



Embedded security you can trust

Standards Watch

Elliptic on security standards activity

Issue 4 – Spring 2007

Welcome to Standards Watch

Welcome to the latest issue of Standards Watch. This issue covers the new mobile profile for WiMAX and what it means for SoC designers and the progress in IEEE P1619 which targets storage security for disk and tape systems.

The WiMAX Mobile Profile of IEEE 802.16

WiMAX Forum has released the first version of its Mobile System Profile to define the features of the IEEE 802.16 standard implemented in Mobile WiMAX. To understand the profile it helps to understand a little about the history of 802.16 and WiMAX. The IEEE 802.16-2004 specification defines a wireless network architecture suitable for broadband networks. It is a large, complicated specification that is over 700 pages long and covering multiple physical layer modulation and encoding schemes below a common MAC sublayer of the link layer. To round out the specification, there are security services that cover optional data confidentiality and integrity protection as well as identification, authentication and authorization (IA&A).

A weakness of the original IA&A protocol (called PKM) in 802.16 is that client stations authenticate themselves to the base station, but the base station does not provide corresponding authentication to its clients. This is typical of many kinds of service provider networks: the network operator (which owns the base stations) cares that rogue clients cannot obtain (steal) network service, but does not care whether clients can be hijacked by rogue base stations. This is simplistic security design, and can be poor business too. Experience with 802.11 Wi-Fi showed that people with ill intent could and would operate rogue base stations to intercept clients for their own purposes. Among other things, this can be a denial of service for subscribers which leads to frustrated users who may lose trust in the network service, leading to lower subscription renewal rates and loss of metered service revenue.

The 802.16-2005 revision to the 2004 specification is a huge amendment that adds features to enable mobility of client stations, including hand-off of clients between base stations as they move through coverage areas. As part of that amendment new security features were included. A second IA&A protocol called PKMv2 was added that provides mutual authentication, as well as distribution of keys for use in multicast services. The combined specification also provides several confidentiality modes, including the AES-CCM mode for packet encryption. This is a much stronger method than those provided in earlier versions of the specification, and includes integrated cryptographic message authentication.

In this Issue

The WiMAX Forum has taken the bold step of building a new, streamlined mobile profile to the IEEE 802.16 standard. This is an excellent move to narrow a complex specification and ensure that designs can be competitive in the tough consumer mobile market.

The IEEE should in turn be commended for its hard work and positive outcome on the P1619 standard aimed at implementing security standards for disk storage systems. After vulnerabilities were found in the original LRW-AES cipher, the committee quickly re-grouped and has now agreed on a replacement cipher – XTS-AES. This is an excellent recovery from a very difficult situation.

All this is to say that the 802.16 specification includes many features, and not all of these are required in any given application. The WiMAX Mobile System Profile provides implementers of 802.16 SoCs and systems guidance about what parts of the specification they need to implement for that particular application. The mobile profile greatly simplifies the complexity of the security sublayer, and reduces the amount of software and hardware needed to implement the standard for use in this profile. Briefly, here are the features included in the profile:

- PKMv2 only for IA&A using EAP-based authorization for initial network entry and network re-entry
- Data encryption suites supported: no encryption or AES-CCM 128 bits authenticated encryption
- Authenticated data suite: CMAC mode of AES
- Support for both static and dynamic security associations
- Unicast services only (no multicast service requirement)

The WiMAX Forum clearly recognized that the complexity of the original IEEE standard would have added cost and unnecessary complexity to SoC and system designs. Since mobile WiMAX is viewed as being an implementation option for 4G networks and handset cost a significant driver to overall penetration, this simplification will help designers reach the cost targets necessary for widespread adoption.

IEEE 1619 Update

The IEEE Storage in Security Working Group (SISWG) has been busy moving its P1619 standards family ahead in the past few months. As discussed previously, the working group voted on and passed its resolution to move the P1619 *Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices* draft to IEEE sponsor ballot. The current revision is draft 14. This standard is designed for encryption of data on disks and other block storage devices. It provides no cryptographic authentication or integrity protection, which is a double-edged sword. On the one hand, stored data retains its same size with and without encryption. On the other hand, defects in the stored data can go undetected (in the absence of other structures in the data applied at higher layers of the system), and there is no protection against modifications to the data after it was originally written to the storage media.

Attention has now shifted to P1619.1 *Draft Standard for Authenticated Encryption with Length Expansion for Storage Devices*, now at draft 18. The title does not really tell one what it is for: simply put, this is a standard for encryption with authentication suitable for tape backup and similar media. In keeping with the long-term retention requirements for backup media, the draft standard includes several variants of 256 bits AES encryption. All of the methods specified incorporate cryptographic authentication, either directly in the mode or using the HMAC-SHA authentication method.

Two other activities are occurring within the SISWG. A new initiative dealing with key management issues has begun, which if approved by IEEE will be designated P1619.3. This will be a huge undertaking, and deals with one of the most critical issues in long-term storage security: proper handling, storage and control of

cryptographic keys used to access data on stored media. The P1619.2 standard has been a relatively low-key effort of late. It deals with a counterpoint to P1619: it will provide authenticated encryption for disks and related block media. This will be appropriate for some applications, less so for others. Expect activity in P1619.2 to increase in the next few months.

Although occasionally criticized for the lengthy and cumbersome standardization process, in the case of P1619, the IEEE has to be commended for a job well done. When the original cipher LRW-AES was found to be vulnerable, the committee responded with admirable speed and dedication to review the flaws in the original cipher and replace it with what appears to be a very robust design in XTS-AES. Although this process had some faint resemblance to the fallible WEP design in Wi-Fi, the vulnerability was detected very early by security experts and remedied in a matter of a few months with little acrimony. Congratulations to the committee on preserving through this initial set-back!

Contact Information:

Elliptic
308 Legget Drive, Suite 202
Ottawa, ON K2K 1Y6
+1 613-254-5456
www.ellipticsemi.com
Email: info@ellipticsemi.com