Understanding the Impact of Encryption on Certified Wireless USB Testing

Mike Micheletti
Wireless USB Product Manager
LeCroy Protocol Solutions Group

Introduction

Certified Wireless USB (WUSB) is a new short-range, high-bandwidth wireless extension to the USB standard, designed to combine the speed and security of wired technology with the ease-of-use of wireless communications. WUSB is based on Ultra-WideBand (UWB) wireless transport defined by the WiMedia Alliance, and is designed to provide 480 Mb/s throughput at distances up to 3 meters (10 feet).

The developers of Wireless USB have strived to maintain the same usage and architecture as wired USB with a high-speed host-to-device connection. But unlike its wired predecessor, Wireless USB mandates more stringent attention to security to prevent snooping of wireless data traffic. These requirements are defined in the Certified Wireless USB Association Model Specification v1.0 and govern how devices will discover and establish secure connections.

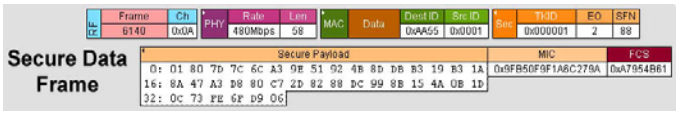

Figure 1:
In Wireless USB, the payload portion of the frame will be encrypted, which will prevent radio-based analyzers from decoding the "scrambled" USB traffic.

The Certified Wireless USB specification requires encryption of user data prior to transferring it between devices. While this security feature is largely transparent to the end user, it has significant impact on test and validation of new wireless devices. What few engineers initially realize is that it is necessary to "crack" the security in order to test the Wireless USB protocol.

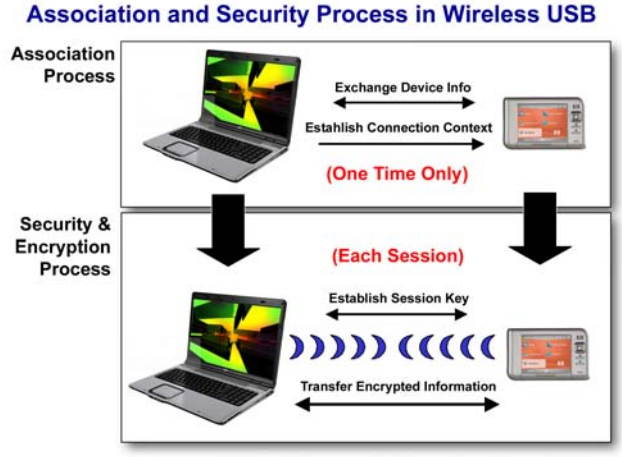

Figure 2:
Wireless USB requires a one-time association to occur between host and device to establish the connection context. All subsequent communications automatically derive a session key from the shared communication context and use this key for encrypted communication.

Association vs. Security

The terms "association" and "security" are separate but related concepts in wireless USB. *Association* is the process of establishing a trusted relationship between two wireless devices. This is a one-time event that requires user involvement to ensure devices are authorized to communicate, and is designed to prevent unauthorized or accidental connections between two unrelated devices. *Security* refers to the encryption mechanism used for protection of data in transit (AES 128). Complete security encryption keys are a combination of a predetermined connection key established dur-

CABLE ASSOCIATION PROCESS

What happens over the USB cable during the association sequence?

• Host sends its host name (CHID) to device using SET_ASSOCIATION_RESPONSE (RetrieveHostInfo)

• Host then asks device if it already has a connection context for the host's CHID using GET_ASSOCIATION_REQUEST (AssociateWUSB)

• Device returns DEVICE_INFO data structure
If device has a connection context, it returns its CDID to the host; Else it returns zero

• Host creates Connection Context (CHID, CDID, CK) and sends it to device using SET_ASSOCIATION_RESPONSE:

The connection context is 384-bit value which includes a globally-unique host ID, a host-unique device ID and a 128-bit symmetric connection key that only changes if devices re-associate. With cable association, the connection context is always generated on the host and downloaded to the device. The purpose of device association is to get the connection context from the host to the device. This can be a challenge, as it must use a secure transmission channel. Cable (out of band) and Numeric Association are two approaches for transferring this data.

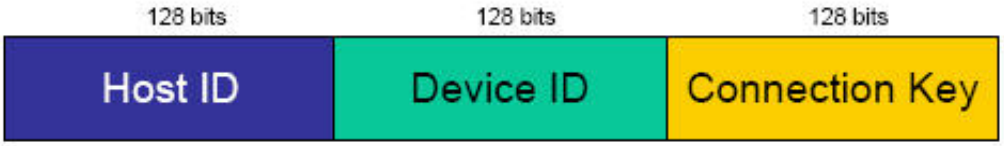

Figure 3:
The Cable Association Process is the most secure way to establish the connection context between two devices, but requires the temporary connection of a wired USB cable between the two devices.

ing the association process and a second temporary "session key" which is generated between devices using a 4-way handshake that occurs every time two devices establish a connection.

