



FY2001 ONR CIP/SW URI



Software Quality and Infrastructure Protection for Diffuse Computing



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

STARTED IN MAY 2001

The SPYCE Team

- Cynthia Dwork* (Microsoft)
- Joan Feigenbaum (Yale)
- Joseph Y. Halpern (Cornell)
- Patrick D. Lincoln* (SRI)
- John C. Mitchell (Stanford)
- Andre Scedrov (U Penn)
- Vitaly Shmatikov* (SRI)
- Jonathan M. Smith (U Penn)
- Paul Syverson* (NRL)



Project Coordination:

Multi-Pronged Approach to Herding Research

- Physical meetings (Dec '01, Dec '02)
 - *Workshop on Economics and Information Security (May '02)*
- Video conference (Oct '01)
- Teleconferences (joint, subgroups)
- Email discussions

- Organization and coordination centered at UPenn

Main Theme: Diffuse Computing

Managing and maintaining a computational infrastructure, distributed among many heterogeneous nodes that do not trust each other completely and may have incentives (needs, priorities).

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: Scaleable High Assurance



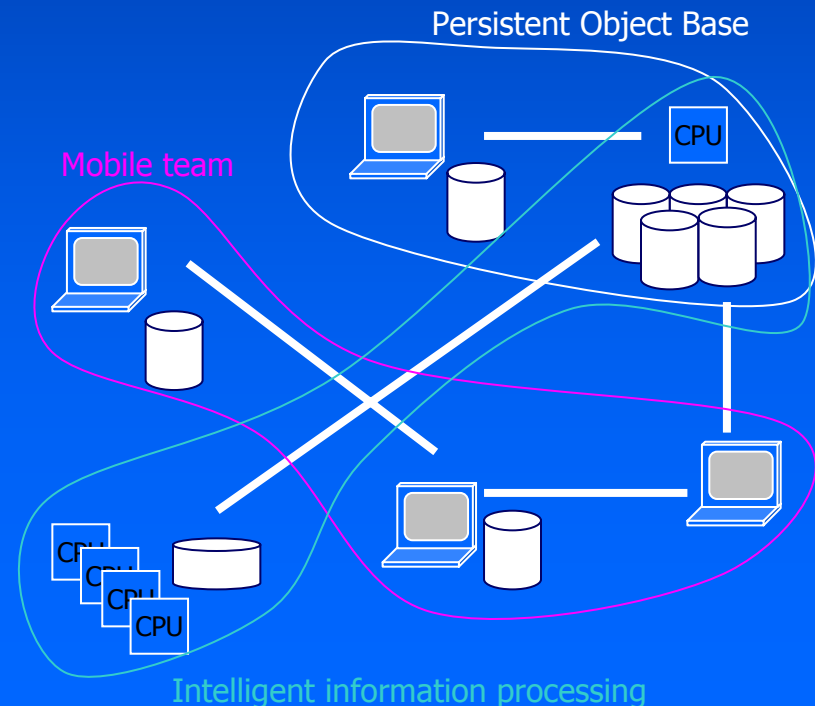
Develop fundamental understanding, models, algorithms, and network testbed, in order to reduce cost, improve performance, and provide higher reliability for networked operations across untrusted networks.

Efficient Diffuse Multimedia Networking

Incentive Compatibility

Authorization Schemes

Secure Data Storage and Communication





Software Quality and Infrastructure Protection for Diffuse Computing



URI, 2001

scedrov@saul.cis.upenn.edu Web URL: <http://www.cis.upenn.edu/spyce/>

March, 2003

Smart devices diffuse into the environment....



Room '40s



Desktop '80s



Wearable '90s



Pervasive '00s

... with control and assurance

URI Objective

Algorithms to model diffuse computing and achieve scaleable high assurance

DoD capabilities enhanced

Reduced cost, improved performance, and higher reliability for networked operations across untrusted networks

Scientific/technical approach

Computing and networking elements diffusing into the environment need:

- Local incentive-compatibility in global distributed computing
- Scaleable authorization mechanisms
- Assured communication
- Experimental evidence

Sample Accomplishments

- Local conditions for stable routes in interdomain routing
- Anonymous communication
- SPAM reduction algorithms
- Content transcoding for heterogeneous clients
- Kerberos V protocol analysis
- Logic for reasoning about digital rights

Conferences where we publish

- Computer Security Foundations Workshop
- Conference on Computer and Communication Security
- International Information Security Conference
- Workshop on Security and Privacy in Digital Rights Management
- Conference on Electronic Commerce
- Symposium on Principles of Distributed Computing
- International Symposium on High-Performance Distributed Computing
- Conference on Computer Communications
- International Workshop on Web Content Caching and Distribution
- International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems

Conferences where we publish

- Computer Security Foundations Workshop
- Conference on Computer and Communication Security
- International Information Security Conference
- Workshop on Security and Privacy in Digital Rights Management
- Conference on Electronic Commerce
- Symposium on Principles of Distributed Computing
- International Symposium on High Performance Computing
- Conference on Computer Communications Security
- International Workshop on Web Content Caching and Distribution
- International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems

Keywords

Computer

Security

Distributed

Communication

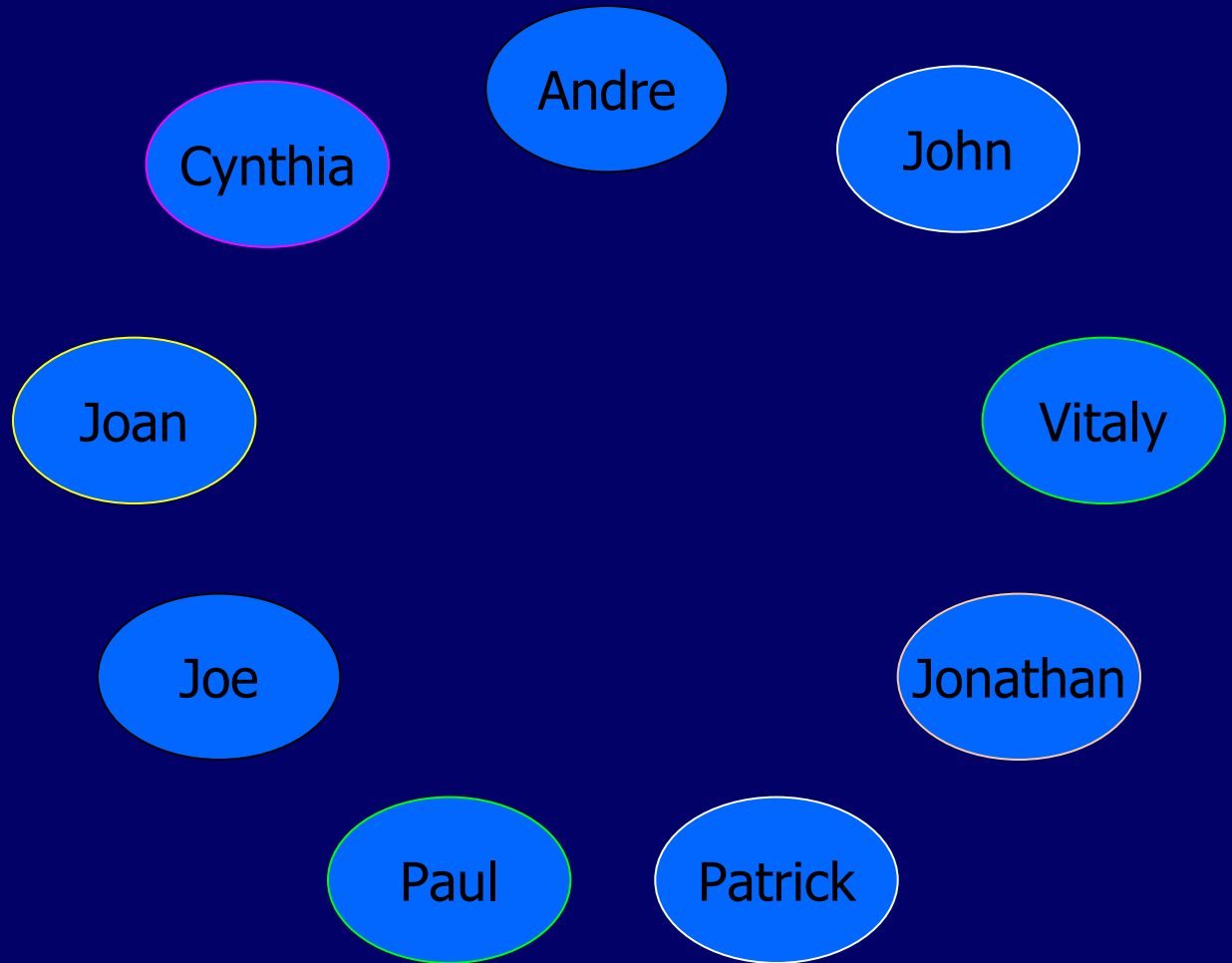
Project Themes

- Combines 4 complementary thrusts:
 - Incentive-compatibility in distributed computing
 - Authorization mechanisms
 - Secure data storage and retrieval
 - Communication protocols
- Multi-institution experimental platform + systematic, formal