Exploiting Asymmetry in Performance and Security for I/O in High-end Computing

PI: Anand Sivasubramaniam
anand@cse.psu.edu

Co-PI: Patrick McDaniel
mcdaniel@cse.psu.edu

Pennsylvania State University

Performance is Critical

- High-performance is essential for storage and retrieval of next generation petabyte datasets.
- Performance issues:
  - Latency
  - Bandwidth/throughput
  - Scalability (with clients, and data volume)
- Considerable investment is being made on sophisticated hardware and software to address performance issues.

Security is equally (or more) important

- At least in some environments
- Business enterprises:
  - Storage outsourcing/consolidation
  - Sharing with different classes of clients
- DOE/Defense labs
  - Needless to explain
- Not just the consequences of compromising data, even the audits/investigations are very expensive.

Usually one comes at the expense of the other!
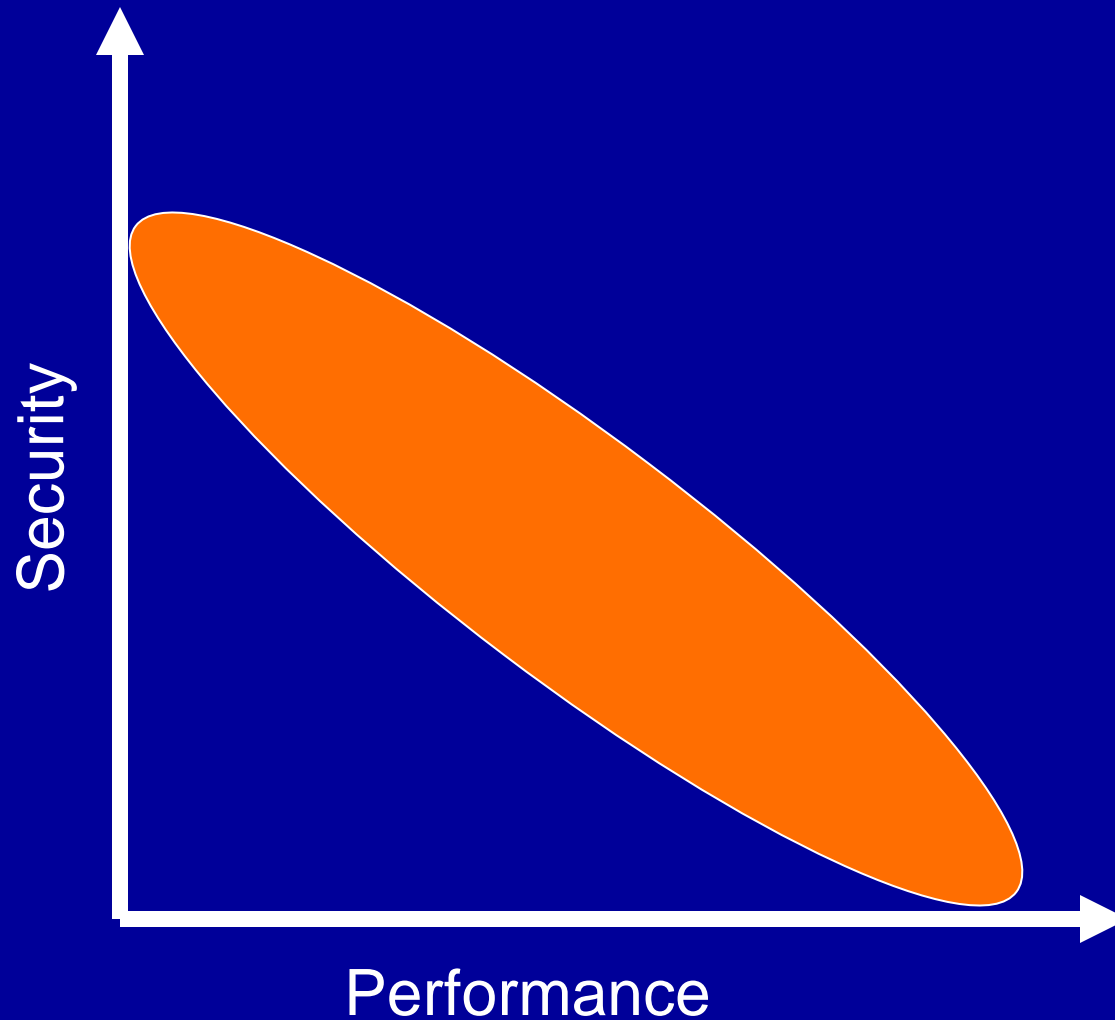
Diversity

