WHITE PAPER

BLUETOOTH SECURITY

JABRA.COM

Jabra®
YOU'RE ON

BLUETOOTH SECURITY

BACKGROUND

During the past years wireless voice communication over *Bluetooth®* has increased rapidly. With over 2 billion units out on the market it is fair to raise the question how secure Bluetooth communication is. Can a Bluetooth headset be used without the risk of being eavesdropped?

This paper explains the security that Bluetooth technology offers and gives a view of the different security risks using the technology.

EXECUTIVE SUMMARY

The risk of unauthorized access to Bluetooth voice calls is very limited. Bluetooth offers security measures that give the user a very high level of actual security. The Bluetooth part of the communication link offers as good security as the other systems that typically are used in such a link e.g. PSTN, VOIP or cellular network.

The risk that an intruder could pick up Bluetooth signals and hack into a voice conversation is very low. Even with access to the data that has been sent, it would require extreme skill and a lot of time to get something meaningful out of data collected.

If someone should gain physical access to the *Bluetooth®* headset or base and pair it with another device it is not possible for the intruder to access conversations taken place between the originally paired devices. If an unwelcome third party should want to get access to confidential information there are easier and more effective ways to follow than trying to hack a Bluetooth connection. Millions of Jabra Bluetooth headsets are used daily, offering its users secure and convenient voice communication.

HOW DOES BLUETOOTH SECURITY WORK?

Bluetooth security keeps unwanted third parties from accessing the information that is exchanged between devices. The security system in Bluetooth builds upon three procedures: Pairing, Authentication and Encryption.

PAIRING

The first time two devices are going to be used together they need to go through a user initiated setup process called pairing. During the pairing process the devices goes through a handshake procedure that creates a commonly shared secret key. The secret key is never transferred over the air and cannot be stolen by a third party. Once the pairing is completed the secret key is stored and used for authentication and creation of encryption keys when 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.

AUTHENTICATION

The idea with the authentication is to check that the other device really belongs to the paired and trusted devices. This is done by a challenge-response scheme. One device uses the secret key with specific rules to create a challenge for the device it wants to authenticate. If the device that is being challenged is paired it will have all the necessary information to calculate the correct answer to the given challenge.

ENCRYPTION

The purpose with encryption is to make the data transmitted between two units unreadable for everyone except the rightful receiver. Data that is sent is encrypted by the sender using an encryption algorithm. The receiving unit will decrypt the data back to its original format based on the same algorithm.
Only the paired units know the information that is necessary to perform encryption and decryption. The encryption information is never sent over the air. It is embedded in the units. This makes it very difficult for an eavesdropper to make anything out of the data even with access to it.

WHAT IS THE SECURITY LEVEL?

Bluetooth is used for many different purposes, data synchronization, wireless keyboards and mice, gaming controls etc. But even with so many user areas voice communication between phone and headset is still one of the biggest.
Since the introduction of Bluetooth there have been attempts to hack different kinds of Bluetooth devices in order to gain access of information that should be kept protected. In almost every case these attacks have explored implementation errors made by manufactures. Once aware of the problem the manufacturers have been able to solve the issues with software upgrades.

In the cases where security flaws in the Bluetooth protocol has existed, the issues have usually been found by engineers in their attempts to show that there is a security issue with the protocol and how it can be improved. This leads to a constant development of the Bluetooth security protocol.
Jabra is not aware of any attacks towards Jabra headset equipment. The known attacks that specifically have been made against headset equipment have not compromised Jabra products.

