TRUST Science & Technology Center

Team for Research in Ubiquitous Secure Technology

Larry Rohrbough
TRUST Executive Director
University of California, Berkeley

California Office of Information Security
CISO Lecture Series

February 25, 2010 | Sacramento, California
Outline

- TRUST Overview
- TRUST Research
- TRUST Education and Diversity
- TRUST Knowledge Transfer
- Summary
Outline

- TRUST Overview
- TRUST Research
- TRUST Education and Diversity
- TRUST Knowledge Transfer
- Summary
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…”

Office of Integrative Activities (OIA)

Directorate for Computer & Information Science & Engineering (CISE)

NSF Center Funding (FY2005 - 2015)

$40M ($4M/Year, 10 Years)
TRUST Overview (cont.)

TRUST: Team for Research in Ubiquitous Secure Technology

**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
- Include external (including international) collaboration for research project sponsorship and technology transition

**Supporting Personnel**
- Graduate Students: 100
- Faculty: 53
- Research Scientists: 10
- Staff/Other: 9
- Undergrad Students: 8
- Post Doctorates: 6
- TOTAL: 186

**Affiliated Institutions**
- Berkeley
- Carnegie Mellon
- Cornell University
- San José State University
- Stanford University
- Smith College
- Mills College

**Supporting Disciplines**
- 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/Diversity**
Curriculum development 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

- Financial Infrastructures
  - Web browser/server security
  - Botnet and malware defenses
  - Secure software infrastructure

- 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/security

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

- TRUST Overview
- TRUST Research
- TRUST Education and Diversity
- TRUST Knowledge Transfer
- Summary
TRUST Research

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
  - Complex regulatory (e.g., SOX) and competitive environment

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
- Security risk management, economics of security, behavioral studies, end-user issues

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

http://blog.washingtonpost.com/securityfix/
TRUST Research (cont.)

Grand Challenge #2: Health Infrastructures

<table>
<thead>
<tr>
<th>Leading Causes of Death</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diseases of the Heart</td>
<td>726,974</td>
</tr>
<tr>
<td>Cancer (malignant neoplasms)</td>
<td>539,577</td>
</tr>
<tr>
<td>Cerebrovascular Disease</td>
<td>159,791</td>
</tr>
<tr>
<td>Chronic Obstructive Pulmonary Disease</td>
<td>109,029</td>
</tr>
<tr>
<td>Medical Errors</td>
<td>44,000–98,000</td>
</tr>
<tr>
<td>Accidents and Adverse Effects</td>
<td></td>
</tr>
<tr>
<td>(motor vehicle accidents = 43,458; all others = 52,186)</td>
<td>95,644</td>
</tr>
<tr>
<td>Pneumonia and Influenza</td>
<td>86,449</td>
</tr>
<tr>
<td>Diabetes</td>
<td>62,636</td>
</tr>
<tr>
<td>Suicide</td>
<td>30,535</td>
</tr>
<tr>
<td>Kidney Disease</td>
<td>25,331</td>
</tr>
<tr>
<td>Liver Disease</td>
<td>25,175</td>
</tr>
</tbody>
</table>

TRUST Research (cont.)

Grand Challenge #3: Physical Infrastructures

Scope and Objectives:
Advances that support next generation Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS), including for power, water, telecom, and address privacy issues.

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
  ▪ As systems evolve, need to ensure adequate control, security, and privacy (as well as securing legacy systems...)

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

Research Highlight: Financial Infrastructures

Exposure of Private Information via Website Timing Attacks

- Most sites have “Forgot my password” pages

- These pages may leak whether an e-mail is valid at that site
  - Identified through outreach to financial services company
  - Vulnerability found on virtually every site tested
  - TRUST communicated results, repair adopted, work published

Bortz, Boneh, Nandy
16th International World Wide Web Conference (WWW2007)

L. Rohrbough, UC Berkeley
Sepsis Treatment Enhanced through Electronic Protocolization (STEEP)

- **Hypothesis**
  - Implementation of an electronic process management tool will result in increased adherence to evidence-based practices, improvement in objective quality indicators, and better clinical outcomes.

