Working Set-Based Access Control for Network File Systems

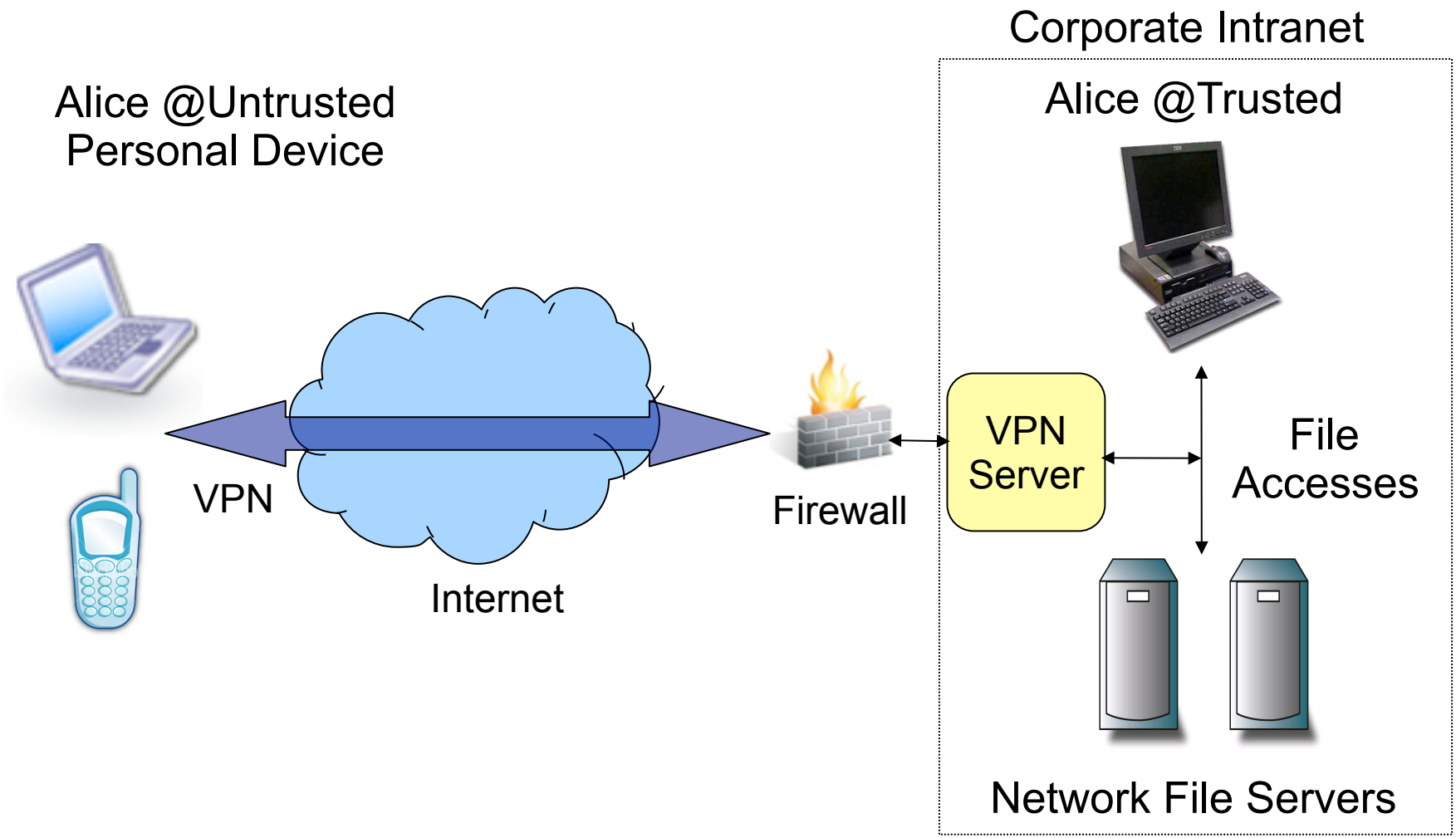
Stephen Smaldone, Vinod Ganapathy, and Liviu Iftode

DiscoLab - Department of Computer Science

Rutgers, The State University of New Jersey

{ smaldone, vinodg, iftode }@cs.rutgers.edu

Mobile Access to Network File Systems Increasing



The Working Set Concept

- The **working set** of a process is the collection of information referenced by the process during a time interval. [Denning 1968]
  - Temporal locality of a process' memory accesses
  - Memory pages to keep resident in memory to optimize performance now and in the near future
  - Informs memory page replacement algorithms to avoid thrashing

WSBAC: Working Set-Based Access Control

- Setting
  - Trusted Devices vs. Untrusted Devices
- Applies the working set principle to network file system security (access control)
  - Learn working set during trusted accesses
  - Enforce working set during untrusted accesses

