GRIDLOCK

Personnel

- Joan Feigenbaum, Yale (jf@cs.yale.edu)
- Angelos D. Keromytis, Columbia (angelos@cs.columbia.edu)
- Jonathan M. Smith, Penn (jms@cis.upenn.edu)
- PhD students: Zhong, Ioannidis, Cook

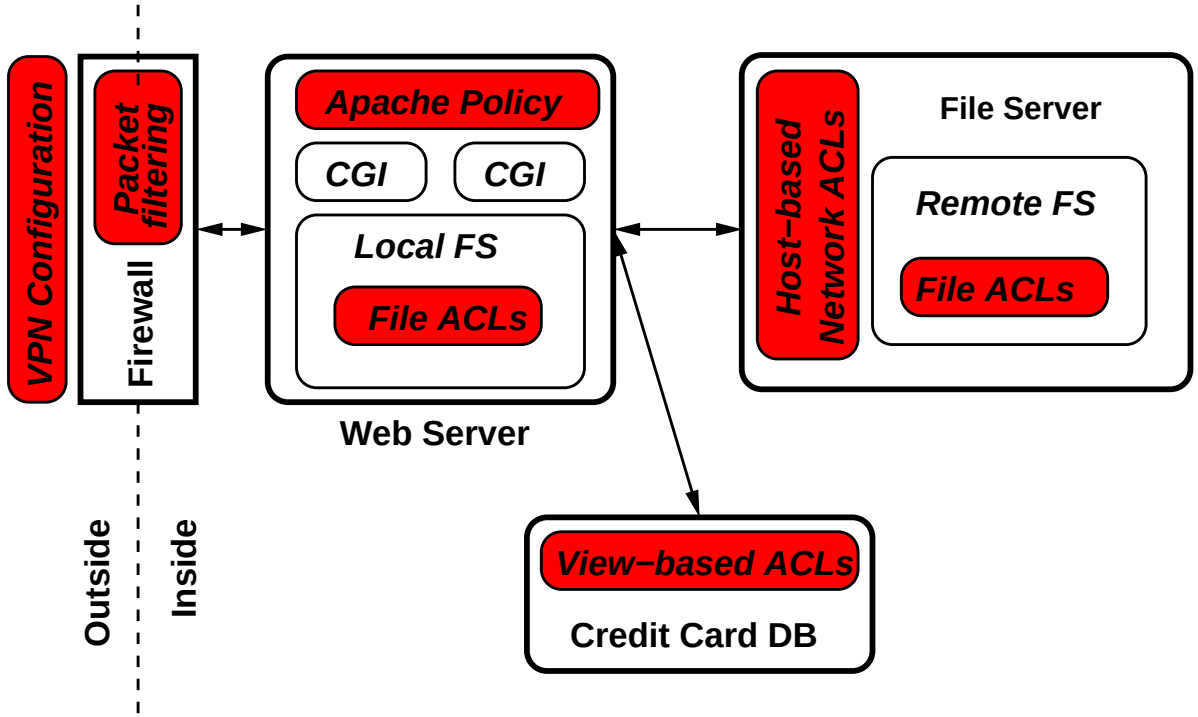
Duration: 3 years, starting in August 2002

Research Goals:

- Security management in large multi-application environments
- Unified approach to network and host security
- Virtual Private Services