SECURITY AND PROTECTION

SECURITY	WHAT IS IT?	HOW IS IT HANDLED?	SECURITY LEVEL
Eavesdropping	A third party gets acces to a *Bluetooth®* connection and listen in on a conversation.	Voice is converted to a digital data stream that is encrypted	**HIGH SECURITY** Equipment that can monitor a Bluetooth connection is expensive. Even with the right equipment it would require that the eavesdropper is present when the pairing takes place and then the eavesdropper would have to psysically follow his target closely.
Virus	A virus is sent to the Bluetooth system over the air	Jabra Bluetooth systems does not offer an environment where a virus can run	**VERY HIGH SECURITY** There have been viruses made by engineers as a proof of concept of security flaws. Currently there are no known Bluetooth vis´ruses that are harmfull.
Third party access equipment	Someone gets compatible radio equipment that can access Bluetooth and uses the equipment to break the authentication and encryption.	Bluetooth has authentication and encryption built in that prevents unauthorized third partys to connect and understand the contents of the communication.	**HIGH SECURITY** The build in security in Bluetooth gives good protection. The intruder needs to use the equipment during the pairing procedure to have a chance.
Man in the middle attack	During the pairing an attacker tries to relay all information over his unit without the knowledge of the units being attacked. If succeeded the attacker can modify data sent between them or connect later to one of the units.	The best way to protect against this type of attacks is to make sure that the pairing takes place in a private environment.	**VERY HIGH SECURITY** It is very difficult to perform this attack in practices. No real-life cases have been reported.
Free calling	A third party tries to pair a headset with a Bluetooth system in order to make phone calls for free.	Pairing and authentication makes sure that a device can't be paired without physical access.	**HIGH SECURITY** The intruder would have to get physical access to the phone to pair his device. If the intruder managed to pair he would only be able to place calls when being in close proximity to the target.
VoIP	Someone accesses a LAN through a Bluetooth unit supporting VoIP.	Bluetooth security is handled in the same way for VoIP as for other voice communication.	**HIGH SECURITY** Jabra products only offer voice data to be transferred from the Bluetooth headset to the connection point. It is therefore not possible to access data in a LAN via a Jabra Bluetooth product.

BLUETOOTH SECURITY IN DETAIL

PAIRING

As mentioned earlier two devices need to go through a setup process to be able to communicate with each other. At this time the devices does not have any common link keys, they therefore calculate an initialization key which is based on a random number, a *Bluetooth®* address and a Personal Identify Number (PIN) code. This key is only used during pairing procedure. After the creation of the initialization key the units shall create their common link key. When the link key has been created mutual authentication shall be performed to verify that it is the same link key that have been created in both devices.

The pairing process is probably the weakest link in Bluetooth security. If an attacker manages to steel e.g. the random number during the initial pairing procedure it significantly increases the chances to derive the link key. Therefore it is recommended that the pairing procedures should be kept as privately as possible.

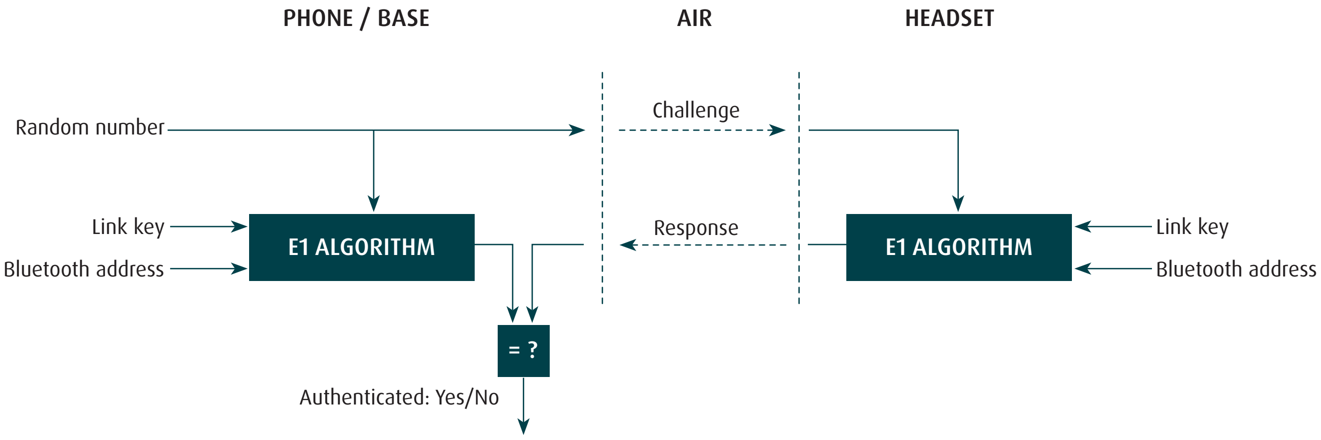
During the pairing the devices are visible to other devices. After a short time or a successful pairing Jabra products automatically return to a non visible mode. For many PCs and older mobile phones this might not be the case. These devices often have to be set to non visible manually. A non visible device is much harder for a potential intruder to localize.

