



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

SPYCE Objective: Scaleable High Assurance



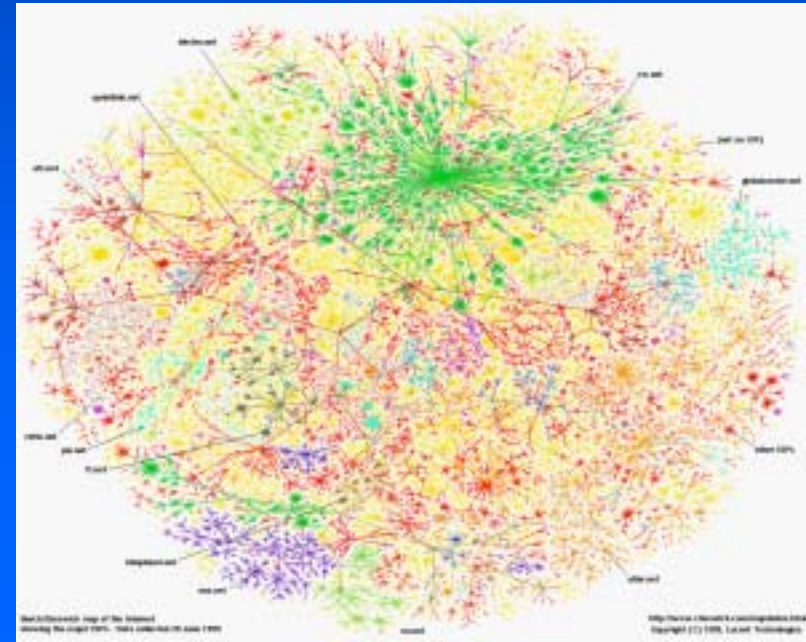
Develop fundamental understanding, models, algorithms, and network testbed, in order to reduce cost, improve performance, and provide higher reliability for networked operations across untrusted networks.

Efficient Diffuse Multimedia Networking

Incentive Compatibility

Authorization Schemes

Secure Data Storage and Communication



"Big Question"

- What is the right model for agent (in the general sense) behavior with respect to information, services, and security on the internet?

World contains:

- ☐ Rational agents who seek to maximize individual utility function
 - ☐ Byzantine agents. Traditional security model with malicious agents.
 - ☐ System components subject to failure
- Design systems to work with heterogeneous population of agents

SPYCE working groups include

- Interdomain routing and the Border Gateway Protocol (BGP)
 - Feigenbaum, Ramachandran : Yale
 - Mitchell, Teague : Stanford
 - Scedrov, Jaggard : Penn
- Networking
 - Smith, Knutsson, Anagnostakis, Scedrov : Penn
 - Mitchell : Stanford
 - Ryger : Yale
- Anonymity, privacy, and authorization
 - Syverson : NRL
 - Lincoln, Shmatikov : SRI
 - Dwork : Microsoft Research

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 Nov 30-Dec 2 '01 (Calistoga)
- Weekly teleconferences in working groups
 - *Workshop on Economics and Information Security*
May '02 (Berkeley)
- Second board meeting June 21 '02 (Penn)
- Continuing visits among sites, teleconferences
- Third board meeting Sep 30 '02 (Cape May)
- Planned group meeting Dec '02 (St. John,USVI)

Sample presented this time

- Privacy and anonymity

- Chair: Paul Syverson

- Networking Demo

- Bjorn Knutsson

- Interdomain routing

- Chair: Joan Feigenbaum

- Security

- Chair: Joe Halpern

*Monday
morning*

*Tuesday
morning*

Privacy and Anonymity

To: Instructors and TA's

Re: Posting of grades

If you want to post grades on the web you should use the grade posting program or use a program that posts only the student's grade and the mean, max, etc. using the student's ID number. You cannot use Social Security Numbers. You should not post grades in a list by student ID because this does invade the students' privacy (e.g. if two or three grades are very low it may become known who the students are.) Also, from my own experience it is bad policy to post grades in such a fashion because students will use it against you in arguing for a grade change (i.e. students on the borderline will know it and argue accordingly.)