The Association Process

In an environment where there may be many Wireless USB hosts and many Wireless USB devices belonging to multiple users, there is a need to identify which devices are allowed to communicate with each other. When two Wireless USB devices are brought together for the first time, they must identify themselves and the user must verify they are authorized to communicate. If there is no record that they have previously been authorized, they must perform a first-time association. The Certified Wireless USB spec defines two methods of establishing this trusted relationship: cable association and numeric association.

Cable Association

With the cable association model, users must associate a host to a device by physically con-

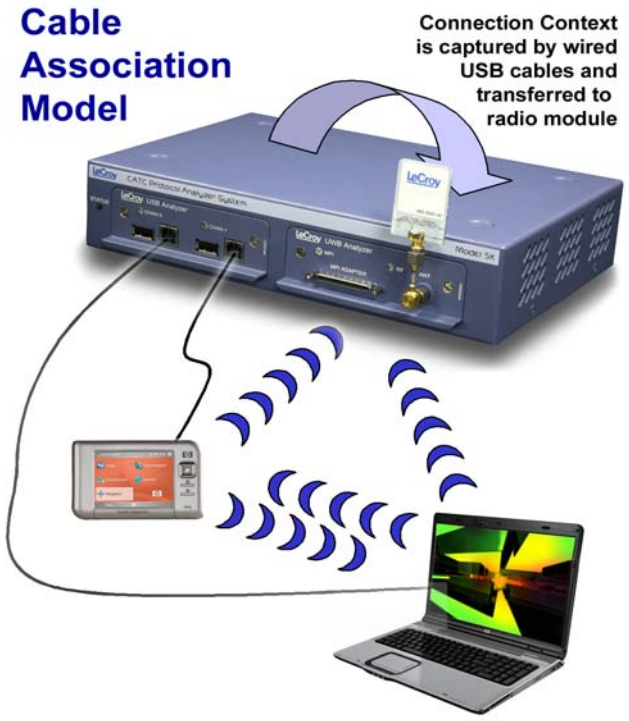

Figure 4:
In the cable association model, the UWB*Tracer* Analyzer captures the connection context and then transfers this information to the radio module, where it is used to capture and decrypt radio traffic between host and device.

necting the two devices together with a standard USB cable. The two devices then exchange a unique 384-bit identifier over the USB cable that is known as the "connection context".

After this initial association, the device and host will communicate wirelessly without the cable. Cable association is considered highly secure because the user must have physical control of the devices in order to attach the cable. In addition, the connection context is exchanged "out-of-band" (not over the air) making eavesdropping virtually impossible.

Numeric Association

In the numeric association model, devices associate without using a wired cable, but require the user to confirm the association by verifying a code number manually. After locating a nearby wireless USB host, the device may show a short code number on its display, which the user will then verify with the host. The specification also has provisions for devices that do not have input capabilities. In this case, the host simply displays the number and the user clicks "OK," if it matches. Alternately, hosts can require the user to enter a predefined code number supplied with the device, a method familiar to users of many existing wireless technologies today. Any of these methods establish a connection context similar to that obtained in the cable association model.

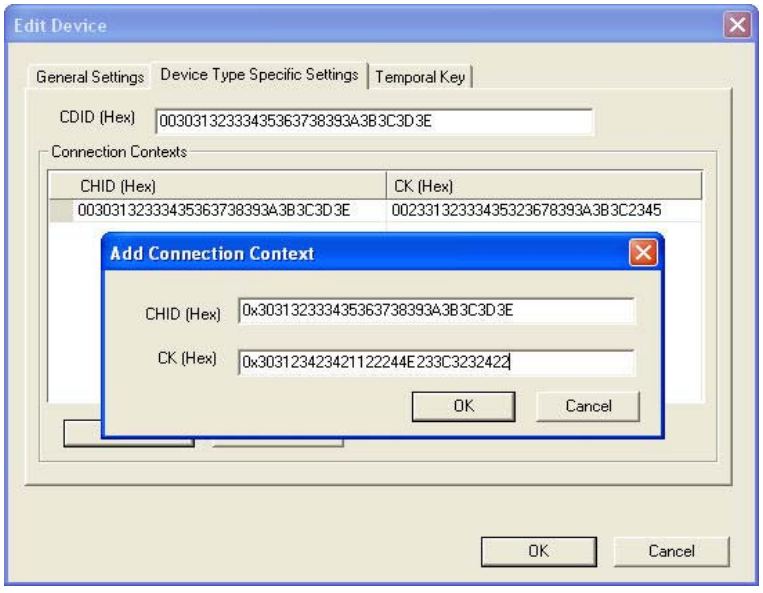

Figure 5:
In the numeric association model, the user must manually enter the Connection Host ID (CHID) and the connection key (CK) for each device. The information must be predetermined by the device manufacturer.

