Team for Research in Ubiquitous Secure Technology (TRUST)

Societal Impact and Lasting Legacy

S. Shankar Sastry, Larry Rohrbough

PI, Exec Director TRUST Center

University of California, Berkeley

National Academy of Engineering

Symposium on Extraordinary Engineering Impacts on Society

August 19, 2022

TRUST Vision

S&T that will radically transform the ability of organizations to design, build, and operate trustworthy information systems for cyber infrastructures

TRUST Approach

- **Research** projects addressing pressing security and privacy issues of national importance
- **Education / Diversity** programs broadening participation and leading efforts in teaching and workforce development
- **Outreach** activities positioning TRUST as a leader engaging with and influencing the broader community

TRUST Overview

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/Outreach

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

TRUST Academy Online

Textbooks

SECuR-IT

WISE

TRUST-REU

TRUST Seminar

Research

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

Financial Infrastructures

- Web browser/server security
- Botnet and malware defenses
- Secure software infrastructure
- Breach notification laws

Health Infrastructures

- Privacy Modeling and Analysis
- HIS/Patient Portal Architectures
- Patient Monitoring Sensors

Physical Infrastructures

- Embedded systems for SCADA and control systems
- Sensor networks for Demand Response systems
- Information privacy and security

Knowledge Transfer

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

BT · CISCO · hp · intel · Microsoft · Sun microsystems · TELECOM ITALIA · United Technologies · U.S. Department of Homeland Security · AFRL The Air Force Research Laboratory · National Security Agency United States of America · CSIT Centre for Secure Information Technologies · iCAST International Collaboration for Advancing Security Technology · Amrita-TIFAC CORE in Cyber Security

TRUST Grand Challenge #1 – Financial Infrastructures

Scope and Objectives:

Trustworthy environment that links and supports commercial transactions among financial institutions, online retailers, and customers.

Fundamental Challenges:

- Systems Not Under Control of One Organization
  - Web browsers are separately administered by non-experts
  - Intra-enterprise financial infrastructure highly networked
- Systems Involve Computers and People
  - Web site wants to authenticate a person, not a machine
  - No control over end-user actions and decisions
  - If browser indicates "buy", is it from the user?
- Rapid Evolution of World-Wide Systems
  - Open-source browser, server, handheld platforms
  - Increasing interest in sharing vulnerability information
  - Striking demand for advanced warning and proactive solutions

TRUST Research and Development:

- Secure application and network infrastructure (front/back end)
- Detection, defenses, and forensics of malware, botnets, spyware, and other online attacks
- Authentication of client to site and site to client
- Design and construction principles for secure web systems
- Studies focused on public policy, economics of security, end-user, issues, security risk management , and behavioral biases

"Go where the money is...and go there often."
Willie Sutton

TRUST Grand Challenge #2 – Health Infrastructures

Scope and Objectives:

"Healthcare Informatics" that supports engaged patients, personalized medicine, and agile evidence-based care.

Fundamental Challenges:

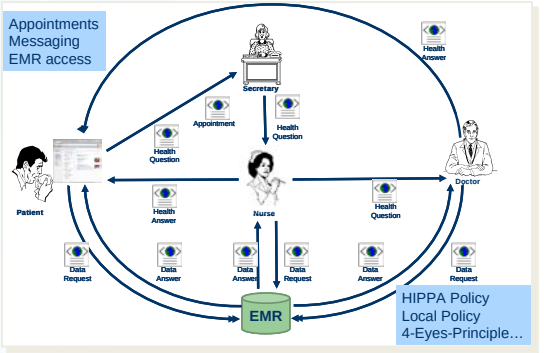
- Accessing and Archiving Electronic/Personal Health Records
  - Critical infrastructure, computer and network security, and data integrity and privacy
- Home-Based Healthcare Delivery
  - Trusted patient/provider technologies that shift healthcare to the home
- Evidence-Based Healthcare
  - Increased automation to control cost, improve quality, and deploy personalized medicine and contract-based care
- Development and Deployment of Enabling Technologies
  - Ubiquitous (mostly wireless) telecommunications , secure web portals, and clinical decision support systems

LEADING CAUSES OF DEATH[1]	
Diseases of the Heart	726,974
Cancer (malignant neoplasms)	539,577
Cerebrovascular Disease	159,791
Chronic Obstructive Pulmonary Disease	109,029
Medical Errors[2]	44,000–98,000
Accidents and Adverse Effects (motor vehicle accidents = 43,458; all others = 52,186)	95,644
Pneumonia and Influenza	86,449
Diabetes	62,636
Suicide	30,535
Kidney Disease	25,331
Liver Disease	25,175

SOURCES: 1. Centers for Disease Control and Prevention, 1997. 2. IOM, *To Err Is Human: Building a Safer Health System*, 2000.

