



***TRUST*: Team for Research in Ubiquitous Secure Technology**

Education Overview

Dr. Kristen Gates, TRUST Education Director

July 18, 2011 | WISE 2011 at CMU

Berkeley
UNIVERSITY OF CALIFORNIA

Carnegie Mellon

Cornell University

San José State
UNIVERSITY

STANFORD
UNIVERSITY



VANDERBILT
UNIVERSITY

TRUST Overview

TRUST: Team for Research in Ubiquitous Secure Technology

TRUST MISSION. Science and Technology 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	88
❖ Faculty	42
❖ Undergrad Students	11
❖ Research Scientists	10
❖ Staff/Other	9
❖ Post Doctorates	8
TOTAL:	168

Affiliated Institutions

Berkeley
UNIVERSITY OF CALIFORNIA

Carnegie Mellon

Cornell University **STANFORD**

UNIVERSITY

San José State
UNIVERSITY



VANDERBILT
UNIVERSITY

Supporting Disciplines

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

TRUST Overview (cont.)

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/Diversity

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 lead to a science base and 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



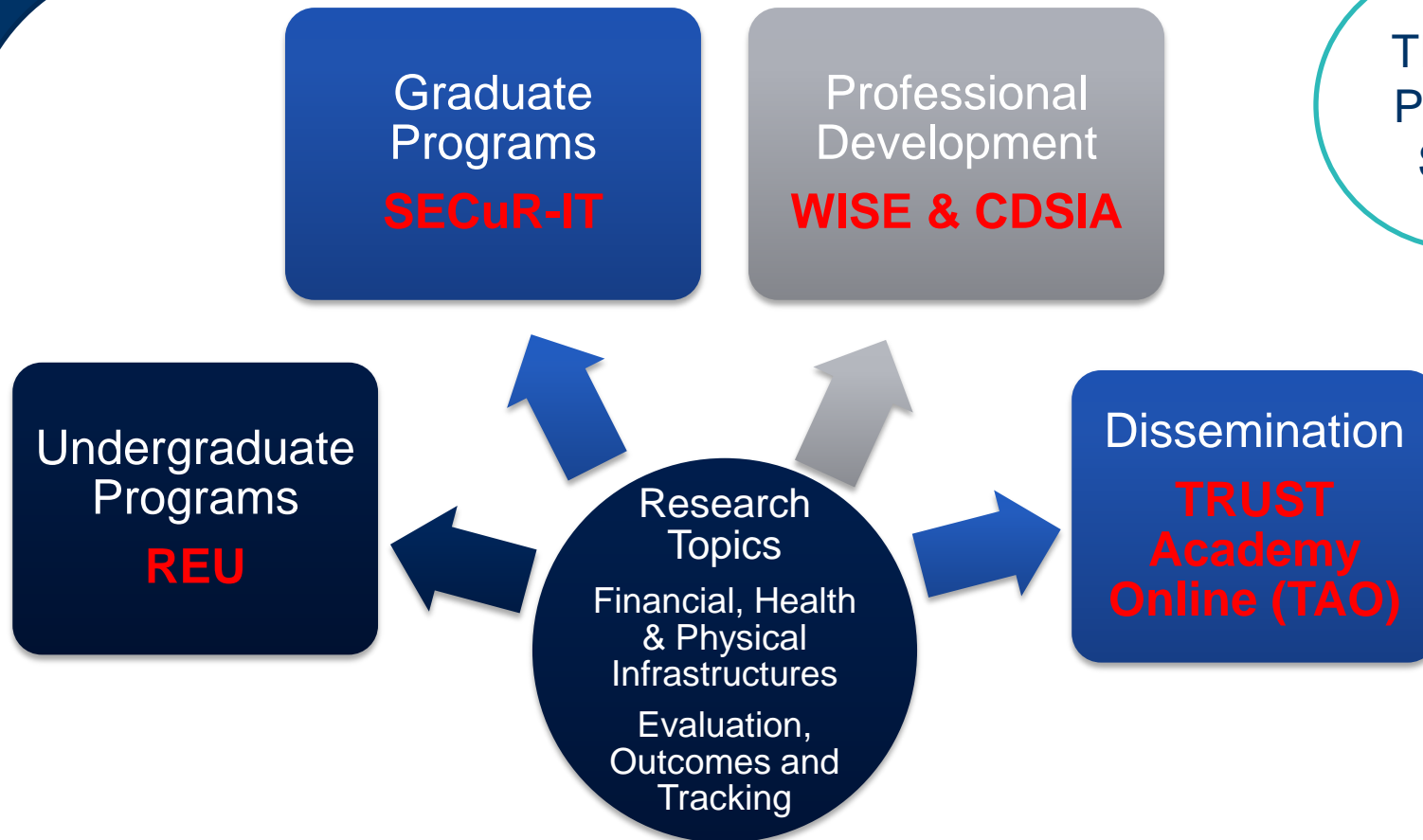
Physical Infrastructures

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

Knowledge Transfer

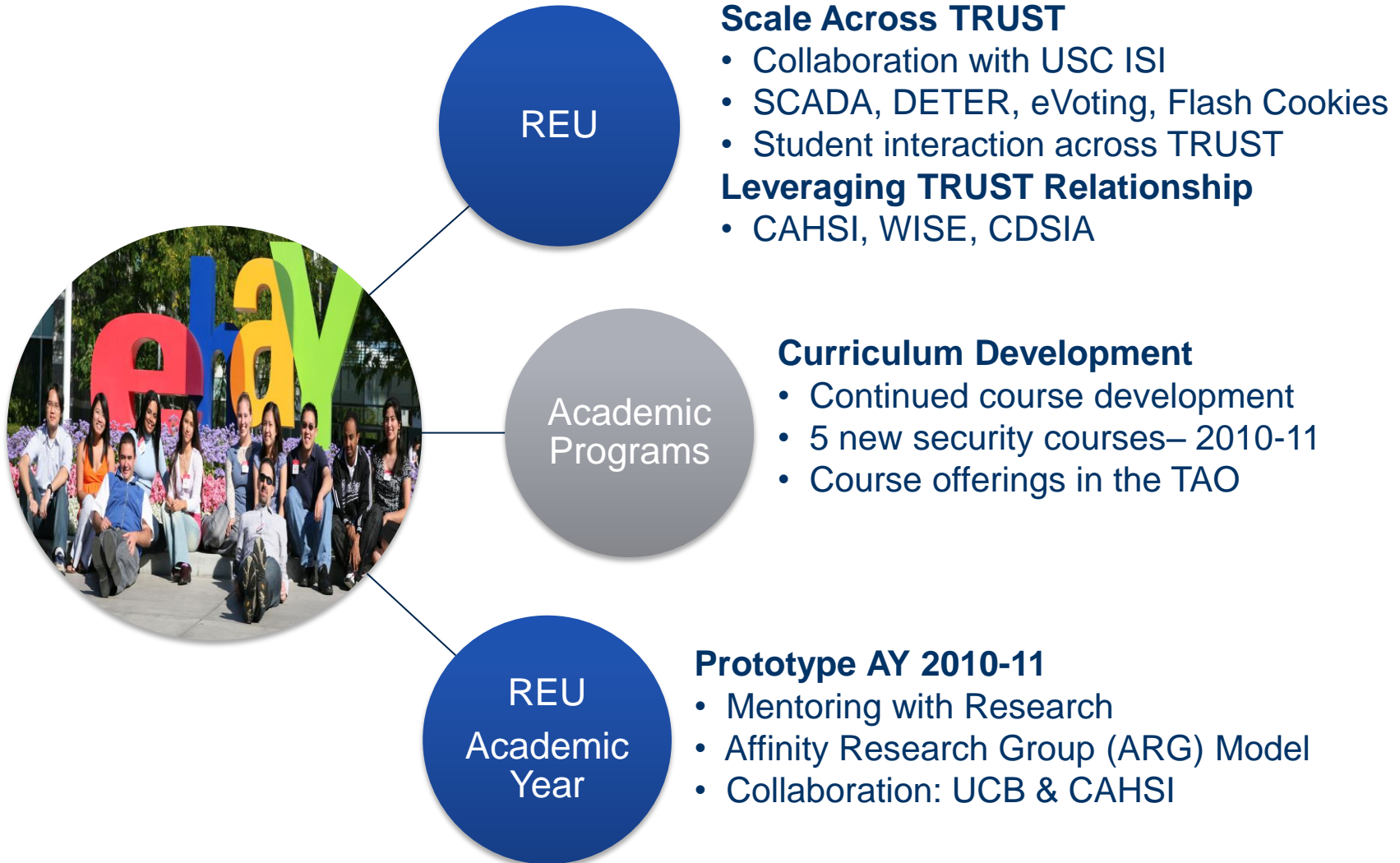
Dissemination and transition of Center research results and collaboration opportunities with external partners





