, time asleep, and other fitness measures.

(U) Google Glass is a wearable computer that resembles a pair of eyeglasses. Google Glass features a camera and display that allow users to search the Internet and use applications.

Users can also use Bluetooth to facilitate Internet connectivity by “tethering” an Internet-ready device to an Internet-connected device. For example, if a user wants to connect his laptop to the Internet, yet there is no Wi-Fi available in the area, he could tether his laptop to the data connection on his smartphone. Through this process, the smartphone and laptop essentially create a network, which allows the laptop to connect to the Internet using the smartphone’s data connection. As a result, Bluetooth-facilitated Internet connectivity is evolving on a grander scale.

The Future of Leveraging Bluetooth Technology

Users can leverage Bluetooth in many ways to expand a device’s capabilities.

- **Using Bluetooth technology to facilitate a mesh network.** A typical Internet connection occurs with a centralized device providing a connection to many devices. For example, within a home network, the modem and router connect the user’s mobile phone, printer, and laptop to the Internet. All data transmitted by these devices passes through the modem/router. In a mesh network, only one device needs an Internet or cellular connection, and the rest of the devices link to each other to provide Internet connectivity. For example, if a mobile phone is connected to the Internet, a laptop, printer, and any other devices within proximity to the mobile phone are also able to connect to the Internet by using Bluetooth capabilities to link to each other. The laptop and printer are able to continue sharing the connection to any other devices in their proximity, and the data transmitted does not pass through any centralized server. Mesh networks do not require a central connection, making them ideal for areas that do not have a robust Internet infrastructure.

- **Apps can use Bluetooth technology to communicate without any cellular or data connection.** The FireChat app builds off the mesh network framework to allow devices to communicate with each other off the grid, without any centralized network. The Citizen Lab recently tested the FireChat messaging app and found that the
app provided little in terms of encryption for transmitted messages. Anyone within the range of the person sending the message would be able to retrieve the content that was transmitted. It was also discovered that network operators could see the message content and the IP address of the person transmitting the message, allowing for further identification of the sender. The Citizen Lab also found that there is no user authentication process, which allows for easy impersonation. With FireChat's popularity gaining, app developers are forecasting that more apps will utilize this framework in the future.

Bluetooth technology supports home automation. There is an ever-growing list of "smart" devices, including mobile phones, televisions, heart rate monitors, light bulbs, and even pool cleaners. By making everyday home objects Internet-ready, users are able to turn off lights, adjust the thermostat, or unlock doors from their smartphones or tablets. For example, imagine a future where a person wearing a heart rate monitor is sprinting on the treadmill, and the heart rate monitor sends a signal to the thermostat to cool down the house, knowing that an increase in heart rate means the person is likely to be sweating. With Bluetooth-facilitated mesh networking, the heartrate monitor is able to communicate with the thermostat.

- **Beacon technology uses Bluetooth to connect interested consumers to real-time information.** Bluetooth beacons are transmitters that retailers, businesses, or even airports can use to provide visitors with information, coupons, or location guidance. For example, someone walking through an airport may come into proximity of a beacon, and if the user has the appropriate app installed, the individual's boarding pass may appear on his or her phone. The beacon works by sending out a unique code, and if the end user has the specific app able to read the code, the user's smartphone will automatically open the application and display the information represented by the transmitted code. Apple is using beacon technology to support the mobile-payment functionality of its new Apple Pay app. PayPal is also developing similar mobile-payment technology.

**Vulnerabilities**

Bluetooth technology allows the use of small and more interconnected networks for multiple purposes. Since joining these networks may be open to any device in range, there is a significant vulnerability for an attacker to enter the network and eavesdrop on the communications or disrupt the signal altogether. Depending on the security protocols in place, a device in the network may be able to access information on all of the devices within the network and even control some functionality of another connected device.

It is commonly accepted that Bluetooth supplies a level of comfort because devices must be proximally close in order to communicate with each other. Many people rely on the assumed safety of Bluetooth's limited-range radio frequency communication for chat apps like FireChat. However, attackers are known to use stronger antennae to boost the distance for intercepts. Some Bluetooth devices can already transmit up to 300 feet, and reports suggest that transmissions can be picked up much further away.
Once a device is paired through Bluetooth, the permissions afforded to the paired device are determined by the Bluetooth profile that the device supports. With more modern technology, it is usually safe to assume the device supports all profiles. Each Bluetooth profile contains different features of the device that the paired device can access and control. Profiles include control of microphone and camera capabilities, mouse and selection capabilities, and keyboard input capabilities.

