

Wireless Security

March 2007

Whitepaper

DECT™ Headset Security

Plantronics DECT wireless products (CS60™, CS70™ and SupraPlus® Wireless) use a digital technology and meet the full requirements of the DECT standard security requirements, as outlined in ETSI EN 300 175-7.

Security is one of the many strong points of a DECT system which uses TDMA/TDD digital radio and dynamic channel selection, together with a three layer security system. This 3-layer system of subscription verification, encryption and authentication ensures a very high level of protection against eavesdropping:

1. Subscription verification

Base and remote devices are paired to one another such that they can easily identify their correct base or remote to a first level. A secret authentication key is calculated using the DECT Standard Authentication Algorithm (DSAA). Definition of this algorithm in full is only made available to the equipment manufacturers.

2. Encryption

The cipher-key is used to encrypt the data being transmitted over the air link.

3. Authentication

Both ends check the appropriate authentication key is used and also calculate cipher keys (used to encrypt the data sent over the air). The DECT Standard Cipher (DSC) is used; again definition of this algorithm is only made available to the equipment manufacturers.

RF Protocol:

With dynamic channel allocation, the RF protocol itself provides a level of security with channels and timeslots changing as the environment suits over 10 carry frequencies and 12 time slots per carrier (for each communication direction).

Bluetooth® Headset Security

Despite quite widespread press reports of Bluetooth security vulnerabilities in devices such as phones and PDAs, the audio connection between a phone and a Plantronics Bluetooth headset is highly secure- using advanced authentication and encryption algorithms.

Headsets need only be “discoverable”, (visible to other devices) for a short time when they are set-up for use with a new device (eg mobile phone). During this process (commonly called “Pairing”) the two devices exchange information to establish a ‘secure’ connection. Note that the base of the Plantronics Voyager™ 510 system which connects to a deskphone is never discoverable.

After pairing is completed, the Plantronics headsets are not visible to any other device and all transmission are encrypted.

The pairing process

For the pairing process to be completed, the following information is exchanged:

1. Each device's Bluetooth addresses
2. A user-entered PIN number.
3. A unique time-stamp generated from the mobile phone

These items are combined to generate a 128-bit security key which is used for future connections between the headset and phone (or Voyager base). The time-stamp is extremely difficult to guess at a later date, even if the address and PIN are already known to a potential eavesdropper.

As all communication between Bluetooth devices uses frequency hopping spread-spectrum radio transmission system, it is particularly difficult to intercept.

Secure conversations

The Plantronics headsets with DECT technology uses the 128-bit security key to digitally encrypt audio between the headset and phone (or Voyager base), similar to the method by which GSM radio signals between the mobile phone and base station are encrypted.

Many widely publicised Bluetooth vulnerabilities do not apply to headsets, but there are some things that can be done to improve security on the phone- the most important being to disable the discoverable mode on the phone:

Disable 'Discoverable' mode:

Unless a user frequently exchanges business cards over Bluetooth, Plantronics recommend setting the phone to hidden or 'non-discoverable' mode to improve security, since the phone does not need to be in 'discoverable' mode to operate with a Plantronics headset; which is always in non-discoverable mode except while pairing.

'Hiding' your phones in this way also reduces the risk of "Bluesnarfing" (the stealing of telephone contact details from a Bluetooth phone or PDA (NOT from Plantronics headsets, which stores no such data).

If used properly, Bluetooth headsets and the phones to which they are paired will be difficult to attack. However, hackers are extremely ingenious in their methods making it impossible to guarantee that any device is completely secure.

However, due to the low power of Bluetooth (typically 10 metres range), it is more difficult for an eavesdropper to 'hack' the secure connection. In fact, they will arguably have more success simply using their ears to simply listen to what is being said.