TRUST Research and Development:

- Privacy modeling and analysis (including HIPAA, COPPA, etc.)
- Architecture for secure patient management systems and portals
- Integration of real-time patient data with patient portals
- Legal, social, and economic frameworks and analysis
- Integrative testbed for technology evaluation and transition



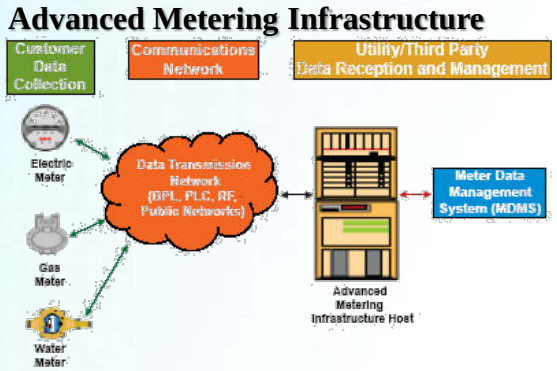
TRUST Grand Challenge #3 – Physical Infrastructures

Scope and Objectives:

Advances that support next generation Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS) as well as security and privacy of Smart Grid infrastructures.

Fundamental Challenges :

- Protecting Immense Investment
  - Financial: Sunk costs and ongoing development and maintenance
  - Human: Established development, maintenance, and regulatory organizations at federal and state levels
- Critical to National Economy
  - Modes of production depend on functionality of these systems
  - Multiple externalities have created system dependencies (e.g., air traffic control dependence on power and telecom infrastructure)
- Increasing Infrastructure Complexity
  - New approaches needed to ensure adequate control, security, and privacy (as well as securing legacy systems…)



TRUST Research and Development:

- Security threat models (external and insider attacks)
- Novel sensor networking technologies for control and maintenance
- Secure control and intrusion resilience
- Privacy-preserving demand response systems, especially for residential consumers

Science & Research Legacy

- Scientific Foundations & Advancements
  - Tools & Techniques
    - Software Security, Network Security, Trusted Platforms, Applied Cryptographic Protocols
    - Complex Interdependency Modeling and Analysis, Secure Network Embedded Systems, Model-based Integration of Trusted Components, Secure Information Management
  - Security & Privacy
    - Digital Forensics and Privacy, Human Computer Interfaces and Security, Identity Theft, Online Tracking, Data Disaggregation
  - Policy & Law
    - Economic Incentives, Public Policy Levers, Technical Standards





TRUST Policy and Privacy Added Value

- Do Not Track (Stanford/Berkeley)
  - Ongoing research to address privacy in online advertising
  - Summer 2011 TRUST REU project
  - FourthParty Platform (http://fourthparty.info/)
  - Active involvement with W3C (TRUST-sponsored workshops, TRUST researchers active in recommendations/standards development)

- Web Privacy Census (Berkeley)
  - Effort to apply web measurement rigor to make empirical statements about the state of internet tracking and privacy
  - http://www.law.berkeley.edu/privacycensus.htm

BerkeleyLaw
UNIVERSITY OF CALIFORNIA

- Mobile Web Tracking (Stanford)
  - Google tracking code for Safari browser to support mobile web advertising (verified for WSJ by former TRUST researcher Ashkan Soltani)

Google™

- Smart Grid Privacy (Cornell, Berkeley)
  - Economic value of consumer privacy
  - Inferring energy usage from aggregated data
  - Privacy in AMI systems

Illustration: Mark Montgomery

TRUST
Team for Research in Ubiquitous Secure Technology

Science & Research Legacy (cont.)

- New Research Programs & Centers

TRUST Added Value

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***

Science & Research Legacy (cont.)