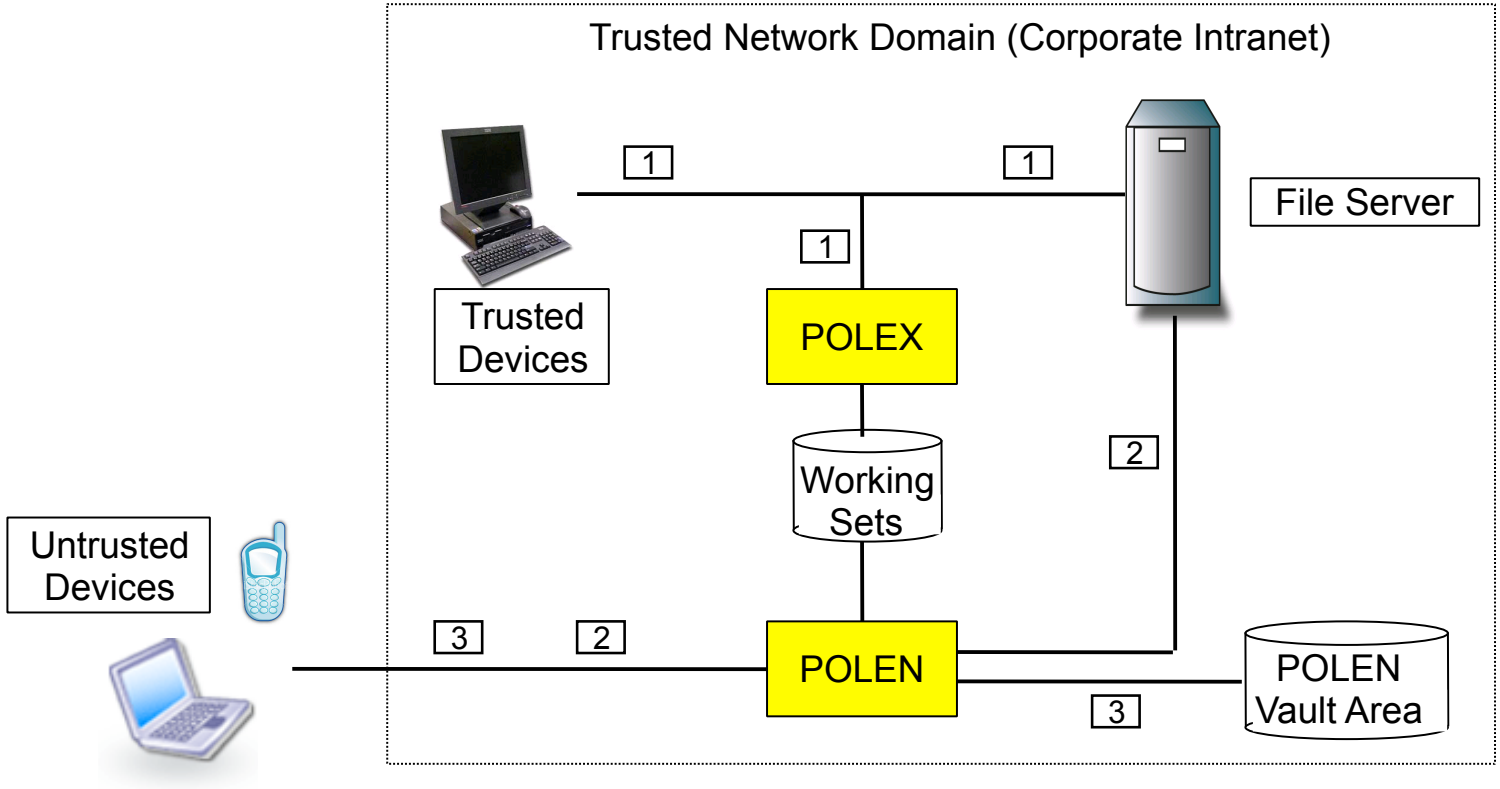
Contributions

- Working Set-Based Access Control (WSBAC)
  - Novel access control technique that estimates per-user file access working sets and enforces during access from untrusted devices
- Prototype Implementation of WSBAC for Network File Systems
  - POLEX: Working set policy extraction
  - POLEN: Working set policy enforcement
- Evaluation using Real-World Network File System Traces
  - Experimental evaluation of WSBAC using real-world NFS traces, which suggests that WSBAC is feasible and highly-effective

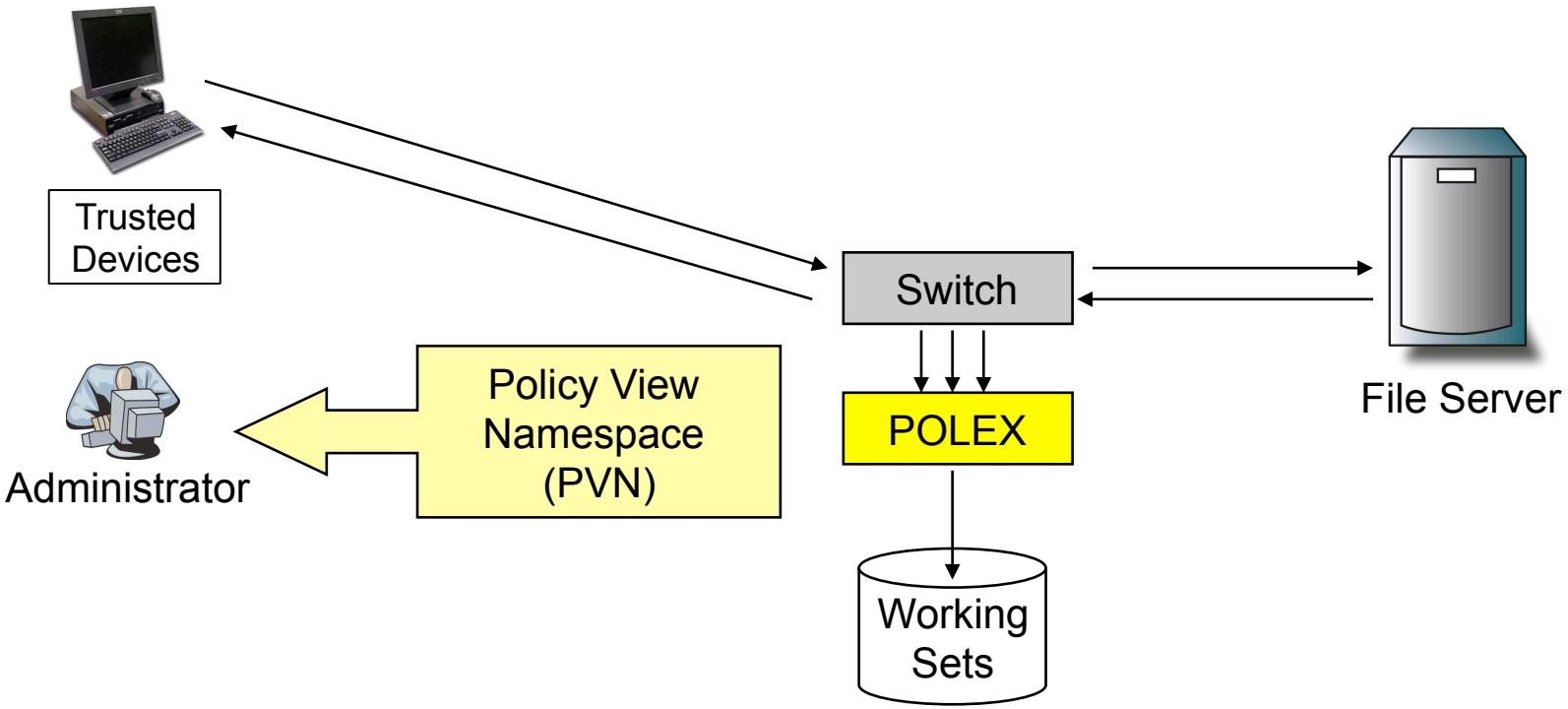
Outline

- Introduction
- WSBAC Architecture
- FileWall
- WSBAC Design and Implementation
- Evaluation and Results
- Related Work
- Conclusions and Future Work

