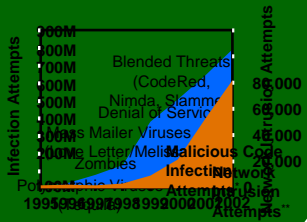


# Trustworthy Infrastructure, Mechanisms, and Experimentation for Diffuse Computing (TIME DC)

U Penn, Stanford, Cornell, Yale

MURI, June 2004 **Email:** [scedrov@cis.upenn.edu](mailto:scedrov@cis.upenn.edu) **WWW:** <http://www.cis.upenn.edu/~timedc> October 22, 2004



Exponentially Increasing Threats



Protected Information Assets

## TIME DC Objective

**Effective, timely, and confidential sharing of security-related information**

**Enable information network defenders to collaboratively share information better than attackers, without compromising sensitive information**

## Information Security Alert Sharing

### DoD Capabilities

- **DoD network administrators will be able to share Intrusion Detection, Firewall, Anti-Virus, and other information security alert information across domains.**
- **More effective and rapid response to widespread threats such as email viruses, internet worms, and concerted intrusive attacks on DoD networks.**

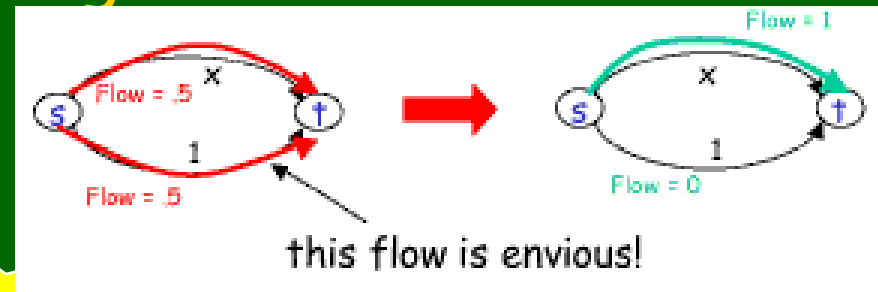
### Scientific/Technical Approaches

- **Cryptographic cleansing techniques**
- **Secure multiparty computation**
- **Incentive-compatible communication protocols**
- **Language-enforced security methodology with policy and programming language aspects**
- **Scalable response to malicious code outbreaks**
- **Leveraging current information security infrastructure, and state-of-the-art antivirus and antiworm research**

# TIME DC New Investigator Tim Roughgarden



- **ACM Thesis Award** (Honorable Mention)
  - Selfish Routing, Cornell University
- Stanford faculty, starting Fall 2004



## ★ Compare two routing situations

- Every router is selfish
- Every router contributes to global welfare

## ★ Amazing result

- If we double the hardware, selfish is as good as optimal

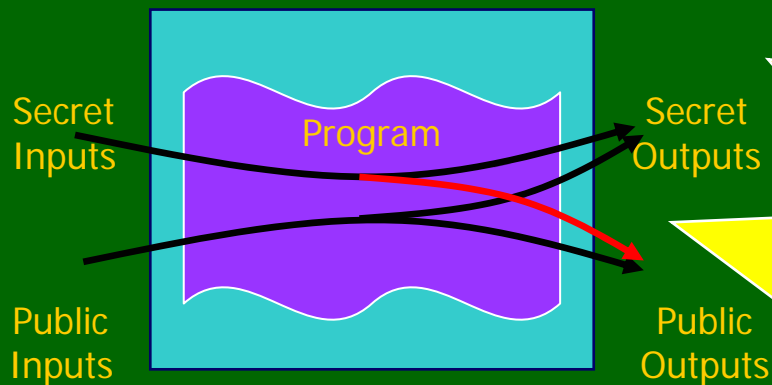
# Roughgarden publications

- Selfish Routing and the Price of Anarchy
  - ACM Award Thesis, published MIT Press
- Sample Recent Papers
  - A Stronger Bound on Braess's Paradox, SODA '04.
  - The Maximum Latency of Selfish Routing, SODA '04.
  - Approximation Via Cost Sharing: A Simple Approximation Algorithm for the Multicommodity Rent-or-Buy Problem, FOCS '03.
  - Pricing Networks with Selfish Routing, Economics of P2P Networks '03.
  - Pricing Network Edges for Heterogeneous Selfish Users, STOC '03.
  - Simpler and Better Approximation Algorithms for Network Design, STOC '03.

# TIME DC New Investigator Steve Zdancewic



- University of Pennsylvania
  - Ph.D. Cornell University 2002
- NSF CAREER Award
  - Language-based Distributed System Security



**Theorem:** A program certified by the compiler will not transmit any secret inputs over a public channel.

# Zdancewic publications

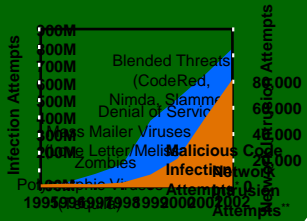
## ● Selected Recent Papers

- Advanced Control Flow in Java Card Programming  
LCTES 2004
- Translating Dependency into Parametricity  
ICFP 2004
- Enforcing Robust Declassification  
CSFW 2004
- Run-time Principals in Information-flow Type Systems  
IEEE Security & Privacy 2004
- Observational Determinism for Concurrent Program Security  
CSFW 2003
- Building Secure Distributed Systems Using Replication and Partitioning  
IEEE Security & Privacy 2003

# Trustworthy Infrastructure, Mechanisms, and Experimentation for Diffuse Computing (TIME DC)

U Penn, Stanford, Cornell, Yale

MURI, June 2004 **Email:** [scedrov@cis.upenn.edu](mailto:scedrov@cis.upenn.edu) **WWW:** <http://www.cis.upenn.edu/~timedc> October 22, 2004



Exponentially Increasing Threats



Protected Information Assets

## TIME DC Objective

**Effective, timely, and confidential sharing of security-related information**

**Enable information network defenders to collaboratively share information better than attackers, without compromising sensitive information**

## Information Security Alert Sharing

### DoD Capabilities

- **DoD network administrators will be able to share Intrusion Detection, Firewall, Anti-Virus, and other information security alert information across domains.**
- **More effective and rapid response to widespread threats such as email viruses, internet worms, and concerted intrusive attacks on DoD networks.**

### Scientific/Technical Approaches

- **Cryptographic cleansing techniques**
- **Secure multiparty computation**
- **Incentive-compatible communication protocols**
- **Language-enforced security methodology with policy and programming language aspects**
- **Scalable response to malicious code outbreaks**
- **Leveraging current information security infrastructure, and state-of-the-art antivirus and antiworm research**

# Today

- Rational Secret Sharing and Multiparty Computation
  - Joe Halpern, Cornell
- Privacy-Preserving Sharing and Correlation of Security Alerts
  - Pat Lincoln, SRI
- Security-Oriented Languages
  - Steve Zdancewic, Penn