TRUST education activities have reached undergraduate and graduate students, postdoctoral scholars and junior faculty, and industry professionals to address the technical, policy, and economic issues essential to improving cyber security and trustworthy systems.

Undergraduate Programs



TRUST-REU Program

TRUST Summer Research Experiences for Undergraduates (TRUST-REU)

- Program Overview

- 8-week summer research experience guided by TRUST 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 Participants

- 2006-2010: TRUST has hosted **60** undergraduate students
 - 47% female
 - 48% URM
 - 97% U.S. persons
 - Most in grad school or applying
- 2011: TRUST **13** students (across four Center 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/>



TRUST-REU Program Data 2006-2010

Participant Tracking – Graduate School for 2006-2010 Cohort

Degrees Earned & In-Progress	TRUST-REU Participants
PhD & MS Degrees Awarded	2
PhD Pipeline	10
MS/MBA Pipeline	5
Applying to Grad School	35
Applying to Law School	2

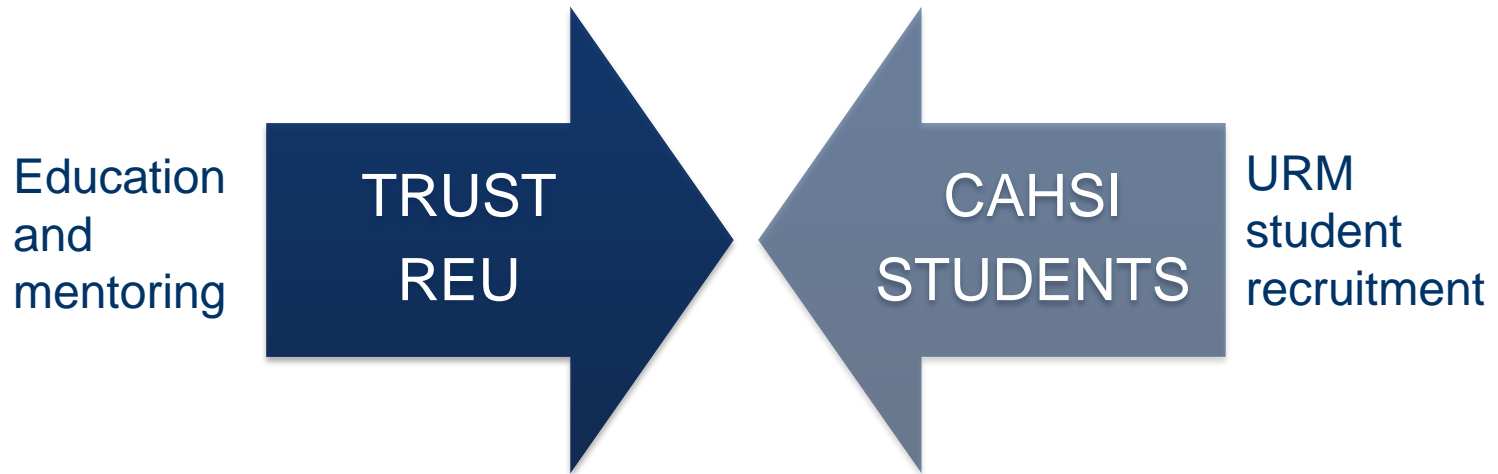
2006-2010 Cohort = 60

90% Pursuing Graduate Study

Leveraging Education Relationships

CAHSI: Computer Alliance for Hispanic Serving Institutions

CAHSI and TRUST working together to advance the mission and mutual goals of both organizations through collaborative efforts.



