Storage Security – From Research to Industry Best Practice

Erik Riedel
Director, Interfaces & Architecture
Seagate Research

NASA Goddard, March 2008
The Research Center currently has a total of 150 employees, all in Pittsburgh, Pennsylvania.

About 120 technical staff from over 20 countries; almost 100 staff with Ph.D. degrees from over 50 universities.

Built up from just two people in a rented office since 1999.
Outline

- Motivation
- Technology
- Standards
- Partnerships
- What’s Next
Motivation

terminology presented at FAST 2002, see survey paper in same conference, credit to my co-authors

hp labs
january 2002
## Motivation – Attacks on Stored Data

(* the fraction of system managers reporting the listed attack to the CSI/FBI survey in 2001 and 2006)

<table>
<thead>
<tr>
<th>Attacks</th>
<th>2001*</th>
<th>2006*</th>
<th>leak data</th>
<th>tampering</th>
<th>destroy data</th>
<th>revoked user</th>
</tr>
</thead>
<tbody>
<tr>
<td>virus</td>
<td>94%</td>
<td>65%</td>
<td>--</td>
<td>--</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>laptop/mobile theft</td>
<td>64%</td>
<td>47%</td>
<td>X</td>
<td>--</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>insider abuse of net access</td>
<td>--</td>
<td>42%</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>unauthorized access to information</td>
<td>49%</td>
<td>32%</td>
<td>X</td>
<td>X</td>
<td>--</td>
<td>X</td>
</tr>
<tr>
<td>denial of service</td>
<td>36%</td>
<td>25%</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>system penetration</td>
<td>40%</td>
<td>15%</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>--</td>
</tr>
<tr>
<td>theft of proprietary information</td>
<td>26%</td>
<td>9%</td>
<td>X</td>
<td>--</td>
<td>--</td>
<td>X</td>
</tr>
</tbody>
</table>
Motivation – Cost of Security

• “Users will not pay for [storage] security technology” – storage marketing circa 2001

• “Almost every customer asks about our security strategy” – storage vendor circa 2006

• Average annual spending on computer security is $200 – $1,350 per employee*

*incubated by Seagate Research (Thibadeau) in conjunction with multiple Seagate technology and product teams
Technology – Basics

- Leak of data – encryption
- Tampering – hashing
  (turns it into destruction)
- Destruction – difficult to fix directly
  (make backups/replicas)
- Revoked users – careful key mgmt
- Denial of service – no great solutions
  (replicas are a start)
Technology – Toolbox

• Additional relevant features
  – Key generation via random #s
  – Key exchange over networks
  – Roots of trust & attestation
  – Audit logs & data provenance

These technology mechanisms must be tied together into secure end-to-end solutions
Technology – DriveTrust

• Seagate FDE
  – Full disc encryption at native data speed
  – No performance penalty
  – Secure partitions w/ fine grain access control
  – Crypto functions
  – Root of trust
  – Command set on SCSI and ATA

Security ID on permanent & perforated label
Technology – Electronics

- high-speed, specialized data movement & protocol processing
Technology – DriveTrust

• Data is stored encrypted
• Encrypted data never leaves the drive
• Repurposing done via fast secure delete
• Access control
  – Partition access managed by SPs
  – Pre-boot authentication
• Hidden areas managed via TCG commands
  – Personal data, License keys, other
Standards
Standards

• Trusted Computing Group (TCG)
  – Estimated 25% of 2006 PCs shipped with a TPM; predicted 50% of 2007 shipments

• Storage WG – includes 6 disk drive makers
  – Key use cases
    • Enrollment – device pairing via public/private keys
    • Encryption of user data
    • Private, hidden storage areas
  – All functions independent of the operating system, managed in a separate computing environment

• T10 (SCSI) and T13 (ATA) command sets
Partners
Partners – DriveTrust

• Burned basic mechanisms into silicon
  – Full interface speed
  – Isolated from host
  – Integrated with data access

• Leave control and management to software APIs

• Enable a variety of software partners
  – Wave Systems (US); Secude (Switzerland); CryptoMill (Canada); GuardianEdge (US);
    seeking additional partners
What’s Next
What's Next – Objects

- Evolutionary and revolutionary
  - variable-size data “blob”
  - attribute list (tags)
What’s Next – Objects (2)

• Object-based Storage Device (OSD) standard developed by SNIA and T10
  – OSD-1 (September 2004); OSD-2 (Early 2008)
• Space management handled by individual devices (arrays, controllers, drives); variable sized objects
• Fine-grained security via a shared key system
  – per-object capabilities
  – per-request authorization
  – authentication & access control at security manager
• Optional in-flight integrity
• At-rest protection possible
  – with hardware acceleration
Enterprise Objects

- High-density and high-capacity arrays being built by all of the system vendors

- 15 drives in 3U (hot-swap)
  - over 200 drives per cabinet
  - 200 TB @ 1 TB/drive

