WHITE PAPER

How secure is Bluetooth?

GN Making Life Sound Better
FOR 150 YEARS

Bluetooth security

Into the blue

Over the past few years, wireless voice communication through Bluetooth® has increased rapidly. With over 2 billion units on the market, people are now starting to ask more questions about security. Can a Bluetooth headset really be used without the risk of someone eavesdropping? How secure is it, really? This paper explains the security that Bluetooth technology offers and gives a view on the different types of security risks that come with using this technology.

Executive summary

The risk of people accessing your Bluetooth voice calls without authorization is actually very low. Bluetooth offers security measures that give the user a very high level of security. The protection offered as part of the Bluetooth communication link is as good as the other systems typically used in such a link e.g. PSTN, VOIP or a cellular network.

If an unwelcome third party wanted to gain access to confidential information, there are easier and more effective ways to do this than trying to hack a Bluetooth connection. Even with access to the data that has been sent, it would require extreme skill and a lot of time to get hold of anything meaningful. If someone should gain physical access to the Bluetooth headset or base, and pair it with another device, it would not be possible for the intruder to access conversations that had taken place between the originally paired devices. Millions of Jabra Bluetooth headsets are used daily, offering users convenient, secure voice communication.

So how does Bluetooth security **actually work?**

The Bluetooth security system

Bluetooth security prevents unwanted third parties from accessing information exchanged between devices. The security system in Bluetooth works in three stages:

- Pairing
- Authentication
- Encryption

1. Pairing: Bringing two devices together

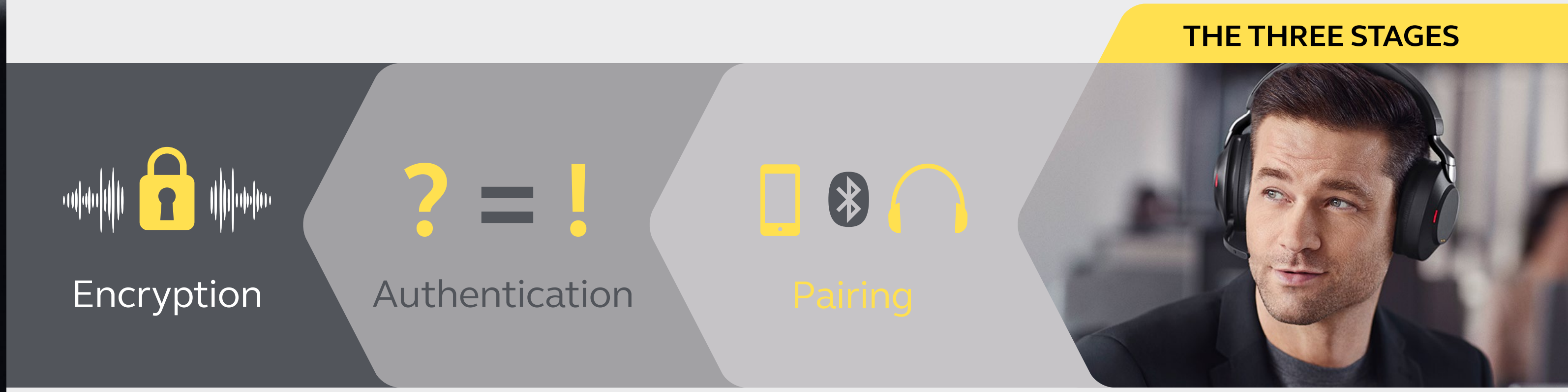
When you want to use two devices together, they need to go through a user-initiated setup process called 'pairing'. First, a commonly shared secret key is created. This secret key is never transferred over the air and cannot be stolen by a third party. Once pairing is completed, this secret key is stored and used for authentication and the creation of encryption keys whenever the devices communicate with each other. Physical access to the devices is needed to perform a pairing; it is not possible to activate the pairing process over the air.

2. Authentication: One device asks a question, the other provides the answer

Authentication is a way of checking that the other device really belongs to the group of paired and trusted devices. This happens through a 'challenge-response' scheme. One device uses the secret key to create a challenge for the device it wants to authenticate. If the device that is being challenged is paired, it will then have all of the information needed to calculate the correct answer to the given challenge.

3. Encryption: The data is hidden by code

An algorithm encrypts the data transmitted between two units, making it unreadable to anybody except its rightful receiver. The receiving unit then decrypts the data back to its original format, based on the same algorithm. Only the paired units know the information necessary to perform encryption and decryption. Encrypted information is never sent over the air, it is embedded in the units. In the unlikely event they should gain access to it, this would make it very difficult for an eavesdropper to understand anything from the data.



