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

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
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.
SPYCE → TIME DC Thread

- Sample thread: protocols research
  - Discoveries
  - Products
  - Transitions
Discoveries: New Methodologies

- Combining formal methods and computational cryptography for high-fidelity security analysis
  - Mitchell, Scedrov, Shmatikov, and students (Bana, Datta, Derek, Ramanathan, and Teague)

- Compositional protocol logic for incremental derivation and protocol synthesis
  - Mitchell, Pavlovic and students (Datta, Derek)
Protocol analysis spectrum

Sophistication of attacks

Low

High

Protocol complexity

Low

High

Combining formal methods and cryptography

Incremental derivation

Hand proofs

Poly-time calculus

Computational Protocol C. logic

Multiset rewriting

Spi-calculus

Athena

Paulson

NPL

BAN logic

Model checking

FDR

Mur$\phi$

Holy Grail

Protocol C. logic

Computational

Protocol C. logic

Multiset rewriting

Spi-calculus

Athena

Paulson

NPL

BAN logic

Model checking

FDR

Mur$\phi$
Products

- Security analysis and improvements of network security protocols
  - IEEE 802.11i wireless LAN
    [Mitchell and He]
  - Kerberos 5 and KINK (Kerberized Internet Negotiation of Keys)
    [Scedrov, Cervesato, Jaggard, Walstad]
Transitions

- Activity on standards setting bodies
  - IEEE 802.11i wireless LAN
    Attack! Fix adopted by IEEE Working Group
    [Mitchell and He]
  - Kerberos 5 and KINK (Kerberized Internet Negotiation of Keys)
    Discussions with IETF Area Directors and Working Group
    [Scedrov, Cervesato, Jaggard, Walstad]
Recent TIME DC Theses

● Stanford
  - Changhua He  Ph.D.
    (supervisor: John Mitchell, 802.11i presentation this afternoon)
  - Mukund Sundararajan  M.S.
    (jointly supervised by Tim Roughgarden and John Mitchell)
This afternoon

● Security Analysis and Improvements for IEEE 802.11i
  - John Mitchell, Stanford

● Decision Theory and Heterogeneous Agents
  - Joe Halpern, Cornell

● Downgrading Policies and Relaxed Noninterference
  - Peng Li and Steve Zdancewic, Penn