- 112 drives in 3U (power-managed)
  - up to 900 drives per cabinet
  - almost 1 PB @ 1 TB/drive

- Used by large enterprises
  - goes by many names
  - clusters; grids; data mining

- Systems will benefit from delegated management
  - offload expensive mechanisms (encryption, compression, search, …)
  - policy managed centrally
Consumer Objects

- Seamless Data – storage-enabled devices communicate peer-to-peer to present a single view of data
For our Home Visits project: “Sticker tour”

We gave people sheets of stickers, and asked them to “tag” things related to photos, videos, and music with different labels. Then they gave us a tour of the stickers, leading us to key objects and places and giving us stories associated with each.

**The Stickers**
- Trapped
- My Stuff
- Most
- Private + Personal
- Avoid
- A Mess
- Well-organized
What’s Next – Data Aware

• Increase semantic understanding of the stored data
  • automated extraction of metadata tags
  • combine with existing user-created tags
  • apply image and video recognition algorithms
  • apply specialized electronics
What’s Next – Privacy

• Infoproperty – information as property
  – Premise – privacy is gone for today’s data, but there is hope for data created in the future
  – Legal status needs to catch up with the technology and the importance of digital data
  – Information and property merge
  – Personal information bound to an infoproperty agent, agreements for use negotiated by agents wherever data is used

• Must include a relevant legal framework
  – See www.istpa.org
  – Int’l Security Trust & Privacy Alliance
Conclusion

• We’ve made a start, but have a long way to go

• Advice to researchers – find relevant user problems, consider paths to solution, stick with it

• Advice to companies – work more closely with researchers for novel solutions, novel views on the problem

• Looking for new software functions and partners to use our mechanisms
Backup Slides
Technology – Trade-Offs

Barracuda 7200
- Up to 1 TB

Over 40 unique drive models

Savvio 10K
- Up to 146 GB

Cheetah 15K
- Up to 300 GB

75 drives / 6U

30 drives / 6U

Over 40 unique drive models
Technology – Design Points

DB35
high-cap, quiet

EE25
small, shakable

ST18
smaller, lower power

Momentus FDE
small, secure

Momentus PSD Hybrid
high-perf, low power

Pocket, Portable
carryable
framework

players

- owners
  - create data
  - determine access to data
- readers - read
- writers - modify
- storage servers
  - store/retrieve bits
- group servers (many flavors)
  - handle “delegated” keys
- adversaries
  - tampers with data
  - may collude w/ others
# Threats and Attacks

<table>
<thead>
<tr>
<th>Attacks, as reported in survey of system managers by CSI/FBI, Spring 2001</th>
<th>% Surveyed</th>
<th>Damage ($ millions)*</th>
<th>msgs</th>
<th>data</th>
<th>revoked user</th>
<th>denial of service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telecom eavesdropping</td>
<td>10%</td>
<td>1</td>
<td>✓</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Active wiretap</td>
<td>2%</td>
<td>n/m</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>System penetration</td>
<td>40%</td>
<td>19</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Laptop theft</td>
<td>64%</td>
<td>9</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>Theft of proprietary info</td>
<td>26%</td>
<td>150</td>
<td>-</td>
<td>✓</td>
<td>-</td>
<td>✓</td>
</tr>
<tr>
<td>Unauthorized access by insiders</td>
<td>49%</td>
<td>6</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>Sabotage</td>
<td>18%</td>
<td>5</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>Virus</td>
<td>94%</td>
<td>45</td>
<td>-</td>
<td>-</td>
<td>✓</td>
<td>-</td>
</tr>
<tr>
<td>Denial of service</td>
<td>36%</td>
<td>4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>✓</td>
</tr>
</tbody>
</table>

*Of ~500 responses, 78% had financial losses, only 37% could estimate damage.
attacks

- attacks on data
  - leak
  - change
  - destroy
- adversary
  - act alone
  - collude w/ server
  - revoked user
- compromise group server
- denial of service
## Security Guarantees - Existing Systems

<table>
<thead>
<tr>
<th>System</th>
<th>Message Attacks</th>
<th>Adversary</th>
<th>W/ Storage SRV</th>
<th>Revoked</th>
<th>Subvert Group Services</th>
<th>Denial of Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>CFS</td>
<td>--</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>--</td>
<td>-</td>
</tr>
<tr>
<td>SFS-RO</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Cepheus</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SNAD</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>NASD</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>iSCSI w/ IPsec</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>--</td>
</tr>
<tr>
<td>LUN Security</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>AFS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>NFSv4</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>PASIS/S4</td>
<td>--</td>
<td>--</td>
<td>--</td>
<td>✓</td>
<td>--</td>
<td>--</td>
</tr>
<tr>
<td>OceanStore</td>
<td>--</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>