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

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

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

- Bjorn Knutsson, Penn
- Ninghui Li, Stanford (till Summer 2003)
- Michael Elkin, Yale (since Fall 2003)

- 16 Ph.D. Students
Project Vision: 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).
Secure services through heterogeneous overlay networks
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
Critical Infrastructure Protection

Many critical infrastructures, national and DoD-specific, are decentralized systems.

Computer networks have, in addition, become critical infrastructures.

Research Question: How to build large-scale, adaptive and robust next-gen. systems?

Critical Infrastructure Protection

- Many critical infrastructures, national and DoD-specific, are decentralized
- Data sharing essential for operation, but data compromise can be catastrophic
- Research Question: How to share data safely, using policies that are easy to formulate, enforce, maintain
- Approach: diffuse trust management
Assuring Software Quality

- Loose coupling leads to natural “sandboxing”
- High decentralization means high autonomy
- New way of writing software
- Pieces of system more robust in face of:
  - Failures / Disruptions
  - Partial Information
  - Software Engineering for highly decentralized, policy-controlled and networked world
Assuring Software Quality

- Technology applicable to managing process interaction
  - Process A delegates rights to process B
    - For limited purpose, limited time, limited locations
  - Fine-grained control of process actions
  - Works for *diffuse systems* that escape normal controls imposed by localized OSs

- Diffuse principle of least privilege
FY2001 CIP/SW URI BAA Topic #9:  
ASSURING SOFTWARE QUALITY  
Research Concentration Areas

How to reason about the assurance and quality in highly distributed systems?

- Reason about uncertainty in all contexts of distributed agent-mediated information systems
- Develop co-algebraic foundations for expressing the semantics of concurrency
- Express knowledge of interactions building upon a game theoretic semantics  
  - Vitaly Shmatikov poster
- Investigate configuration management in terms of distributed services, policy coordination  
  - John Mitchell talk
- Develop highly dependable self-configuring operating services for net-centric, resource-aware mobile computing  
  - Jonathan Smith talk, Bjorn Knutsson demo
- Investigate real-time/fault tolerant middleware and component integration in hybrid control  
  - Kostas Anagnostakis demo
- Develop collaborative problem solving theories that emphasize computing as mediation
- Express the meaning of software artifacts, interfaces, aspects, and operating environments
- Extract and synthesize computational knowledge about algorithms and protocols  
  - Joe Halpern talk
- Investigate the economics of software technology diffusion into commercial infrastructures  
  - Joan Feigenbaum talk
DoD Impact

- Joint Vision 2010 / Joint Vision 2020 of “Network Centric” operations
- DoD requirements addressed by project:
  - Agile and rapidly evolving
    - CING/Active Networks
    - Proxies
  - Secure and Robust
    - *AME A.N. approach
  - Scalable
    - Massively populated persistent worlds concepts
DoD Impact

- Dynamic coalitions
  - Partial sharing based on partial trust
- Joint Vision 2010 / Joint Vision 2020 of “Network Centric” operations
  - Can use policy to push data, overcome network bandwidth limitations
  - Right data to right place at right time
Project Metrics

• Criteria by which success of the project should be measured
  – Good research
  – Strong collaboration
  – Educational impact
  – Relevance to CIP/SW, DoD, and Industry
  – Transition Potential and Anticipated Impact
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 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

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

- Protocol Analysis
- Formal Methods for Cryptography
- Anonymity
- Privacy
- Algorithmic Mech Design
- Authorization
- Decision Theory
- Networking
- Digital Rights
Spyce Interaction Graph
Number of publications

- Protocol Analysis 14
- Formal Methods for Cryptography 6
- Anonymity 5
- Privacy 4
- Algorithmic Mech Design 6
- Authorization 7
- Decision Theory 4
- Networking 19
- Digital Rights 3
Sample 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 V analysis [Penn-NRL]
- **Logic for reasoning about policies** [Cornell-Stanford]
- **SPAM reduction algorithms** [Microsoft-Stanford]
- **Privacy in databases** [SRI-Microsoft]
- **Anonymity and information hiding** [Cornell-NRL]
- **Content transcoding for heterogeneous clients** [Penn]
Impact on Education

- This grant has enhanced the ability to educate and train students in science and engineering and perform CIP/SW-relevant research.
- **10** Spyce-related courses taught, including:
  - Economics and Computation
  - Computer and Network Security
  - E-Commerce Doing Business on the Internet
  - The Internet: Co-Evolution of Technology and Society
  - Sensitive Information in the Wired World
  - Decision Theory
  - Reasoning About Knowledge
  - Mathematical Foundations of Computer Security
- **Active seminars on computer and information security**
- **New undergraduate major and minor program at Penn in Logic, Information, and Computation including SPYCE-related courses**
- **16 Students in Degree Program Supported by Project (25% or more FTE)**
  - Penn 4, Cornell 4, Stanford 5, Yale 3
Project Statistics

