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

HEC FSIO Conference '08

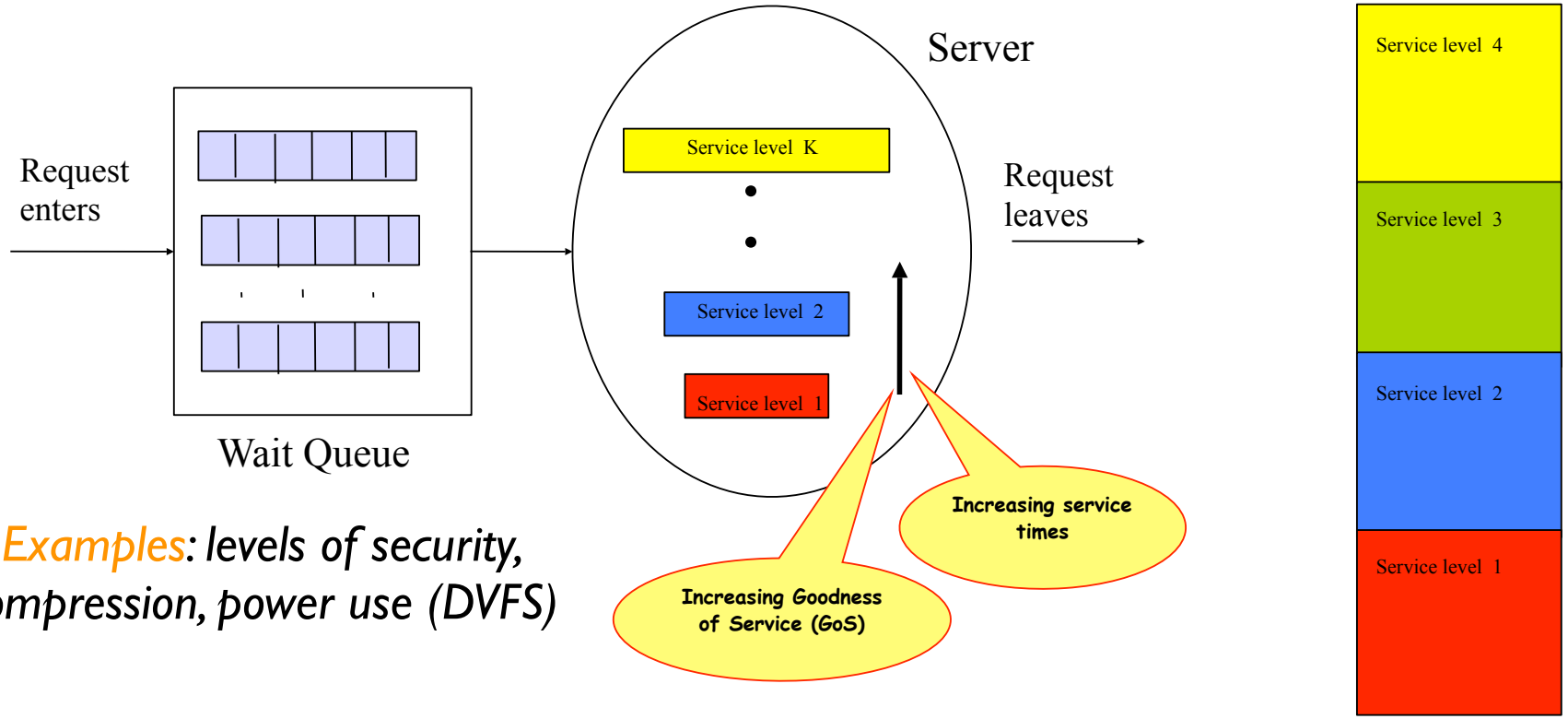
*Patrick McDaniel* (co-PI) and Anand Sivasubramaniam (PI)

August 6, 2008

# Question

- How do you serve divergent security and performance requirements of the high end storage systems?
  - What security can you afford (optimization and scheduling)?
    - QDSL (*Queuing model for Differential Service Levels*)
  - How you provide security (policy/architecture)?
    - ASD (*Autonomously Secure Disks*)

# QDSL: Differential Service Levels



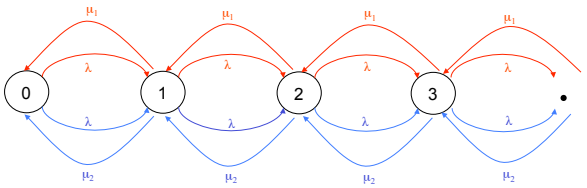

*Examples: levels of security, compression, power use (DVFS)*

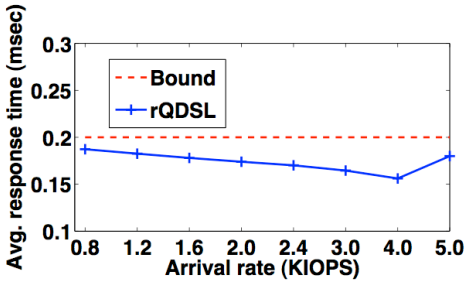
- Optimization: how do I optimize "goodness of service" in QDSL?
  - Response time (minimize response under target revenue per unit time)?
  - Revenue (maximize revenue under hard minimum response time)?