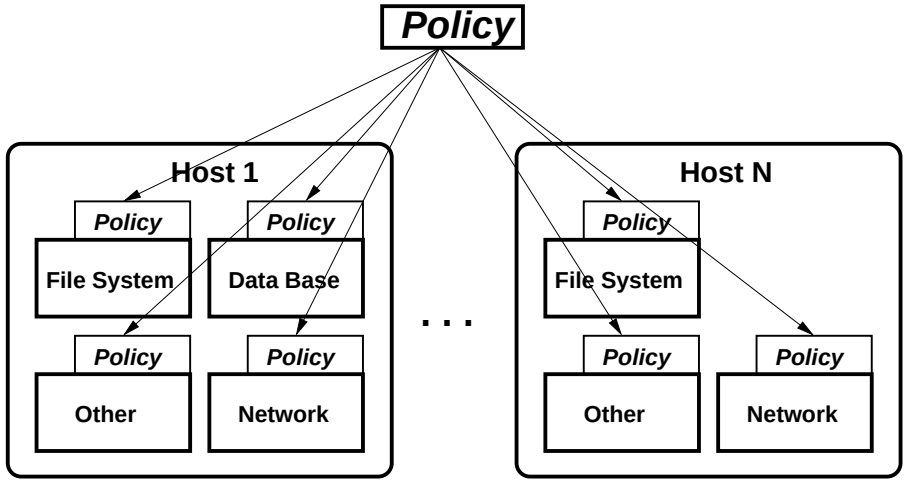
General Problem

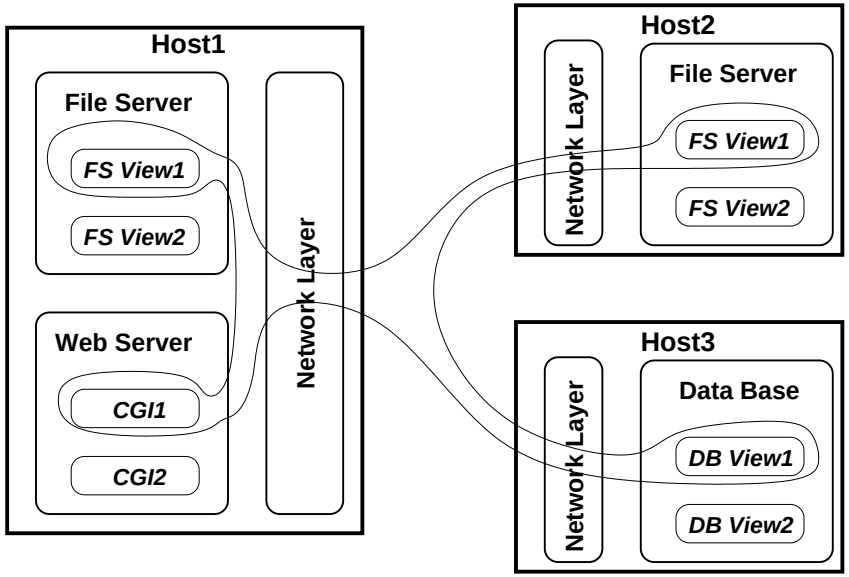
- Network and host security are now handled separately
  - Incompatible configurations of components
- Leads to lack of end-to-end coherence
  - Security vulnerabilities
  - Loss of functionality



GRIDLOCK Hypothesis

- Unification of network and host access-control mechanisms
- Technical components:
  - Globally specified, locally interpreted policies
  - Domain-specific policy meta-languages
- Virtual Private Services:
  - Extend OS notions of virtual machine and process isolation to distributed systems





Virtual Private Services

- Examples, in increasing order of complexity:
  - Distributed database
  - Virtual network infrastructure
  - Virtual organization
- To achieve vision, we need:
  - Efficient policy-enforcement mechanisms for the different components
  - High-level, domain-specific policy languages
  - Tools for verifying correctness and consistency
  - Automated administration
- Starting point: trust management
  - KeyNote trust-management system
  - Distributed policy expressed explicitly and via credentials

Challenges

- Devising good application-domain (AD) languages
  - Expressive, usable, efficiently implementable
  - Cover multiple applications within a domain
- Managing diverse security mechanisms
  - Example: filesystem vs. firewall semantics
- Conflict resolution and non-monotonicity
- Scalability
  - Automating administration
- Performance

Current Activities

- Develop tools
  - PEPL: framework for creating AD-specific languages
  - DisCFS: credential-based network filesystem
  - WebDAVA: user-managed, web-based file storage
- Translate AD-specific policies to KeyNote
- Use conflict-resolution capabilities of trust-management engines
- Augment existing access-control points with KeyNote
  - Lightweight decision making
  - Leverage localization of access control for scalability
- Enhance KeyNote as needed

Planned Experimentation

- Deploy shared filesystem across the three institutions
- Combine file-access control, firewall configuration, and web-server ACLs
  - Use environment for joint authoring of reports and papers
  - Implement full-fledged distributed database
- Extend to storage marketplace
  - Integrate payment mechanism
- Virtual organization
  - Combine network services and distributed-database services
  - Integrate VPN and QoS capabilities

First-Year Accomplishments

- Sample of publications from first year

- "EasyVPN: IPsec Remote Access Made Easy," USENIX LISA, October 2003
- "Secure and Flexible Global File Sharing," USENIX Freenix, June 2003
- "Experience with the KeyNote Trust Management System: Applications and Future Directions," 1st International Conference on Trust Management, May 2003
- "Design and Implementation of Virtual Private Services," IEEE WETICE, June 2003
- "WebDAVA: An Administrator-Free Approach to Web File-Sharing," IEEE WETICE, June 2003
- "Sprite: A Simple, Cheat-proof, Credit-based System for Mobile Ad-Hoc Networks," IEEE Infocom, April 2003
- "Verifiable Distributed Oblivious Transfer and Mobile Agent Security," DIALM/POMC, September 2003

- DisCFS prototype (http://www.seas.upenn.edu/~miltchev)
- PEPL compiler (http://www.cs.columbia.edu/~angelos/Code/canon31.tar.gz)
- WebDAVA prototype (http://www.cs.columbia.edu/~angelos/Code/dava-demo.tar.gz)