Decrypting Encrypted Bluetooth® data with ComProbe BPA 600

How Encryption Works in *Bluetooth*

Bluetooth devices on an encrypted link share a common "link key" used to exchange encrypted data. How that link key is created depends on the paring method. Paring methods have evolved and changed throughout *Bluetooth* history. The earlier legacy method was used up through *Bluetooth* 2.0. Improved and simpler pairing methods began with Bluetooth 2.1 and remain in the current version *Bluetooth* 4.0.

For a *Bluetooth* sniffer to be able to decrypt the encrypted data, it must also have this shared link key. For obvious security reasons, the link key is never sent over the air, so either the user must get the key out of one of the devices being sniffed and supply the key to the sniffer or the sniffer must create the key itself.

Legacy Pairing (*Bluetooth* 2.0 and earlier)

In legacy pairing, this link key is derived from a shared PIN code, the master's *Bluetooth* clock, the master's BD_ADDR and a random number that is passed between the two devices. If the sniffer has all of this same data, it can create the link key in the same way that the devices do. The sequence of events used to create this key, or pairing process, is shown in the ComProbe software Frame Display below.

AVDTP Signaling | AVDTP Media

Unfiltered | Baseband | Extended Inquiry Response | LMP | Bluetooth FHS

B...	Frame#	LT_Addr	Original Opcode	Opcode	Role	Initiated by
●	246	1		in_rand	Slave	slave
●	247	1		in_rand	Master	master
●	249	1	in_rand	accepted	Slave	master
●	250	1		comb_key	Master	master
●	251	1		comb_key	Slave	master
●	252	1		au_rand	Master	master
●	253	1		sres	Slave	master
●	254	1		au_rand	Slave	master
●	255	1		sres	Master	master
●	256	1		setup_complete	Master	master
●	257	1		encrypt_mode_req	Slave	slave
●	258	1	encrypt_mode_req	accepted	Master	slave
●	259	1		encrypt_key_size_req	Master	slave
●	260	1	encrypt_key_size_req	accepted	Slave	slave
●	261	1		start_encrypt_req	Master	slave

Frame 247 is the LMP_in_rand which is where a random number generated by the master is passed to the slave. The slave acknowledges that it has accepted the number in frame 249. The initialization key has been passed to the slave and is now shared by both devices. Both devices now independently generate combination keys.

In frames 250 and 251, the combination keys are passed between master and slave. In frame 252, the master sends its LMP_au_rand. This is the random number that has been encrypted using the link key that master has calculated. The slave then responds with frame 253, an LMP_sres confirming that it was able to compute the same number. That process is repeated in the other direction (slave to master) in frames 254 and 255. This completes the authentication between devices, and the the setup_complete message is sent and the slave requests encryption mode in frame 257, and the master accepts in frame 258. The actual encryption starts after the start encryption request in frame 261.

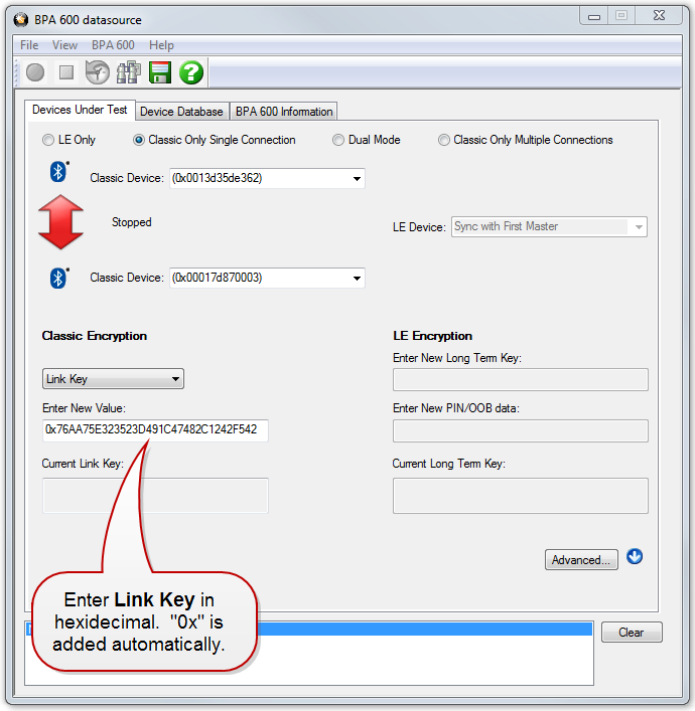
In order for the ComProbe software to decrypt an encrypted *Bluetooth* conversation, the ComProbe software must compute the same link key being used by the devices being sniffed. Since this link key is never sent over the air, the ComProbe software must have all of the same information the devices being sniffed have so that it can calculate the same link key that each of the two devices does. To decrypt successfully, the ComProbe software must know the PIN code and capture:

- The LMP_in_rand
- Both LMP_comb_keys
- Both LMP_au_rand/LMP_sres pairs.