- Startups

TRUST External Partners/Sponsors for 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, IBM, Sun microsystems, Cisco, Intel, Symantec, NTT DoCoMo, Microsoft, TATA Consultancy Services, EADS, Oak Ridge National Laboratory, Telecom Italia, HP, Qualcomm, United Technologies, SELEX Sistemi Integrati (A Finmeccanica Company)

Government Sponsors

NSF, National Security Agency, Office of Scientific Research, DARPA, U.S. Department of Homeland Security, AFRL (The Air Force Research Laboratory)

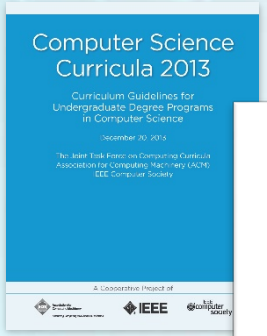
Related Programs

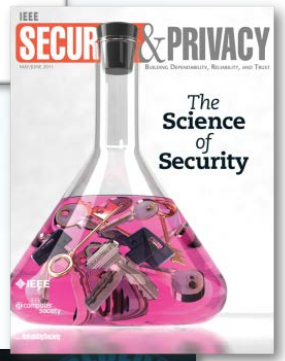
SHARPS — Strategic Healthcare IT Advanced Research Projects on Security

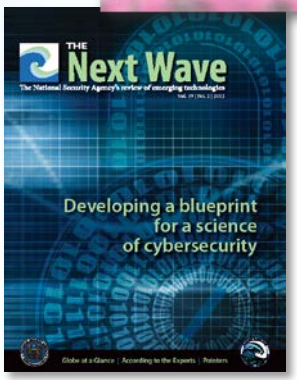
ONR (Department of the Navy, Science & Technology) — **FY2011 MURI** "Science of Cyber Security"

Science & Research Legacy (cont.)

- Community and Advising





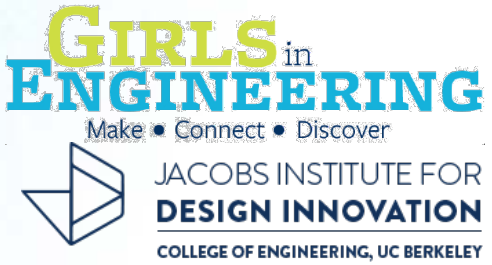


Education & Training Legacy

- New & Expanded Security Courses
  - ~40 new/expanded security courses
  - ~10 courses online via Coursera, edX
  - ~100 modules in TRUST Academy Online
- Graduate Programs
  - Graduate (MS/PhD) specializations in security across all campuses
  - Professional Masters & Certificate Programs in security at San Jose State, Stanford, and Berkeley (all ongoing)

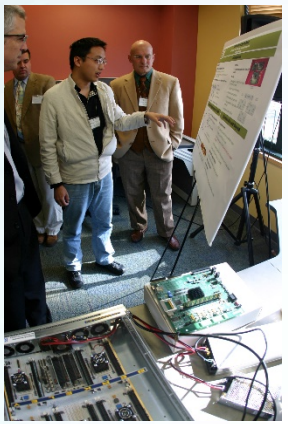
Education & Training Legacy (cont.)

- Summer Programs
  - Women's Institute in Summer Enrichment (WISE)
    - Women in Cybersecurity Conference (WiCyS)
  - Research Experiences for Undergraduates (REU)
    - Now an REU Site
  - Computing for Youth at Berkeley with Education And Research (CYBEAR)
    - Expanding via GenCyber program
  - Girls in Engineering
    - Long-term funding and home in new Jacobs Institute for Design Innovation



Human Resource Development Legacy

- Current/Future Workforce Development
  - **156** Ph.D. students graduated across the Center
    (~15 per year, 2006 – 2015)
  - **140** summer undergraduate students hosted
    (36 states + Puerto Rico; 90% STEM/grad school retention)
  - **38** summer high school students hosted
    (58% female, 65% URM)
  - **90** summer middle school girls hosted
    (25% URM; surveys will track impact through high school)
- Broadening Participation
  - Underrepresented Minorities = 15%
    (9% for Graduate Students)
  - Female Participants = 29%
    (33% for Graduate Students)



TRUST Education and Outreach (cont.)