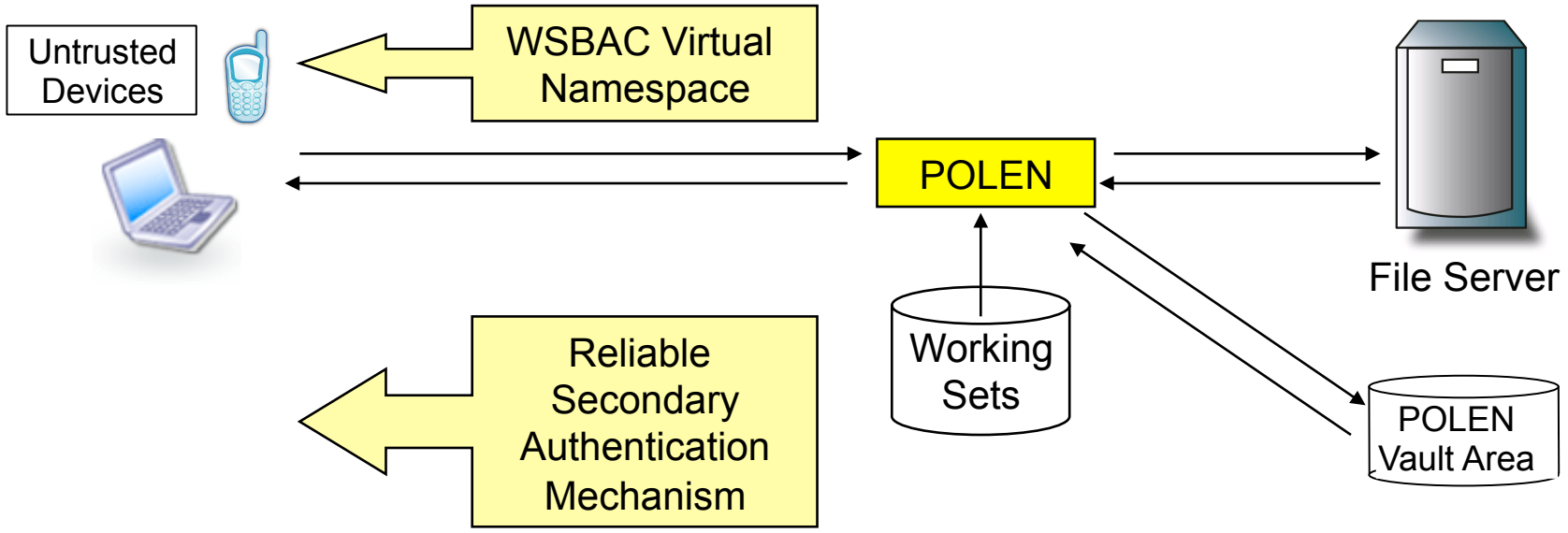
WSBAC Architecture Overview



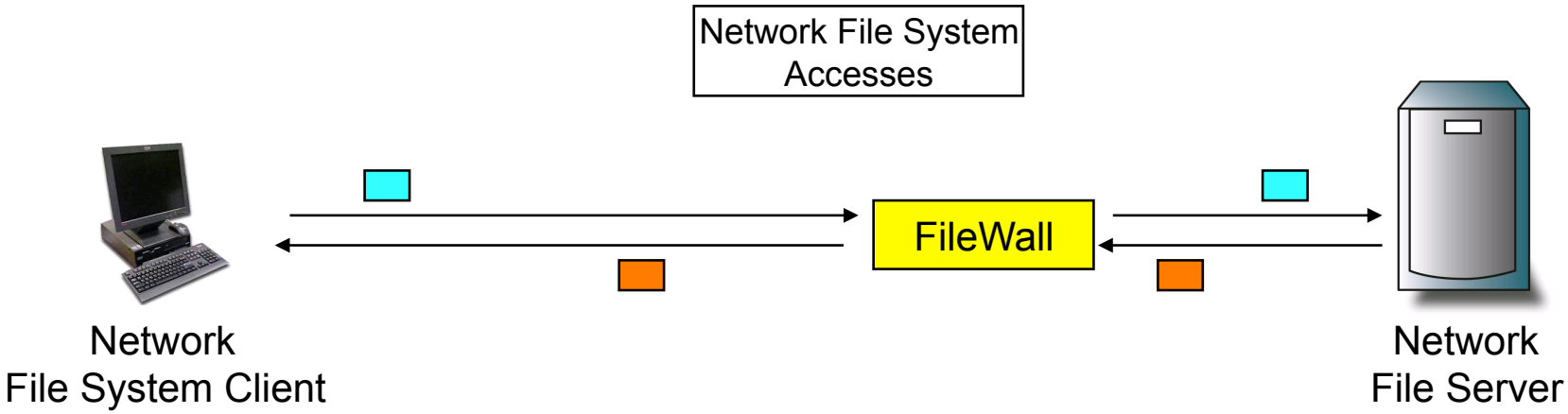
POLEX: POLicy EXtraction for Network File Systems