TRUST-REU 2011 placed **six** REU students having research/academic affiliation with CAHSI



CAHSI and TRUST will work together to prepare CAHSI students for a successful REU with TRUST



Pending: NSF Program Solicitations

- Computing Education for the 21st Century (CE21)
Pathways to the Baccalaureate: to Recruit and Advance Women and Latinos/Latinas in Computer Science for community college students
- Research Experiences for Teachers (RET)
TRUSTed Pathways: TRUST Education, Pathways into Computer Security Research an RET for community college faculty
- Cyberinfrastructure Training, Education, Advancement, and Mentoring for Our 21st Century Workforce (CI-TEAM) **Pathways to the Baccalaureate: to Recruit and Advance Women and Underrepresented Minorities in Computer Science** for high school, community college and four-year baccalaureate STEM students

Graduate Programs

Across TRUST Partners



Graduate Cohort

- 66 student cohort (Year-5)
- Collaboration with USC ISI

TRUST Technical Seminar

- 2010-11: 23 speakers (920 participants)

SECuR-IT Internship

- 2011 Applicant pool: 153 MS & PhDs
- 8 Industry sponsors with 15 interns

Curriculum Development

- 7 new course 2010-2011

Graduate and Post-Doc mentors

- TRUST research topics into REU
- Mentor and advise undergraduate
- Tech talks for summer REU

SECuR-IT Cybersecurity Internship

Summer Experience, Colloquium and Research Experience in Information Technology



SECuR-IT is a 10-week academic summer immersion program in computer security

Program Overview:

- Paid internship at a Silicon Valley and San Francisco technology company
- Learning cohort of MS and PhD students
- Program cost funded by industry partner
- Seminars conducted by TRUST faculty and industry experts that expose students to a range of information technology and computer security research topics
- Program details at: <http://truststc.org/securit>












TRUST Research initiatives drive curriculum development across the center

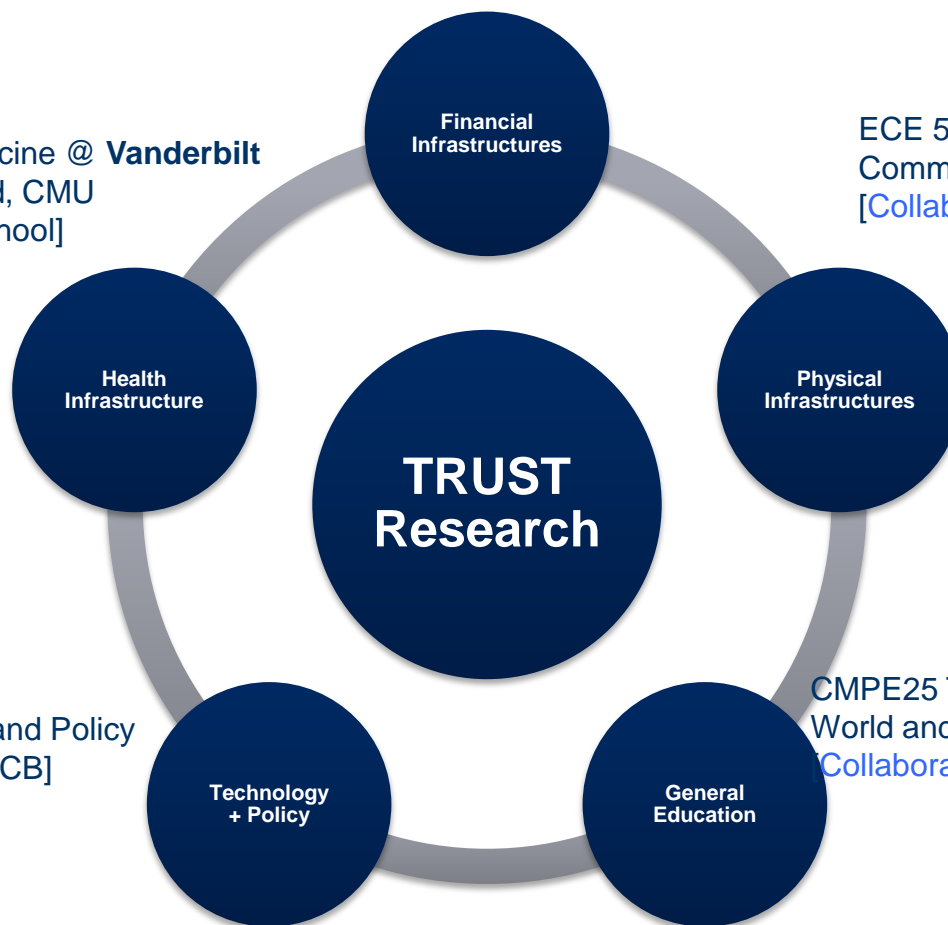
CS142 Web Programming and Security @ **Stanford**
[Collaborators: UCB & CMU]

