Critical Infrastructure Protection and High Confidence Adaptive Software
University Research Initiative Program

Welcome to the “3rd Year” Option Component Review for
The University of Pennsylvania Research Project
Software Quality and Infrastructure Protection for Diffuse Computing

Washington, D.C.
27 Oct 2003
Workings of the URI Program

- This Multi-disciplinary URI Program (MURI) started back in ‘96
- MURI Awards are for 3 years with a 2 year option component
- Average award is between $800K and $1,000K per year
- Process for Determining Whether to Exercise the Option in Yr 3
  - Outside Panel of Experts in-person review the project as a whole
  - Written recommendation of findings by the Panel chair person (in 1-2 weeks)
  - Recommendation to ONR Manager and ONR Corporate Programs Division
  - Senior Decision Makers do their thing
  - February notification of results by ONR Corporate Programs Division

Basic Questions for the Panel:
- Is the project doing excellent 6.1 basic research?
- Is this the right direction to continue pursuing?
The Pre-Decisional Review Criteria

1. Scientific and technical research accomplishments in basic science and/or engineering research
2. Capability for the Research Team to work effectively
3. Productivity of the Project
4. Student Participation
5. Relevance and usefulness of contributions of the research to CIP/SW BAA, DoD, and Industry
6. Transition Potential and Anticipated Impact of the Proposed Option Research

Rating Scale for Each Criteria: Excellent (21-25), Good (16-20), Satisfactory (11-15), Weak (6-10), Poor (1-5)

At the end of the day your hand-written completed form is to be turned in to the Panel chair.
Software Quality and Infrastructure Protection for Diffuse Computing

The Panel and Advisors

Panel Chair Person: Sylvan Pinsky (NSA)

Panel

- Behzad Kamgar-Parsi (ONR311)
- Ramesh Bharadwaj (NRL)
- Carl Landwehr (NSF/CISE)
- Steve King (OSD)
- Gary Koob (DARPA)
- Wendy Martinez (ONR311)
- Ralph Wachter (ONR311)

Government Advisors

- Cathy Meadows (NRL5543)
- Paul Syverson (NRL5543)
- Tim McChesney (NRL5540)
- Julia Abrahams (ONR/363)
Today’s Agenda

7:45 - 8:30  Breakfast
8:30 - 9:00  Ralph Wachter, ONR: Welcoming & Opening Remarks
9:00 - 9:50  Andre Scedrov, UPenn: Overview of the SPYCE Project
9:50 - 10:15  Joan Feigenbaum, Yale: Incentives, Privacy and Anonymity
10:15 - 10:40  Joseph Halpern, Cornell: Protocol Design and Analysis
10:40 - 10:55  Break
10:55 - 11:20  Jonathan Smith, UPenn: Networking
11:45 - 12:00  Andre Scedrov, UPenn: Concluding Presentation
12:00 - 12:05  Sylvan Pinsky, NSA: Closing Remarks
12:05 - 01:30  Working Lunch
1:30 - 4:30  Closed Session of Review Panel
The CIP/SW Program Overview
Mission

... to ensure that the warfighters today and tomorrow have superior and affordable technology to support their missions, and to give them revolutionary war-winning capabilities.

Office of the Deputy Under Secretary of Defense for Science and Technology

Defense Science and Technology
Critical National Infrastructures

Infrastructures which are so vital that their incapacitation or destruction would have a debilitating impact on defense or economic security.

October 1997
The University Research Initiative (URI) Program

**U.S. university efforts to accelerate 6.1 basic research in CIP/SW and to hasten the transition of research findings to practical application**

**6.1 Basic Research is:**
- Research directed toward increasing knowledge in science
  
  *Article 35.001 of the Federal Acquisition Regulations*

- Research that analyzes properties, structures, and relationships toward formulating and testing hypotheses, theories, or laws
  
  *National Science Foundation*
Critical Infrastructure Protection and High Confidence, Adaptable Software URI Program

13 Basic Research topics in FY01

- Understanding Mobile Code
- Network Surveillance
- Information Assurance for Wireless Networks
- CIP Performance Assessment
- Protecting COTS
- Dynamic Network Management
- Understanding and Countering Deception

- Novel Network Architectures
- Protecting Infrastructures
- Assured Development Technology for High-Confidence Embedded Systems
- Heterogeneous Distributed Computing Systems
- Digital Libraries for Constructive

• Assuring Software Quality
Motivation
software for critical applications requires greater assurance at all stages of its life….. and, the essence of quality is the assurance that software performs usefully and efficiently as expected in all contexts

Objective
understand, express, and effectively reason about software and quality

Footnote: This topic was just about the “catch-all” topic in the BAA. We received proposals that covered the gamut of software quality. Two (2) awards were made including the UPenn Project.
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
• Investigate configuration management in terms of distributed services, policy coordination
• Develop highly dependable self-configuring operating services for net-centric, resource-aware mobile computing
• Investigate real-time/fault tolerant middleware and component integration in hybrid control
• 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
• Investigate the economics of software technology diffusion into commercial infrastructures

Note: Submitted proposals addressed only subsets of these very tersely worded areas
OSD/ONR FY01 CIP/SW MURI
Software Quality and Infrastructure Protection for Diffuse Computing

Research Team
- Stanford University
- UPennsylvania
- Yale University
- Cornell University
- Experiment

Principal Investigator
- Andre Scedrov
- U.Pennsylvania

MURI Objective
Algorithms to model diffuse computing and achieve scalable high assurance

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

Motivation
Smart devices diffuse into the environment....
Room ‘40s
Desktop ‘80s
Wearable ‘90s
Pervasive ‘00s

...with control and assurance
Let me introduce the **SPYCE** Principal Investigator