treatment of underlying models, algorithms & data structures

SPYCE areas of concentration

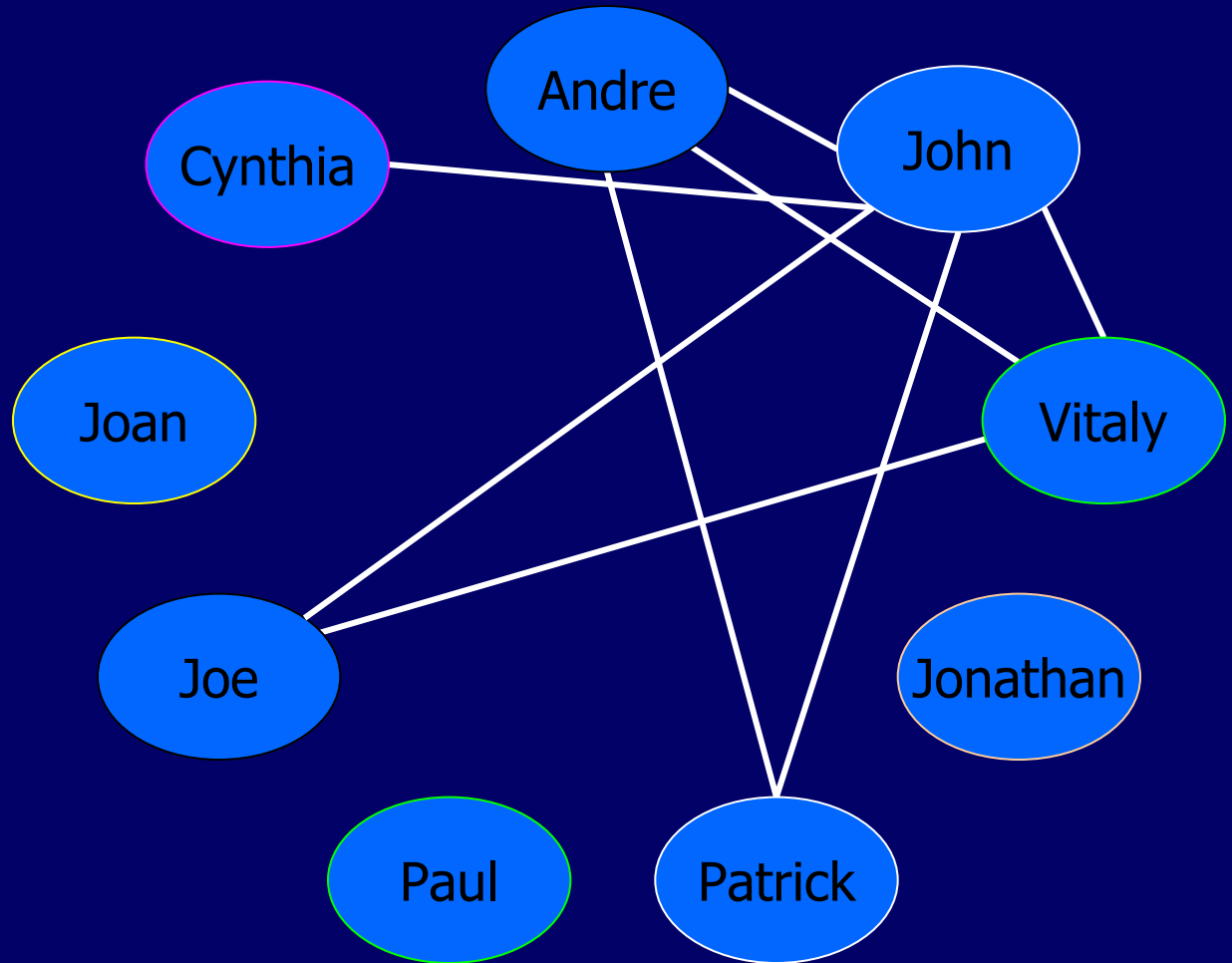
- Market-based computation (incentive-compatibility)
- Communication and security protocols analysis
- Authorization mechanisms (trust management)
- Privacy and anonymity
- Networking, experimental platform