How secure and effective is Bluetooth?

Bluetooth is used in lots of different ways: for data synchronization, wireless keyboards and mice, gaming controls and so many more. Out of all of these use cases, voice communication between a phone and a headset is still one of the most common.

Testing, testing

Since Bluetooth was introduced, there have been attempts to hack different types of Bluetooth devices to gain access to information that should be kept protected. Almost every time, these attacks have explored implementation errors made by manufacturers. Once they were made aware of the problem, manufacturers have solved these issues with software upgrades. This has led to the constant development of Bluetooth security protocol. There have been no known attacks made specifically against Jabra headsets.

Let's get into the detail and take a closer look at the three stages of Bluetooth security.

Pairing

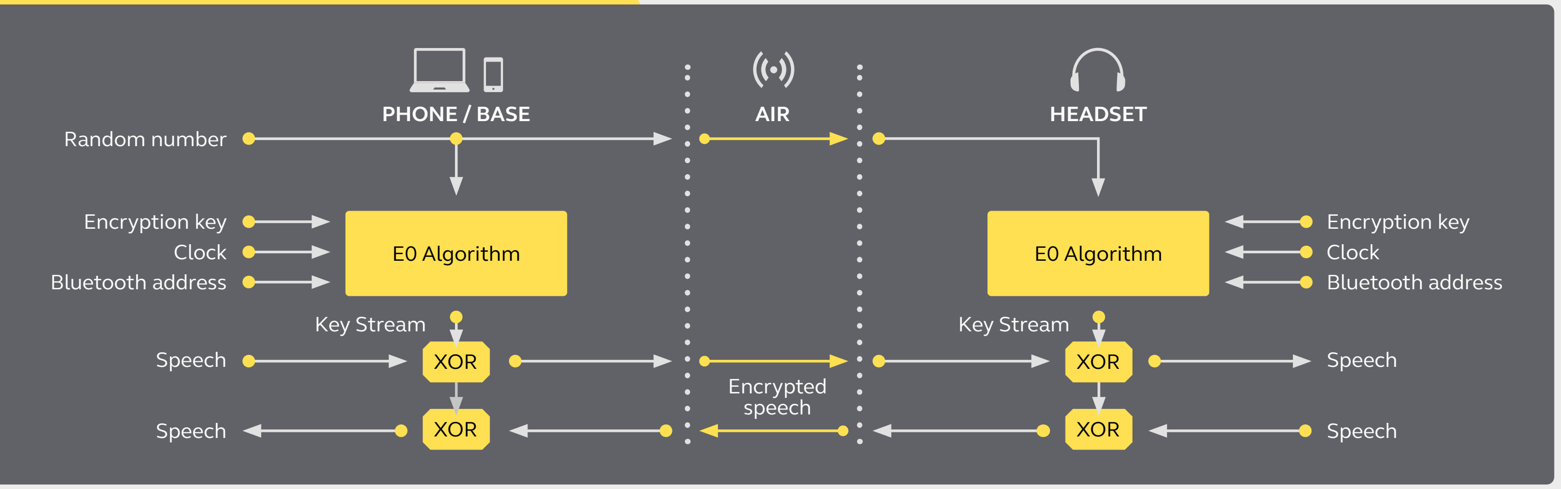
To be able to communicate with each other, two devices need to go through a setup process. At this time, the devices do not have any common link keys, so they calculate an initialization key based on a random number, a Bluetooth address and a Personal Identify Number (PIN) code. This key is only ever used during pairing. After the initialization key has been created, the units then create their common link key. Mutual authentication happens next, to verify that the same link key has been created in both devices. The pairing process is probably the weakest link in Bluetooth security. If, for example, an attacker managed to steal a random number during pairing, it would significantly increase the chances of them stealing the link key.

For this reason, pairing procedures should always be kept as private as possible.

So we go 'invisible'

During pairing, the devices in play are visible to other devices. After a short time, or a successful pairing, Jabra products automatically return to 'non-visible' mode. For many PCs and older mobile phones, however, this may not be possible. These devices often have to be set to non-visible manually. As you can imagine, a non-visible device is much harder for a potential intruder to identify. The introduction of Bluetooth 2.1+EDR specification has brought further security improvements. The pairing between devices supporting the new specification does not require the use of PIN codes. This makes the pairing process less complicated for the end users, and security is even stronger.

