

Bluetooth is 2.5 Quintillion Years Secure

In the July 11, 2005 issue of The Green Sheet, an article titled "Security Flaw Exposed in Bluetooth", discussed the findings of two researchers relative to the pairing process, a process by which two devices, using Bluetooth communications, associate themselves with each other for the wireless transfer of information. The research referenced in the article focused on the PIN which is used as the secret shared between two Bluetooth devices. It was correctly noted that most Bluetooth implementations use a short 4-digit numeric-only code for their PIN.

There is a version of Bluetooth, utilized by Ingenico, which uses a full-length (128-bit) PIN in the pairing process. In the article it was stated that a 4-numeric digit PIN could be discovered in less than a second (0.06 seconds). However while longer PINs were mentioned as a more secure alternative, no figures of the relative strength were presented. In fact when compared to the time to discover a 4-digit PIN, it would take over 2.5 quintillion years (25 with 17 zeros) years to find a 128-bit PIN. A full-length PIN is essentially uncrackable.

The 128-bit PIN version of Bluetooth used by Ingenico has been tested and confirmed as secure by a number of credible laboratories. Additionally, Ingenico provides SSL encryption in our products, so that our customers can use state-of-the-art encryption for communications between our terminals and acquiring institutions.

While nothing is completely unbreakable, our Bluetooth security is state of the art and not prone to the weaknesses as described in The Green Sheet article.

Collectively, Ingenico has shipped well over 200,000 short-range wireless devices. Our company is a recognized leader in secure transaction acceptance. Through careful and responsible implementations such as found with Ingenico's complete range of wired and wireless communications products it is possible to provide secure payment transactions.