Spyce Interaction Graph



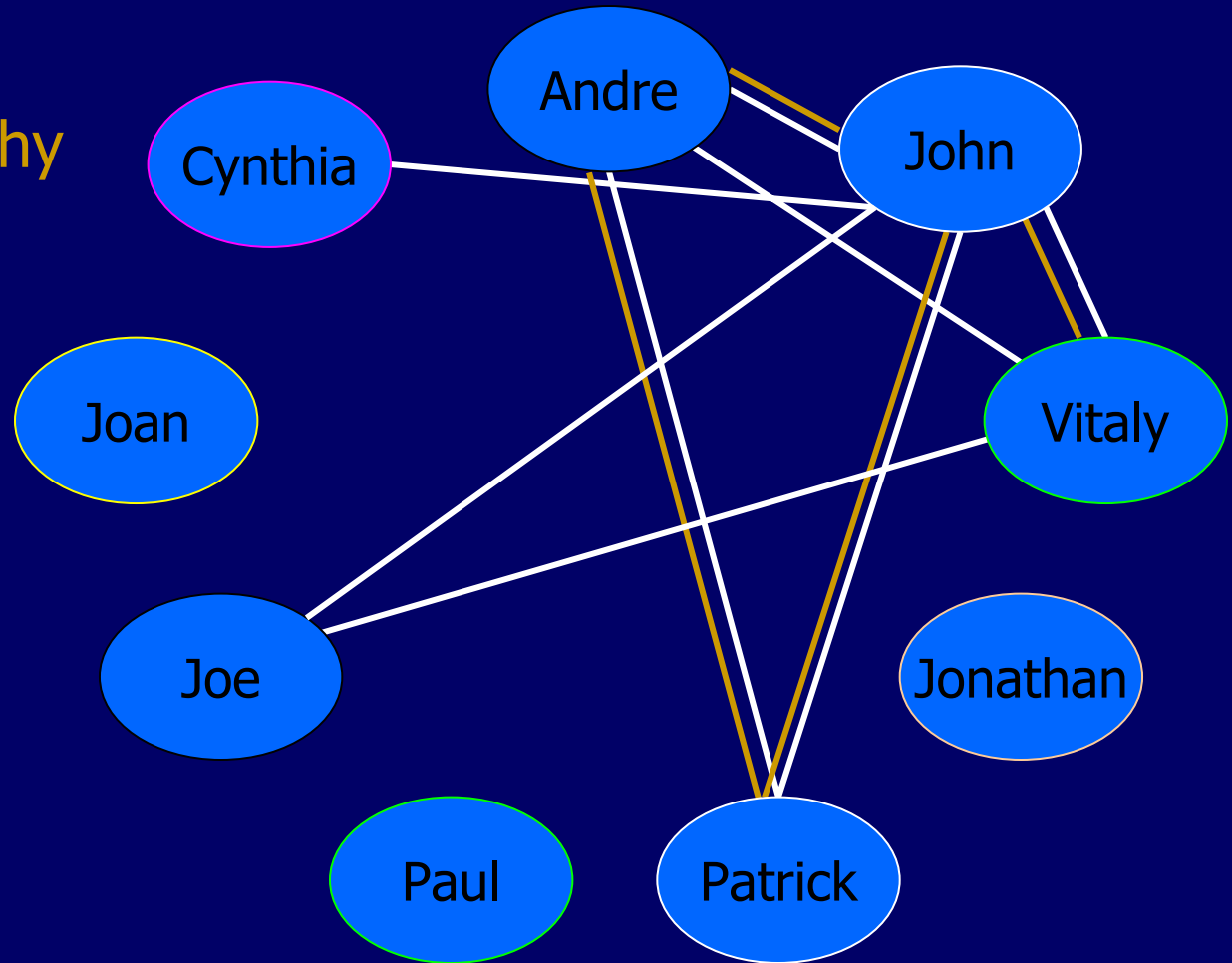
Spyce Interaction Graph

- Protocol Analysis



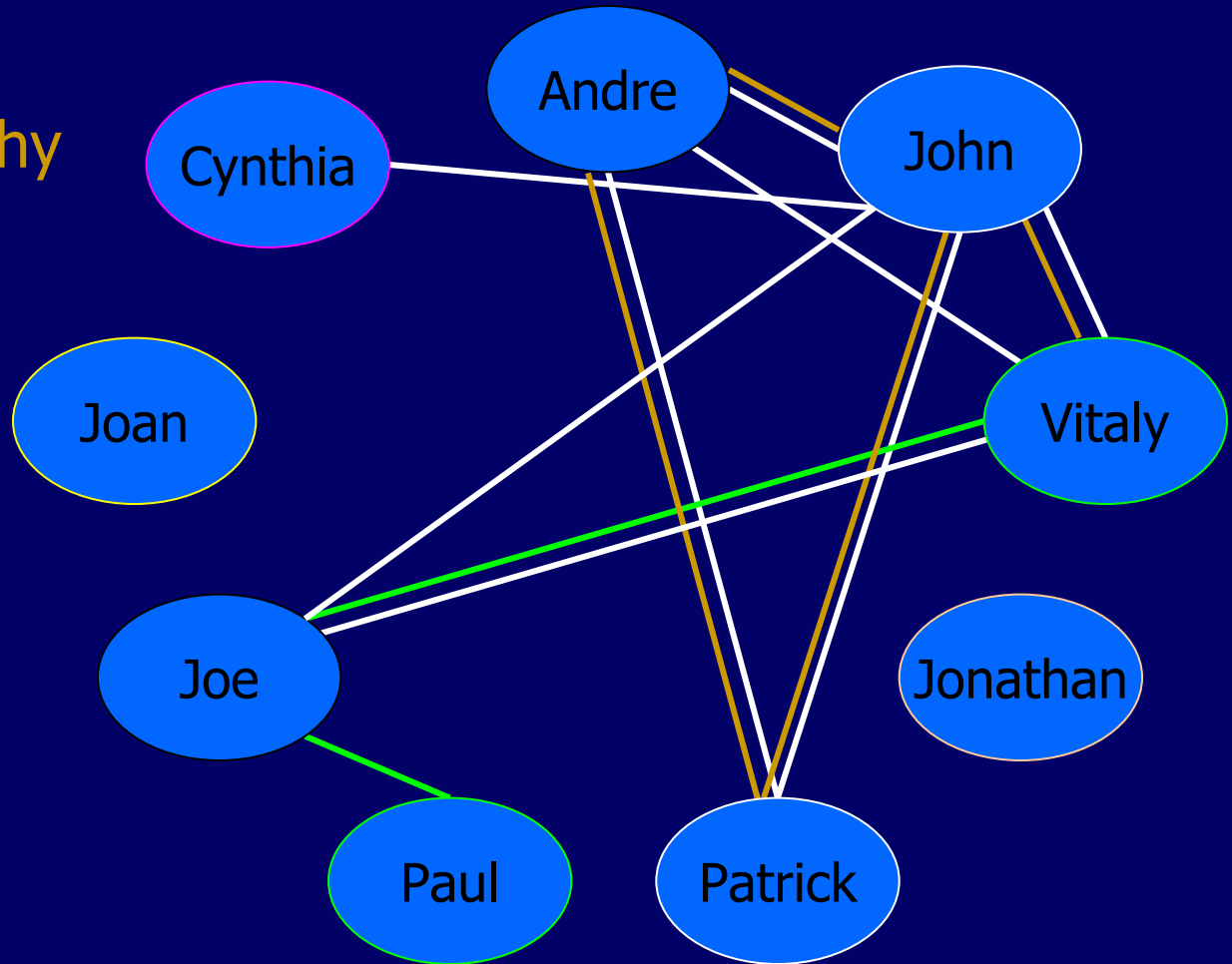
Spyce Interaction Graph

- Protocol Analysis
- Formal Methods
for Cryptography