BMIF380/CS396
Data Privacy in Biomedicine @ **Vanderbilt**
[Collaborators: Stanford, CMU
& Vanderbilt Medical School]

ECE 5680 Mobile
Communications @ **Cornell**
[Collaborator: UCB]

CEC18-630
Introduction to Security and Policy
@ **CMU** [Collaborator: UCB]

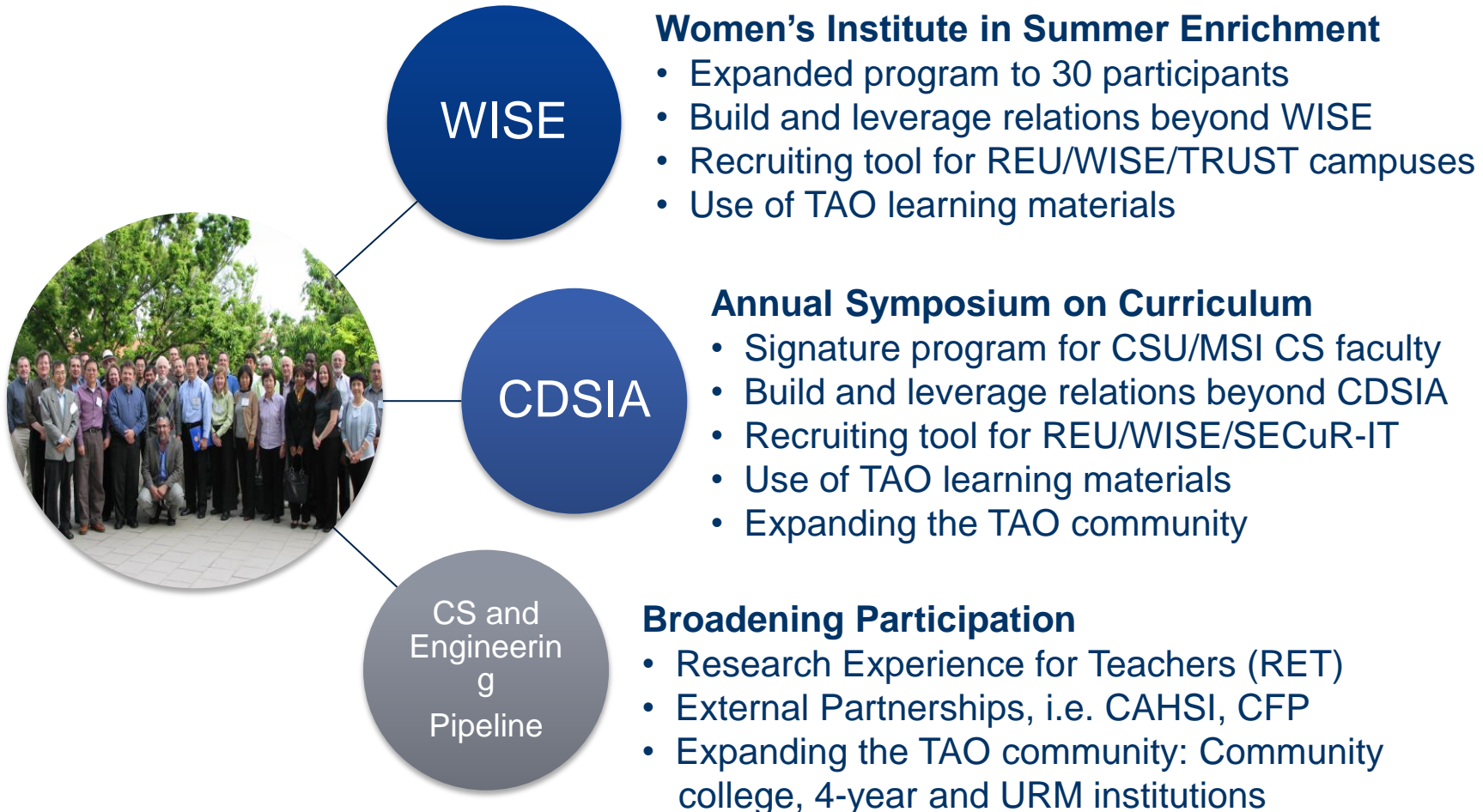
CMPE25 The Digital
World and Society @ **SJSU**
[Collaborators: UCB & Vanderbilt]



