Securing Data in Storage

The Anatomy of an Attack
The Architecture of Defense

October 2003
Agenda

- Introduction
- Networked Storage Overview
- NAS vulnerabilities
- SAN vulnerabilities
- Conclusions
Introduction

Data Security:
A Harsh Environment
History Repeating

- Ethernet circa 1990
  - No perimeter defense
  - No practical encryption/VPNs
  - Limited access controls
  - No auditing

- Networked storage today
  - No defense in depth
  - No encryption
  - Limited access controls
  - Limited auditing
Networked Storage Adoption
Eliminates Traditional Compartmentalization of DAS

Revenue Forecast for Disk Storage Systems

Source: Gartner Dataquest, 8/02

DECRU
Networked Storage Advantages

- More efficient utilization of storage resources
- Centralized management and backup
- Improved performance and access to data
- Consolidated disaster recovery
- Improved scalability

*Note: Improved security is not a driving factor!*
Network Attached Storage (NAS)

- High density NAS appliances enable centralized storage and file sharing
- Typically connected via gigabit Ethernet
- Frequently serve heterogeneous environments
Storage Area Networks (SANs) are a network architecture designed for high availability, high performance data access and storage.
Networked Storage

A Rich Target
Digital assets at risk

- Sensitive/regulated data
  - Customer data
  - Financial transactions
  - Patient data
  - Intellectual property
  - Corporate financial records
  - Legal files
  - Human Resources data
As storage becomes more aggregated, a single breach can expose terabytes

- **Dec 2002 - TriWest Healthcare**
  - Stolen disks contained medical records on 500,000 military personnel

- **Jan 2003 – IBM Global Services**
  - Notifies customer, Co-operators Life Insurance, that a disk containing personal and financial information on its customers is missing, presumed stolen.

- **Feb 2003 – Visa, Amex, Mastercard**
  - Hacker breaches 8 million credit card accounts through a third-party processor

- **May 2003 – Coca-Cola Inc.**
  - Unauthorized employee downloaded salary information and Social Security numbers of about 450 co-workers, leading the company to warn employees to check their bank accounts and credit cards.

- **August 2003 – Acxiom Corp.**
  - A computer hacker gained access to private files at Acxiom Corp., one of the world’s largest consumer database companies, and was able to download sensitive information about some customers of the company’s clients.
But I have Firewalls...
Spending Mismatch

- Organizations are rapidly building networked storage and aggregating data
- Security is an afterthought
- **Spending mismatch:**
  - Security spending today focused on network and perimeter
  - Highest exposure: terabytes of poorly secured storage
Insider Threat

- 50-80% of electronic attacks originate inside the firewall
- 67% of companies reported internal breaches in last 12 months
- Average loss from breach of proprietary data was $2.7 million

Source: FBI/Computer Security Institute
Insider Threat

• Hostile insiders are far more dangerous than external hackers & script kiddies
  – They know what’s valuable, and where it lives
  – Familiar with existing security systems
  – Months or years to watch and plan
  – Physical access to machines, networks, storage
  – Ample opportunities for social engineering

• Perimeter holes give insider access to outsiders
  – VPNs, partner networks, contractors
Accelerating need for storage security...

- As storage becomes more aggregated and networked, a single breach can expose terabytes
- Perimeter security insufficient as threats evolve
- Growing vulnerability of storage systems:
  - Administrator and “root” privileges in the network
  - Human error, theft or misuse of ID/credentials
  - OS & application exploits, viruses
  - SAN vulnerabilities, arrival of iSCSI
  - Physical security of disks (repair, theft, disposal)
  - Replication and offsite backup multiply risks
Networked Storage Vulnerabilities
Data Stored in Cleartext

- Storage devices lack integrated security capabilities
- Without encryption, no effective method to compartmentalize data in shared storage
- Disk/tape: small, portable, contain GBs of data and are easy to steal
- Disk repair and disposal: even “wiped” drives can still yield information
Offsite Backup and Disaster Recovery Increases Risk

- Data duplication significantly increases exposure and risk
- Loss of physical control increases chance of media loss or theft
- Outsourcing = subcontractors with access to your sensitive data
Limited Access Controls

- Unlimited access points
- No security barriers/firewalls
- Storage administrator has unlimited access to data
- System administrator can abuse privileges to access sensitive data and cover their tracks
- No defense in depth for storage: single breach gets you everything
Limited Auditing