If any of these are missed, the ComProbe software will not be able to decrypt. If you capture encrypted data and find that everything captured after the LMP_start_encryption_request is in error, look back at the LMP frames previous to that and you'll probably find one or more of these missing. The Start Encryption Request with also be marked by the ComProbe software with an error that indicates that the link key calculated by the ComProbe software is different from the one used by your devices.

Secure Simple Pairing (SSP) (Bluetooth 2.1 and later)

To capture and decrypt data between two Bluetooth devices using Secure Simple Pairing we have two choices. If one of your devices can be put into Secure Simple Pairing Debug Mode, all that needs to be done in I/O Settings is to choose your devices. It doesn't matter what's been selected in the Pairing Method drop down, the ComProbe software will see the debug messages being sent and calculate the correct key. Only one of the devices needs to be in debug mode and it doesn't matter which one.



If neither of your devices can be put into debug mode, you'll need to know the link key being used by one of your devices, generally by accessing the HCI on one of the devices. If that is the case, enter the link key into the box provided.

Note that the link key is sometimes stored in your device in reverse order. The ComProbe software will automatically reverse the link key, if needed.

Once the link key has been entered, decryption operates the same way it does in legacy pairing.

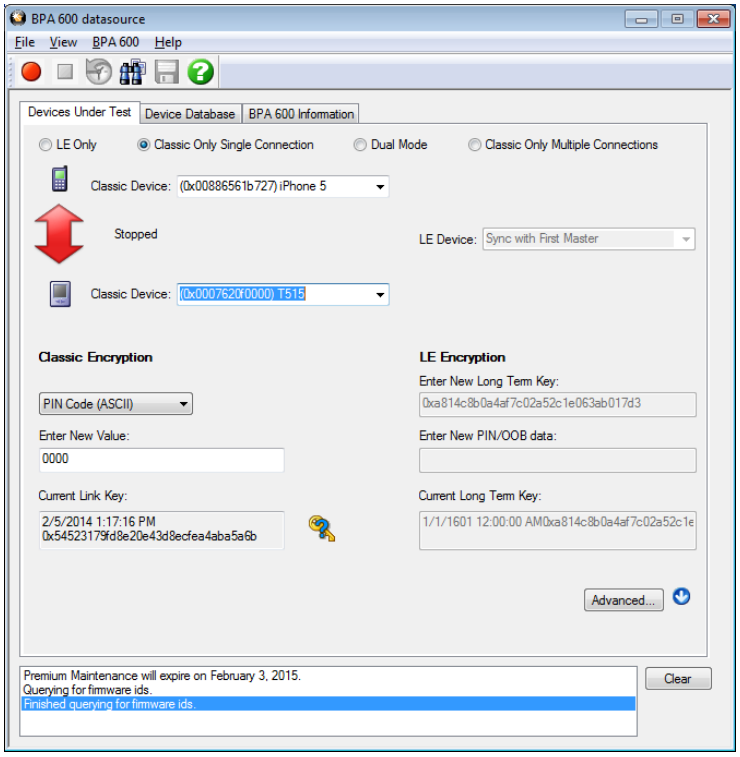
How to Capture and Decrypt Data (Legacy Pairing)

Run the ComProbe software and select Bluetooth Classic/low energy (BPA 600). This will open the Control window and the BPA 600 Datasource where ComProbe device parameters are set for sniffing including the

devices to be sniffed and how the link key is to be encrypted.

Select the Devices Under Test tab. Make both your *Bluetooth* devices discoverable.

Click the Discover Devices  on the datasource toolbar. The ComProbe software will find any discoverable *Bluetooth* devices within its range. You will then be able to select your devices from the drop down lists. If one or both of your devices cannot be made discoverable, you may type in the BD_ ADDR(s) directly.



