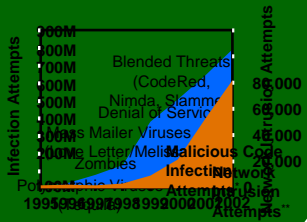


Trustworthy Infrastructure, Mechanisms, and Experimentation for Diffuse Computing (TIME DC)

U Penn, Stanford, Cornell, Yale

MURI, June 2004 **Email:** scedrov@cis.upenn.edu **WWW:** <http://www.cis.upenn.edu/~timedc> August 17, 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.**

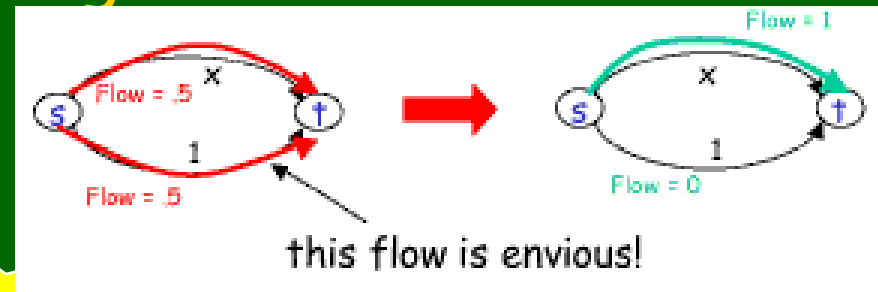
Scientific/Technical Approaches

- **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

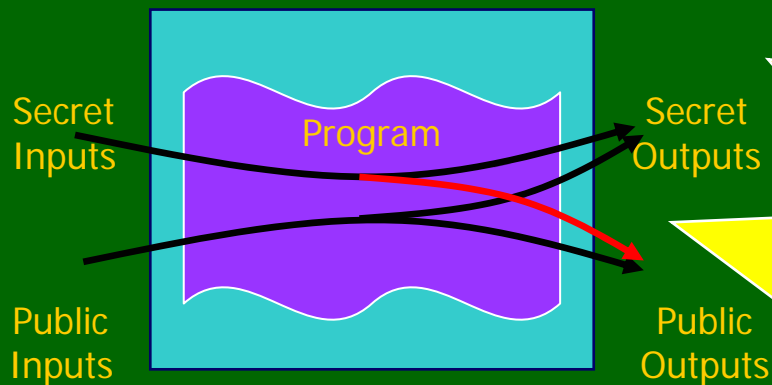
Roughgarden publications

- 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

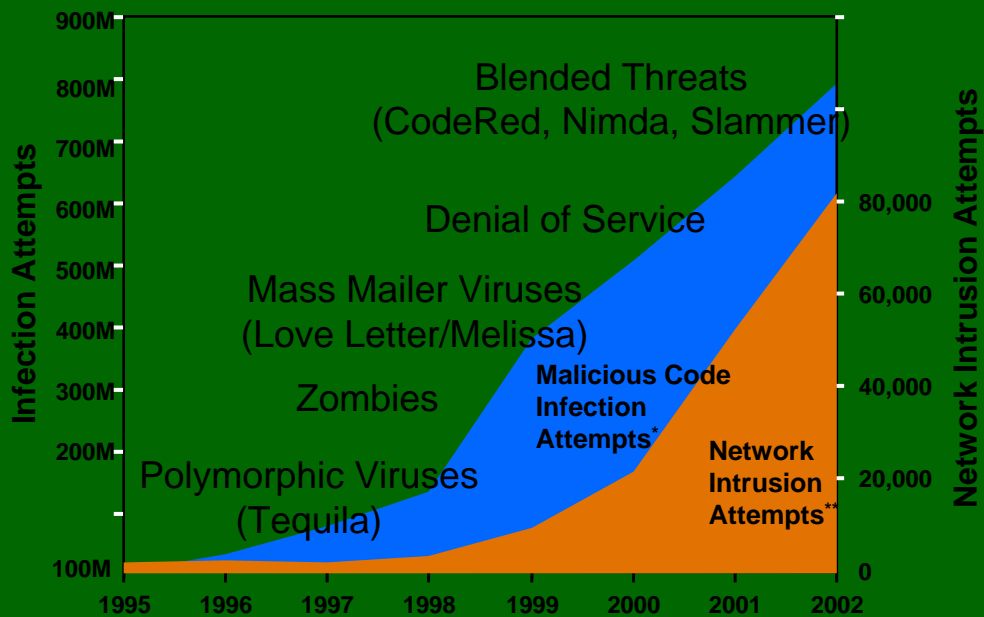
● Selected Recent Papers

- 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

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**

Network Defense Requires Data



- Scale and sophistication of attacks are growing rapidly
 - Faster propagation
 - Human response not scaling up
- Need tools for rapid detection of Internet-scale network threats
 - Tool development requires actual network data
- A public source of historical security alert data would be a useful resource

Information Asymmetry is a Problem

- **Attackers think in the large, share information**
 - Information about vulnerabilities and attack tools is widely disseminated through IRC, web sites, P2P, etc.
 - Network effects work to attackers' advantage
- **Defenders think in the small, don't collaborate**
 - Conventional defense tools are intended to defend a single organization, not the entire network
 - People are paranoid about sharing security alerts
 - Alerts leak tons of information about network topology, defense capabilities and configurations, sensitive data contained in packet fragments and network traces
 - Precious little real-time information

Solving the Asymmetry Conundrum

- Few incentives for sharing sensitive data
 - For the network to become more secure, members must reveal some information about their security postures
- If it were easier and safer to share, more good guys would share more data more often
 - We don't need everybody to share to get a useful picture of Internet-scale trends and phenomena!
- Need better technology for controlled sharing
 - Better source of data for research purposes
 - Sacrifice some functionality to guarantee that contributors' sensitive data remains private

Our Vision: No-Trust Alert Sharing

[Lincoln-Porrás-Shmatikov]

- **Develop a network of public alert repositories**
 - Collect security alerts for **unrestricted access and analysis** by third parties
 - Develop tools for contributors to sanitize sensitive fields and associations contained in their alerts
 - Alert contributors do not need to trust the repository
 - Repository has no legal responsibility for contributed alerts
 - Can even hide alert origin from the repository
 - There is a tradeoff between privacy and functionality
- **Short-term goal: collect data for research**
- **Longer-term goal: Internet-scale threat detection**

Requirements and Tradeoffs

privacy

Hide sensitive data and suppress sensitive associations between IP addresses, ports, sensor IDs, ...

tradeoffs

Low overhead;
no complicated crypto

functionality

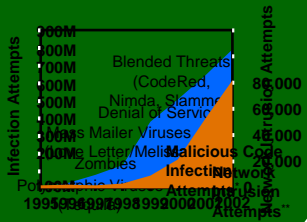
Support coarse-grained analysis:
event trends, identification of
common attack sources, ...

efficiency

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

U Penn, Stanford, Cornell, Yale

MURI, June 2004 **Email:** scedrov@cis.upenn.edu **WWW:** <http://www.cis.upenn.edu/~timedc> August 17, 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**