POLEN: POLicy ENforcement for Network File Systems

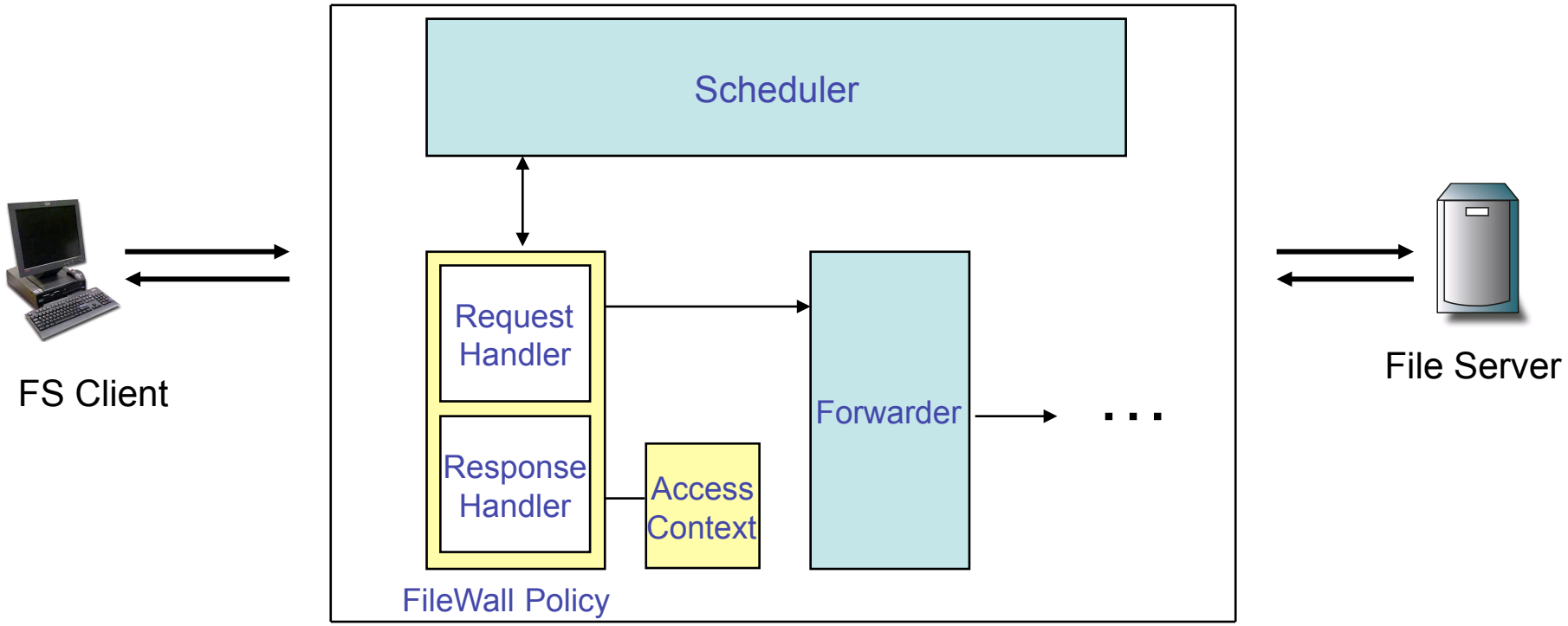


Implementation using FileWall



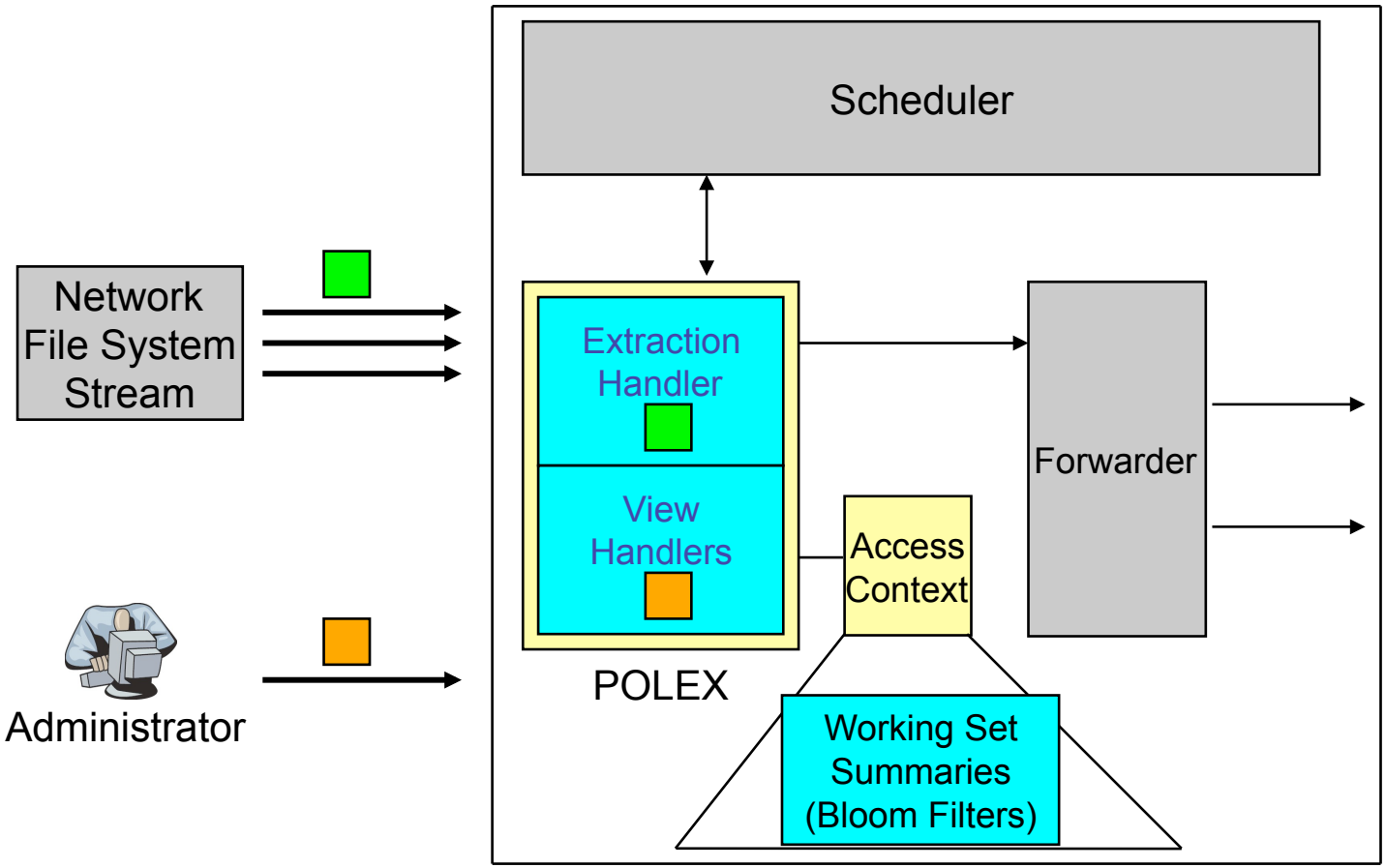
- Network File System Protocols
  - Composed of client/server messages
  - Requests sent by client
  - Responses sent by server
- FileWall: An NFS Middlebox
  - Interposed on client/server path
  - External to client/server path

