KEY CONSIDERATIONS FOR SECURING BLUETOOTH CONNECTIONS IN MISSION-CRITICAL APPLICATIONS

MOTOROLA SOLUTIONS

OVERVIEW

Bluetooth is an open standard for a short range radio technology that is primarily used to establish wireless personal area networks. Today, Bluetooth technology has been integrated into many types of connected devices, such as two-way radios, body-worn cameras, weapon sensors and smartphones. The technology promises myriad benefits to public safety scenarios, including minimising safety hazards from cables through wirefree communications, helping to track the location of lone workers in indoor environments.

Like all wireless networks, Bluetooth technology is susceptible to wireless networking threats, such as denial of service (DoS) attacks, eavesdropping, spoofing and man-in-the-middle (MITM) attacks. Some attacks also target known vulnerabilities in Bluetooth implementations.

This paper presents key countermeasures that organisations can implement to improve the security of Bluetooth connections in mission-critical applications. Among the key recommendations are the need for organisations to use the strongest Bluetooth security mode that is available for their Bluetooth-enabled devices. In the case of Bluetooth-enabled two-way radios and smartphones, a key recommendation is for organisations to always use the Secure Connections feature for Bluetooth links.

Secure Connections is implemented in Bluetooth version 4.1 and later devices for connections that use the Bluetooth Classic radio. For connections using the more power efficient Bluetooth Low Energy standard, Secure Connections is available in Bluetooth Low Energy version 4.2, 5.0 and later devices.

BLUETOOTH TECHNOLOGY: A BRIEF HISTORY

By 2024[1], annual shipments of Bluetooth enabled devices are expected to exceed 6 billion. Originally devised to replace cables, Bluetooth technology has evolved and now addresses innumerable wireless connectivity use cases across multiple industries. The benefits of Bluetooth connectivity extend to public safety applications, and include enabling wirefree communications, enhancing situational awareness, and improving location accuracy in both indoor and dense urban environments.

WIREFREE PUSH-TO-TALK COMMUNICATIONS

Bluetooth-enabled two-way radios and audio accessories can be concealed more effectively, allowing covert or surveillance teams to communicate discreetly.

BLUETOOTH-ENABLED WIRELESS PERSONAL AREA NETWORK

A Bluetooth-enabled wireless personal area network (WPAN) with a two-way radio at its hub can help public safety organisations harness the growing number of IoT and Internet connected devices. Through analytics, audio, video, and IoT capabilities can be combined to improve frontline personnel safety, while providing critical incident decision-makers with better situational awareness.

INDOOR LOCATION TRACKING WITH LOCATOR BEACONS

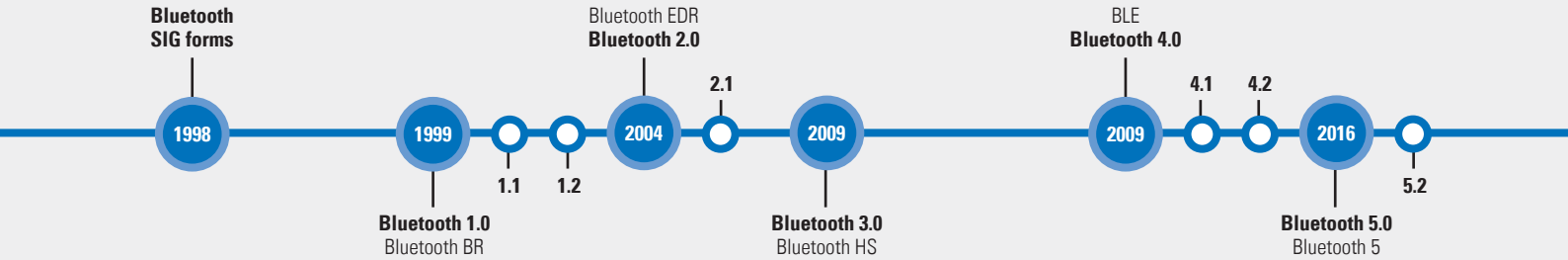
Bluetooth positioning systems can work in conjunction with two-way radio devices to achieve metre-level accuracy, enabling the precise location of personnel working in indoor environments to be determined.

