TRUST: Team for Research in Ubiquitous Secure Technology

A Collaborative Approach to Advancing Cyber Security Research and Development

Larry Rohrbough
Executive Director, TRUST
University of California, Berkeley

June 12, 2008
Science & Technology Center (STC) established in 1987 to fund important basic research and educational activities and to encourage technology transfer and innovative approaches to interdisciplinary problems.

Per NSF, the STC Program:

- “Enables innovative research and education projects of national importance…”
- “Requires a Center mode of support to achieve the goals…”
- “Conducts world-class research in partnerships…”
- “Creates new and meaningful knowledge of significant benefit to society…”

Core Funding (FY2005 - 2015)

$40M ($4M/Year, 10 Years)
TRUST MISSION
S&T that will radically transform the ability of organizations to design, build, and operate trustworthy information systems for critical infrastructure.

Center Approach
- Address fundamental cyber security and critical infrastructure protection problems of national importance
- Tackle “Grand Challenge” scale integrative research projects
- Expand industry collaboration, research project sponsorship, and technology transition

Supporting Personnel
- Undergraduates: 7
- Graduates: 97
- Post Docs: 6
- Research Scientists: 4
- Faculty: 51
- Staff/Other: 10
- TOTAL: 175

Affiliated Institutions
- Computer Engineering
- Computer Science
- Economics
- Electrical Engineering
- Law
- Public Policy
- Social Science
To achieve the TRUST mission and objectives, Center activities are focused in three tightly integrated areas...

**Education**
Curriculum reform and teaching the next generation of computer/social scientists and engineers

- TRUST Academy Online
- Textbooks
- SECuRT
- WISE

**Research**
Interdisciplinary projects combine fundamental science and applied research to deliver breakthrough advances in trustworthy systems

- Electronic Medical Records
- End User Security
- Network Defenses
- Policy
- Secure Sensor Networks
- Trustworthy Systems

**Knowledge Transfer**
Dissemination and transition of Center research results and collaboration opportunities with external partners

- BT
- CISCO
- HP
- Intel
- Microsoft
- Sun
- United Technologies
- TELECOM
- AFRL
- iCAST

International Collaboration for Advancing Security Technology
TRUST Organization (cont.)

Education – Diverse Set of Education and Outreach Activities

**OBJECTIVE**
Conduct Education and Outreach activities focused on integrating trustworthy technologies, systems, and policy into learning opportunities for a broad range of community participants

**TEACHING**

- **New Courses**
  - Software Security Technologies
  - Networking Security
  - The Digital World and Society
  - Security Specialization
  - IT in Society
  - Data Privacy in Biomedicine

- **Textbooks**

- **Professional Development**

**DISSEMINATION**

- **TRUST Academy Online**
  - TRUST Seminar Series
  - ... https://tao.truststc.org

**OUTREACH**

- **Alliance for Minority Participation**
  - HBCU Summer Partnership
  - Information Systems
  - Carnegie Mellon

- **SUPER-B-IT**

- **Women’s Institute in Summer Enrichment**

Team for Research in Ubiquitous Secure Technology, L. Rohrbough

TRUST Organization (cont.)

Research – Center Research Portfolio, Year 3 (2007-2008)

OBJECTIVE

Combine fundamental science with a broader multidisciplinary focus on economic, social, and legal considerations to deliver breakthrough advances in the development and use of and trustworthy systems.

Electronic Medical Records
Security and privacy issues associated with the rapidly increasing use of electronic media for the archival and access of patient medical records.

End User Security
Web authentication, end-user privacy, next-generation browser security, malware detection, and improved system forensic techniques to combat online attacks.

Network Defenses
Application defenses for network-level intrusions and attacks including viruses, worms, spyware.

Policy
Policies, procedures, and legal aspects that enhance system security, privacy, and trustworthiness.

Secure Sensor Networks
Secure embedded sensor networks for large-scale applications (e.g., SCADA, energy, healthcare) and associated control systems.

Trustworthy Systems
Techniques that secure hardware, improve software robustness, and increase the survivability of critical systems.
TRUST Organization (cont.)