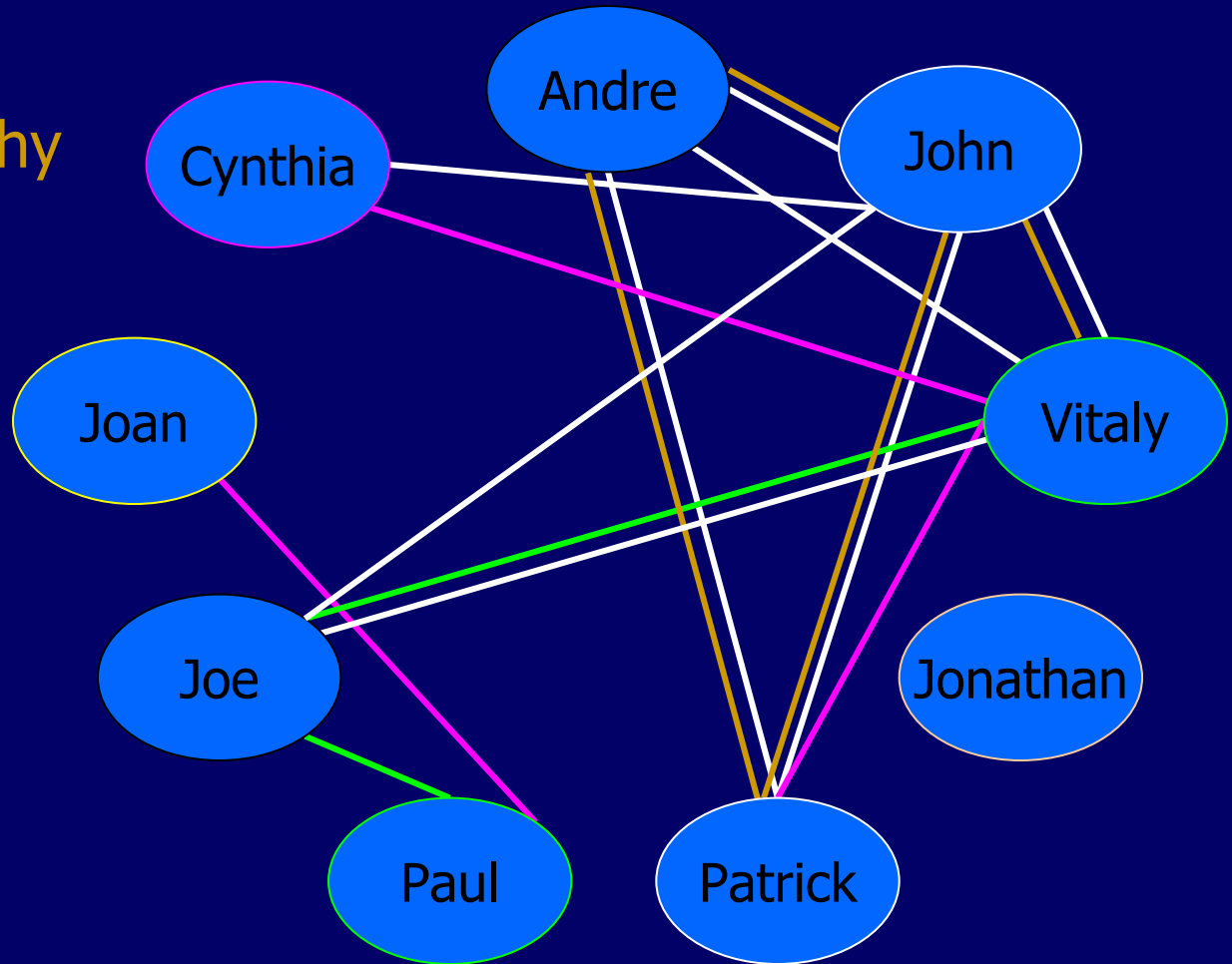
Spyce Interaction Graph

- Protocol Analysis
- Formal Methods
for Cryptography
- Anonymity



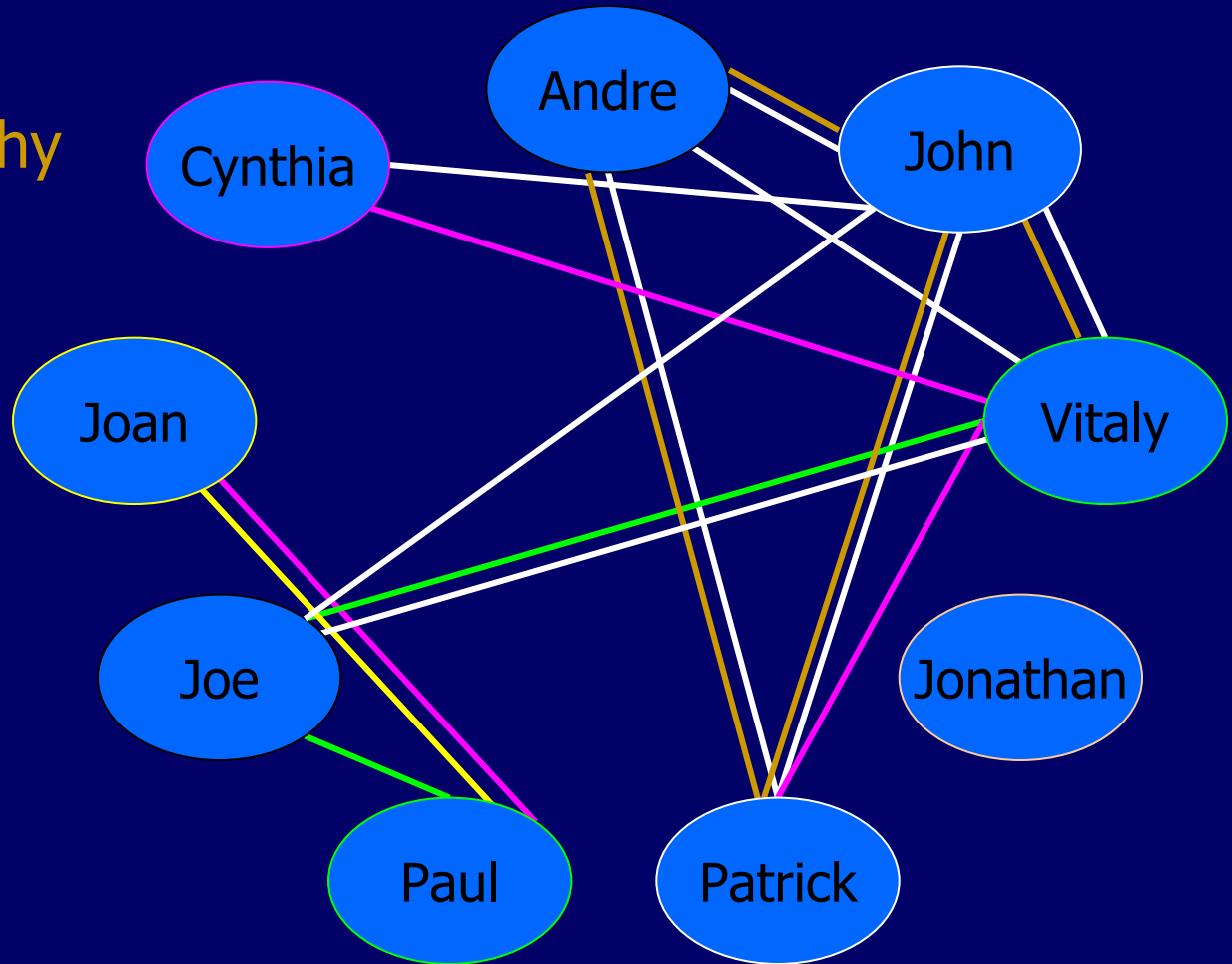
Spyce Interaction Graph

- Protocol Analysis