CDSIA Leveraging TRUST to Build a Broad Community of Educators

Multiple years of community building…

- 61 Universities
- 75% HSI/MSI/HBCU Institutions
- 21 California State University Institutions
- 5 Historically Black Colleges/Universities
- 1 Historically Female Institution
- 346 seats/159 distinct attendees
- 30% Female Participants
- 12% URM

TRUST Education and Outreach

Diverse Set of Education and Outreach Activities

Programs focused on integrating trustworthy technologies, systems, and policy into learning opportunities for a broad range of participants

TEACHING/TRAINING

New Courses

- Foundational topics such as computer security, network security, software security.
- Emerging topics such as web programming and security, data privacy in biomedicine.
- Domain-specific topics such as security of electric energy systems

New Graduate Specialization

- Developing an MS/PhD research area in *Cyber Security and Trustworthy System* at all TRUST partner institutions

Professional Development

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

TRUST-REU

Women's Institute in Summer Enrichment

TRUST Education and Outreach

Example New and Enhanced Academic Courses (Undergraduate + Graduate)

Educate the next generation of computer scientists, engineers, lawyers, policy makers, and social scientists in cyber security and trustworthy systems

Course Title	Level	Campus	Started	Enrollment
Wiretaps to Facebook: Security, Privacy, & Information Network Design (ENGRI 1280)	Lower Division	Cornell	2010	80
Software Security Technologies (CMPE279)	Graduate	SJSU	2009	50
The Digital World and Society (CMPE025)	Lower Division	SJSU	2009	40
Web Programming and Security (CS142)	Lower Division	Stanford	2009	100
Internet Policy Challenges in a Global Environment (INF290)	Graduate	UCB	2009	15
Mobile Communications (ECE5680)	Graduate	Cornell	2009	50
Information Technology in Society (CS39M)	Freshman	UCB	2008	25
TechLaw with Progressive Minds (CS302)	Graduate	Stanford	2008	20
Electric Energy Systems (EGR 325)	Upper Division	Smith	2007	12
Data Privacy in Biomedicine (BMIF380/CS396)	Graduate	Vanderbilt	2007	5
Fault-tolerant Distributed Computer Systems (CS514)	Upper Division	Cornell	2007	80
Sensor Networks (ECE7940)	Graduate	Cornell	2007	20
System Security (CS5430)	Upper Division	Cornell	2006	80
Introduction to Security and Policy (CEC18-630)	Graduate	CMU	2005	80
Network Security (18-731)	Graduate	CMU	2005	80
Network Security (CMPE 209)	Graduate	SJSU	2005	100
Computer Security (CS161)	Upper Division	UCB	2005	80
Network Security (CS291)	Upper Division	Vanderbilt	2005	15
Computer Security (CS5430)	Graduate	Cornell	2005	50

TRUST Education and Outreach

TRUST Programs Positively Impacted Professional Trajectories

TRUST Education & Outreach National Reach

Graciela Perera, ‘09
Asst. Professor

Hen Su Choi, ‘12
Student UCLA

Jenifer Sunrise Winter, ‘11
Assoc. Professor

Annie Edmundson, ‘11
Ph.D. Student Princeton

Manuel Sabin, ‘13
Ph.D. Student Berkeley

- Education and Outreach has had a national impact
  - Drew participants from 36 U.S. states and Puerto Rico
- Undergraduate student retention in STEM fields = 95%
  - Students have matriculated to top graduate schools and leading companies in IT, high tech, and defense
- Faculty/graduate student retention in STEM fields = 99%
  - 62% of WISE participants are currently teaching across the country

Stewardship of Investment

- Success Leveraging NSF Funding
  - $40M investment from NSF (over 10 years)
  - $157M brought in…
    - $10M from universities (match)
    - $20M from industry partners
    - $55M from philanthropic organizations
    - $72M from U.S. Federal Government and international agencies
- Engagement with Foundations & International Partners
  - Hewlett Foundation, The Thomas and Stacey Siebel Foundation, The Peggy and Jack Baskin Foundation
  - Philippine Commission on Higher Education (CHED), Taiwan Science and Technology Council

Thank You!

Berkeley
UNIVERSITY OF CALIFORNIA

Carnegie Mellon

Cornell University

San José State
UNIVERSITY

STANFORD
UNIVERSITY

VANDERBILT
UNIVERSITY

TRUST
Team for Research in Ubiquitous Secure Technology