With legacy pairing, select PIN Code (ASCII) from the Classic Encryption drop down and fill in the PIN. As mentioned above, the ComProbe software needs the PIN code in order to calculate the link key the two *Bluetooth* devices are using. Alternately, you may enter the Link Key manually if it is known. The ComProbe software also keeps a database of the link keys it previously calculated, which may be accessed on theDevice Database tab.

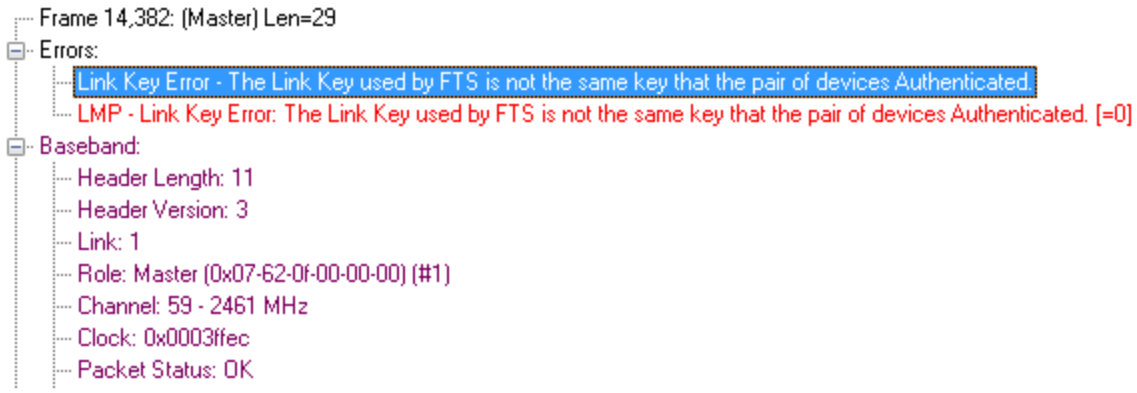
The Start Sniffing button  should now be available. If Start Sniffing is grayed out, there is something set up incorrectly in the datasource Device Under Test tab. For example, if you selected PIN code in the encryption drop down but you neglected to fill in the PIN code, then Start Sniffing will be grayed out.

Click on the toolbar Start Sniffing button. The Control window will display a capture status message. When you start sniffing, the colored arrow be red indicating that the Bluetooth devices are initializing. . After a few seconds the arrow will turn green  and the status will change to “Waiting for the master to connect to the slave”. At this point the BPA 600 is synchronized and waiting for a baseband connection.

When your connection is established, the arrow will turn blue  , signifying that a baseband link has been established and data should start to appear in the Frame Display. The direction of the arrow indicates which device is master and which is slave. The arrow points from master to slave.

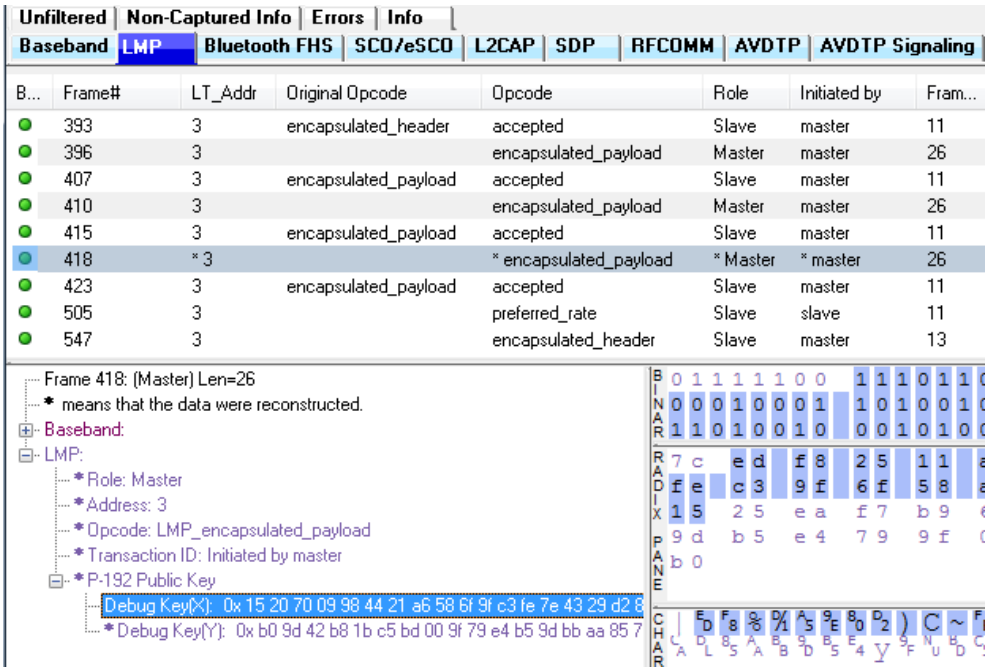
If ComProbe software successfully calculates the correct link key, the Link Key icon  on the datasource is updated with a check mark to indicate that the link key has been verified. Should the link key be incorrect the link key icon will show  .