If people can figure out a student's grade from what is posted we are in **LEGAL TROUBLE.**

Privacy and anonymity

- C. Dwork and M. Naor
 - SPAM reduction
- V. Shmatikov and D. Hughes
 - Specification framework for security properties that involve information hiding
- P. Golle, M. Jakobsson, and P. Syverson
 - Universal re-encryption
 - Receiver communicates with sender anonymously

Networking Demo

- B. Knutsson

- Distributed, loosely coupled heterogeneous devices
- Problems of scale
- Diffuse applications impose new networking requirements
- Diffuse computing techniques may solve network problems
- Example: Images to small devices

Example: Images to small devices

Broadband



Example: Images to small devices

Broadband

Dial-up



Scaled

Preserved

Scaled

Preserved

Image
Removed

Example: Images to small devices

Broadband

Dial-up

Wireless/PDA



Swapped

Converted to Text

Interdomain routing

- J. Feigenbaum: Overview of interdomain routing and the Border Gateway Protocol

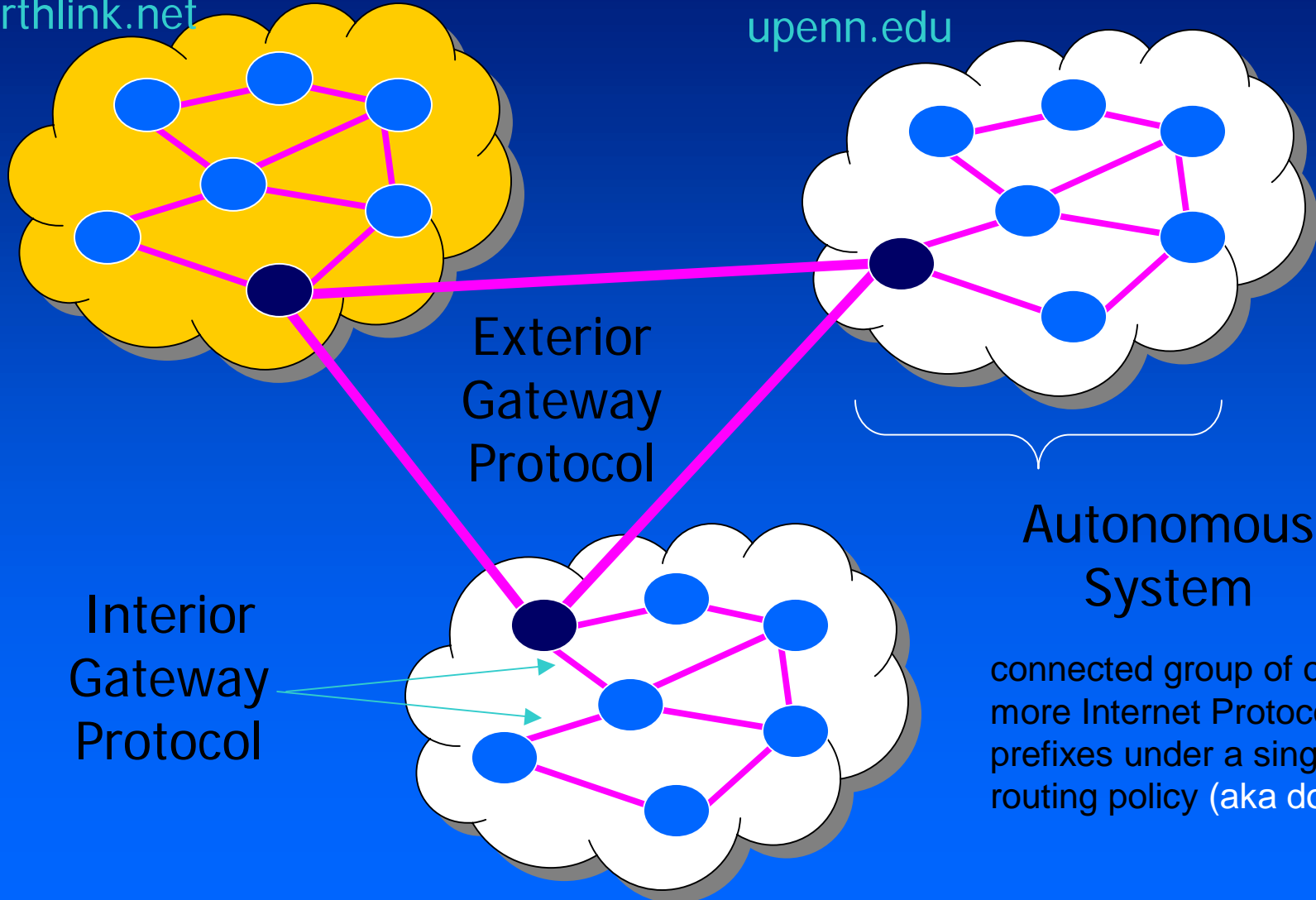
New collaboration:

