WHITE PAPER

DECT PROVIDES HIGH PROTECTION AGAINST UNAUTHORIZED ACCESS

JABRA.COM

Jabra®
YOU'RE ON

BACKGROUND

Wireless communication for voice and data is growing worldwide. The amount of DECT (Digital Enhanced Cordless Telecommunications) and GSM phones, *Bluetooth*® -enabled devices and WLAN equipment in enterprises and private homes has increased enormously in recent years.

But in the wake of the wireless revolution, concerns are rising as more and more people – experts and laymen - question the security of wireless communication: is it safe from eavesdropping and vandalism? Could unauthorized third parties enter a network and access information to personal or corporate detriment? Answers to these and other securityrelated questions are desperately needed; corporations and their employees are entitled to full assurance that their conversations cannot be hacked and that they are not exposed to any personal or commercial security breach as a consequence of using wireless communication devices.

Jabra supplies wireless headsets for DECT-based telecommunication. In this paper we examine the security the DECT protocol offers to give a true and fair view of the actual security levels involved.

EXECUTIVE SUMMARY

The security level towards unauthorized access to DECT voice calls is extremely high.

DECT standard security measures ensure a very high level of security. DECT is a certified standard in 110 countries used by millions of people, and is one of the most secure wireless standards for civil use. No matter whether employees use DECT handsets or headsets, protection against wireless intrusion is very high.

The possibility that intruders could pick up DECT signals and hack their way to critical information in telephone conversations is unfounded, due to the lack of suitable equipment to perform such an intrusion.

Even in the very unlikely scenario of DECT radio signals being picked up by a third party, it would require an enormous amount of computer power and transactions collected over a period of several months to make anything meaningful out of the signals.

Should someone obtain direct access to DECT equipment and succeed in pairing a DECT hand-set or headset with a DECT base station, access to conversations on DECT units other than that in their possession would not be possible.

Finally, it could be argued that the wireless DECT connection in itself offers a higher security level than a traditional copper line since it is both digital and encrypted. Hence, the more copper lines replaced by DECT connections, the higher the total communication security level becomes. In comparison to such devices as WLAN and *Bluetooth*®, DECT's security routines are embedded in the protocol and cannot be deactivated.

WHAT IS DECT?

DECT is a radio technology ideal for voice, data and networking applications with range requirements of up to a few hundred meters. It is a fully digital communication technology that provides wireless connection between two or more units in residential, corporate and public environments. The DECT standard delivers high speech quality and security against radio interference. Since the introduction of the first ETSI approved standard in 1992 DECT has been most widely used for voice communication in wireless phones and wireless headsets.

DECT transforms analog sound (e.g. a conversation) into a digital data stream before transmitting from one DECT unit to another. When the stream reaches the receiving unit it is transformed back to an analog signal and sent to the handset or headset speaker. DECT is a proven technology with great potential for many years to come. In recent years the number of data applications developed for DECT has increased slightly, but voice communication still accounts for the lion's share of DECT traffic.

WHAT IS SECURITY?

DECT communication security keeps unwelcome third parties from accessing the content of electronic transactions, in this case voice calls. Wireless security has two main constituents: Authentication and Encryption.

AUTHENTICATION

Initial authentication is the process by which the base station and the handset/headset connect with each other for the first time by "pairing". They exchange a unique handshake based on specific rules and calculations, unit identities are exchanged, and both base station and handset/headset run a secret authentication key to be used for every following call set-up. The secret key is not transferred over the air and cannot be "snatched" by an external third party even with physical access to the units involved. Once paired, the two units "remember" each other and will be able to authenticate each other automatically based on the handshake exchanged when pairing.
Pairing can only be done with physical access for the units, as it cannot be activated over the air.
During pairing, encryption data unique to the two specific units is also exchanged. This is vital to make the encryption of transactions between the two units work.

ENCRYPTION

Encryption in DECT is a process which deliberately mixes (encrypts) the digital data stream while it is transmitted between two units using an algorithm (a very complex calculation), presenting only a meaningless stream of electronic gobbledygook in the very unlikely event that a third party obtains access to it. When the data stream reaches the rightful receiver it is decrypted (transformed back) to its original format.
Conversion is done by a range of factors known only to the paired units. None of the encryption factors are transmitted with the data stream, but are either embedded in the units or authenticated in the initial pairing (see authentication).
This means that it is practically impossible for any potential eavesdropper to make anything out of the data stream.

HOW BIG IS THE CHALLENGE?

DECT is, both in theory and practice, a very secure wireless standard. Jabra is are not aware of any instances of a DECT transaction being compromised since its introduction – and we're in the business!

DECT security is influenced by the fact that the DECT protocol has primarily been – and still is – used for voice communication via DECT phones and headsets. Voice transactions (telephone calls) are neither stored in Jabra bases nor in headsets, and the content of a DECT transaction does not exist when a conversation has ended. Hence, an intrusion must be made in real time, while the voice conversation takes place, in order for an intruder to access any information.

Today, no commercially available equipment exists that can monitor a DECT line and decrypt data streams to recreate the voice stream. DECT is digital, not analog, and uses a very complex encryption algorithm that is only known by DECT manufacturers.

Remote access through wireless equipment modified and debugged for control by a PC was demonstrated by a collaboration of European universities in late 2008. However, the documented eavesdropping was only possible on unencrypted links originating from handsets not taking advantage of the security options in the DECT technology. Proper implementation of authentication and encryption still protects the wireless link against such attacks.