To support growing connectivity requirements, the Bluetooth specification has gone through a number of revisions, covering multiple radio options operating in the 2.4GHz unlicensed industrial, scientific, and medical (ISM) frequency band:

Bluetooth Classic, also referred to as Bluetooth Basic Rate/Enhanced Data Rate, is designed for continuous two-way data transfer with high application throughput (up to 2.1 Mbps[2]). Bluetooth Classic radio is well suited to real-time communications and audio streaming applications, and is typically used for wireless remote speaker microphones.

Bluetooth Low Energy is designed for very low power operation, and prior to Bluetooth 5.0, provides 0.3 Mbps of application throughput. BLE data is sent in small (up to 251 bytes) packets, but range can be up to 100m with minimal latency (3ms) to be ready to send data. In contrast, the corresponding latency for Bluetooth Classic is 100ms. BLE's low power consumption makes it ideal for devices that are powered from a small battery and that need to transfer small amounts of data, such as wireless push-to-talk pods and health monitoring sensors.

TIMELINE OF BLUETOOTH SPECIFICATION RELEASES



Bluetooth 5 brings a number of major advances to the technology making it well suited to public safety scenarios. In addition to supporting the BLE v4.2 physical layer, Bluetooth 5 introduces two new radio options: the LE Coded PHY which enables a 4-fold increase in range, and the LE 2M which offers a 2-fold increase in raw data rate compared with BLE v4.2. When compared to BLE v4.2, Bluetooth 5 offers the combined benefits of longer battery life with higher application throughput (up to 1.4Mbps) or with greater range (up to 200m).

Currently, wireless audio is delivered over Bluetooth Classic and is limited to just a single audio stream. Announced in January 2020, the new Bluetooth LE Audio standard is set to transform the wireless audio experience while reducing power consumption. Bluetooth LE Audio adds support for multi-stream audio, and will allow audio from multiple sources to be received by a single headset.

Notwithstanding the significant operational benefits that Bluetooth promises, a robust security framework must be in place to drive wider adoption by the public safety community. As is the case with wireless technologies, any would-be attacker within the range of radio transmissions can introduce the threats of eavesdropping, unauthorised access and man-in-the-middle (MITM) attacks. Informed by a Motorola Solutions' threat and risk assessment performed on a generic security model consisting of a Bluetooth device communicating to a second Bluetooth device, the next section summarises key steps and countermeasures that should be considered.

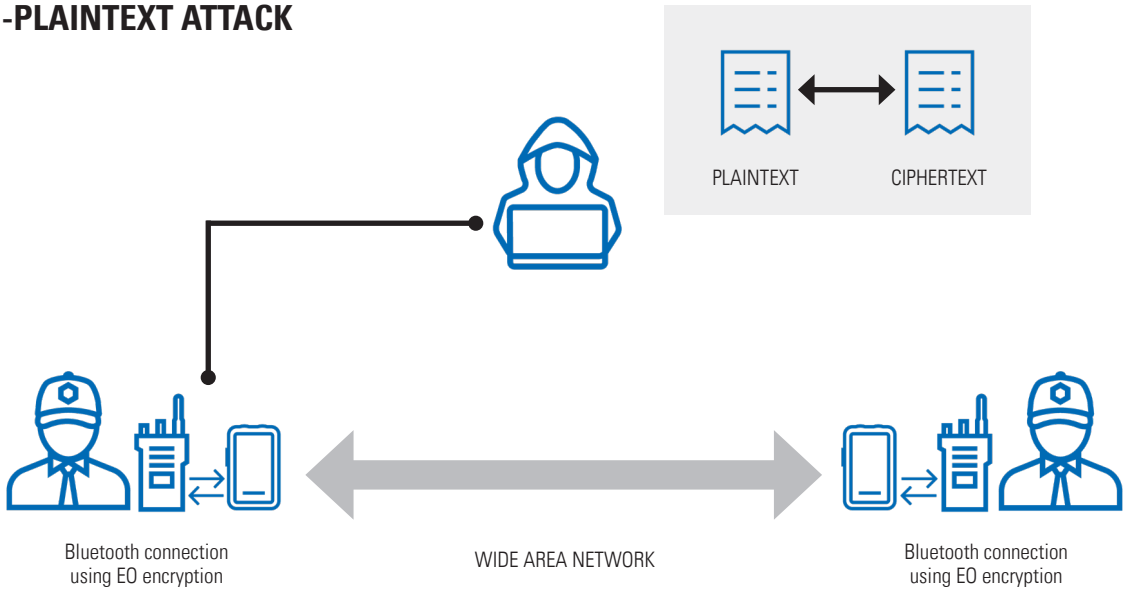
The countermeasures include references to Bluetooth Security Modes, which essentially define how well they protect Bluetooth communications and devices from potential attack. In line with NIST security principles, it is recommended that organisations choose the most secure mode available for each case.