1. Transition to Tenure-Track Faculty: Ninghui Li
   - NYU PhD (advisor: Feigenbaum) → Stanford postdoc → Purdue faculty

5. PhDs Awarded:
   - R. Sami: Yale → MIT
   - R. Chadha: Penn → U. Sussex
   - A. Jaggard: Penn → Tulane
   - N. Durgin: Stanford → Sandia Livermore Labs
     - Computer Security Group
   - A. Chander: Stanford → NTT DoCoMo US Labs
     - Proof-carrying-code-based security applications for 4G wireless product
     - Direct application to commercial wireless security

Sometimes the most effective way to transfer information and technology is to transition people
Project Endorsements

- Microsoft: Cynthia Dwork
- Intel: Tim Griffin
- IBM: Ran Canetti
- HP: Tomas Sander
Spyce Interaction Graph

- Protocol Analysis
- Formal Methods for Cryptography
- Anonymity
- Privacy
- Algorithmic Mechan Design
- Authorization
- Decision Theory
- Networking
- Digital Rights
Plans for Option

● In the first two years
  - Thoroughly familiarized ourselves with each others areas
  - Achieved accumulated knowledge of SPYCE

● In option
  - Will take this to the next level
  - Apply this collective knowledge in the following areas
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
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
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.
Plans for Option (4)

- **Kostas Anagnostakis Ph.D research:**
  - **ITRUST** - Incentive TRust for Ultrascale Services and Techniques [P,Y,Columbia]
    - Ultrascale diffuse approach to distributed anomaly (e.g., worm) detection
    - Ultrascale resource (e.g., file) sharing
- **Bjorn Knutsson Post-Doctoral research:**
  - Experimental Validation of Massively Populated Persistent Worlds MPPW on PlanetLab (& new anomaly detection algorithms)
  - **DHARMA** - Distributed Home Agent for Reliable Mobile Access (diffuse approach for mobility; advanced adaptive configuration management)
- **Continuing evolution of SPYCELab**
Plans for Option (5)

- Applications and Transitions
  - Work with XrML developers on language and algorithm
  - IBM Privacy Project
    ▪ Use RT algorithms for EPAL, P3P applications
  - Pursue commercial and DOD applications
  - Application to large policy sets (social security policies)
- Generalize results: $RT \Rightarrow \text{Datalog} \Rightarrow \text{PFOL}$
- Improve implementation: $RT_0 \Rightarrow \text{Datalog} \Rightarrow \text{PFOL}$
- Policy development environment and tools
  - User interface, XML-format, interoperability
  - Testing methodology, analysis methods
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
**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
- SPAM reduction algorithms
- Privacy in databases
- Content transcoding for heterogeneous clients
- Formal methods for cryptography
- Logics for reasoning about policies
**Project Statistics**

- **Special Awards or Honors**
  - Joan Feigenbaum
    - ACM Fellow, Member NAS Computer Science and Telecommunications Board
  - Joe Halpern
    - ACM Fellow, AAAI Fellow
  - Pat Lincoln
    - Member Defense Science Board task force on Science and Technology
  - John Mitchell
    - Invited Speaker USENIX '02
  - Andre Scedrov
    - Program Co-Chair, International Symposium on Software Security, Tokyo, Japan, 2002
  - Jonathan Smith
    - Olga and Alberico Pompa Professorship of Engineering and Applied Science, University of Pennsylvania
  - Cynthia Dwork
    - SIAM/SIGEST Best Paper 2003
  - Paul Syverson
    - Member Board of Directors, International Financial Cryptography Association
Project Statistics

- 68 Publications
  - 6 refereed journal articles
  - 60 refereed conference proceedings
  - 2 book chapters
- 5 Prototypes
- 1 Transition to Industry
  - IBM Privacy Research Institute
- Related Sponsored Research includes:
  - DARPA POSSE, Penn
  - DARPA Coalitions, Stanford and SRI
  - NSF ITR PORTIA, Stanford and Yale
  - DARPA/AFOSR MURI APPeers, UIUC and Stanford
  - NSF CCR-TC GRIDLOCK, Columbia and Penn and Yale
  - NSF ITR Networks of strategic agents, Cornell
Project Interactions

- **Industry**
  - Microsoft: Cynthia Dwork
  - Intel: Tim Griffin
  - IBM Privacy Research Institute

- **Labs**
  - NRL: Paul Syverson
  - SRI: Vitaly Shmatikov
  - Kestrel: Dusko Pavlovic

- **Other universities**
  - UC Berkeley, Columbia, UIUC
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