The most concerning Bluetooth profiles have the ability to provide access to just about any type of data stored on the paired device, from contacts to saved e-mail attachments and other messages. If a malignant device is paired, the attacker can essentially control any of the target device’s capabilities that the Bluetooth profile supports. This could include enabling or shutting off applications, controlling the target device by powering it on or off, reading through messages, or even just simply watching the keystrokes to gain passwords for accounts.

In 2012, the National Institute of Standards and Technology (NIST) released a report on Bluetooth security, which included a list of potential attacks. The bullets below lists some of the threats referenced in the NIST report.

- **Bluesnarfing.** Bluesnarfing enables attackers to gain access to a Bluetooth-enabled device by exploiting a firmware flaw in older devices. This attack forces a connection to a Bluetooth device, allowing access to data stored on the device, including the device’s international mobile equipment identity (IMEI). The IMEI is a unique identifier for each device that an attacker could potentially use to route all incoming calls from the user’s device to the attacker’s device.

- **Bluejacking.** Bluejacking is an attack conducted on Bluetooth-enabled mobile devices, such as cell phones. An attacker initiates bluejacking by sending unsolicited messages to the user of a Bluetooth-enabled device. The actual messages do not cause harm to the user’s device, but they may entice the user to respond in some fashion or add the new contact to the device’s address book. This message-sending attack resembles spam and phishing attacks conducted against e-mail users. Bluejacking can cause harm when a user initiates a response to a bluejacking message sent with a harmful intent.

- **Bluebugging.** Bluebugging exploits a security flaw in the firmware of some older Bluetooth devices to gain access to the device and its commands. This attack uses the commands of the device without informing the user, allowing the attacker to access data, place phone calls, eavesdrop on phone calls, send messages, and exploit other services or features offered by the device.

- **(U) DoS.** Like other wireless technologies, Bluetooth is susceptible to DoS attacks. Impacts include making a device’s Bluetooth interface unusable and draining the device’s battery. These types of attacks are not significant, and because of the proximity required for use of Bluetooth, users can easily avert the attack by simply moving out of range.

- **Fuzzing Attacks.** Bluetooth fuzzing attacks consist of sending malformed or otherwise non-standard data to a device’s Bluetooth radio and observing how the device reacts. If a device’s operation is slowed or stopped by these attacks, a serious vulnerability potentially exists in the protocol stack.
• **Pairing Eavesdropping.** PIN/legacy pairing (Bluetooth 2.0 and earlier) and Low Energy (LE) Pairing (Bluetooth 4.0) are susceptible to eavesdropping attacks. The successful eavesdropper who collects all pairing frames can determine the secret key(s), given sufficient time, which allows trusted device impersonation and active/passive data decryption.

• **Secure Simple Pairing (SSP) Attacks.** A number of techniques can force a remote device to use Just Works SSP and then exploit its lack of MITM protection (e.g., the attack device claims that it has no input/output capabilities). Further, fixed passkeys could allow an attacker to perform MITM attacks as well.

### Security Measures

Recognizing the potential for Bluetooth exploitation, the NSA released a report detailing several steps that an individual can take to avoid being exploited.

- Avoid leaving Bluetooth enabled when not in use.
- Avoid making the device discoverable unless absolutely necessary.
- Never accept connections from unknown devices or devices that you do not recognize.
- Enable device firewalls and anti-virus software.
- Attempt to keep the devices that you would like to connect as proximally close as possible.
- Always keep the paired devices in sight; never connect devices that have been lost or stolen.

Individuals and organizations should maintain an ongoing awareness of the Bluetooth technology with which they interact. Proper training and education are essential to understanding and safely utilizing the technology. Users should be mindful of the permissions that they are allowing any paired device when they enable Bluetooth. Organizations should establish a security policy defining which Bluetooth-enabled devices, like commercial headset or car systems, are allowed to be used with organization devices. Individuals should choose strong PIN codes if given the option, and should choose by default that their device be “undiscoverable” to any other devices in the area. Proper encryption and authentication measures are also strongly recommended for any transmissions over Bluetooth.