- No deterrent: Nobody is watching storage
- Administrator and “root” privileges in the network give insiders free rein
- Limited methods for capturing IT insider attacks on storage
  - Add name to secure group
  - Grant access
  - Read classified/sensitive docs
  - Erase footsteps
- Difficult to determine if logs have been manipulated or deleted
Typical NAS Infrastructure

- Firewall
- Directory Server
- File Server/NAS Appliance
- Tape Backup
- DR Site

Ethernet

Department 1 Subnet

Department 2 Subnet
NAS Threats

- Host/UID Spoofing
- Admin Abuses
- Disk theft/repair
- Network sniffering
- Unauthorized Storage Admin Access
- Stolen passwords
- Tape theft
- VPN Partner Access
- Firewall
- Department 1 Subnet
- Department 2 Subnet
- Directory Server
- File Server/NAS Appliance
- Tape Backup
- DR Site

DECRU
SAN Vulnerabilities
Threat Mitigation

Layered Access Controls

Firewall

Department 1 Subnet

Directory Server

IPSec/SSL

Layered Access Controls

Department 2 Subnet

Compartmentalization Contains Damage

Layered Access Controls

File Server/NAS Appliance

Encryption

DR Site

Tape Backup

Layered Access Controls

Compartmentalization Contains Damage

Encryption
SANs are Changing

**Historically:**
- Originally intended to exist as a standalone, “trusted” network
- Physical security thought to be “good enough”
- Single administrator
- Few individuals with SAN expertise

**Today**
- Connect hundreds (not dozens) of hosts and storage devices
- FC increasingly serving IP networks
- Co-mingling of sensitive and non-sensitive data
- Multiple administrators
SAN Security Weaknesses

- FC SAN designed as a trusted network, so security was not built in
- Primary function of zoning/LUN masking was for ease of administration, not for security
- Complexity leads to administrative errors or misconfiguration, which can expose terabytes of data
- No authentication for hosts paves way for spoofing attacks
- Increasing number of people with SAN knowledge
Management Interfaces are Vulnerable

- FC specs include in band management functionality:
  - Zone configuration
  - Unrestricted SNS access
  - Time service
  - Key distribution service
- Authentication is not required
- Illegitimate access to management services could render standard access controls ineffective
Risks of Physical Access

- Plug into a port and get access to everything
- Savvy attacker with the right tools on the host can breach everything
- Avoid zone restrictions by changing ports
- Drive/tape removal: all data is in cleartext
Typical SAN Infrastructure

SAN MANAGEMENT

FIREWALL

DATABASE SERVER

WEB APPLICATIONS

Fibre Channel

SWITCHES

FC

FIBRE CHANNEL STORAGE DEVICES

OFFSITE DR MIRROR

TAPE BACKUP
SAN Threats

SAN MANAGEMENT

FIREWALL

DATABASE SERVER

WEB APPLICATIONS

HOST AUTHENTICATION

Fibre Channel

FC SWITCHES

Layered Access Controls

DATABASE SERVER

STORAGE DEVICES

OFFSITE DR MIRROR

SAN THREATS

WWN Spoofing

Storage Encryption

Host Authentication

FIREWALL

TAPES

TAPE BACKUP

Storage Encryption

STORAGE DEVICES

HOST AUTHENTICATION

HOST AUTHENTICATION
Securing DR: A Closer Look

Diagram showing the connection between headquarters and DR site/outsourced site, with data secured at various points through Cipher Text and Security Appliance. The diagram highlights the flow of data through FC switches and WAN, ensuring data security at key points such as encryption at the tape system and storage.
Building Defense in Depth
Encrypting Data

- Creates a security model for lifecycle of data
- Enables effective compartmentalization
- With encryption, the default state of data is secure: all replicated copies are secure in flight and at rest.
- Facilitates role-based storage management
- Locks all “backdoor” access to stored data
Encryption Considerations

- **Strong encryption**
  - Standard algorithms
  - Large key space

- **Performance**
  - Low latency
  - Hardware acceleration

- **Key management**
  - Ease of administration
  - Archival and recovery

- **Data availability**
  - Clustering and failover
  - Methods of decryption
Layered Access Controls

- SAN host authentication
- Two factor authentication for sensitive operations
- Group review of administrative actions
  - Unauthorized access requires collusion
- Role separation
  - Storage admin provisions storage, but has no data access
Logging and Auditing

- Maintain several sources for logging data access and administrative events
- Auditing provides a level of deterrence
- Provides evidence of unauthorized access
## Building Defense in Depth

