Bluetooth Security – Truths and Fictions

Foreword

Bluetooth security is a complex and often-misunderstood topic. A good understanding of security principles is important, but it is equally important to understand how protocol analyzers handle security in order to correctly define security requirements in a *Bluetooth* device.

This paper will cover a few often-misunderstood topics and will provide clarifications accordingly. Take the quick "test" below and see how you do!

Truth or Fiction?

PIN-code based pairing is not secure: Truth
This pairing method does not provide any real security. A modern protocol analyzer such as the Ellisys BEX400 can automatically determine a 6-digit PIN-code and deduce the related link key in a few hundred milliseconds, just by passively looking at the pairing traffic exchanged over the air. What does this mean for *Bluetooth* users? Pair your devices in a safe environment.

Simple Secure Pairing, as its name implies, is secure: Truth
While PIN-code based pairing is not secure, SSP-based pairing is a major improvement and can certainly be considered secure (at least until a major breakthrough is done on computing power). SSP is based on the Diffie-Hellman key exchange, a strong asymmetrical key exchange algorithm used in critical applications such as banking, online payments, etc. What does this mean for *Bluetooth* developers? Debugging SSP *Bluetooth* devices is now trickier. Find out more about *Bluetooth* security and SSP in the "Secure Simple Pairing Explained" Expert Note.

***Bluetooth* is not secure: Fiction!**
Any security algorithm can be defeated with a sufficient amount of computational power, but even with today's super-computers it would require years to decrypt data securely sent over *Bluetooth*. As indicated above, the PIN-code based pairing is not secure, since the traffic can be captured and decrypted with a whole-band sniffer. Therefore, in Bluetooth communications involving critical data, it is best to consider SSP or other secure forms of pairing.

It is impossible to decrypt traffic whenever SSP is used: Fiction!
SSP is a just another pairing method used to create a shared link key between paired devices. The only hard requirement for decrypting traffic is obtaining the link key. There are various methods for obtaining the link key, some vendor-specific, and some standard, such as through an HCI capture or via SSP Private Key injection. Find more information about *Bluetooth* security and SSP in the "Secure Simple Pairing Explained" Expert Note.

The only way to debug SSP-enabled devices is by using the SSP Debug Mode: Fiction!
The SSP debug mode is just one of the methods available for determining the link key. When SSP debug mode is used, a known SSP Private/Public key pair is used, allowing determination of the link key. Several other options are available. Find more information about *Bluetooth* security and SSP in the "Secure Simple Pairing Explained" Expert Note.

The link key must be provided before capturing traffic: Fiction!
This may be true with some analyzers, which are using the single-channel capture method, but not for the Ellisys BEX400. With its whole-band capture approach, the Ellisys BEX400 is capable of capturing any traffic, encrypted or not, and decrypting it afterwards by post-processing. This gives the user a lot more flexibility when taking captures. Find more information about the whole-band capture method in the "Capturing Bluetooth Traffic, the Right Way" Expert Note.

It is impossible to decrypt traffic from an already-established connection: Fiction!
While this is certainly not a simple task, it is actually possible. The right information simply has to be provided to the analyzer software. The link key alone is not sufficient, as the data is not encrypted directly with the link key, but rather with a temporary session key derived from the link key and the random numbers that are exchanged at the connection. If the random numbers are known, or alternatively the temporary session key, then it is possible to decrypt the traffic even if the connection has not been recorded by the analyzer.

So, what is your score? If you knew the correct answer to all topics above, get in touch with Ellisys at the next UPF and you will get a free beer!

Feedback

Feedback on our Expert Notes is always appreciated. To provide comments or critiques of any kind on this paper, please feel free to contact us at expert@ellisys.com.

Other interesting readings

- EEN_BT01 - Capturing Bluetooth Traffic, the Right Way
- EEN_BT03 - Your First Wide-Band Capture
- EEN_BT07 - Secure Simple Pairing Explained
- More Ellisys Expert Notes available at: http://www.ellisys.com/technology/expert_notes.php

Rev. A. Updated 2011-05-16