NSF

TRUST
Team for Research in Ubiquitous Secure Technology

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

CyberSecurity
Knowledge Transfer Network

Berkeley University of California
Carnegie Mellon
Cornell University
Mills College
San José State University
Smith College
Stanford University
Vanderbilt University

TRUST Background

National Science Foundation STC Program

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**.

National Science Foundation
Office of Integrative Activities
(OIA)

Core Funding
(FY2005 - 2015)

$40M ($4M/Year, 10 Years)

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*…"

TRUST Background (cont.)

TRUST National Science Foundation Science & Technology Center (STC)

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

Berkeley
UNIVERSITY OF CALIFORNIA

Carnegie Mellon

Cornell University

MILLS
COLLEGE

San José State
UNIVERSITY

SMITH COLLEGE

STANFORD
UNIVERSITY

VANDERBILT
UNIVERSITY

Supporting Disciplines

- Computer Engineering
- Computer Science
- Economics
- Electrical Engineering
- Law
- Public Policy
- Social Science

TRUST Organization

TRUST
Team for Research in Ubiquitous Secure Technology

Center Structure – Core Research with Integrated Education and Knowledge Transfer

To achieve the TRUST mission and objectives, Center activities are focused in three tightly integrated areas…

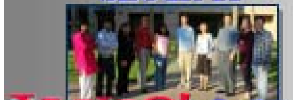
Education

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

TRUST Academy Online

Textbooks

SECuR-IT



YAHOO! Sun RAPPORT ebY

WISE

SUPERB-IT

TRUST Seminar

Research

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

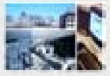
Electronic Medical Records

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

TELECOM United Technologies

AFRL

iCAST
International Collaboration for Advancing Security Technology

TRUST Organization (cont.)

Education – Diverse Set of Education and Outreach Activities

Education

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

Research

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

Knowledge Transfer

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

iCAST
International Collaboration for Advancing Security Technology

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

Computer Security in the 21st Century
Information Security
Reliable Distributed Systems

…

Professional Development

ebay RAPPORT Sun hp Salesforce YAHOO!

DISSEMINATION

TRUST Academy Online

https://tao.truststc.org

TRUST Seminar Series

OUTREACH

San José State University

Alliance for Minority Participation

HBCU Summer Partnership

H&SS Information Systems Carnegie Mellon

SUPERB-IT

Center for Underrepresented Engineering Students
University of California, Berkeley

Women's Institute in Summer Enrichment

TRUST Organization (cont.)

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

Education

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

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

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

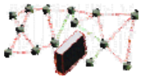
Web authentication, end-user privacy, next-generation browser security, malware detection, and improved system forensic techniques to combat online attacks

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

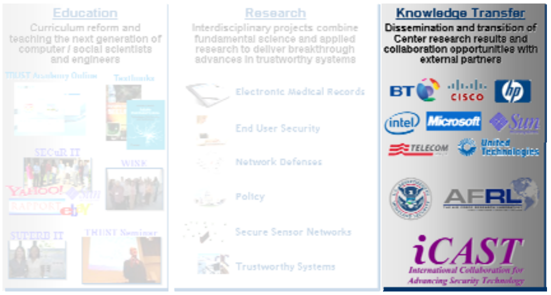
Trustworthy Systems

Techniques that secure hardware, improve software robustness, and increase the survivability of critical systems

TRUST Organization (cont.)