- **Sepsis**
  - Common: ~750,000 cases/year
  - Deadly: ~25-35% mortality rate
  - Expensive: $17B/year (40% of ICU costs)
  - Treatable: Validated treatment protocols

- **Challenges**
  - Operational protocols, healthcare policies, and treatment guidelines are rarely phrased in a mathematically sound manner
  - Semantics of the protocol modeling language
  - Validation/verification of protocol models
  - Integration with Clinical Information Systems
  - Clinical barriers to adoption

- **Model-Based Approach**
  - Complexity of these systems is a major concern.
  - Model verification for security and privacy properties of the modeled architecture.
  - Models are protocol-driven, evidence-based, customizable, and integrated.

- **Development and Deployment**
  - STEEP Treatment Management Console (TMC), which shows recommended actions and displays patient health information.
  - Deployed at the Vanderbilt University Medical Center
Privacy Concerns in Upcoming Demand Response Systems

- **Next generation demand-response architectures**
  - **Advantages:** cost savings, increased grid reliability, new modes of consumer-utility interaction.
  - **Disadvantage:** Increased availability of data creates privacy/security issues.
  - **Claim:** Detailed household consumption data gathered by AMIs can reveal personally identifying information.
  - **Goal:** Metric which associates the degree of data availability with potential privacy risks, providing a robust and reliable indicator

- **Field Experiment**
  - Energy-usage monitors and cameras
  - Behavior-extraction algorithms to determine Presence/Absence, Appliance Use, and Sleep/Wake Cycle.

**Findings**
- Smart Metering Provides Data Equivalent to a “Search”: Algorithms perform well in determining presence and sleep cycles—over 90% of total interval length was correctly classified.

Lisovich, Mulligan, Wicker

L. Rohrbough, UC Berkeley
Outline

- TRUST Overview
- TRUST Research
- TRUST Education and Diversity
- TRUST Knowledge Transfer
- Summary
TRUST Education and Diversity

Education and Human Resource Development Challenges

“To ensure that federal cyber policies enhance our security and our prosperity...we're making a new commitment to education in math and science, and historic investments in science and research and development.”

President Barack Obama, May 29, 2009

Cyberspace Policy Review

“Expand support for key education programs and research and development to ensure the Nation’s continued ability to compete in the information age economy.”

“Develop a strategy to expand and train the workforce, including attracting and retaining cybersecurity expertise in the Federal government.”

Cyber IN-security: Strengthening the Federal Cybersecurity Workforce

“Develop a government-wide strategic blueprint to acquire, train, and retain the cybersecurity talent the federal government needs.”

“Provide significant funding to develop and keep federal cybersecurity talent knowledgeable at a ‘state of the art’ level of readiness through training and development.”

“Ensure adequate funding of successful programs that provide graduate and undergraduate scholarships in the cybersecurity field.”
TRUST Education and Diversity (cont.)

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

<table>
<thead>
<tr>
<th>TEACHING/TRAINING</th>
<th>DISSEMINATION</th>
<th>DIVERSITY</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New Courses</strong></td>
<td><strong>TRUST Academy Online</strong></td>
<td><strong>Alliance for Minority Participation</strong></td>
</tr>
<tr>
<td>✓ Foundational topics such as computer security, network security, software security.</td>
<td><a href="https://tao.truststc.org">https://tao.truststc.org</a></td>
<td><strong>HBCU Summer Partnership</strong></td>
</tr>
<tr>
<td>✓ Emerging topics such as web programming and security, data privacy in biomedicine.</td>
<td><strong>TRUST Security Seminar</strong></td>
<td><strong>Information Systems</strong></td>
</tr>
<tr>
<td>✓ Domain-specific topics such as security of electric energy systems</td>
<td></td>
<td><strong>Carnegie Mellon</strong></td>
</tr>
<tr>
<td><strong>New Graduate Specialization</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓ Developing an MS/PhD research area in Cyber Security and Trustworthy System at all TRUST partner institutions</td>
<td></td>
<td><strong>Women’s Institute in Summer Enrichment</strong></td>
</tr>
</tbody>
</table>

**Professional Development**

- eBay
- RAPPORT
- Sun
- HP
- SalesForce
- Yahoo!

