A Revolabs White Paper

Solo Executive Wireless Microphone System Security

Security Features Provided By DECT Protocols

By Thomas Zimmerman, CTS
Staff Engineer

The information contained in this document represents the opinions of Revolabs, Inc. based on the analysis of data collected by other subject matter experts. This paper should not be interpreted as a commitment on the part of Revolabs, Inc., and is presented for informational purposes only.

REVOLABS, INC. MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Revolabs, Inc. • 63 Great road, Maynard, MA01754 • USA www.revolabs.com

Revision 1.6, August 2006

WHAT IS DECT?

DECT stands for the Digital Enhanced Cordless Telecommunications standard for radio transceiver equipment operating in the 1.9 GHz frequency spectrum. These standards are the work of the European Telecommunications Standards Institute (ETSI) created in the early 1990's to provide reliable, high quality and secure wireless telecommunications equipment. The standards evolved throughout the decade to include robust security features and encryption algorithms to preclude covert interception of wireless conversations and other transmitted data.

HOW DOES DECT WORK?

DECT equipment has two parts: a fixed part (such as the Solo Executive Base Station), and a portable part (the Solo Wireless Microphone). The two parts communicate with each other using Multi-Carrier, Time Division Multiple Access and Time Division Duplex (MC/TDMA/TDD) radio access methodology. Very simply, this means that the allocated RF spectrum of frequencies is split up into sub-carrier channels and these are then arranged into timeslots of available communications paths (seen like the rows (channels) and columns (time) of a spreadsheet). Bursts of digital data (users' speech in this case) are sent and received along these paths. Simultaneously, the paths are monitored by the fixed part for interference from other sources and the bursts are re-assigned to un-used paths as required.

HOW ARE DECT COMMUNICATIONS MADE SECURE?

There are three levels of security employed by DECT based equipment.

The lowest level of security is based on the fact that the system uses digital codec's (coder / decoder) to send data over the air. To someone using a simple frequency scanner in a very close range (less than 30 meters), the only sound heard would be 10ms bursts of digital noise.

The second level of security is performed when a portable part (microphone) requests access rights to communicate with the fixed part (base station). Each microphone in a Solo system has a secret User Personal Identity (UPI), like an ATM PIN code, assigned to it during manufacturing that it uses to create an authentication key for Solo Base Station communication. The Base Station issues a "challenge" to devices requesting access, and the microphone responds by using the UPI to create the answer to the challenge. If the challenge is responded to correctly, using the Base Station requested sub-carrier channel and in the shortest of time increments, the units can then pass data. Otherwise the connection is refused. This is called "pairing the microphone" to the Base Station. *Note: The UPI is never sent directly in the response, but is run through an algorithm modifying it according to random sequences generated and transmitted by the Base Station. Further, the authentication key changes each time a microphone is removed from the Charger Base.*

The third level of security is an encryption cipher key. During the authentication process between a Base Station and a microphone as described above, a 128 bit cipher key is generated by both the base station and microphone to encrypt the digital data sent over the air. An encryption / decryption algorithm using this cipher key then manipulates the data at both devices. Even if the algorithm is known, without knowing the cipher key the transmitted speech remains digital noise. And because the cipher key is generated by the devices, no user knows the key.

WHAT IS THE DECT ENCRYPTION SCHEME?

Fortunately, just knowing how data is encrypted does not make translating the data back to speech any easier. As such, the technical details described here don't really benefit would-be secret stealers.

According to Manuel Alverez in his DECT-related patent application *Device for Implementation of DECT Encryption Algorithm with Reduced Current Consumption*

> The "ciphering algorithm, like most data ciphering algorithms, makes use of generators of pseudorandom sequences of a certain length developed from primitive polynomials.
>
> In this case, there are four sequence generators implemented with four shift registers with intermediate feedback signals of the type known as Gallois, with lengths of 17, 19, 21 and 23 stages respectively, that perform a variable number of shifts for each data clock cycle and from which a memory bit is obtained that is a logical combination of some of the bits of the shift registers mentioned and of the previous value of this memory bit."

Figure 1, below is taken from the ETSI EN 300 175-7:V1.9.1 DECT Standard showing how this process is implemented in the equipment.