E0 ALGORITHM



Authentication

Authentication between Bluetooth devices happens by a 'challenge-response scheme'. The idea is to check that the other device really belongs to paired devices listed. A commonly shared secret is used to check this - the link key. The link key is established during the pairing process. In the challenge-response scheme, the verifier challenges the other unit by sending out a random input. The responding unit calculates a response based on the E1 algorithm. This algorithm uses the random input + responding units Bluetooth address + the link key to calculate a response to the verifier. Part of this response is then sent back to the verifier, which compares the result with its own calculation of the E1 algorithm. If there is a match, it means the verifier has successfully managed to authenticate the responder. The responding unit may choose to authenticate the verifier by repeating the procedure.

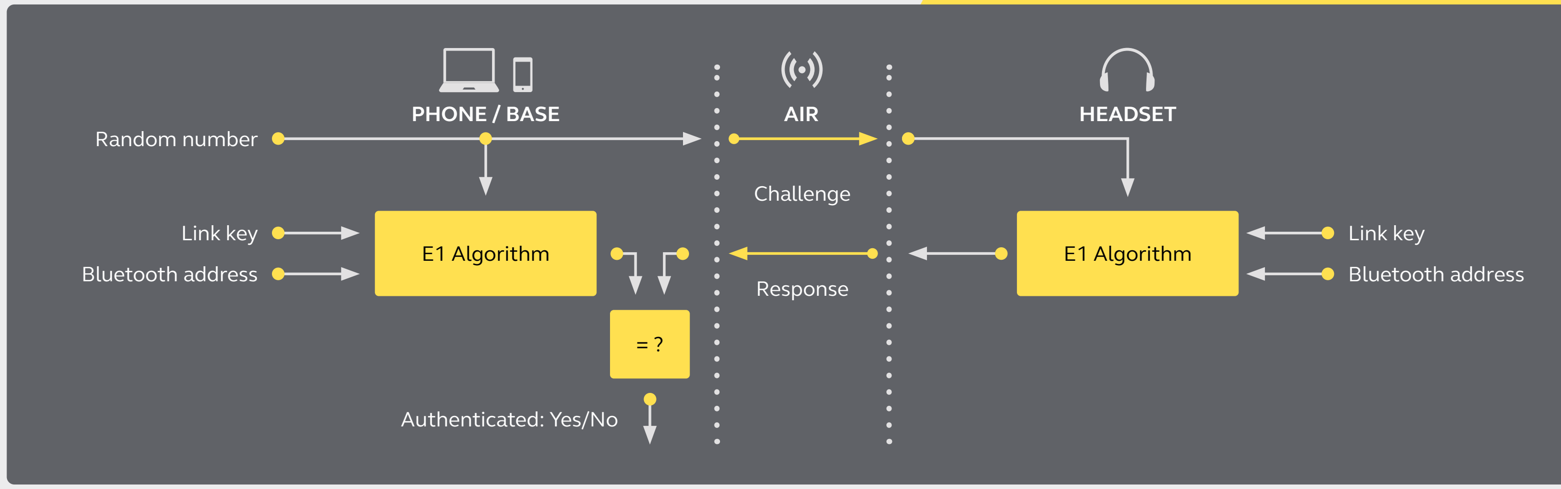
Encryption

The packet payload can be encrypted. This happens through a stream cipher called E0. This cipher re-synchronizes for every payload, minimizing the risk of correlations and attacks. The E0 algorithm uses the master Bluetooth address, the master real-time clock and the encryption key. The encryption key comes from the current link key, ciphering offset and a random number. Jabra products use a 128-bit long encryption key. The master sends the random number in plain text to the other devices before encryption starts. The E0 algorithm delivers a key stream which is XOR-ed to the data that needs to be encrypted. Since the cipher is symmetrical, decryption is handled in the same way.

Overall, Bluetooth security is strong

We hope you found this white paper informative and useful. We have outlined the main principles of Bluetooth security, and looked at how effective it is. There are risks attached to anything, but in general, Bluetooth security is strong, and is only ever getting stronger, thanks to developments in engineering and product testing.

E1 ALGORITHM



Ask us anything

If you have any more questions about Bluetooth security with Jabra products, please do not hesitate to contact your Jabra representative.

WHO WE ARE

Jabra is a leader in communications and sound solutions. We create intelligent headsets and communications tools that help professionals work more productively; wireless headphones and earbuds that let consumers enjoy better calls, music, and media; and pioneering video conferencing solutions for more inclusive meetings.

Thoughtfully designed. Purposefully engineered. Expertly built.

Jabra WP Bluetooth security 231020