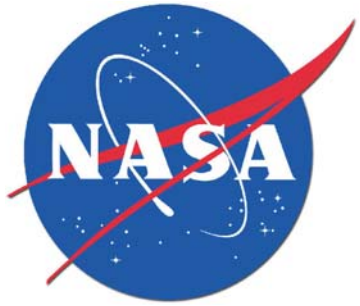
HEC FSIO
Security Breakout Review

Ellen Salmon, NASA

August 2009



Security- Current R&D Gaps
2009 Workshop Update

- Long term key management
  - Removed, but not solved. This gap area is recognized as not a file system specific problem, but a more general problem.
- End-to-end encryption
- Performance overhead and distributed scaling
- Tracking of information flow, provenance, etc.
- Ease of use, ease of management, quick recovery from compromise, ease of use API
- (added) Alternate architectures, e.g., asymmetrical lightweight authentication
- (added) Distributed persistent storage/memory (e.g., dealing with cloud architectures, nonvolatile memory)

Discussion: Security- Current R&D Gaps

2009 Workshop Update

- Long term key management *(not discussed)*
  - Removed, but not solved. This gap area is recognized as not a file system specific problem, but a more general problem.
- End-to-end encryption
  - Some felt this is not a HEC FSIO topic, no “Ranked” votes for “top 3”
- Performance overhead and distributed scaling
  - “Ranked,” medium importance, needs research, (one) ready for commercialization
- Tracking of information flow, provenance, etc.
  - “Ranked”
- Ease of use, ease of management, quick recovery from compromise, ease of use API
  - (Fewest) ranked, “clarify: add ‘usability,’ ‘how to express mechanisms for…’ ”
- (added) Alternate architectures, e.g., asymmetrical lightweight authentication
  - (Highly) “Ranked,” very important, (greatly) needs research, not ready for commercialization
- (added) Distributed persistent storage/memory (e.g., dealing with cloud architectures, nonvolatile memory)
  - Moderately “Ranked”

Supporting Slides

2008 Security Gap Area

Area	Researchers	FY 06	FY 07	FY 08	FY 09	FY 10	FY 11	Rankings
Long term key management	Odlyzko							Current researcher need data to validate designs This is not a file system issue or HEC FSIO, but a problem everyone has. We are hampered by this problem
End-to-end encryption	Odlyzko							Current researcher need data to validate designs
Performance overhead and distributed scaling	Sivasubramaniam							Problem reasonably well understood, unclear if enough demand for product
Tracking of information flow, provenance, etc.	*None*							Industry will help some, but not in HEC context.
Ease of use, ease of management, quick recovery, ease of use API's	Sivasubramaniam							Current researchers need data to validate designs Nothing to commercialize yet. Note: NSF should incorporate this into a call for security research; this topic is larger than FSIO.

This gap area is recognized as not a file system specific problem, but a more general problem. Thus, the gap sub area is being removed from the Security Roadmaps. It must be noted that this problem is NOT solved.

2006 HECURA/CPA Projects

- Exploiting Asymmetry in Performance and Security Requirements for I/O in High-end Computing; Anand Sivasubramaniam, Pennsylvania State University University Park
- Integrated Infrastructure for Secure and Efficient Long-Term Data Management; Andrew Odlyzko, University of Minnesota-Twin Cities

2009 HECURA Projects and Presentations

- Secure Provenance in High-End Computing Systems; Patrick Mc Daniel, Penn State