FileWall Architecture

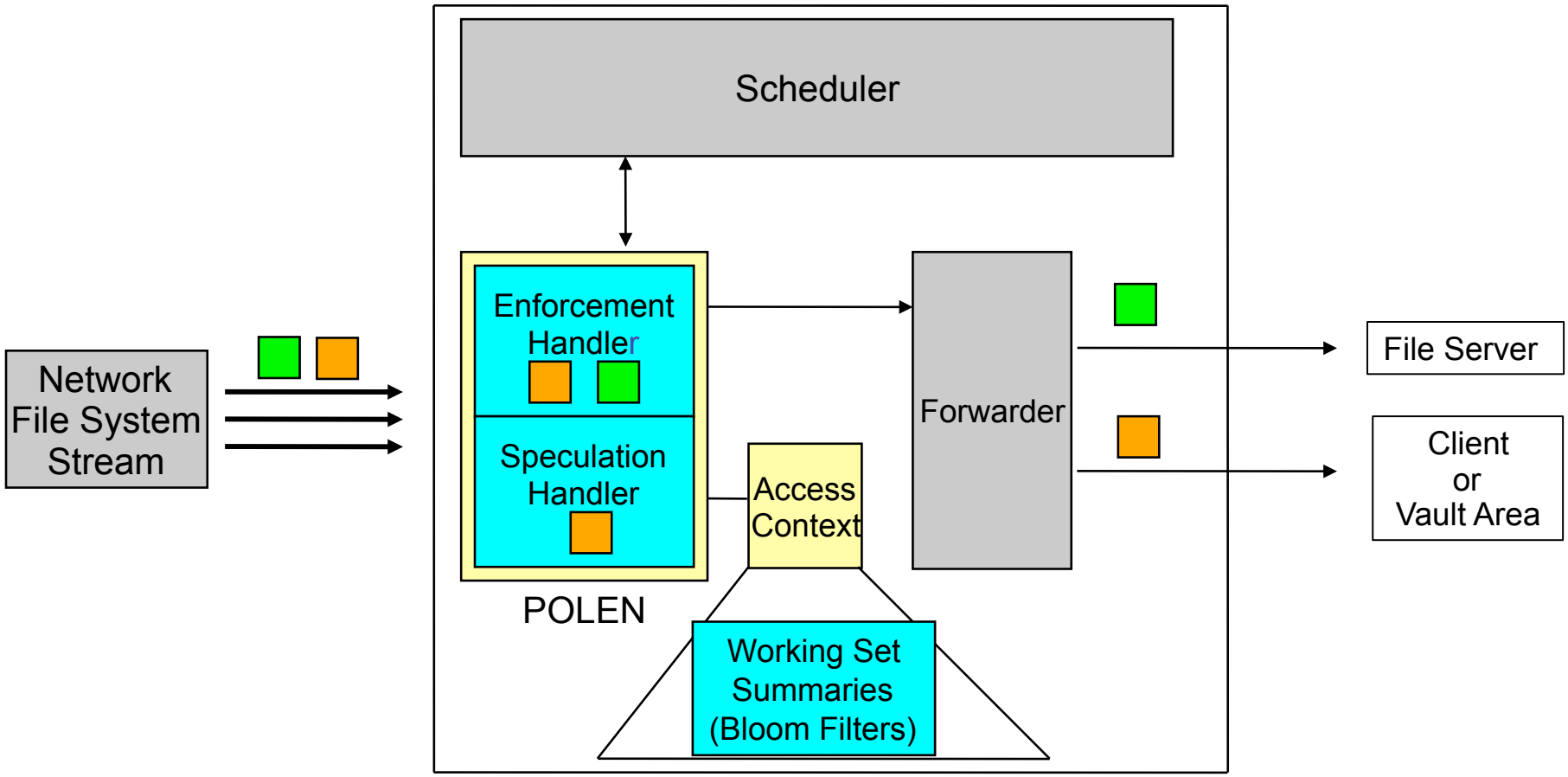


FileWall: A Firewall for Network File System, S. Smaldone, A. Bohra, and L. Iftode. *In the Proceedings of the 3rd IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC'07).*

The POLEX Implementation



The POLEN Implementation



Outline

- Introduction
- WSBAC Architecture
- FileWall
- WSBAC Design and Implementation
- Evaluation and Results
- Related Work
- Conclusions

Evaluation

- Goals
  - What are the working set estimation costs (space and time)?
  - How accurate is working set estimation?
  - How time sensitive are working set estimates?
  - How much does speculation reconciliation impact users?
  - What are the network file system performance overheads?
- Setup
  - Systems: Dual 2.4 GHz CPUs, 3 GB RAM, Linux 2.6
  - Perform offline analysis using Harvard File System Traces [Ellard'03]
  - Custom NFS fine-grained file access generation utility
  - OpenSSH compilation as application performance benchmark