- Formal Methods
for Cryptography
- Anonymity
- Privacy



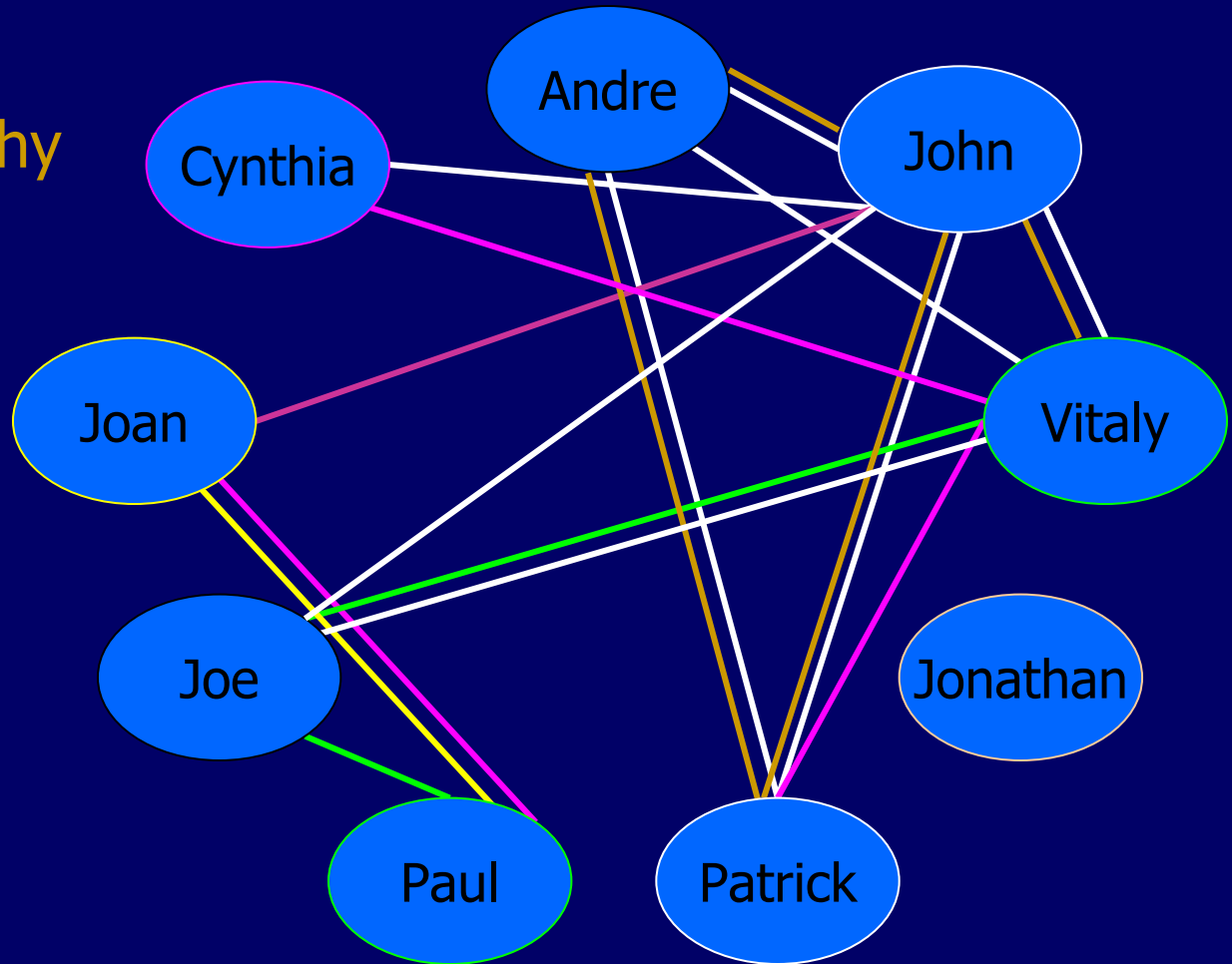
Spyce Interaction Graph

- Protocol Analysis
- Formal Methods
for Cryptography
- Anonymity
- Privacy
- Algorithmic
Mech Design



