Software Quality and Infrastructure Protection for Diffuse Computing

Principal Investigator: Andre Scedrov
Institution: University of Pennsylvania
URL: http://www.cis.upenn.edu/spyce

OPTION STARTED IN MAY 2004
The SPYCE Team

- Joan Feigenbaum (Yale)
- Joseph Y. Halpern (Cornell)
- Patrick D. Lincoln
- John C. Mitchell (Stanford)
- Andre Scedrov (U Penn)
- Jonathan M. Smith (U Penn) (until December 2003)
External Collaborators

- Cynthia Dwork (Microsoft)
- Tim Griffin (Intel)
- Vitaly Shmatikov (SRI)
- Paul Syverson (NRL)
URI Objective

Algorithms to model, manage and maintain a computational infrastructure, distributed among many heterogeneous nodes that do not trust each other completely and may have incentives (needs, priorities).

Scientific/Technical Approaches

Computing and networking elements diffusing into the environment need:
- Local incentive-compatibility in global distributed computing
- Scalable authorization mechanisms
- Assured communication
- Experimental evidence

DoD Capabilities

Reduced cost, improved performance, and higher reliability for networked operations across untrusted networks
Secure services through heterogeneous overlay networks

- Communication
- Cooperation
- Incentives
- Delivery
Diffuse Computing

- Paradigm developing rapidly as a result of
  - commercial computing markets
  - now-recognized potential of peer-to-peer computing and grid computing
  - the need for distributed network-centric systems

- Raises challenges for
  - system design
  - software production
  - the development of mechanisms ensuring stable equilibria of diffuse systems
SPYCE Objective: Scalable Distributed Assurance

Develop fundamental understanding, models, algorithms, and network testbed, in order to reduce cost, improve performance, and provide higher reliability for networked operations across untrusted networks.

Incentives, Privacy, and Anonymity

Protocol Design and Analysis

Network Architecture

Trust Management
Software Quality and Infrastructure Protection
for Diffuse Computing
U Penn, Stanford, Cornell, Yale

Scientific Accomplishments
• Interdomain routing
  Path vector protocols [Penn-Yale-Intel]
  Local conditions for stable routes [Yale]
• Analysis of cryptographic protocols
  Formal methods for cryptography [Penn-Stanford]
  Kerberos 5 analysis [Penn-NRL]
• Logic for reasoning about policies [Cornell]
• SPAM reduction algorithms [Microsoft-Stanford]
• Privacy in databases [SRI-Microsoft]
• Anonymity and information hiding [Cornell-NRL]
• Content transcoding for heterogeneous clients [Penn]
• Flexible Lightweight Active Measuring Environment [Penn]

Educational Accomplishments
• Enhanced the ability to educate and train students in science
  and engineering and perform CIP/SW relevant research
  • 10 refereed journal publications
  • 55 refereed conference proceedings
• 5 prototypes
• 7 PhD students graduated, 16 PhD students supported
• Members of NAS Computer Science and
  Telecommunications Board, Defense Science Board Task
  Force on Science and Technology, ACM Fellows, AAAI
  Fellows, ...

Project Contact Information
• PI: Prof. Andre Scedrov
  co-PIs: Prof. Joan Feigenbaum,
         Prof. Joseph Halpern,
         Dr. Patrick Lincoln, Prof. John Mitchell

• Prof. Andre Scedrov
  Department of Mathematics
  University of Pennsylvania
  209 South 33rd Street
  Philadelphia, PA, 19104-6395

WWW: http://www.cis.upenn.edu/spyce
Email: scedrov@cis.upenn.edu

August 17, 2004
Sample Plans for Option (1)

- Secure, reliable network infrastructure
  - Combine security mechanism and incentives
  - Examples: BGP, DNS, NTP, ...

- General theory of computational mechanism
  - Mechanism specification and verification
  - Computational complexity analysis combining network communication and incentives

- Discrete information management
  - Multicentric information delivery and retrieval
  - Access control, anonymity, and privacy
Sample Plans for Option (2)

- Further investigation of practical protocols
- Automating verification
- Adding utilities to specifications
- Verifying mechanisms
  - mechanism = set of rules for playing a game, designed to encourage “good” behavior
    e.g., tax system, type of auction
Sample Plans for Option (3)

- Combine the study of incentives, privacy, and anonymity
- Derive **hardness** results in diffuse computing
  - Hardness stems from interplay of computational requirements and incentive-compatibility requirements (as in budget-balanced MCS).
- Use hardness as a building block in *private algorithmic mechanisms* or *anonymous algorithmic mechanisms*. 
SPYCE Objective: Scalable Distributed Assurance

Develop fundamental understanding, models, algorithms, and network testbed, in order to reduce cost, improve performance, and provide higher reliability for networked operations across untrusted networks.

Incentives, Privacy, and Anonymity

Protocol Design and Analysis

Network Architecture

Trust Management