POLEX Time and Storage Requirements

Size of Trace	Time to Analyze	State Size
1 Day (~3.3 GB - 6,308,023 Req/Res Pairs)	52 min	154MB
1 Hour (~140 MB - 262,834 Req/Res Pairs)	2.49 min	154MB

POLEX Accuracy

	Average Error Rate	Over-Estimation Rate
Run 1	1.08%	31.6%
Run 2	0.76%	41.2%
Run 3	1.02%	42.5%
Run 4	0.79%	36.5%
Run 5	0.97%	42.9%
Average	0.92%	38.9%

POLEX Sensitivity

	Day 1	Day 2	Day 3	Day 4	Day 5
User 1	0.26%	0.03%	0.02%	0.01%	0.01%
User 2	0.31%	4.4%	0.0%	3.3%	0.27%
User 3	0.37%	0.36%	0.82%	2.5%	0.61%
User 4	0.48%	1.8%	0.55%	0.66%	0.11%
User 5	0.18%	0.28%	0.18%	0.34%	0.27%
Average	0.32%	1.4%	0.31%	1.4%	0.27%

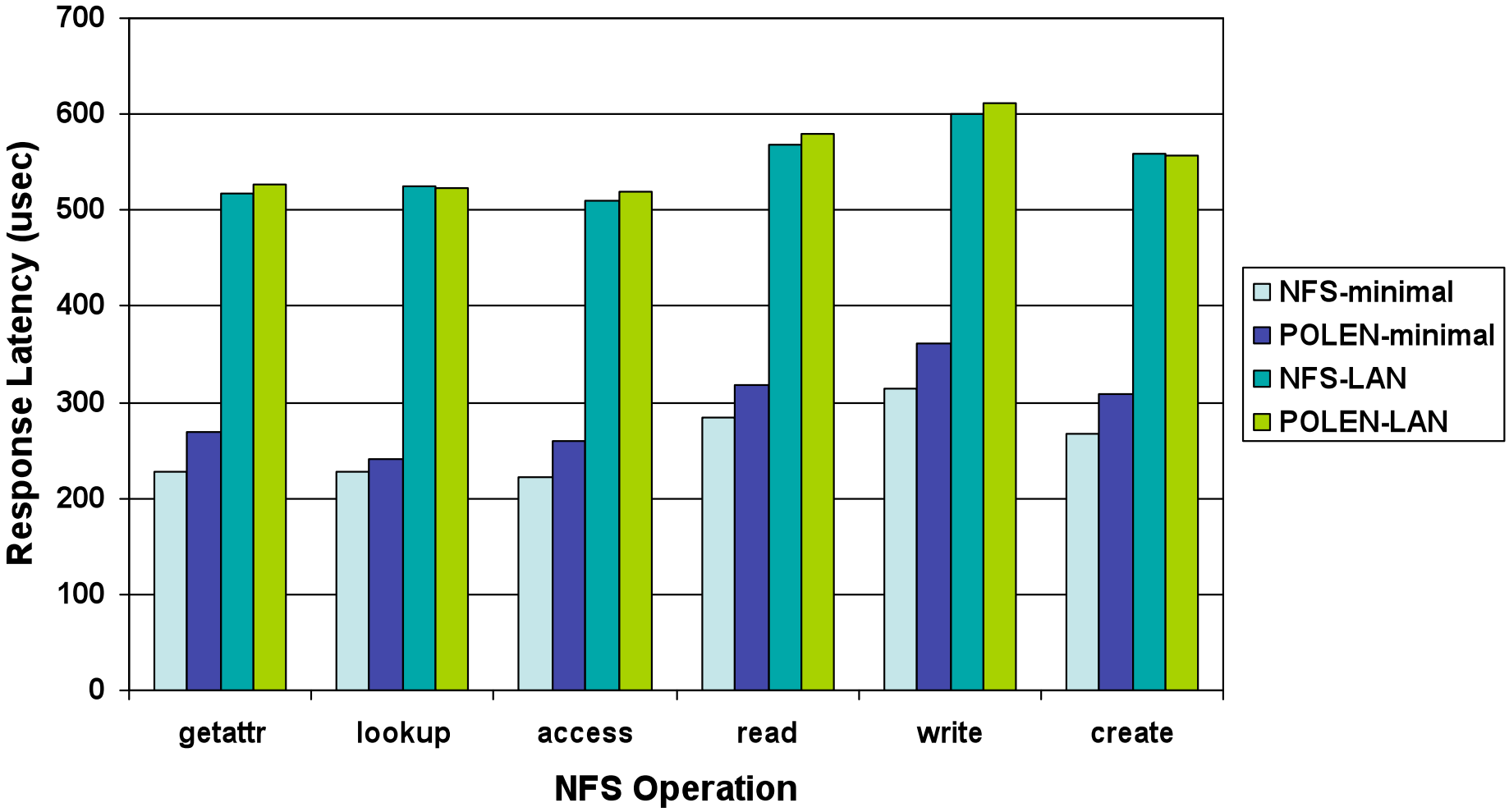
Speculation Rates

Average	Max	Min
1.4%	2.4%	0.028%

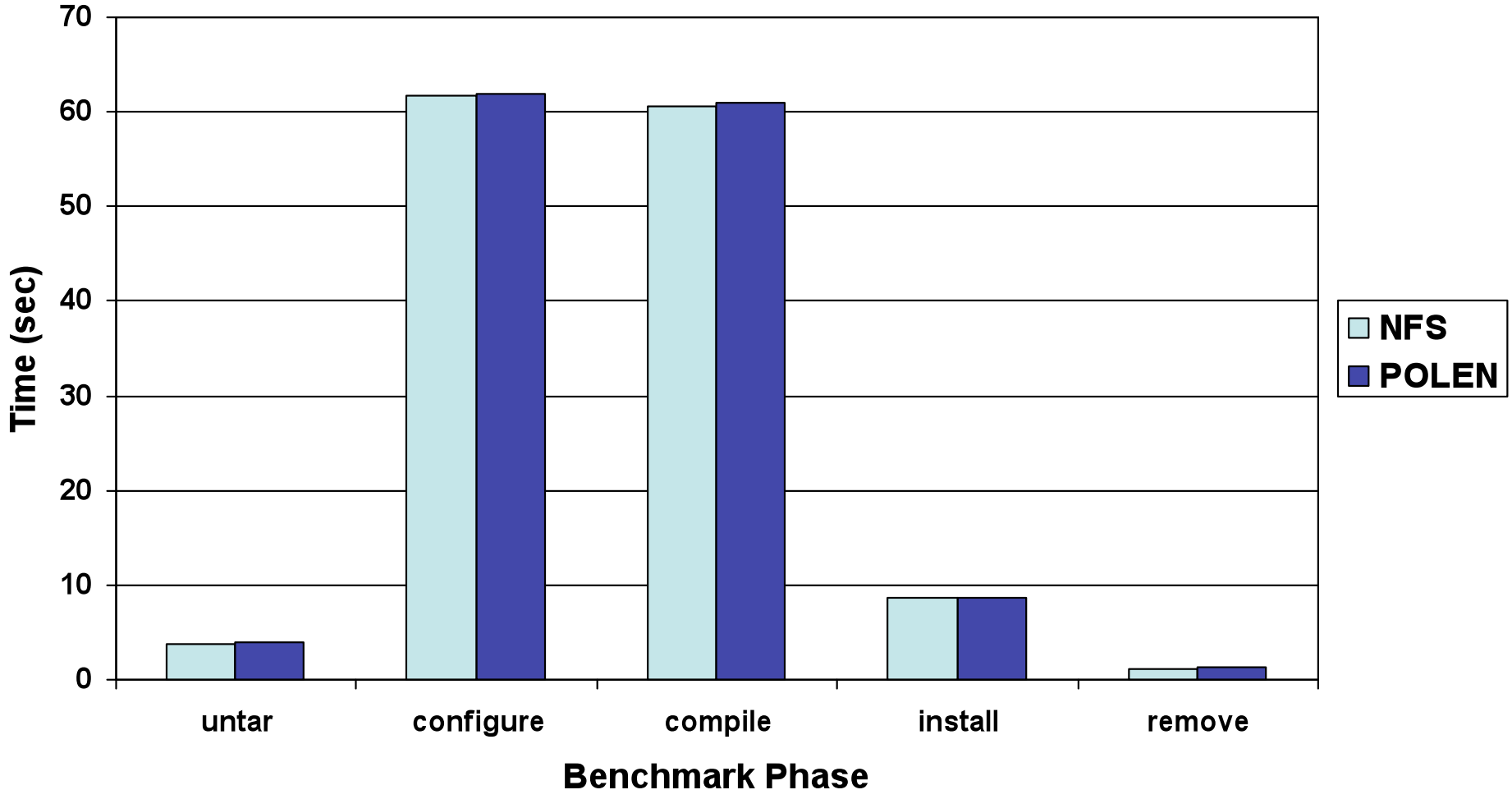
- **For Heavy Users (~500 rqst/day):**

Average	Max	Min
7 speculative rqst/day	12 speculative rqst/day	>1 speculative rqst/day

POLEN Operating Costs



POLEN Application Performance



Related Work

- Policy Extraction and Inference
  - RBAC Role Mining [Kuhlmann'03, Schlegelmilch'05]