An incorrect link key will show up in the Frame Display. Open the Frame Display LMP tab and search for frames with errors appearing in red. In the Decode pane a link key error will appear in red under Errors.

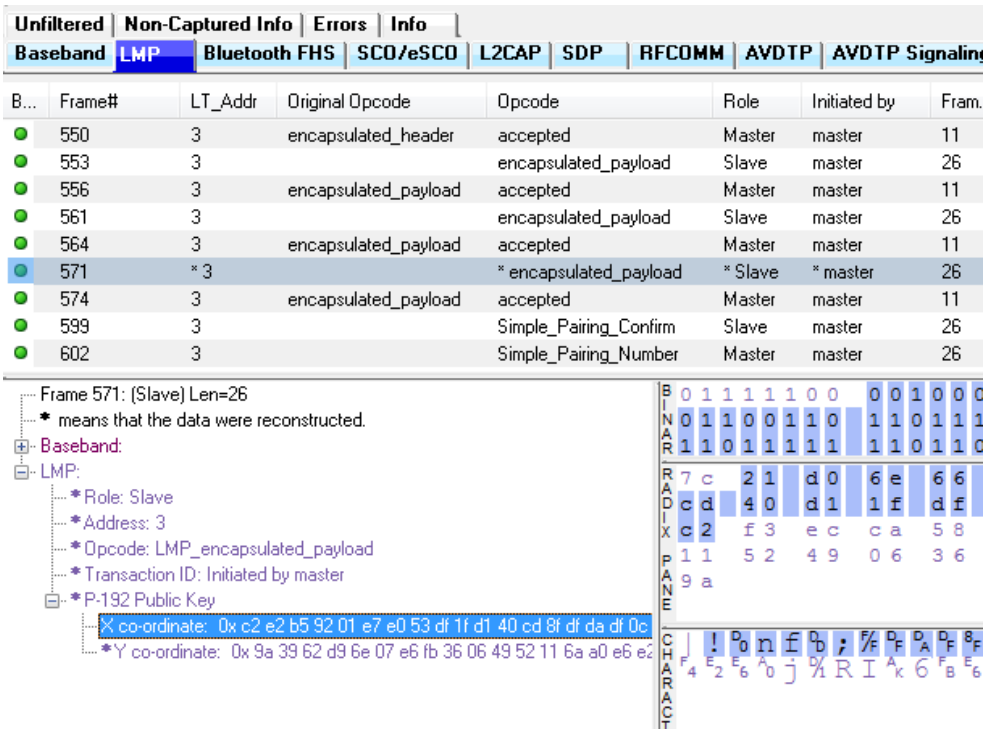


How to tell if a device is in Secure Simple Pairing Debug Mode

When a device is configured in SSP debug mode, the ComProbe software will decode and display the debug key in the Encapsulated Payload message of the Frame Display Summary pane. There will be an Encapsulated Payload message sent from both the master and the slave. The message from the device that is in debug mode will show the debug key, the other will show the public key. Refer to the Frame Display Decode pane in the screenshots below where the master is in SSP debug mode. Remember, only one of the *Bluetooth* devices needs to be in SSP debug mode.



Encapsulated Payload Message from a *Bluetooth* Device in SSP Debug Mode



Encapsulated Payload Message from a *Bluetooth* Device NOT in SSP Debug Mode

Technical Support

Technical support is available in several ways. The online help system provides answers to many user related questions. Frontline's website has documentation on common problems, as well as software upgrades and utilities to use with our products.

Web: http://www.fte.com, click Support

Email: tech_support@fte.com

If you need to talk to a technical support representative, support is available between 9am and 5pm, U.S. Eastern time, Monday through Friday. Technical support is not available on U.S. national holidays.

Phone: +1 (434) 984-4500

Fax: +1 (434) 984-4505

Author: Sean Clinchy

Publish Date: February 2014