SECURITY THREAT:
PASSIVE EAVESDROPPING

Up to Bluetooth version 4.0, the E0 stream cypher algorithm was used for Bluetooth Classic data encryption. While the E0 algorithm is initialised with key of up to 128 bits, a published theoretical known-plaintext attack[3] is able to recover the encryption key in 2^{38} computations. With modern computers able to process upwards of 300,000 million instructions per second, there is a significant risk that a determined adversary could capture sufficient plaintext and ciphertext to recover the encryption key and eavesdrop on communications.

As the diagram illustrates, the vulnerability here is between the radio and the smartphone, enabling the hacker to eavesdrop on the information exchange and potentially listen in on confidential communications.

KNOWN-PLAINTEXT ATTACK



COUNTERMEASURE
ONLY USE SECURITY MODE 4 LEVEL 4 WITH BLUETOOTH CLASSIC DEVICES

Security Mode 4, Level 4 requires Secure Connections and provides the highest security available for Bluetooth Classic devices. Crucially, Secure Connections uses authenticated pairing and encryption using 128-bit strength keys generated using FIPS-approved AES encryption, for which a brute-force attack would be impractical.

Secure Connections on Bluetooth Classic is available on certified Bluetooth v4.1 and later devices.

SECURITY THREAT:
MAN-IN-THE-MIDDLE ATTACK ON BLUETOOTH LE CONNECTION

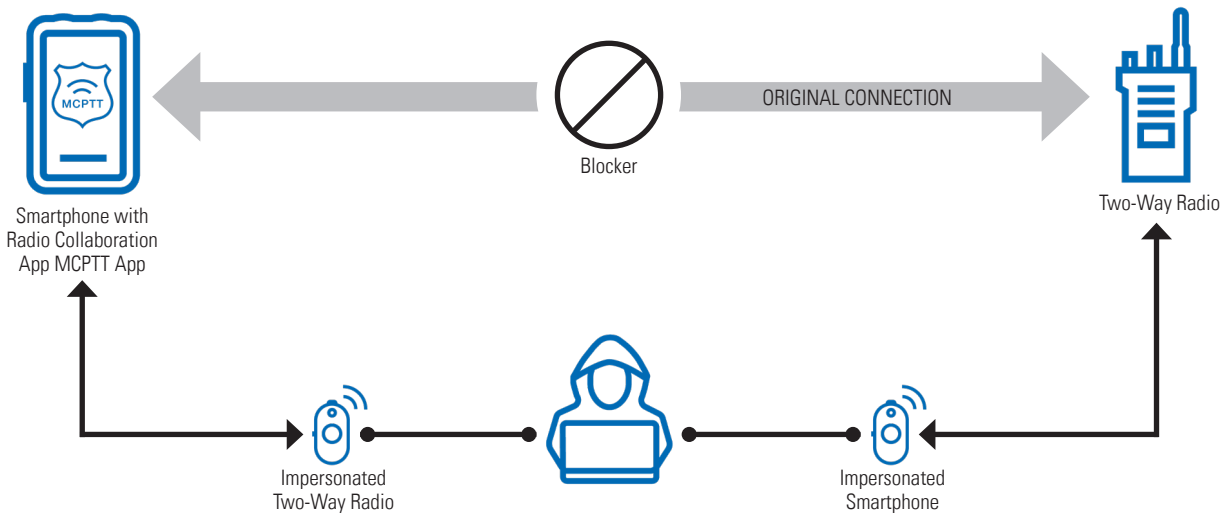
An emerging application within public safety involves the use of a Bluetooth LE Personal Area Network (PAN) to interconnect an array of smart devices. In a law enforcement use case, the PAN connects on-body sensors, body-worn cameras, with a two-way radio and smartphone serving as a hub, tethering the individual's communications to other frontline officers and the control room.