*Chaitanya, S., Urgaonkar, B., and Sivasubramaniam, A. 2008. QDSL: a queuing model for systems with differential service levels. SIGMETRICS Perform. Eval. Rev. 36, 1 (Jun. 2008), 289-300.*

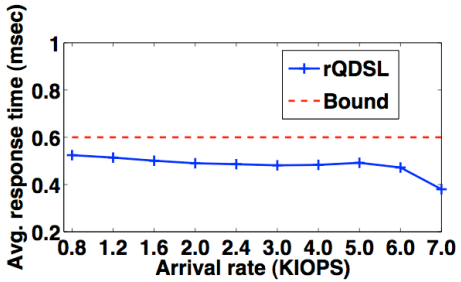
# QDSL Contributions/Results

- Characterization of QDSL class capturing environment
  - *fixSL* (fixed service level) reduced to MDP (avg. reward max.)
  - *varSL* (variable) reduced to MDP
- Performance analysis (qSecStore)
  - Service increasing security levels (integ, conf, integ+conf)
  - On live iSCSI disk system over IP (fixed 16k blocks reqs)

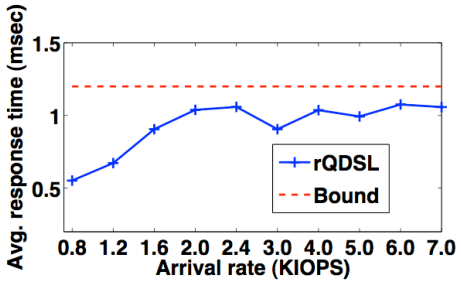



(a) Resp. time bound 0.2 msec




(b) Resp. time bound 0.6 msec




(c) Resp. time bound 1.2 msec

**Figure 5: rQDSL policy meeting the three response time bounds for a range of arrival rates**

# Autonomously Secure Disks

PENNSTATE 1855

- Disks now provide more computing power and security features (FDE) and have ancillary storage (e.g., NVRAM)
- ... thus, they provide a platform for enforcing a tightly constrained security perimeter around sensitive data,
- ... with smaller and more stable TCB and
- ... moves work to storage.


- The "*security perimeter is the disk enclosure*" ...

# Rootkit Resistant Disks

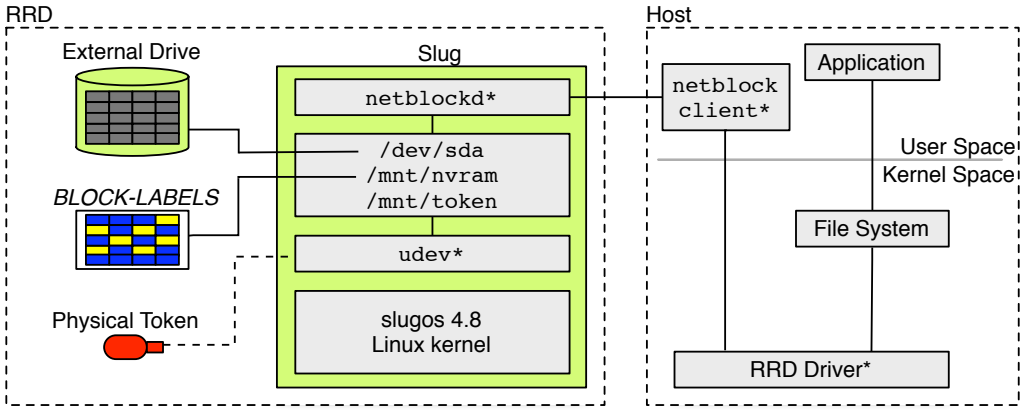
- Rootkits are now common and difficult to defend against.
  - Replaces operating system components and bypasses internal security measures (e.g., system call table replacement)
  - Often well hidden/difficult to detect


- *Idea*: use the ASD to *isolate persistent storage* from OS
  - Label all disks blocks with a mutable/immutable label
  - Use security token to ensure protected blocks modified only under the control of the system administrator.

*Kevin Butler, Stephen McLaughlin, and Patrick McDaniel. Rootkit-Resistant Disks. Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS), November 2008. Alexandria, VA.*