Knowledge Transfer – External Partners/Sponsors Support Technology Transition

**OBJECTIVE**
Transition security, privacy, and infrastructure protection research to *industry, government agencies, and international partners* to promote the use and evolution of ubiquitous secure technology

**Industry Partners**

- BT
- Intel
- Sun Microsystems
- Cisco
- Microsoft
- Symantec
- Esher
- Oak Ridge National Laboratory
- Telekom
- IBM
- Qualcomm

**Government Sponsors**

- NSF
- Department of Defense
- AFRL

**International Collaborators**

- iCAST
- TWIST
- Industrial Technology Research Institute
TRUST Collaboration Highlights

Industry – Adoption of Center Research Results by Industry Partners

Use and evolution of ubiquitous secure technology via transition of TRUST research to commercial companies and other industrial partners

**Electronic Medical Records**
- Model-Based Trustworthy Health Information Systems (MOTHIS)
- Technologists, medical experts, legal policy experts
- Model-based methods for HIS (architectures, privacy and security policies, security mechanisms, web authentication, and human factors)

**End User Security**
- Identity theft (anti-phishing) and authentication/verification web browser tools
- Malware detectors (Minesweeper, Panorama) and botnet zombie detection system (BotSwat)
- Computer forensics tools and testbed

**Secure Sensor Networks**
- CareNet – System for assisted living in the home
TRUST Collaboration Highlights

Government – Transfer of Center Research Findings and Results

Advising and shaping policy and legislation at the Federal, State, and Local government level (US) as well as working with international governments

**US Federal/State/Local**
- Privacy implications of residential demand-response systems
- Federal Trade Commission identity management best practices
- Data Breach Notification laws expanded from California (SB 1386) to 39+ states
- Privacy and security vulnerabilities of RFID and end-user comprehension of real and perceived risks
- Federal (DHHS) and regional (RHIOs) health agency initiatives for specifying and enforcing privacy policies

**UK House of Lords**
- Science and Technology Committee visit to UC Berkeley March 2007
- TRUST briefings on *Network Monitoring, Data Breach Notification, Telecommunications Legal Issues, and Industry/Academic Partnerships*
TRUST Collaboration Highlights (cont.)

Security technology to enhance national defense, improve infrastructure networks and systems, and address the growing threat of cyber attacks

**Air Force Office of Scientific Research / Research Laboratory**
- Time-criticality/quality of service with COTS and web services
- Legacy application / system-of-system information assurance
- Secure and dynamic service discovery and mediation
- Secure the Global Information Grid (GIG) and improve security for Network Centric Enterprise Systems (NCES)

**Scientific Advisory Boards / Strategic Studies Groups**
- Implications of Cyber Warfare (2007)
- Cyberspace and Maritime Operations in 2030 (2007)
- Defending and Operating in a Contested Cyber Domain (2008)

**Defense Advanced Research Projects Agency**
- Large-scale cyber network testing & evaluation
- Possibly build on TRUST cyber testbed (DETER) architecture
- Leverage experimentation experience of DETER team
TRUST Collaboration Highlights (cont.)

International – U.S / Taiwan Partnership for Advancing Security Technology

OBJECTIVE:
Joint U.S./Taiwan R&D of security technologies for cryptography, wireless networking, network security, multimedia security, and information security management.

PARTNERSHIP:
- 3-year collaboration agreement (2006-2009)
- U.S. $2M per year investment by Taiwanese government
- Joint research and publications
- Prototyping and proof-of-concept for Taiwanese and U.S. industry
- Student/faculty exchange program

RESEARCH:
- Security for Pervasive Computing
- Trusted Computing Technologies
- Wireless Security
- Sensor Network Security
- Intrusion Detection and Monitoring

Team for Research in Ubiquitous Secure Technology, L. Rohrbough

Conclusion

- TRUST is addressing fundamental cyber security and critical infrastructure protection problems of national importance.

- TRUST is tackling problems via a three-pronged approach.

- TRUST is working to make a true Academic/Government/Industry model successful.

- TRUST legacy will be the results of large, multi-disciplinary, integrative research projects ("Grand Challenges").

**Future Activities to Broaden TRUST Impact**

- Expand partnerships in industry, the government, and the research community.
- Increase international collaboration presence and influence.
Thank You!

Questions???

TRUST Contact Information

Larry Rohrbough
Executive Director
TRUST Science and Technology Center
University of California, Berkeley
510-643-3032 (Work)
703-328-5221 (Mobile)
larryr@eecs.berkeley.edu

www.truststc.org