In the following threat scenario, the two-way radio and smartphone share collaborative functionality, allowing the smartphone access to, via the Bluetooth connection, two-way radio services and vice versa. For example, collaborative services may include allowing the smartphone to compose short data service (SDS) messages and sending them via the two-way radio network.

By using device impersonation, blockers, Bluetooth sniffing, and downgrade attacks, researchers[4] have been able to exploit security flaws in some legacy Bluetooth implementations that could lead to a man-in-the-middle attack. A determined adversary that is able to implement this active MITM attack would have access to messages sent between the smartphone and the two-way radio, by-passing the security provided by the wide area radio network.

This type man-in-the-middle attack exploits an implementation flaw that allows weaker security modes to be used. BLE v4.1 and earlier devices do not support LE Secure Connections and may be more vulnerable to this type of attack.

MAN-IN-THE-MIDDLE ATTACK



COUNTERMEASURE
ONLY USE SECURITY MODE 1 LEVEL 4 SECURE CONNECTIONS WITH BLUETOOTH LOW ENERGY DEVICES AND ENABLE PRIVACY MODE

LE Secure Connections Only mode should be used for all LE Bluetooth connections. This ensures the use of FIPS-approved algorithms, AES-CMAC and P-256 elliptic curve, for authenticated pairing and encryption. Specifically, the Secure Connections feature ensures that a secure association model is used for pairing the smartphone with the two-way radio, thereby mitigating the MITM threat.

It is also recommended that Privacy Mode is enabled for the LE connected link. Enabling Privacy Mode mitigates against device spoofing and limits the ability for hackers to track user activity and movements.

The LE Secure Connections feature is available in certified BLE v4.2 and later devices.

PUTTING IT ALL INTO PRACTICE

Bluetooth has evolved markedly in recent years, making a unique contribution to how we use technology to keep public service personnel safe. Bluetooth devices benefit from significant security enhancements, but it's imperative to keep several steps ahead of threats such as eavesdropping, MITM and DoS attacks. The countermeasures that we've shared here do not require enormous efforts or investment; the degree of implementation should be based on the acceptable level of risk for your organisation. However, it's important to work with a vendor that has the technology in place to fully execute all the countermeasures, especially where the cost of a security breach is significant.

Learn more at:
motorolasolutions.com

[1] Source: ABI Research, 2020.

[2] Morehead, S. 2019. "How to Pick the Best Bluetooth Protocol for Your Application", Microwaves & RF.

[3] National Institute of Standards and Technology (2017), Guide to Bluetooth Security, https://doi.org/10.6028/NIST.SP.800-121r2 , NIST Special Publication 800-121 Revision 2.

[4] Zhang, Y et al. 2020. 'Breaking Secure Pairing of Bluetooth Low Energy Using Downgrade Attacks'. 29th USENIX Security Symposium.

Motorola Solutions Ltd. Nova South, 160 Victoria Street, London, SW1E 5LB, United Kingdom.

MOTOROLA SOLUTIONS