Security and Encryption

Once association is complete using either of these two methods, the devices are now authorized to communicate using the connection context that is established during the association process. During each session, the devices will initially derive a "session" key (also called a "pair-wise temporal key" or PTK) which is based on the pre-established connection context. Wireless traffic between devices is encrypted using the session key, and therefore any receiver, including any analysis tools, must have prior knowledge of the connection context in order to determine the session key and decrypt the wireless traffic. However if the connection key is known, the analysis tool can determine the session key by listening in to the wireless traffic as the devices begin to communicate.

Analyzing Secure Traffic

Protocol layer testing for wireless technologies generally involves a radio-based "sniffer" to eavesdrop on the exchange between devices. Analysis tools must perform this task with minimal impact on the real-world operating environment for the devices. WiMedia devices do not encrypt the PHY and MAC header information. This allows devices (and analysis tools) to identify framing and routing information for each packet. But all wireless USB logical transfers within the user payload are encrypted. The

ability to trigger on protocol events requires that the analysis tools can decrypt the traffic in real-time to identify the logical USB parameters. ***Unless the analyzer has this secret key, it will be unable to trigger on protocol events***!

During early validation, for convenience developers of drivers, firmware and MAC silicon may perform testing with encryption disabled. However complete testing of prototype designs will require the ability to decrypt and view these transfers to verify security.

LeCroy's UWB*Tracer*™ Protocol Analyzer provides an innovative solution to this security problem. For devices that use the cable association model, LeCroy offers an integrated plug-in for capturing the cable association sequence. Similar to a USB analyzer, this module transparently taps the wired link between host and device. It automatically records and passes the connection context to the radio-based analysis engine contained within the UWB*Tracer*. The analyzer radio channel can then automatically follow the 4-way handshake and use the connection context to derive the "session" key (or PTK). With this unique session key in the hardware recording engine, the analyzer can automatically decrypt the scrambled wireless traffic.

For devices that use the Numeric Association model, LeCroy's UWB*Tracer* provides a software interface for tracking the connection context manually between devices.

After manually entering the connection context, the software provides a mechanism to download the connection context to the analyzer hardware. The analyzer preserves this information for the host-device pair. Equipped with the same connection context, it can follow the 4-way handshake and derive the same "session key" (PTK) as the devices under test.

In both the cable and numeric methods, the LeCroy analyzer has the ability to preserve this pairing information in non-volatile memory. The UWB*Tracer* System will recognize when these devices establish future connections and automatically derive a new PTK whenever a new 4-way handshake protocol takes place between the devices.

Important points:

- The session keys are regenerated every time the two devices power up. The analyzer must be powered on and record the 4 way handshake sequence at this stage to automatically derive the PTK and decrypt the scrambled traffic.

- In some cases, developers can use a diagnostic key (CK= 0) for debug environments. But most validation labs will require testing with commercial products using real CK values.

- In the Numeric model, the user must enter the Connection Host ID and the Connection Key in the analyzer software for a given device. The CK is generally a known value that is pre-programmed in firmware (but is never transmitted over the air).

- If a host-device pair have already established a connection context using a cable association model prior to the introduction of the analyzer, it will be necessary to repeat the cable association while monitoring the USB traffic between the host and the device in order for the analyzer to capture the connection context.

Testing of both the association process and the security process will be required to gain certification of wireless USB devices. This will be enforced through the USB-IF certification program, which will allow companies to test device and host compliance to all Certified Wireless USB specifications.

Summary

The association models in Certified Wireless USB are designed to deliver secure data transfers and ease-of-use to consumers. Efficient device-level validation requires that the analyzer have a mechanism to capture and recall the connection context. The ability significantly improves test workflow by allowing protocol testing to occur unencumbered by the security features. In addition to efficiently managing security keys, the analysis platform must have sufficient processing power to use these keys to decrypt and trigger on USB events in real-time. From security to evolving PHY specifications…only LeCroy's Protocol Solutions Group could anticipate and deliver the innovative features needed to accelerate product testing in this emerging wireless market.