Main Theme: Diffuse Computing

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

SPYCE Objective:
Scalable Distributed Assurance

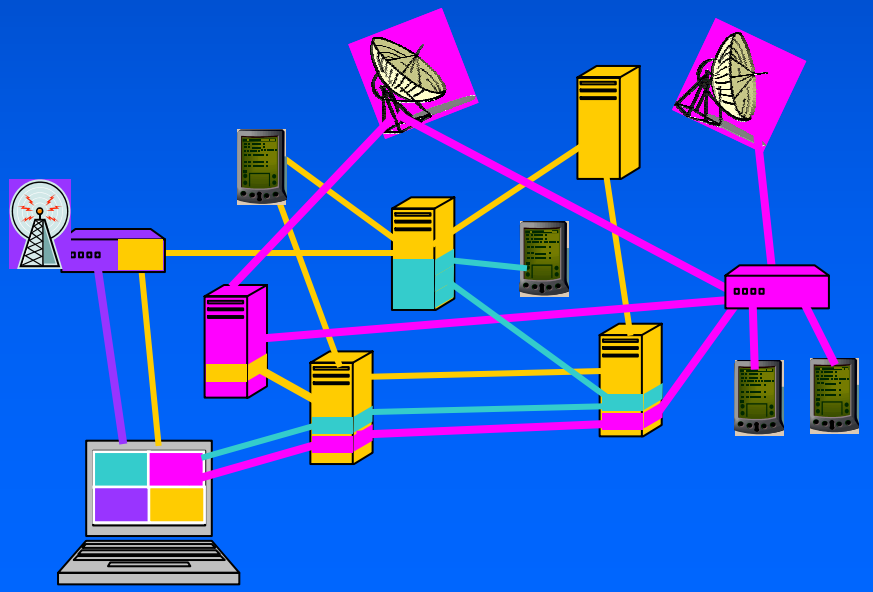
Develop fundamental understanding, models, algorithms, and network testbed, in order to reduce cost, improve performance, and provide higher reliability for networked operations across untrusted networks.

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
- Networks have, in addition, become critical infrastructures
- Research Question: How to build large-scale, adaptive and robust next-gen. systems?
- Approach: New Diffuse Computing concept
  - results with *extremely* loosely-coupled modules

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

- 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

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

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

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 SPYCE topics

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 $\Rightarrow$ Datalog $\Rightarrow$ PFOL
- Improve implementation: $RT_0 \Rightarrow$ Datalog $\Rightarrow$ PFOL
- Policy development environment and tools
  - User interface, XML-format, interoperability
  - Testing methodology, analysis methods

Spectrum of Research

- Span the spectrum from theoretical computer science to practical experiments and systems research
- Body of deep results enables understanding complex phenomena of diffuse computing
  - 66 peer-reviewed publications
- SPYCELab experimental platform instruments visits to the diffuse computing future
  - 5 prototypes
- Practically-motivated basic research
  - Organized, energetic, efficient

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