  - XACML AC Property Inference [Anderson'04, Martin'06]
  - Firewall Policy Inference [Golnabi'06, Tongaonkar'07]
  - Gray-Box Systems [Arpaci-Dusseau'01]
- Context-Aware Access Control
  - Secure Collaborations in Mobile Computing [Toninelli'06]
  - Ubiquitous Services [Corradi'04, Yokotama'06]
  - Ad-Hoc Networks [Saidane'07]
  - Web Services [Bhatti'05, Kapsalis'06]

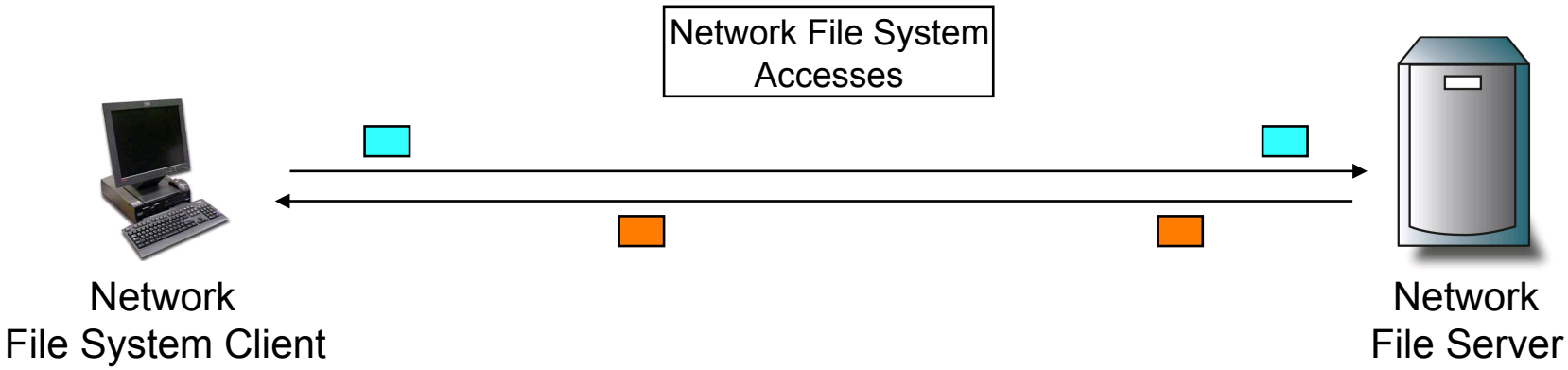
Conclusions and Future Work

- WSBAC: Working Set-Based Access Control for Network File Systems
  - Access control technique that estimates per-user working sets to formulate access control policy for accesses from untrusted devices
  - Prototype design and implementation of POLEX and POLEN
  - Experimental evaluation suggests that WSBAC is highly effective, exhibiting low error rates
- Future Work: Real-World Deployment and User Study
  - Study qualitative impact on users (usability)
  - Produce better network file system traces for future access control studies

Thank You!