- Diversity of tolerance to security overheads (sensitivity of information, batch vs interactive, overlapping abilities, …)
- Diversity of security needs over time.
- Diversity of threat models (network/storage/client attacks, ensuring authenticity, confidentiality, confinement, ….)
- Diversity of storage environments (cluster/SAN, physical isolation vs public networks, …)
- Diversity in mechanisms for implementing desired goals
- Diversity in the expertise of users

Too much investment and overhead is involved in trying to implement a customized system for each environment.
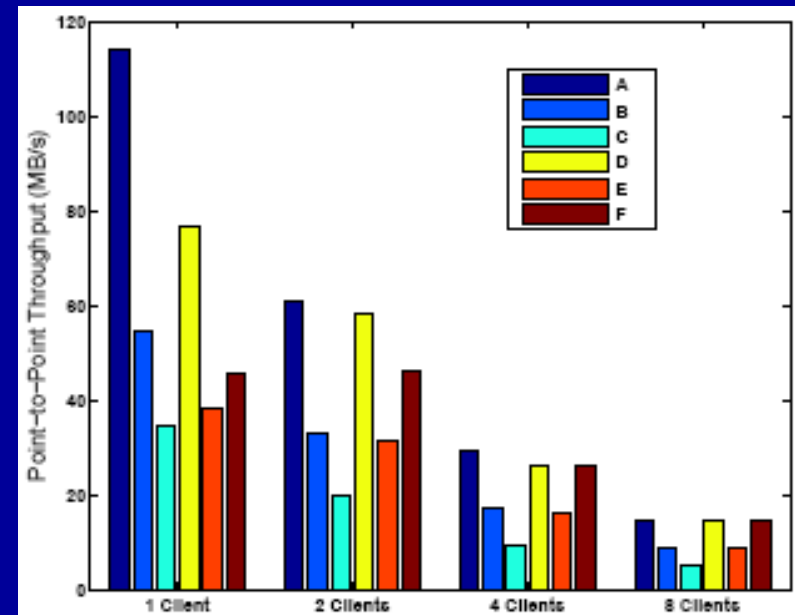
Proposed DataVault Framework

- Offer mechanisms for cluster and SAN based architectures for different operating points in Performance-Security space (mainly focus on transfer path between storage devices and clients) with the same parallel file system interface to the end-user.
- Provide a 3-tier (object, user, system) objective-driven policy system for translating objectives to a customized configuration.
- Dashboard for specifying objectives and monitoring system state (both security and performance)
- Implementations on PVFS (cluster) and GFS (SAN) platforms

Data Transfer Alternatives
Securing iSCSI (StorageSS'06)
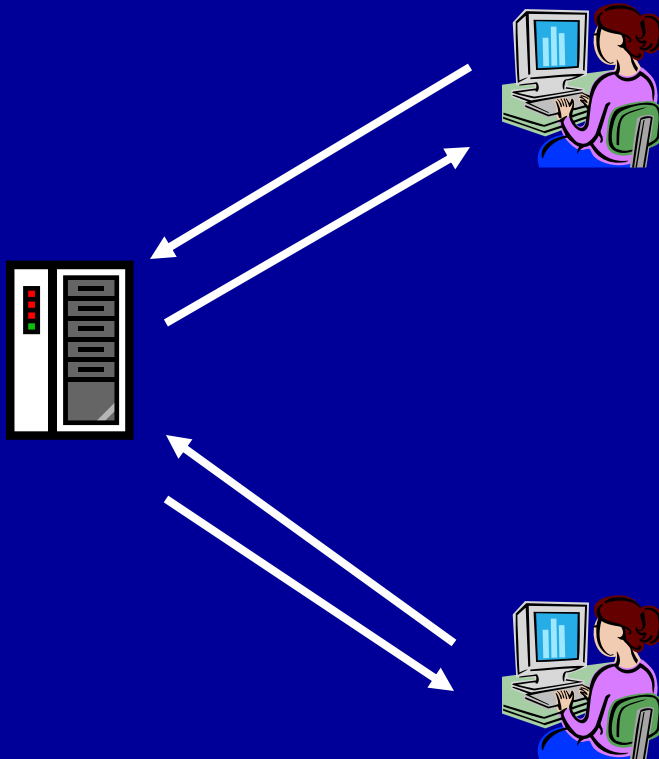
	Header Auth.	Header Confid.	Body Auth.	Body Confid.
A				
B	Eager		Eager	
C	Eager	Eager	Eager	Eager
D	Eager		Lazy	
E	Eager	Eager	Eager	Lazy
F	Eager	Eager	Lazy	Lazy

Access Control Alternatives

(a) Server/cluster style   (b) NASD style   (c) Peer-to-peer style