

Understanding WiMedia Association models and security

Learning from mistakes of the past, the WiMedia Alliance has forged a secure future for UWB.

By Preston Hunt

Security has been a prominent issue for wireless technology. The computing industry's track record has not been good. Attacks and vulnerabilities seem to occur every few months, leading to consumer distrust and slower mainstream adoption of wireless technology. From day one, the WiMedia Alliance set out to learn from past mistakes and to provide a common radio platform with a security solution that would meet users' needs. Recognizing the pitfalls of having multiple levels of security, for example, it sagaciously required all devices to have mandatory security support. WiMedia's goal was and is clear: "keep the bad guys away from users' stuff while not being too hard to use."

While numerous properties have been addressed by WiMedia, this article will focus on the encryption and authentication properties of security. WiMedia security is separated into two parts. Association is performed at the application layer for the first-time setup. Once products have been set up, ongoing operational security is provided by the WiMedia Common Radio Platform. More details on each are as follows:

■ **Operational security.** The ongoing operational security is the same for all protocols based on the WiMedia Common Radio Platform: All data packets for secure products are encrypted at the MAC level using the advanced encryption standard (AES), which is approved by the U.S. government. Encryption and decryption occur in hardware at the full line speed of 480 Mbps, with no significant overhead or delay.

■ **Association.** While ongoing operational encryption is uniform for WiMedia products, the association process for first-generation products will be protocol-specific. Wireless USB and WiNet have custom association protocols that provide security for their respective needs. When Bluetooth and Wireless 1394 release their WiMedia-based products, they will likely use a protocol-specific association method. The reason for these incompatible solutions is that designing security systems is hard work. The development of a single, generic architecture to meet everyone's needs would take longer and cost more. Although each protocol has a specialized association method that is not binary compatible, the user experience for all association methods is similar and consistent.

One of the most important aspects of association is that all WiMedia products require permission from the user before they are allowed to connect with other products. Without this requirement, products would try and connect with one another all the time—frustrating users and posing a security

risk. Mandatory user interaction requires additional steps from the user for device setup, and it will require increased cost to provide display and input capabilities. However, the security and usability benefits far exceed the associated costs.

Association protocols

Wireless USB products can be associated using one of two methods. In the numeric association model, a device will show a short number (two to four digits) on its display, which the user will verify with the host. On limited hosts that do not have input capabilities, the host displays the number to the user and the user clicks "ok" if the numbers match. Alternately, hosts can ask the user to enter the number. The cable association model allows the user to associate a device to a host by using a USB cable during the first use. After this one-time action, the host and device will remember each other and communicate wirelessly. Host manufacturers are required to implement both models to ensure that all Wireless USB-branded products can associate with each other.

The association protocol used for Wireless USB could not be reused for WiNet because WiNet is a peer-to-peer networking technology. In contrast, Wireless USB is a host-centric peripheral technology (see the sidebar, "WiNet Basic"). The absence of a central controlling host and the possibility of belonging to multiple simultaneous groups led the WiNet authors to adopt the same protocol used by the Wi-Fi Alliance for setup, Wi-Fi protected setup (simple config). While the protocol used by WiNet is the same as the Wi-Fi protocol and binary compatible, it is a separate implementation and not bound by the Wi-Fi Alliance rules.

The simple config protocol is an extensible framework that can support multiple association methods, including USB flash drive, PIN entry, near field communication and Ethernet. In order to make WiNet association as similar as possible to Wireless USB, the decision was made to augment simple config with a numeric comparison method similar to the one used by Wireless USB and Bluetooth. This will ensure a common user experience among WiMedia products. The other association methods supported by simple config will not be used in the initial WiNet release. The extensibility of the framework ensures that they will remain as options should the need arise.

The WiMedia and Bluetooth organizations worked closely to ensure maximal user experience consistency for association. The upcoming Lisbon release of the Bluetooth

protocol will include security enhancements. In addition, Bluetooth supports a numeric comparison method in which the user compares six-digit numbers. When Bluetooth releases products based on the WiMedia platform, the usability of all WiMedia products will remain consistent.

WAM 2.0: The future

Despite improvements in wireless security promulgated by first-generation WiMedia devices, there is room for improvement. Starting in 2007, the WiMedia Association Models Working Group will begin work on the Wireless Association Models (WAM) 2.0 specification. The goal is to achieve binary protocol compatibility for existing and future protocols based on the WiMedia platform, including Certified Wireless USB, WiNet, Bluetooth and Wireless 1394.