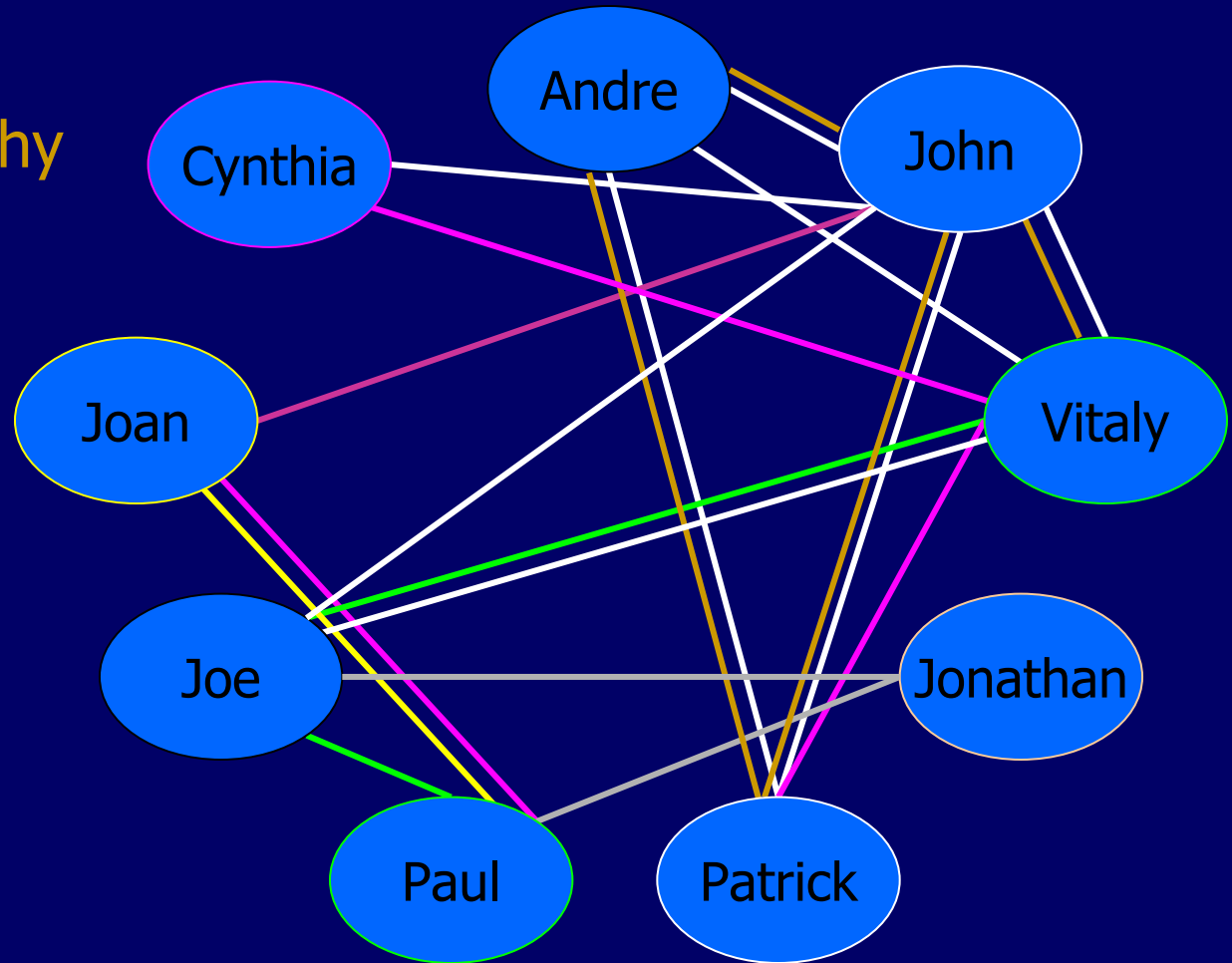
Spyce Interaction Graph

- Protocol Analysis
- Formal Methods
for Cryptography
- Anonymity
- Privacy
- Algorithmic
Mech Design
- Authorization



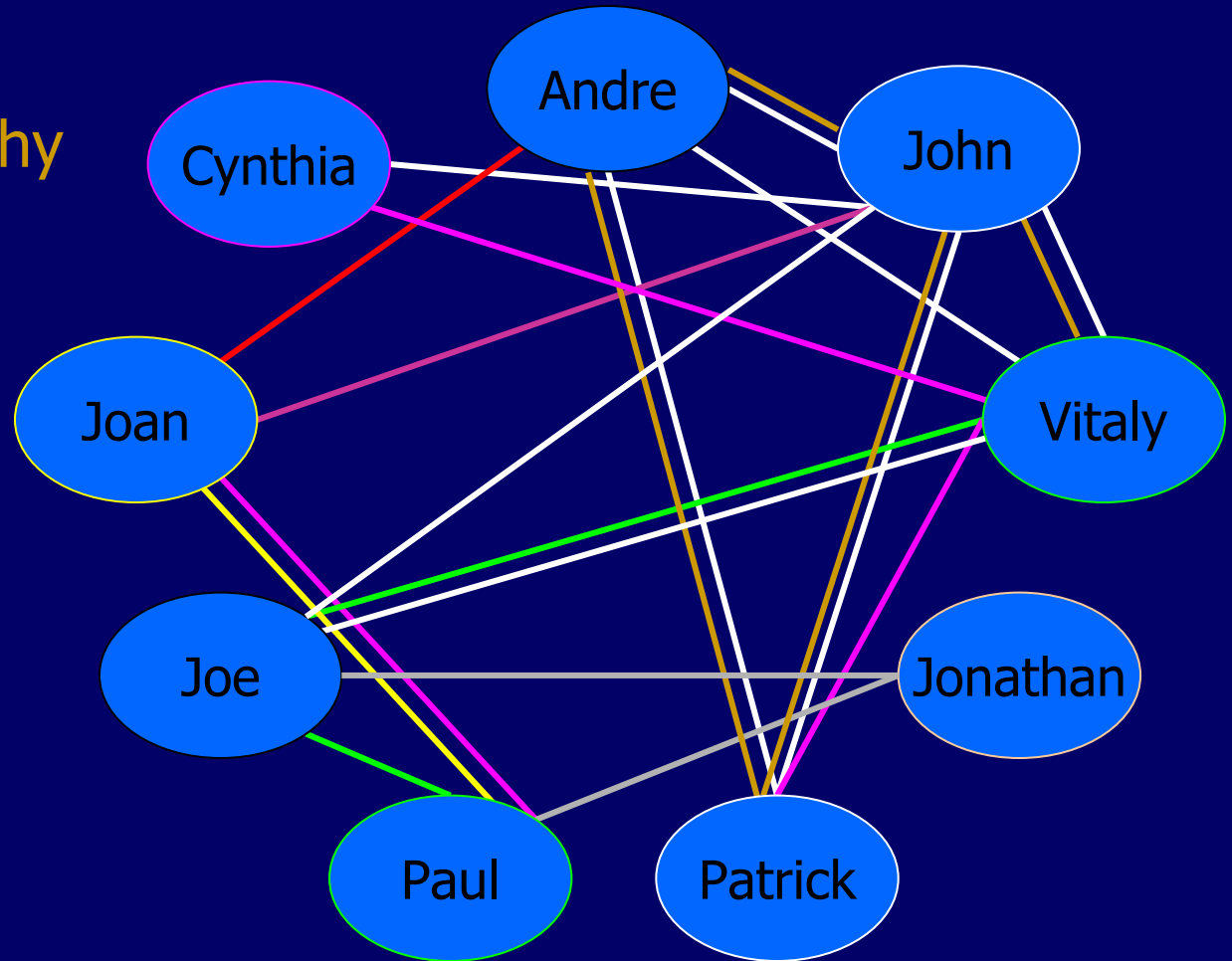
Spyce Interaction Graph

- Protocol Analysis
- Formal Methods
for Cryptography
- Anonymity
- Privacy
- Algorithmic
Mech Design
- Authorization
- Decision Theory