Consequently, neither hard- nor software for DECT monitoring or scanning has ever appeared on the market. Other ways of accessing confidential information are likely to be far less demanding in terms of time and resources.

We share the views of other security experts that DECT offers an extremely secure platform for voice communication – in fact, it is probably the most secure standard technology for voice communication in residential, corporate and public environments.

What's more, hackers often look for data stored on servers or local disc drives which are accessed through a company's LAN rather than the phone system, putting the DECT usage Jabra applies in its wireless portfolio safely beyond their reach.

DIRECT OR REMOTE ACCESS

In theory, if a person has direct access to the DECT equipment inside the company, it could be easier to intrude. However, the mandatory pairing prevents intrusion if a third party does not have access to the base station.

In the highly unlikely event of someone breaking into a company, getting physical access to a base station, succeeding in pairing a handset or headset with the DECT system and leaving unnoticed, that person will still not be able to access other voice conversations on the DECT system. Hence, there is no risk of eavesdropping even though the person has access to the phone system. If the person has paired a handset with the DECT system, the most critical problem is free calls over the company's switchboard.

Remote access through wireless equipment e.g. connected to a PC is – as mentioned earlier – very unlikely since such equipment is more or less impossible to get hold of.

SECURITY AND PROTECTION

SECURITY	WHAT IS IT?	HOW IS IT HANDLED?	SECURITY LEVEL
Eavesdropping	A third party gains access to a DECT transaction and listens in on a conversation	Voice is converted to a digital data stream that is encrypted using 64-bit encryption	**HIGH SECURITY** Equipment that can monitor a digital radio transaction is very hard to obtain, and it is very difficult to develop software that can decrypt a data stream. The combination of the two is very unlikely
Virus	A virus is sent to the DECT system over the air	The DECT standard does not allow execution of code strings, programs or macros	**VERY HIGH SECURITY** It is not possible to interfere with the processing power in DECT equipment, since the DECT standard is not open to foreign code, macros etc.
Third party acces equipment	Someone gets hold of PC-compatible radio equipment that can access DECT and uses it to break the authentication and encryption	DECT has authentication and encryption built-in that prevents unauthorized third parties from accessing the network and its contents	**HIGH SECURITY** Due to DECT's built-in security and the fact that this type of equipment is inaccessible, since it hardly exists
Piggy-in-the-middle attack	A unit will masquerade as a base station and a handset and place itself between the units it intends to attack. The authentication pro-cedure between the units attacked will take place as normal, with the difference that all data is exchanged via the attacker. In this way an attacker may obtain the information he needs to be able to connect	The best way to protect against this type of attack isto use encryption to prevent the attacker from deactivating it or preventing it from activating	**HIGH SECURITY** This is theoretical
Free calls	A third party succeeds in pairing a handset with a DECT base system and can make unauthorized calls for free	Pairing routines provide a very high security level	**HIGH SECURITY** It is very unlikely that an intruder could enter a company unnoticed, get access to a DECT system and pair a handset. Furthermore, the intruder would have to remain in close proximity in order to use the phone
VoIP	Someone accesses the LAN through a DECT unit supporting VoIP	DECT radio communication is secure as described above – no matter what carrier is used	**HIGH SECURITY** DECT offers the same high security no matter what type of network protocol is used in the network

DECT AND SECURITY ROUTINE IN DETAIL

As already mentioned, DECT security is based on authentication algorithm) and encryption (a key stream generator). Below you will find a more in-depth description of the security routines in DECT.

DECT AUTHENTICATION

DECT uses an authentication algorithm called the DECT Standard Authentication Algorithm (DSAA). The specification for DSAA is not publicly available, only DECT manufacturers have access to it. The authentication works as follows: The base station sends a random number (challenge) to the handset over the air.

The handset calculates and sends a response to the base station by using the random number and its own authentication key (exchanged in the initial pairing). The response is checked by the base station against what is expected. If there is a match the base station authenticates the handset.

DECT ENCRYPTION

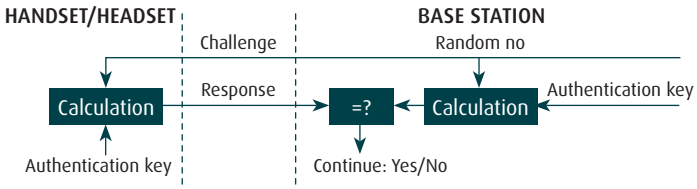
DECT uses the DECT Standard Cipher (DSC) for data encryption. DSC is a stream cipher which uses a 35 bit long initialization vector (IV) and a cipher key as input for generation of the key stream. The DSAA (standard algorithm) for DSC specification is not publicly available. There are two types of cipher key that could be used as input for the key stream generator:

- Derived Cipher Key, an output value from an authentication between a base station and handset. If authentication is performed for each call established, a new cipher key will be used for all calls.

- Static Cipher Key, this key could be used to establish encryption without going through the authentication process. DECT does not support generation or distribution of this key.

The IV will be initialized with the frame number for the frame to be encrypted. For each frame sent the IV will be increased according to that frame number. With the IV and cipher key as input, a key stream is derived by DSC. The key stream will then be XOR-ed with the data field that is going to be sent. Depending on the kind of data field sent some part of the key stream may be discarded in the XORing process. Decryption of the data field is done in the same way as encryption.

DECT Authentication



DECT Encryption