- T. Griffin (AT&T), A. Jaggard (Penn), and V. Ramachandran (Yale)
 - theoretical framework for the interdomain routing
 - characterization of interdomain routing involving local policies
 - local conditions that guarantee stable routes

Interdomain Routing

earthlink.net

upenn.edu



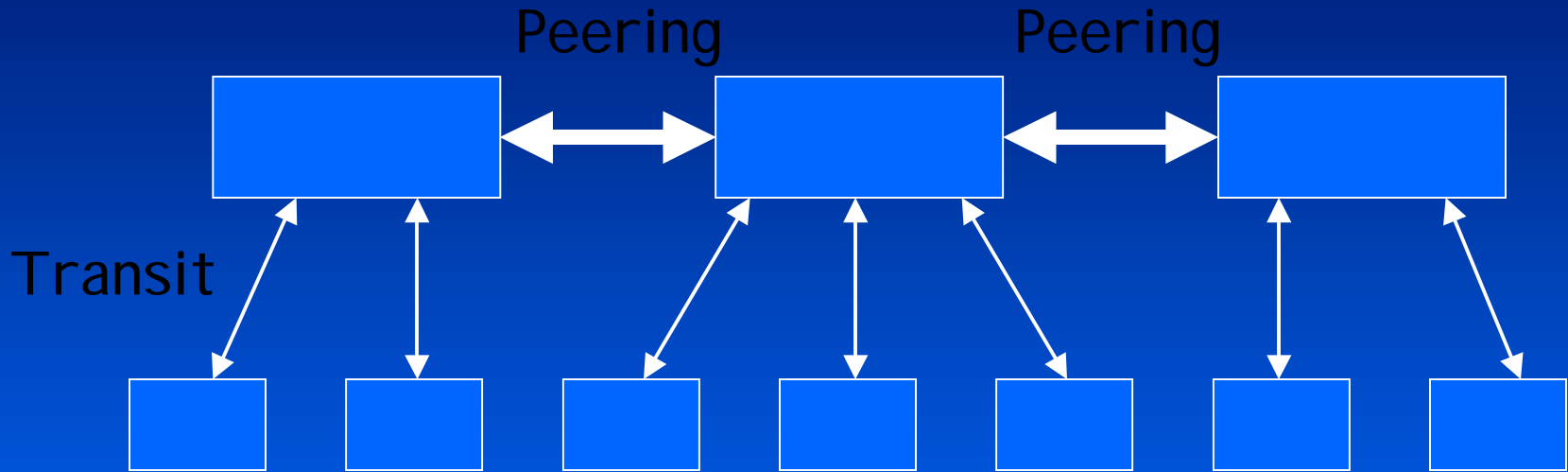
Exterior
Gateway
Protocol

Autonomous
System

Interior
Gateway
Protocol

connected group of one or
more Internet Protocol
prefixes under a single
routing policy (aka domain)

Transit and Peering



Transit: ISP sells access

Peering: reciprocal connectivity

BGP protocol: routing announcements for both

Security analysis

- R. Pucella, V. Weissman

- A logic for reasoning about licenses
- Small specifications can be analyzed efficiently

- I. Cervesato, F. Butler, A. Jaggard, and A. Scedrov

- Scaling up formal methods to real-world authentication protocols
- Recent results on Kerberos version 5

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



Software Quality and Infrastructure Protection for Diffuse Computing



URI, 2001

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

September, 2002



Smart devices diffuse into the environment....



Desktop '80s



Wearable '90s



Pervasive '00s

Room '40s

... with control and assurance

URI 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

Scientific/technical approach

Computing and networking elements diffusing into the environment need:

- Local incentive-compatibility in global distributed computing
- Scaleable authorization mechanisms
- Assured communication
- Secure data storage and retrieval
- Experimental evidence

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