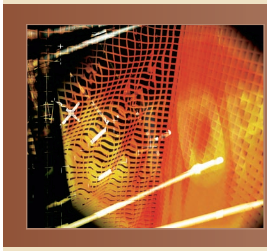
Key Management Infrastructure for Protecting Stored Data

Luther Martin, Voltage Security



The P1619.3 standard seeks to make interoperable key management possible by abstracting the infrastructure of a cryptographic system into three core components.

Any secure use of encryption requires good key management. Historically, it has been hard to do key management well and there has been almost no interoperability between key management products from different vendors. But help is on the way, at least for some of the most important cases.

A new standard from the IEEE P1619 Security in Storage Working Group (SISWG) (https://siswg.net/) will make it easier to manage the keys used to encrypt data in storage. This standard will greatly simplify key management and finally make interoperable key management possible. Products that implement the standard should be available by next year.

Encryption has traditionally been both expensive and difficult to use. This limited its widespread use to little more than SSL, the protocol that's used to authenticate Web servers and encrypt connections to them. The recent proliferation of data security and privacy laws, however, has made the use of encryption attractive in many other cases.

On the one hand, it's fairly easy to convince auditors that sensitive data is being protected adequately when it's encrypted. On the other hand, because encryption is actually one of the best ways to protect sensitive data, it's actually much more than just a check box that will keep auditors happy.

STORAGE HOLDS THE SENSITIVE DATA

Storage devices are a particularly attractive target for hackers because they concentrate the sensitive data that they want—one backup tape can easily hold more credit card numbers than a hacker could obtain in a lifetime of intercepting online payment information.

To defend against such attacks, security experts' adoption of technologies that encrypt data in storage has outpaced the adoption of most other encryption uses. This has resulted in an entirely new set of difficult problems related to key management, but the SISWG is looking to solve them with the P1619.3 standard, "Key Management Infrastructure for Cryptographic Protection of Stored Data"(https://siswg.net).

Key management covers everything that's done with cryptographic keys and other related security parameters during the keys' entire life cycle. It includes how keys are generated, stored, used, and destroyed, as well as the policies that define how these things must be done.

This is hard to do in a secure and useful way. The protection provided by encryption relies on it being infeasible for an adversary to recover a cryptographic key in any way. But to be useful, systems that encrypt data also need to make it easy for authorized users to get the keys they need. These two requirements are hard to do well on their own. Doing them both simultaneously is even harder, but that's what key management systems must do.

ENCRYPTING STORAGE

Figure 1 shows two typical uses of storage encryption. In one case, an encrypting tape drive gets keys from its key server and uses them to encrypt all data it writes to tapes or to decrypt all data it reads from tapes. In another case, an encryption appliance gets keys from its own key server and uses them to encrypt all data written to a RAID array and to decrypt all data read from that array.

In most cases, there's very little interoperability between different vendors' key management systems. So we can't always expect a tape drive to be able to get keys from an encryption appliance's key server, or for an encryption appliance to be able to get keys from a tape drive's key server.

Even worse, we can't expect a storage device to be able to get keys from a distant key server. So if we encrypt a backup tape in the New York data center and send the tape to an offsite backup facility, we can't always expect that the data can be decrypted at the backup facility because the storage device there might be unable to reach the key server that can provide the decryption key.

P1619.3

The P1619.3 standard's ambitious goal is to eliminate all these problems and make interoperable key management possible. To do this, the standard abstracts the components of a cryptographic system into a key management server, a key management client, and a cryptographic unit. Figure 2 shows how these components interact.

In this model, a key management server creates and distributes keys as well as the policies covering their use. Key management clients get keys and policies from a key management server on behalf of a cryptographic unit. These units perform the actual encryption and decryption operations with the keys the key management clients manage. Any product that complies with the P1619.3 standard will support a standard set of operations between these components.

In addition, the P1619.3 standard also defines operations between key management servers. Any compliant implementation will also support a standard set of operations that let key management servers work together by securely exchanging both cryptographic keys and policies. This means that future key management systems will be able to interoperate in ways that aren't possible today, and that users of storage encryption will no longer be locked into single-vendor solutions.

SOONER THAN YOU THINK

SISWG's current plan calls for the P1619.3 standard to be ready for ballot review, the point at which it is essentially complete, no later than August 2008. Then, by February 2009, the Working Group will address all the comments that arise in the approval process. Products compliant with the standard should start appearing later that year.

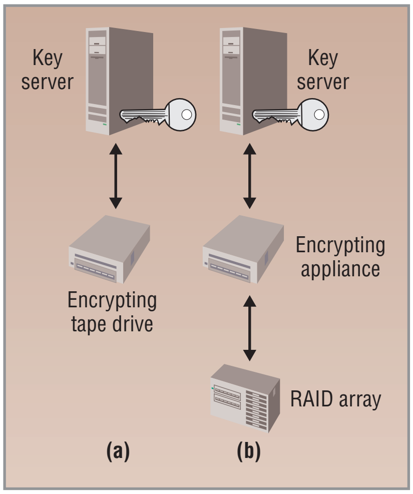


Figure 1. Encrypting storage. (a) An encrypting tape drive gets keys from its key server and uses them to encrypt all data it writes to or reads from tapes. (b) In another case, an encryption appliance gets keys from its own key server and uses them to encrypt all data written to a RAID array and decrypt all data read it.

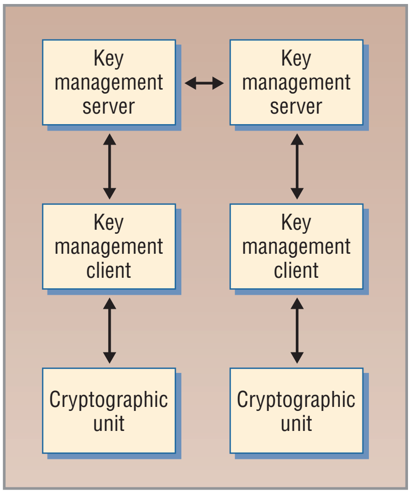


Figure 2. P1619.3 storage encryption abstraction. The standard abstracts the components of a cryptographic system into a key management server, a key management client, and a cryptographic unit.

This is an aggressive schedule, but one which the SISWG should be able to meet, due to both the experience of the Working Group in the previous P1619 and P1619.1 projects as well as the considerable vendor support that the P1619.3 project has gained. If the rapid adoption of the Working Group's previous efforts, like the XTS mode of AES, is any indicator of how quickly the P1619.3 standard will be adopted, expecting compliant products to be on the market by 2009 should be realistic.

By virtue of their participation in the SISWG, most storage and key management vendors are familiar with the direction in which the P1619.3 standard will take key management. Outside the storage and key management communities, however, this work remains largely unknown. To address this, the SISWG is organizing the first Key Management Summit (http://www.keymanagementsummit.com/2008/), an event to be held in September 2008. This meeting will bring together the vendors creating key management products and the users of those products to discuss the challenges of key management and how the P1619.3 standard can solve the key management problems users now face.

Readers who either produce or consume key management technology will want to track the progress of the P1619.3 standard as well as what's discussed at the Key Management Summit. Their input will give a good idea of key management technology's future directions and what products will soon be available to support interoperable key management. Key management might be difficult today, but by next year, the P1619.3 standard should make it much easier. ■

Luther Martin is the chief security architect at Voltage Security. Contact him at martin@voltage.com.

Editor: Jack Cole, US Army Research Laboratory's Information Assurance Center, jack.cole@ieee.org; http://msstc.org/cole