In addition to ensuring 100% user consistency, binary compatibility will reduce the implementation cost on manufacturers. Because the design and implementation of security systems is prone to error, the use of a common code base will allow developers to focus their efforts on building products without worrying about the security subsystem. Also, the security analysis and review can be focused on the single code base instead of spread among multiple implementations.

Unifying the code base is one benefit of WAM 2.0. Another feature will be the addition of association methods that may increase the usability and security of WiMedia products. Foremost among these potential improvements is the adoption of near field communication, a short-range RF technology.

Conclusion

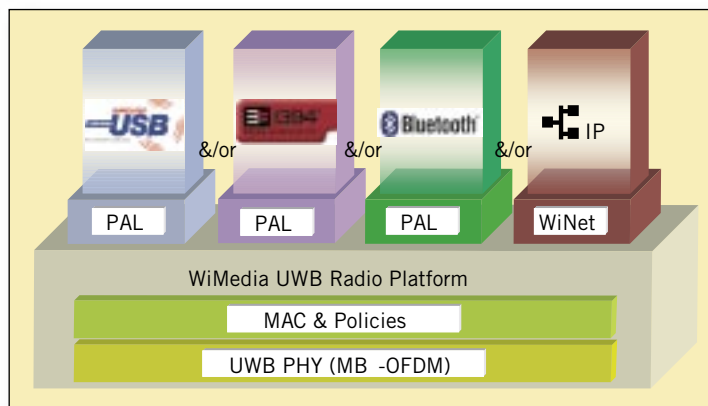
The security and association solutions provided by WiMedia are a balance of cost, usability and security. The data encryption capabilities built into the WiMedia platform provide protection against eavesdropping of information sent over the air. The association techniques for first-time setup, most notably the numeric comparison method, ensure that products will be reliably and securely connected, with minimal chance that an attacker can intercept the connection. With this security, WiMedia products will be built for success. **EWT**

ABOUT THE AUTHOR

Preston Hunt is a technology marketing engineer for Intel's Wireless USB & UWB group. He is also the chairman of the Wireless USB Association Models Working Group and chairman of the WiMedia Association Models Working Group.

WiNet basics

WiMedia's networking specification is called WiNet and can be referred to as a protocol adaptation layer (see the figure). It acts as the interface between higher-layer networking protocols and the WiMedia media access controller (MAC). WiNet defines a logical link control layer networking protocol for the WiMedia radio platform to model the behavior of an IEEE 802 network. This facilitates easy migration of applications compatible with an IEEE 802 environment to a WiMedia environment with few or no changes. For example, a TCP/IP protocol stack designed for an IEEE 802.3 (Ethernet) environment will work with a WiMedia environment. The WiNet protocol preserves the IEEE 802 headers to facilitate the design of bridges between a WiMedia network and other IEEE 802 or compatible wired or wireless networks.



PAL: protocol adaptation layer.

Since WiNet is designed for TCP/IP, it maintains support for the routable nature of Internet applications, meaning that WiNet packets contain a device address as well as a network address. Mobile WiNet devices are designed to communicate with the Web using standard Internet routers.

WiNet is a true peer-to-peer protocol, meaning that devices may communicate with each other directly. This facilitates the creation of ad-hoc wireless personal area networks (WPANs) for mobile devices and applications. Bandwidth is not reduced by the requirement for devices to transfer data through an intermediary node, such as an access point, master or host.

In WiNet, bridging to other networks is based on IEEE 802.1D. This avoids a potential legacy issue of requiring two classes of devices: those that are bridge-aware and those that cannot operate in a bridged environment. WiNet provides control messages that allow devices to select the level of bridge-forwarding services that are desired. Bridge service requests allow a device to designate which packets should be filtered based on protocol identifiers and multicast addresses. WiNet also allows devices to omit the 802 headers for more efficient data transfer if the packets are destined for WiMedia wireless network.

Another major feature is a new advanced hibernation algorithm, which makes use of mechanisms already built into the MAC. While the MAC has an information element that announces when a device will hibernate, there is no way for a set of devices to coordinate their sleep cycles. WiNet defines a local cycle, which allows a device to announce when it will be active. It further defines a global cycle, which is used to synchronize neighbors' local cycles. This hibernation scheme allows devices to conserve power when their data transfer requirements are low.

As an added benefit, WiNet is fully complementary with 802.11 and 802.16. Consequently, it can be used to extend the local area network (LAN) and the metropolitan area network (MAN) to the WPAN space.

ABOUT THE AUTHOR

Alan Berkema is an engineer scientist at Hewlett Packard.