



Embedded security you can trust

# Standards Watch

Elliptic on security standards activity

Issue 5 – Winter 2008

## Welcome to Standards Watch

Welcome to the latest issue of Standards Watch, in which we look at the approved IEEE 1619 standards 1619 and 1619.1 developed by the Security in Storage Working Group (SISWG). These represent an interesting contrast in styles, yet were developed by largely the same group of people. Whereas 1619 is admirable for its focus and simplicity, 1619.1 is more of a “kitchen-sink” standard. We’ll also touch briefly on 1619.2 although progress on this proposed standard has been slow pending closure on the other two standards. Read on to find out more.

## IEEE 1619 Security in Storage Standard

IEEE 1619 defines a standard for protecting data on “block oriented storage devices”, the most common example of which are disk drives. The widespread availability of large storage arrays on SCSI and Fiber Channel transport networks operating in high availability configurations with hot swap capabilities means that large quantities of data on disks may be moved and removed from storage systems to satisfy requirements for data backup, lifecycle management, and so on. Every so often a disk or array is misplaced or stolen, and exposes the original owner to huge risk that the data on those devices may be misused, leading to problems ranging from technical and governance violations of requirements for data retention and security to outright identity theft. This is an example of a case where there is a clearly understood need, but the complexity and performance requirements of the system environment are such that simple ad hoc solutions like software on a host do not work. The result has been that there are few widely deployed solutions for disk data encryption. Which has the advantage that there is no entrenched legacy product with sufficient market presence that it is necessary to take into account in developing an industry-wide standard. This has allowed the SISWG to be able to develop a clean, single-purpose standard driven only by the technical requirements for storage on disks.

The basic requirements are to

- support efficient encryption and decryption of data to and from disk;
- deal with that data in a manner consistent with the underlying block structure of the storage medium; and
- protect that data from easy analysis even when the same data is repeated in many blocks.

The response has been the development of the new XTS mode of AES, based on Rogaway and Halevi's XEX encryption scheme, and using cipher-text stealing (CTS) to deal with storage data units that are not an integral

## In this Issue

We discuss the ratified versions of the IEEE 1619 and 1619.1 standards. Working from a clean slate, the 1619 working group for disk storage security has been able to pull together a very coherent standard without worrying about legacy systems and backward compatibility. 1619.1, which is targeted at tape storage security, has had to deal with existing implementations and as such has generated a standard which includes four different ciphersuites with some inconsistency between key strength chosen for encryption and message authentication.

In the next issue of Standards Watch, Elliptic will review the activities of the U.S. National Institute of Standards and Technology in developing additional hash functions in a public competition that is underway now.

multiple of the 128 bits block size of the AES cipher. XEX mode creates a “tweak” based on a characteristic parameter of the storage system block (typically the disk block number on the storage device) to incorporate in the encryption scheme. The use of the tweak provides an efficient means to add variability so that repeated patterns in the plaintext do not result in corresponding repeated patterns in the ciphertext. The use of the CTS scheme ensures that the ciphertext is exactly the same size as the original plaintext.

Thus an IEEE 1619 implementation can be inserted in an existing disk controller subsystem without changing the organization of data on the disk. The only option in the specification is the key size used for encryption and decryption, which may be 128 or 256 bits, and this has only the effects of changing the security of the encrypted data, and possibly affecting the speed at which data may be written to and from disk.

Contrast this with the 1619.1 standard that provides both cryptographic authentication and data confidentiality (encryption) for use in tape encryption. Rather than opting for the simplicity of 1619, four different encryption modes are defined over a total of six different ciphersuites. Compliant implementations are required to implement one of the specified modes and ciphersuites, but no single scheme is required by all compliant implementations. The result is that interoperability between implementations will be hit and miss.

What's included in the 1619.1 standard? The AES encryption algorithm with 256 bits cipher key is the common thread in all specified schemes. The following set of ciphersuites is defined: AES in CCM mode, producing a 128 bit authenticator; AES in Galois/Counter mode, producing a 128 bit authenticator; AES in CBC mode, producing HMAC-SHA authenticators with 160, 256 and 512 bits; and AES in XTS mode, producing an HMAC-SHA authenticator of 512 bits. This is an odd collection of schemes with mixing of key sizes between encryption and authentication. First, many of the schemes have poor compatibility with each other, making it less likely that many implementations will opt for all the schemes. XTS and GCM are reasonably compatible, so one may find systems that combine those two functions, possibly in addition to XTS for disk encryption as specified 1619. Both are inherently high performance, making them suitable for forward-looking implementations. HMAC-SHA-512 will be the performance constraint here as it does not scale very well; however, the use of XTS for disk and GCM for tape will make for a high performance storage subsystem encryption solution. The second group is the CCM and CBC suites. These do not scale up very well to high performance. These are most likely present as a concession to existing implementations. Secondly, we observe that the mixture of strengths between authentication and encryption key sizes is a little odd. In general, the strength of a good cryptographic authentication algorithm is about half the authentication key size. By this measure, the two suites that use HMAC-SHA-512 are preferred. So how big an issue is interoperability in this realm? Unlike, say, standardized communications protocols which must be interoperable to be useful, the answer here is more complicated. Users that have large legacy libraries will need at least a means to read back and decrypt existing stored data. In many cases, those organizations that encrypt their tape storage are using software today, so that should continue to be a viable solution for data recovery. In future, however, users will have to know exactly which schemes are implemented in their hardware and either be satisfied to be locked into one vendor, or a small subset of vendors, that implement the same schemes that they use, or choose more expensive hardware that can deal with any scheme. This problem will become exacerbated as key management migrates to hardware, with key import and export being performed through key management modules that may also select among different key wrapping schemes. And this looks like a gaping hole left by this standard, and portends what is to come with the 1619.3 Key Management standard.

The IEEE is also working towards a standard called P1619.2 Wide-Block Encryption. The discussion in the committee is at a very early stage. While the only circulating draft was d0, work has started to pick up with completion of the other standards. There are currently six different algorithms under consideration by the

committee – XCBC, EME, PEP, HCTR, ABL4 and HCH. Wide Block Encryption provides data integrity protection (authentication), but this comes at the cost of increasing the storage required, and more importantly imposing a different underlying logical structure on data stored using it, as compared with the structure of data on the native storage subsystem. In addition, there is likely to be significant work done to analyze some of the encryption schemes under consideration for inclusion in an eventual standard. Progress on this standard should be rapid throughout 2008 now that the other bulk data storage security standards have been ratified.

## Updated Contact Information

As of December 20th, 2007 Elliptic has moved to a new and larger facility here in Ottawa. Please note the new address for your records. All phone numbers remain unchanged but are repeated below for your convenience:

Elliptic  
62 Steacie Drive, Suite 201  
Ottawa, ON K2K 2A9  
Phone: +1 613 254-5456  
Fax: +1 613 254-7260  
[www.ellipticsemi.com](http://www.ellipticsemi.com)  
Email: [info@ellipticsemi.com](mailto:info@ellipticsemi.com)