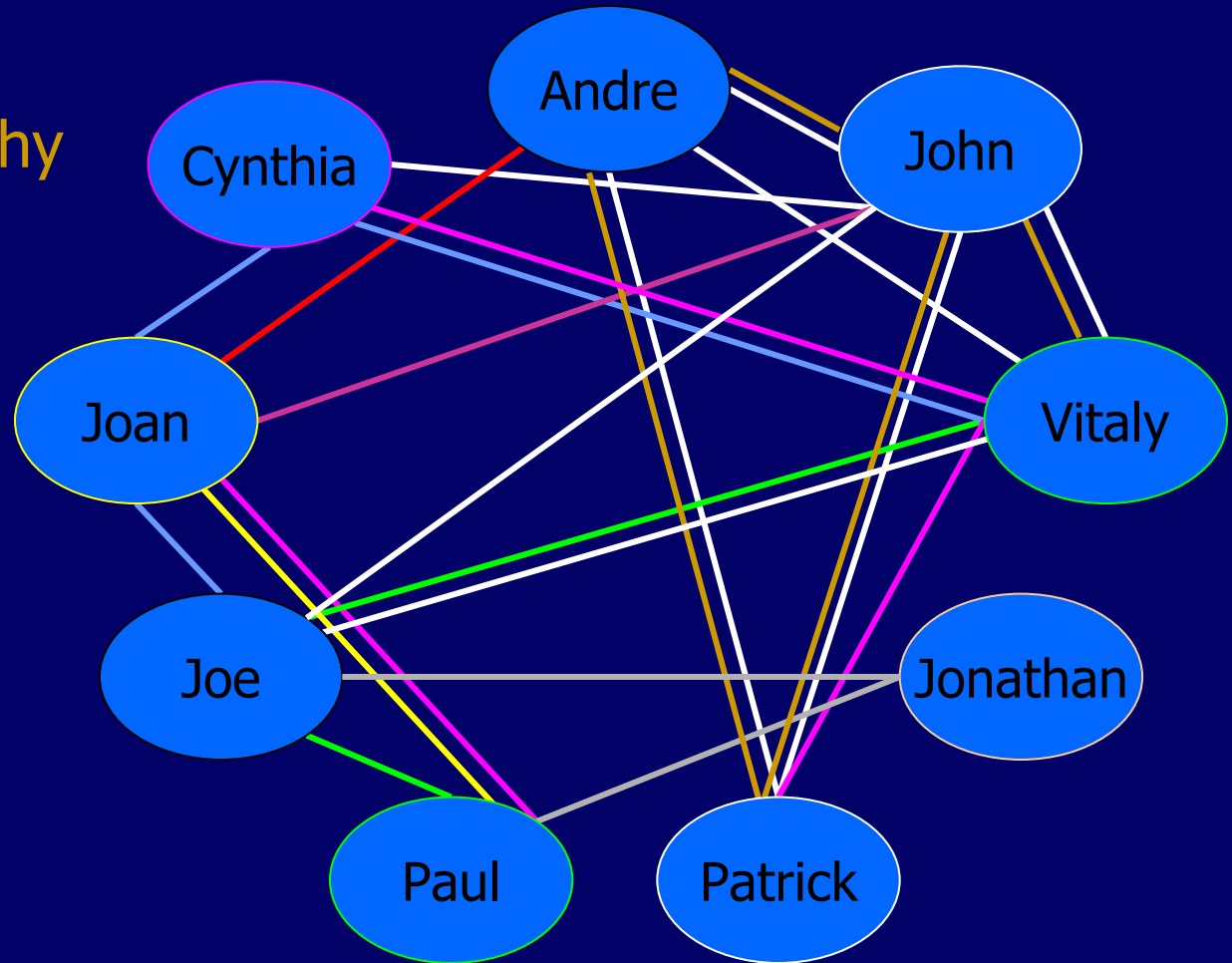
Spyce Interaction Graph

- Protocol Analysis
- Formal Methods
for Cryptography
- Anonymity
- Privacy
- Algorithmic
Mech Design
- Authorization
- Decision Theory
- BGP



Spyce Interaction Graph

- Protocol Analysis
- Formal Methods
for Cryptography
- Anonymity
- Privacy
- Algorithmic
Mech Design
- Authorization
- Decision Theory
- BGP
- Digital Rights



Presentations today

- Feigenbaum *Market-based computation*
- Halpern *Communication and security protocols*
- Mitchell *Authorization mechanisms*
- Everyone *Poster Session*
- Lincoln *Privacy and anonymity*
- Smith *Networking*

Summary of Project: Multidisciplinary Research

- Software Quality and Infrastructure Protection for Diffuse Computing
- Algorithms to model diffuse computing and achieve scaleable high assurance
- Multi-institution experimental platform





FY2001 ONR CIP/SW URI



Software Quality and Infrastructure Protection for Diffuse Computing



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

STARTED IN MAY 2001

Diffuse Computing

- Diffuse computing is an emerging paradigm in which computational tasks are performed by aggregated computational services, distributed over a network.
- This paradigm, developing rapidly as a result of commercial computing markets, the now-recognized potential of peer-to-peer systems, and the need for distributed network-centric systems, raises challenges for system design, software production, and the development of mechanisms ensuring stable equilibria of diffuse systems.

Project Meetings

- URI kickoff meeting July 7 '01 (DC)
- Video conference Oct 8 '01 (Penn-SRI)
- First board meeting Nov 5 '01 (Penn)
- Group meeting Dec '01 (Calistoga, CA)
 - *Workshop on Economics and Information Security*
May '02 (Berkeley)
- Second board meeting June 21 '02 (Penn)
- Third board meeting Sep 30 '02 (Cape May)
- Group meeting Dec '02 (St. John, USVI)
- Continuing visits among sites, teleconferences
- Fourth board meeting Mar 31 '03 (Penn)

Diffuse Computing