<table>
<thead>
<tr>
<th>Attack</th>
<th>Countermeasures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized admin access</td>
<td>Encryption, ACLs, secure logging</td>
</tr>
<tr>
<td>Hostile admin adds user, changes passwords</td>
<td>Secondary authentication, secure logging, 2-step authorization</td>
</tr>
<tr>
<td>Stolen passwords</td>
<td>Compartmentalization limits damage</td>
</tr>
<tr>
<td>Network sniffing</td>
<td>Implement IPSec between clients/hosts and storage</td>
</tr>
<tr>
<td>UserID spoofing</td>
<td>IP range ACLs, IPSec authentication</td>
</tr>
<tr>
<td>WWN Spoofing</td>
<td>SAN Host Authentication</td>
</tr>
<tr>
<td>Disk theft/repair</td>
<td>Encryption of all data “at rest”</td>
</tr>
<tr>
<td>DR/Mirror attacks</td>
<td>Original copy of data is encrypted, providing transmission security</td>
</tr>
</tbody>
</table>
Conclusions
Data is Increasingly Persistent

- Regulations requiring data storage timeframes
  - HIPAA: worldwide capacity of compliant healthcare records will increase from 68PB in 2003 to 238PB in 2006 (Source: ESG)
  - Sec17a-4: Trading account records -- end of account plus 6 years
- Continued growth of reference data
  - (92% CAGR, 2001-2005)
  - Larger file sizes
  - Kept for decades, not months
Gramm-Leach-Bliley Act (July 2001)

“... each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.” [15 U.S.C. § 6801(a)]

Institutions must develop safeguards:
(1) to insure the security and confidentiality of customer records and information;
(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and
(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer. [15 U.S.C. § 6801(b)]
Regulatory Pressure: HIPAA Healthcare & Pharma

Sec. 164.306 Security Standards

• “Covered entities must:
  
  – ensure the confidentiality, integrity and availability of all electronic protected health information they create, receive, maintain, or transmit

  – protect against any reasonably anticipated threats to the security or integrity of such information

  – protect against any reasonably anticipated uses or disclosures of such information that are not permitted

  – ensure compliance with these rules by their workforce (officers and employees)”
Regulatory Pressure: SB1386
All Businesses Operating in California

California's Database Security Breach Notification Act
(Effective July 1, 2003)

SEC. 2. Section 1798.29 is added to the Civil Code:
“(a) Any agency that owns or licenses computerized
data that includes personal information shall disclose
any breach of the security of the system following
discovery or notification of the breach in the security of
the data to any resident of California whose
unencrypted personal information was, or is
reasonably believed to have been, acquired by an
unauthorized person. “
Secure by Default

Considering the myriad threats to data, why not make the default state of data secure?

<table>
<thead>
<tr>
<th>CUSTOMER</th>
<th>SSN</th>
<th>AMT</th>
</tr>
</thead>
<tbody>
<tr>
<td>John Magnus</td>
<td>544-89-3021</td>
<td>$304.31</td>
</tr>
<tr>
<td>Susan Wong</td>
<td>522-35-1105</td>
<td>$91.05</td>
</tr>
<tr>
<td>Ken Hernandez</td>
<td>670-32-1145</td>
<td>$21.88</td>
</tr>
<tr>
<td>Alicia Sparr</td>
<td>435-98-0498</td>
<td>$209.95</td>
</tr>
<tr>
<td>M.J. Satyr</td>
<td>594-22-9038</td>
<td>$76.55</td>
</tr>
<tr>
<td>Dan Spencer</td>
<td>543-09-3451</td>
<td>$413.03</td>
</tr>
<tr>
<td>Mary Jones</td>
<td>495-38-8971</td>
<td>$90.74</td>
</tr>
<tr>
<td>Jerome White</td>
<td>613-98-8932</td>
<td>$247.11</td>
</tr>
<tr>
<td>Martin Ng</td>
<td>339-77-9201</td>
<td>$20.89</td>
</tr>
<tr>
<td>Fay Dunlap</td>
<td>784-29-6290</td>
<td>$401.92</td>
</tr>
<tr>
<td>Takeshi Doi</td>
<td>544-09-3193</td>
<td>$29.01</td>
</tr>
<tr>
<td>Sarah Fisher</td>
<td>432-92-7105</td>
<td>$142.28</td>
</tr>
<tr>
<td>Ingrid Parker</td>
<td>595-29-7406</td>
<td>$102.48</td>
</tr>
</tbody>
</table>