With the introduction of Bluetooth 2.1+EDR specification there has been enhancements made to the security. The pairing between devices supporting the new specification will not require the use of PIN codes. This makes the pairing process less complicated for the end users at the same time as security is improved.

AUTHENTICATION

Authentication between Bluetooth devices are done by a challenge-response scheme. The idea is to check that the other device really belongs to the list of paired devices. A commonly shared secret is used to check this, the link key. The link key is established during the pairing process of the devices.

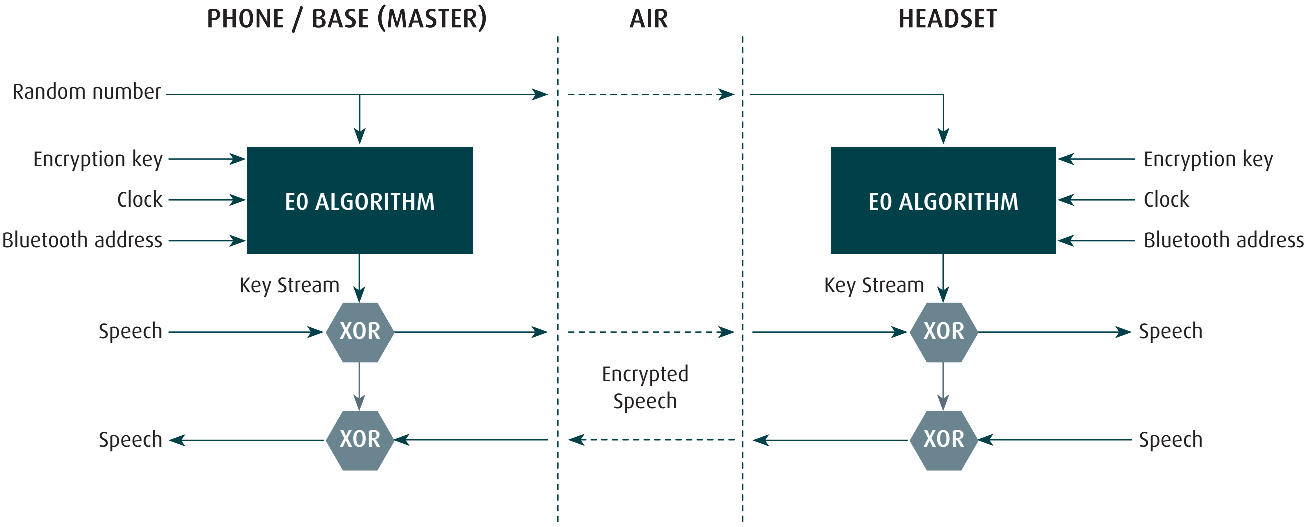
In the challenge-response scheme the verifier challenge the other unit by sending a random input. The responding unit calculates a response based on the E1 algorithm. This algorithm uses the random input + responding units Bluetooth address + the link key to calculate a response to the verifier. A part of the response is sent back to the verifier which compares the result with its own calculation of the E1 algorithm. If there is a match it means that the verifier successfully has managed to authenticate the responder. The responding unit may choose to authenticate the verifier by repeating the procedure.



BLUETOOTH SECURITY IN DETAIL

ENCRYPTION

It is possible to encrypt packet payload, this is carried out by a stream cipher called E0. The cipher re-synchronizes for every payload, by doing that it minimizes the chance that correlations attacks should be successful. As input the E0 algorithm uses the master *Bluetooth*® address, the master real-time clock and the encryption key. The encryption key is derived 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 is started. The E0 algorithm delivers a key stream which is XOR-ed to the data that shall be encrypted. Since the cipher is symmetric, decryption is handled in the same way.


PHONE / BASE (MASTER)
AIR
HEADSET
Random number
Encryption key
Clock
Bluetooth address
E0 ALGORITHM
Key Stream
Speech
XOR
XOR
Speech
Encrypted Speech
E0 ALGORITHM
Encryption key
Clock
Bluetooth address
Key Stream
XOR
Speech
XOR
Speech