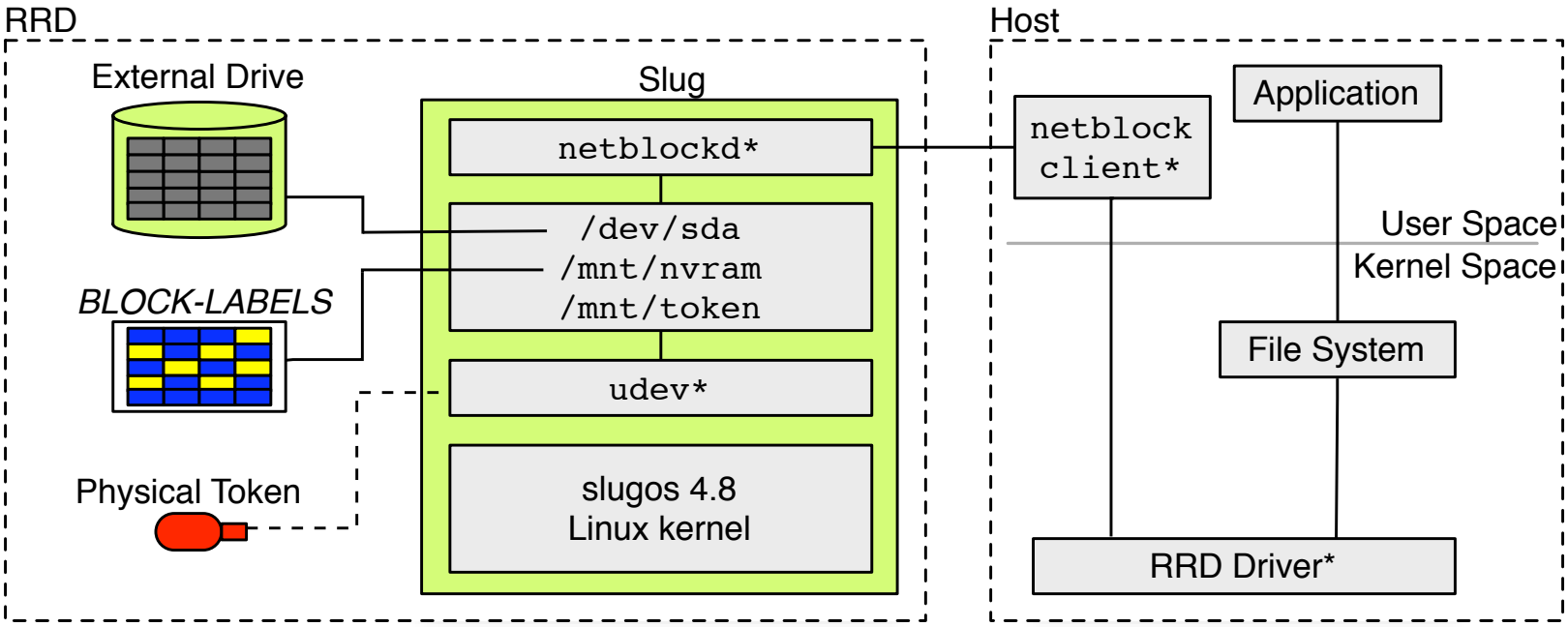
# RRD Use

- During system critical install and upgrade, token is inserted into USB slot on disk, blocks labeled (flash used to hold block labels)
  - Disk contains a "*write capability*" that enables modification or destruction of immutable blocks
- During normal operation, token not available
  - Writes to immutable blocks are blocked
- Provides a extensible read-only filesystem (more sophisticated "live-CD")
  - without the performance problems, allows mixing of mutable system and user data



# Prototype

- Hardware
  - Linksys NSLU2 (SlugOS Linux), SG ATA disk
  - 1MB Thumb drive token
- Software
  - Modified* host operating system
  - Modified netblockd service (I/O over IP)



# Performance/Future

- In general, costs small (not optimized)
- Label management largely hidden by I/O
  - Block ranges and caching help reduce overheads enormously
- *Label creep* not a problem.
- Prevents rootkits from *persisting*.

| *Configuration* | *Completion (s)* | *% Overhead* | *95% C.I.* |
|---|---|---|---|
| nosec | 501.1 | — | [497.0, 505.5] |
| sec | 508.2 | 1.4% | [505.3, 511.2] |

**Table 1: Average completion time in seconds for Postmark**

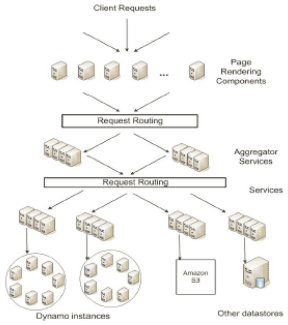
| *Configuration* | *TPS* | *% Decrease* | *95% C.I.* |
|---|---|---|---|
| nosec | 235.1 | — | [233.2, 236.7] |
| sec | 231.7 | 1.4% | [230.3, 232.7] |

**Table 2: Average Transactions Per Second for Postmark**

| *Component* | *Total Time* | *% Of Measured* | *95% C.I.* |
|---|---|---|---|
| disk | 132.9 | 59.0 % | [130.6, 135.2] |
| net | 78.4 | 34.8 % | [77.0, 79.9] |
| security | 14.1 | 6.2 % | [12.6, 15.5] |

**Table 3: Average microbenchmark results showing the amount of time spent on disk and network I/O and security operations in the RRD for Postmark.**

- Future: ASDs are a platform for implementing security policies
  - Extending to more complex policy [with Seagate]
    - XACML integration
    - MLS (extending label models)
  - More applications
    - Scaling to large distributed environments, mobile storage.



# Questions?

- Sponsors



- URL: http://siis.cse.psu.edu/storage.html
- Contact: mcdaniel@cse.psu.edu