Storage security – who cares?

Bjarne Madsen, SNIA Europe Nordics Committee Chair, nordicschair@snia.org.

One of the great advantages being an 'oldie' in the IT industry is the pleasure of being witness to the changes of focus and priority for various topics over the years. In the past, storage security was not high on the IT department's agenda mainly because the storage was strictly attached to a single host and associated applications. Later on storage became shared and accessed trough networks such as SANs and LANs, and that was when IT administrators first realised the importance of a strong security strategy to protect their storage infrastructures. But did they follow through? Not really. Storage security was mostly still a 'tick in the box' feature – customers didn't understand it or didn't care about it much. All that mattered was that the solution could provide data storage to the enterprise while minimising the risk of data loss and corruption. Today's solutions usually involve the geographic distribution of data for business continuity for example; but multiple points of entry also mean multiple opportunities for security breaches. After many meetings with end users I strongly believe that the need for security around the storage infrastructure is highly recognised, but mostly not implemented.

So what will change the status quo? The major drivers that will take storage security from buzz word to reality at the moment seem to be the increasing legislation that companies have to comply with in terms of information management, together with the rapid growth in the rate of security incidents throughout the industry. Regulatory mandates such as the Sarbanes-Oxley Act of 2002, the California Database Protection Act of 2001, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act (HIPAA), the Basel II accords, Markets in Financial Instruments Directive (MiFID) and EuroSox being active in 2008 are an additional catalyst for applying due diligence in the security decision and implementation process. These laws impose strict requirements on enterprises to establish or identify, document, test and monitor necessary internal control processes. Because information technology supports most, if not all, of these processes, these laws significantly affect companies' security strategies. As a result these new regulations force security designers and architects to impose and maintain suitable security controls throughout their enterprises.

What is storage security?

Storage security represents a major component of the overall information security plan for a data centre and a business. Consequently, business policies and practices must augment any hardware- or software-level security model, including network and system security. Security however, is not a simple commodity that you can order by weight and bolt onto an IT infrastructure. Security considerations permeate every aspect of your IT Infrastructure – from application to the management of technology and of people.

Another perception is that when security has been implemented we are done. Sorry - not true! Storage security requires specialised maintained knowledge, careful attention to detail, and ongoing reviews to ensure that the storage infrastructure continues to meet the organisation's evolving needs. Measuring security is difficult – how safe are we at any point? Unlike processor speed or storage capacity, we do not measure security in simple units – except after an incident when we can objectively demonstrate that the deployed security mechanisms were inadequate. As a result, enterprise security has traditionally been handled reactively in a fashion which is somewhat reminiscent of the old saying 'they shut the stable door after the horse had bolted'.

An exhaustive storage security strategy involves several areas; even the simple movement of data from point to point either trough a network or to different media such as tapes and CDs, requires specific processes and procedures along with the appropriate encryption of the information. In fact, data should be protected both as Data In-Flight (DIF) and Data At-Rest (DAR); see Figure 1. for SNIA's view of storage security.

Generally speaking storage security includes the following elements:

- Authentication – validates user, system and/or application
- Access control – determines what can be seen
- Integrity – validates that data is in the original it what stored in
- Confidentiality – use of encryption to protect content
- Secure key management – keys must be available *whenever* and *wherever* data is accessed

In 2007 we noticed that data protection and ILM were among the most popular projects undertaken by user organisations. To continue and complete these projects thereby fulfilling regulatory and specific SLAs you need to integrate storage security into the overall company strategy for information management. Due to the tight integration of existing IT challenges such as data protection, information growth, and compliance, and their associated and increased costs, 2008 might be the year where we finally see well-developed and documented IT strategy plans across the IT community.

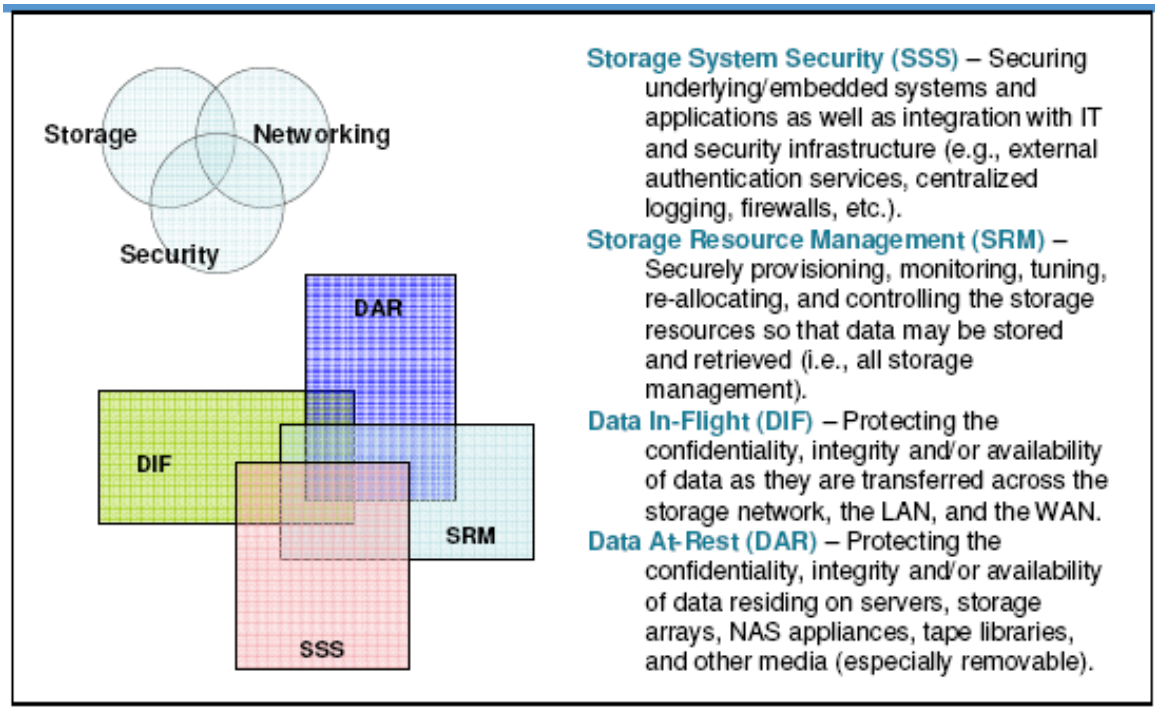

Figure 1. SNIA's view of storage security

For more information:

SNIA Security Technical Work Group (TWG)
http://www.snia.org/tech_activities/workgroups/security/

Storage Security Industry Forum (SSIF)
http://www.snia.org/ssif