**SUPERB-IT**

Center for Underrepresented Engineering Students

University of California, Berkeley
**TRUST Education and Diversity (cont.)**

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

<table>
<thead>
<tr>
<th>Course Title</th>
<th>Program Level</th>
<th>Campus</th>
<th>Offered</th>
<th>Enrollment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Security Technologies (CMPE279)</td>
<td>Graduate</td>
<td>SJSU</td>
<td>2009</td>
<td>50</td>
</tr>
<tr>
<td>The Digital World and Society (CMPE025)</td>
<td>Lower Division</td>
<td>SJSU</td>
<td>2009</td>
<td>20</td>
</tr>
<tr>
<td>Web Programming and Security (CS142)</td>
<td>Lower Division</td>
<td>Stanford</td>
<td>2009</td>
<td>100</td>
</tr>
<tr>
<td>Internet Policy Challenges in a Global Environment (INF290)</td>
<td>Graduate</td>
<td>Berkeley</td>
<td>2009</td>
<td>15</td>
</tr>
<tr>
<td>Mobile Communications (ECE5680)</td>
<td>Graduate</td>
<td>Cornell</td>
<td>2009</td>
<td>50</td>
</tr>
<tr>
<td>Information Technology in Society (CS39M)</td>
<td>Freshman</td>
<td>Berkeley</td>
<td>2008</td>
<td>25</td>
</tr>
<tr>
<td>TechLaw with Progressive Minds (CS30M)</td>
<td>Graduate</td>
<td>Stanford</td>
<td>2008</td>
<td>20</td>
</tr>
<tr>
<td>Electric Energy Systems (EGR 325)</td>
<td>Upper Division</td>
<td>Smith</td>
<td>2007</td>
<td>12</td>
</tr>
<tr>
<td>Data Privacy in Biomedicine (BMIF380/CS396)</td>
<td>Graduate</td>
<td>Vanderbilt</td>
<td>2007</td>
<td>5</td>
</tr>
<tr>
<td>Fault-tolerant Distributed Computer Systems (CS514)</td>
<td>Upper Division</td>
<td>Cornell</td>
<td>2007</td>
<td>80</td>
</tr>
<tr>
<td>Sensor Networks (ECE7940)</td>
<td>Graduate</td>
<td>Cornell</td>
<td>2007</td>
<td>20</td>
</tr>
<tr>
<td>System Security (CS5430)</td>
<td>Upper Division</td>
<td>Cornell</td>
<td>2006</td>
<td>80</td>
</tr>
<tr>
<td>Introduction to Security and Policy (CEC18-630)</td>
<td>Graduate</td>
<td>CMU</td>
<td>2005</td>
<td>80</td>
</tr>
<tr>
<td>Network Security (18-731)</td>
<td>Graduate</td>
<td>CMU</td>
<td>2005</td>
<td>80</td>
</tr>
<tr>
<td>Computer Security (CS161)</td>
<td>Upper Division</td>
<td>Berkeley</td>
<td>2005</td>
<td>80</td>
</tr>
<tr>
<td>Network Security (CS291)</td>
<td>Upper Division</td>
<td>Vanderbilt</td>
<td>2005</td>
<td>15</td>
</tr>
</tbody>
</table>
TRUST Education and Diversity (cont.)

TRUST Graduate-Level Security Specialization

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

EECS Research Area begun at UC Berkeley in 2007

(http://eecs.berkeley.edu/Research/Areas/SEC)

- Enhanced Curriculum Development
  - Create five new courses in trustworthy systems: Pilot at UC Berkeley
    - Internet Technologies
    - Societal and Ethical Implications of Trustworthy Systems
    - Security and Computer Forensics
    - Internet Law
    - IT consulting and professional services
  - Cross-listed with the College of Engineering, School of Information, and the School of Law

- **MS/PhD Program Specialization in Security**
  - Open to all graduate level students
  - Leverage existing graduate-level courses + new courses offering
  - Will increase security exposure across TRUST institutions
Summer Programs: Research Experiences for Undergraduates

- **Program Overview**
  - 8-week research experience guided by faculty mentors and graduate students
  - Educational activities include lab tours and industry field trips
  - Graduate school advising and subsidized GRE prep course
  - $4,000 Stipend + travel allowance + room and board provided

- **Program Impact**
  - 2006-2008: TRUST hosted 18 undergraduate students
    - 72% female/39% URM
    - 100% U.S. persons
    - 94% in grad school or applying
  - 2009: TRUST hosted 10 students
  - 2010: TRUST hosting 28 students (across five TRUST institutions)

- **Participant Testimonial**
  “The best part was the exposure to both the academic and industrial pathways. Without the first-hand company seminars and research experience I gained from the program, I would have made a much weaker decision as in which path to choose!”

