Security for Flash Storage Systems

Forum D-12: Enterprise Storage Design, Part 1
Hu Yoshida
Hitachi Data Systems
Why Security Is Important

- **Data Breaches are costly** - Direct costs for notifications, customer service support, credit monitoring, customer incentives, restitution, card replacement, etc.
- **Damage to the firm's reputation and brand**
- **Regulators can impose fines and penalties**, including jail time.
- **A bank’s risk profile goes into the calculation that determine the bank’s capital reserve ratio.**
- **Consumers flood the courts with class action lawsuits** over breaches.
- **Business partners may sue to recover the costs** of responding to a breach.
- **Investors may sue over stock losses.**
Summary of Security Requirements
For Flash Arrays

STANDARDS-BASED SECURITY

Secure Management
Multi-Tenancy
Authentication & Authorization

Audit Logging
Directory Services
Encryption and Key Management
Media Sanitization

Standard Corporate Security Environments
# Encryption and Key Management

<table>
<thead>
<tr>
<th></th>
<th>Drive Level</th>
<th>Storage System Level</th>
<th>Fabric Level</th>
<th>Application Level</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pro</strong></td>
<td>Easy to deploy</td>
<td>Easy to deploy</td>
<td>Often easy to deploy</td>
<td>Very fine grain control over how data is encrypted</td>
</tr>
<tr>
<td></td>
<td>Scales with the number of drives</td>
<td>Scales with number of drives</td>
<td>Easy to add into existing system</td>
<td>Requires no additional hardware</td>
</tr>
<tr>
<td></td>
<td>Good performance</td>
<td>Good performance</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cost efficient to apply to existing system</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Con</strong></td>
<td>Expensive to retrofit existing storage system</td>
<td>Often dependent on external key management systems for basic storage systems operations</td>
<td>Expensive to deploy</td>
<td>Expensive to maintain</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Difficult to scale</td>
<td>Can have high performance impact</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Throughput limited</td>
<td>Key management could be difficult</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Key management can be a challenge</td>
<td>Tough to retrofit to existing apps</td>
</tr>
<tr>
<td></td>
<td>Expensive to maintain</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• Symmetric Encryption for bulk encryption efficiency

• AES-256 encryption is the current industry standard

• **XTS mode of operations enhances protection of data at rest** by incorporating the logical position of a block to “tweak” the block cipher so that no two blocks have the same cipher

• **FIPS 140-2 certification** is required to meet federal encryption and security standards

• **Safe Harbor for Data Protection** Many data breach laws define “breach” to exclude data that is encrypted according to the definitions in the particular law
Key management, can be one of the more difficult aspects of data-at-rest encryption. Key management can be an impediment to using encryption, or worse, it can cause data loss due to operator error or lack of action.

Key Management Interchange Protocol (KMIP) is specified by OASIS for use with third party key managers for trusted source operations.

Key management is needed for key protection, backup, and recovery.

A single key per drive should be supported.

Encryption keys should be deleted from the system automatically, any time a drive is removed from the system, in the case of drive failure, etc.,.
Media Sanitization

- **Sanitization** – When storage media is transferred, becomes obsolete, or is no longer usable or required, it is important to ensure that the residual representation of existing data is deleted and not easily recoverable.

- **DoD overwrites that can be used for disks do not work for Flash.**

- **If the Flash media is encrypted, cryptographic erase can be used** as described in NIST SP 800-88r1 and ISO/IEC 27040

- **Unencrypted media should be Sanitized with Data Eradication**, purge and verification of all user data including user data stored in over provisioned (inaccessible) cells. Some users require this even if data is encrypted

- **All important sanitization events are recorded in the audit log.**