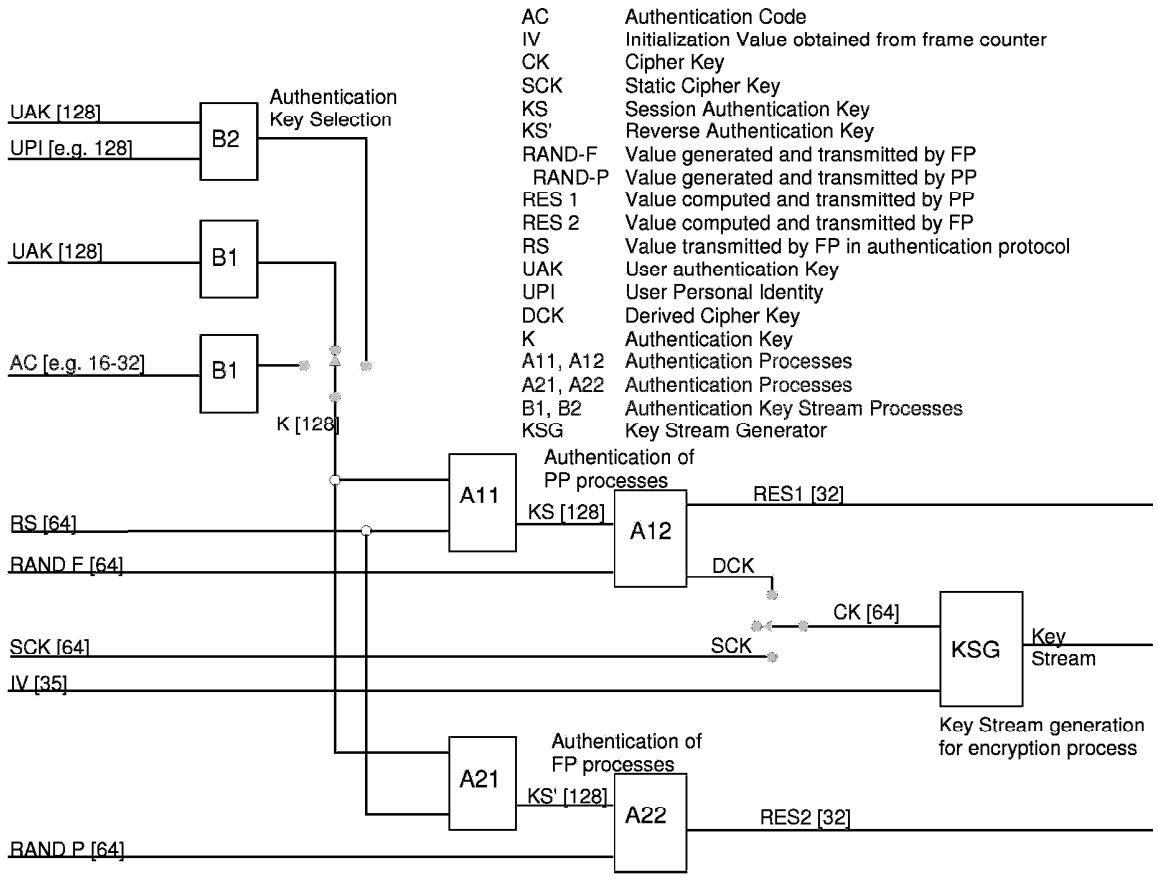

Figure 1: Overview of DECT security processes

WHAT ADDITIONAL SECURITY FEATURES ARE BUILT INTO SOLO EXECUTIVE WIRELESS MICROPHONE SYSTEMS?

One potential risk to system security could occur if a wireless microphone is “removed” from the users’ conference room. Because the microphone contains an analog audio earpiece port, there is the potential for eavesdropping on future meetings. Fortunately, a missing microphone is normally obvious because of the absence of a microphone from the Charger Base. Even though it is unlikely that someone could get within range (less than 30 meters) to use the microphone to listen in surreptitiously, the system provides an easy method to remove a missing microphones ability to access the Base Station. Simply holding down the pairing button for that microphone channel on the Base Station until it enters the pairing mode removes permission for that specific microphone to access the system (see the *Solo Executive Wireless Microphone Owners Manual* for instructions).

Another feature of the system that makes it more difficult to decipher the data streams between microphone and Base Station is audio data compression. As stated above, the audio data is digitized before being sent through the air. In order for the data to be sent as efficiently as possible, the digitized data is then compressed using another algorithm to remove bits of information that don’t affect the audio quality. As a result, the data steam is yet again modified providing no easily decipherable speech information.

References

ETSI EN 300 175-7:V1.9.1 "Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 7: Security Features".

Einstein Informatik at http://einstein.informatik.uni-oldenburg.de/rechnernetze/seite24.

Software Patent: Device for implementation of DECT encryption algorithm with reduced current consumption. Alvarez, Manuel José (ES) http://gauss.ffii.org/PatentView/EP661843 08-12-1994