- **More Information Online**
  - Program Description at: [https://www.truststc.org/reu/](https://www.truststc.org/reu/)
TRUST Education and Diversity (cont.)

Summer Programs: Security Summer Internship

SECuR-IT: Summer Experience, Colloquium, and Research in Information Technology

- **Program Overview**
  - 10-week graduate student summer program in computer security
  - Paid internship at a Silicon Valley technology company
  - Housing at San Jose State
  - Seminars in security related topics
  - College units for summer educational program
  - Program funded by industry partners

- **SECuR-IT Interns**

- **Participating Companies**

- **Participant Testimonials**
  - “SECuR-IT was a great combination classes and work! Loved all of it!”
  - “The eBay internship program is great! I enjoyed it very much! This is my best summer ever, both on learning and having so much fun!”

- **More Information Online**
  - Program Description at: [https://www.truststc.org/securit/](https://www.truststc.org/securit/)
TRUST Education and Diversity (cont.)

TRUST Academy Online (TAO)

Back-end repository and web-based portal for collecting and disseminating learning material to faculty and researchers working in TRUST-related areas

- TRUST research materials become module content and project profiles on the TAO
- TAO contains teaching modules that can be incorporated into diverse curricula (e.g., privacy modules for engineers working on SCADA control systems; cryptography modules that introduce DRM concepts to law students)

https://tao.truststc.org
Outline

- TRUST Overview
- TRUST Research
- TRUST Education and Diversity
- TRUST Knowledge Transfer
- Summary
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

Government Sponsors

External Partners/Sponsors Support Technology Transition

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

**Electronic Medical Records**

- Adoption of model-based methods for HIS (architectures, privacy and security policies, security mechanisms, web authentication, and human factors)
- DexterNet – Body sensor network for patient monitoring and in-home healthcare.

**End User Security**

- Identity theft (anti-phishing) and authentication/verification web browser tools
- Malware detectors (Minesweeper, Panorama) and botnet zombie detection system (BotSwat)

**Network Defenses**

- Network intrusion detection and monitoring technology
- Portcullis/SNAPP – High network availability during massive attacks (e.g., DDoS)
TRUST Knowledge Transfer (cont.)

Government: Technology + Policy Advising

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

**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

**Taiwan Science & Technology Advisory Group**
- Reviewer on STAG panel investigating Taiwan’s “Information-Communication Security” capabilities, August 2009
- Topics: global competitiveness, industry, education, e-government/e-commerce, health/medical
TRUST Knowledge Transfer (cont.)

Department of Defense: Security Research + Experimentation + Advising

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

**Defense Advanced Research Projects Agency**
- Desire for large-scale cyber network testing & evaluation
- Possibly build on Berkeley/USC-ISI cyber testebed (DETER) architecture
- Leverage experimentation experience of TRUST DETER team

**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)
TRUST Knowledge Transfer (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
Outline

- TRUST Overview
- TRUST Research
- TRUST Education and Diversity
- TRUST Knowledge Transfer
- Summary
Summary

- **TRUST is addressing challenge of building trustworthy systems**
  - Multi-disciplinary team addressing fundamental cyber security and infrastructure problems of national importance.
  - Researchers at the forefront many emerging cyber threats (ID theft, data breaches, cyber attacks, malware, botnets, …).

- **TRUST hallmark and legacy**
  - Results of large, integrative research projects.
  - Comprehensive education program to groom the next generation of cyber security/privacy researchers and professionals.
  - Successful knowledge transfer of results—technology adoption, policy/legal reforms, researcher/practitioner community building.

- **TRUST opportunities**
  - Looking for new ideas and collaborators in government and industry.
  - Looking for hard problems to solve and applications for Center research.
  - Interested in sharing lessons learned for making an Academic/Government/Industry model successful.
Thank You!

Contact Information

Larry Rohrbough
Executive Director
TRUST Science and Technology Center
University of California, Berkeley
+1 510-643-3032 (Work)
+1 703-328-5221 (Mobile)
larryr@eecs.berkeley.edu

www.truststc.org