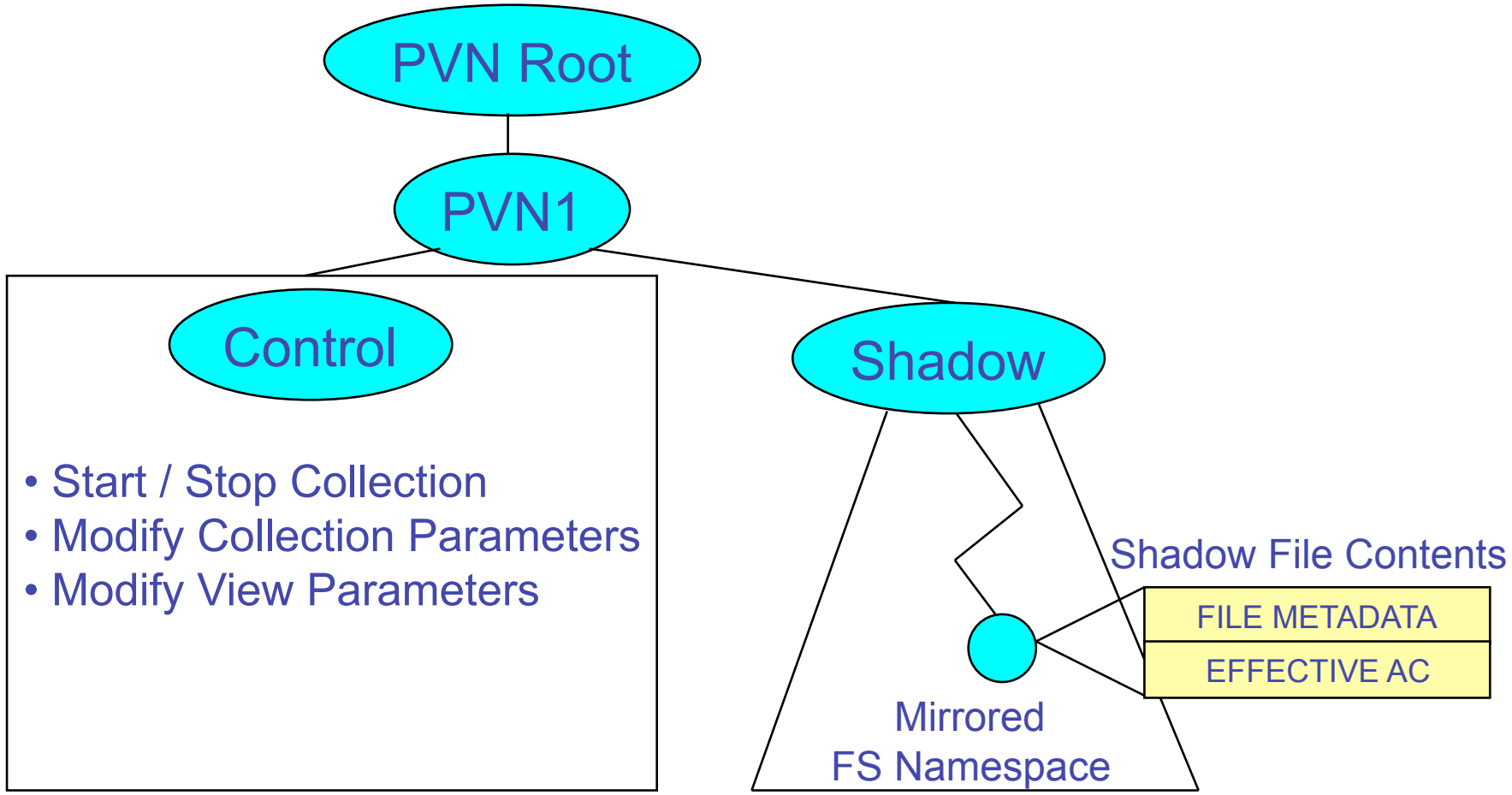
http://discolab.rutgers.edu

What is a Network File System?



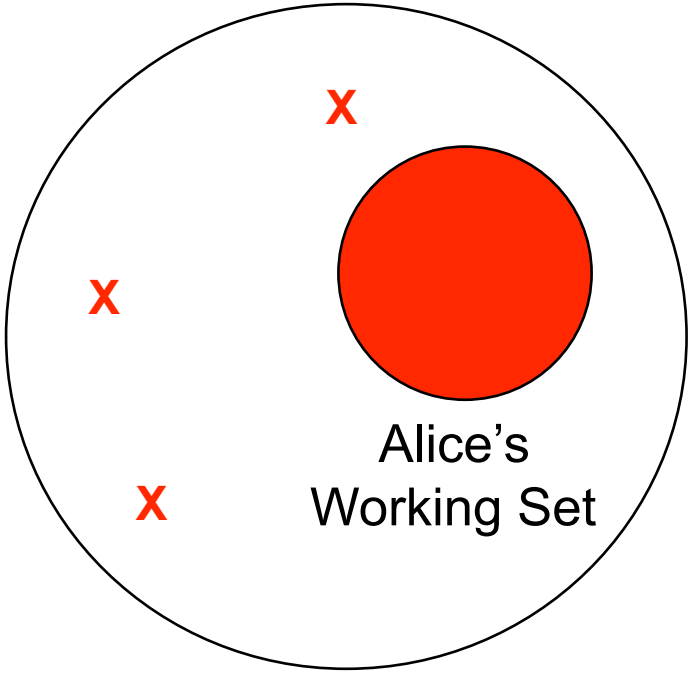
- Network File System Protocols
  - Composed of client/server messages
  - Requests sent by client
  - Responses sent by server
- NFS (UNIX), CIFS/Samba (Windows), etc.

Policy View Namespace (PVN)



Accuracy: Errors and Over-Estimations

What does an error mean?



What does over-estimation mean?