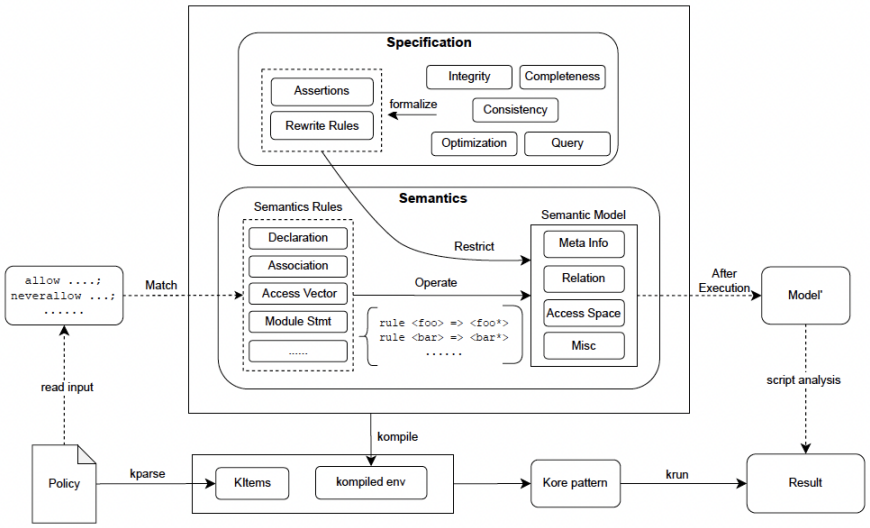
K-SELinux: Formal Analysis and Verification of SELinux Policies via Semantic Execution

Jinhui KANG, Jianhong ZHAO, Yongwang ZHAO

Frontiers of Computer Science, DOI: 10.1007/s11704-024-40495-7

Problems & Ideas

- Problems of SELinux policy analysis and verification:
  - SELinux policy grows with the complexity of systems.
  - Existing works focus on particular analysis objectives and lack a unified approach for comprehensive analysis.
  - Popular policy analysis tool lack formal guarantee.
- Ideas: Establish the semantic model of the SELinux policy language. Analyze and verify policies during semantic execution.



Combine specifications with formalized semantics to analyze and verify policies via semantic execution, where kparse, kompile, and krun are tools supplied in K

Main Contributions

- Contributions:
  - A novel approach for the formal analysis and verification of SELinux policies through semantic execution.
  - Complete formal semantics of the SELinux policy language, formalized and expressed by rewrite rules in K.
  - Techniques to formalize abstract requirements and security properties.
  - A SELinux policy analysis prototype tool that encompasses several aspects of SELinux policy analysis.

Comparison between policy analysis tools

Analysis tools	Consistency check	Completeness check	Integrity check	Information flow analysis	Policy opt / rewriting	policy query
SETools			✓	✓		✓
SEGrapher				✓		
SPTrack				✓		
SEEdit				✓	✓	
GOKYO		✓	✓			
SEAnalyzer				✓		✓
SCIATool			✓	✓	✓	✓
SELAC			✓			
EASEAndroid				✓		
SELint					✓	
K-SELinux	✓	✓	✓	✓	✓	✓