TRUST
Team for Research in Ubiquitous Secure Technology

Knowledge Transfer – External Partners/Sponsors Support Technology Transition



Education

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

TRUST Academy Online · Textbooks · SECuR IT · WISE · SUPERB IT · TRUST Seminar

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

iCAST
International Collaboration for Advancing Security Technology

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.
- ESCHER Research Institute
- Oak Ridge National Laboratory
- Telecom Italia
- hp
- Pirelli
- United Technologies
- IBM
- Qualcomm

Government Sponsors

- NSF
- Air Force Office of Scientific Research
- U.S. Department of Homeland Security
- AFRL

International Collaborators

iCAST

- TWISC – Taiwan Information Security Center
- 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)

My Health at Vanderbilt

Nashville 2007
Workshop on Model-Based Trustworthy Health Information Systems
In conjunction with MODELS 2007 September 30, 2007

Microsoft HealthVault

Google Health BETA

dossia

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

RSA SECURITY

Google Code

Adobe

vmware

Sun microsystems Java

Secure Sensor Networks

- CareNet – System for assisted living in the home

Intel

TELECOM ITALIA

Vanderbilt Home Care
Hearts and Minds at Home

TRUST Collaboration Highlights

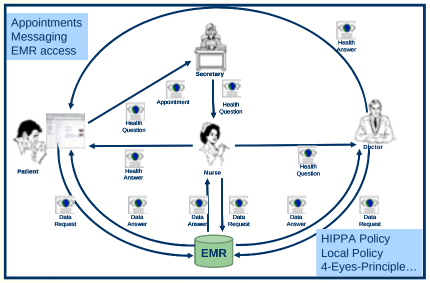
Government – Transfer of Center Research Findings and Results

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

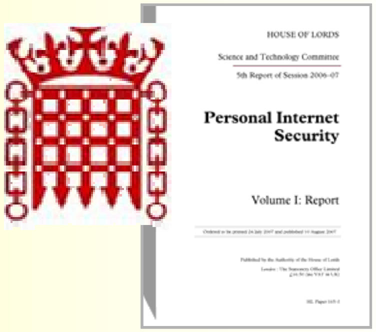
- Privacy implications of residential demand-response systems
- Federal Trade Commission identity management best practices
- Data Breach Notification laws expanded from California (SB 1386) to 39+ states
- Privacy and security vulnerabilities of RFID and end-user comprehension of real and perceived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

The Enhanced Driver License and ID Card
UNITED STATES OF AMERICA • PASSPORT CARD •
UNITED STATES DEPARTMENT OF STATE



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*



HOUSE OF LORDS

Science and Technology Committee

5th Report of Session 2006–07

Personal Internet Security

Volume I: Report

Ordered to be printed 24 July 2007 and published 10 August 2007

Published by the Authority of the House of Lords

London : The Stationery Office Limited
[illegible]

HL Paper 165-I

TRUST Collaboration Highlights (cont.)

Military – U.S. Department of Defense Research

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 testebed (DETER) architecture
- Leverage experimentation experience of DETER team

TRUST Collaboration Highlights (cont.)

TRUST
Team for Research in Ubiquitous Secure Technology

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

NTUST

iCAST
International Collaboration for Advancing Security Technology

TWISC
Taiwan Information Security Center

Industrial Technology Research Institute

Berkeley
UNIVERSITY OF CALIFORNIA

Carnegie Mellon

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***

Conclusion

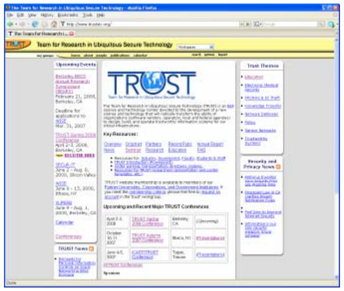
- TRUST is addressing fundamental cyber security and critical infrastructure protection problems of national importance
- TRUST is tackling problems via three-pronged approach
- TRUST is working to make a true Academic/Government/Industry model successful
- TRUST legacy will be the results of large, 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



Team for Research in Ubiquitous Secure Technology

Upcoming Events

February 21, 2008, Berkeley, CA

Deadline for applications to WISE Mar. 31, 2007

April 2-3, 2008, Berkeley, CA

Key Resources:

Upcoming and Recent Major TRUST Conferences

TRUST News

Trust Themes

Security and Privacy News

www.truststc.org