IMPACT: Courses Across the Center

Course Title	Program Level	Partner Campus	First Offered	Enrollment Per Course
The Digital World and Society (CMPE 25)	Lower Division	SJSU	2010	40
Security, Privacy, and Information Network Design: Wiretaps to Facebook (ENGRI 1280)	Lower Division	Cornell	2010	40
Computer Security (CS 161)	Upper Division	UCB	2010	100
Network Security (CMPE 209)	Upper Division	SJSU	2010	40
Embedded Systems (ECE 3140)	Upper Division	Cornell	2011	100
Secure Software Systems (ECE 18732)	Graduate	CMU	2010	32
Privacy, Security, and Cryptography (IS 219)	Graduate	UCB	2010	20
Security in Networked Systems (14-741/18-631)	Graduate	CMU	2010	60
Privacy in the Digital Age (94806)	Graduate	CMU	2010	40
Technology & Policy Lab (IS 290)	Graduate	UCB	2011	8
Graduate seminar in high assurance cloud computing architectures (CS7412)	Graduate	Cornell	2011	16
Data Privacy in Biomedicine (BMIF-380 / CS-396)	Graduate	Vanderbilt	2011	7

Building a **critical mass** of cyber security and trustworthy systems faculty and practitioners in teaching and research universities.



Women's Institute in Summer Enrichment

WISE 2011 at Carnegie Mellon University

“We came across miles with diverse backgrounds, lived like teens, convened daily for learning and most evenings for play. Everyone was smart, engaged in their careers and lovely in their own ways and demeanors. It was an honor to spend the week together, from which I have learned many lessons...”



<http://www.truststc.org/wise>

- One-week residential summer seminar
- Graduates, post-doctoral, and professors
- Program topics: cyber security, healthcare and privacy
- 2011 Speakers:
 - Lorrie Cranor: CyLab, Carnegie Mellon University
 - Dorothy Glancy, Santa Clara University Law
 - Leslie Lambert: Juniper Networks
 - Brenda Fellows: Fellows Corporate Consortium
 - Michelle Nix: McKesson
 - Adrian Perrig: TRUST, Carnegie Mellon University
 - Brad Malin: TRUST, Vanderbilt University
 - Deb Frinkie, National Security Agency



IMPACT: Building Community

CDSIA: Curriculum Development in Security and Information Assurance 2011



“It was an excellent space to learn from the expertise of Industry and academic leaders... a good platform for education to exchange ideas in IA, especially building capacity in IA.”

“My department is considering development of new courses in MBA and bachelors program of Information systems. I will take advantage of this seminar to coordinate the development of new curriculum.”

Demographics

- 25% Female Participants
- 55% HSI/MSI/HBCU Institutions
- 15 California State University Institutions
- 4 Historical Black College or University
- 1 California Community College
- 1 Historically Female Institution

Participating Universities

Cal Poly Pomona (HSI)
Cal Poly San Luis Obispo
CSU Chico
CSU Dominguez Hills (HSI/MSI)
CSU East Bay
CSU Humboldt
CSU Los Angeles (HSI/MSI)
CSU Long Beach (HSI)
CSU Northridge (HSI)
CSU Sacramento
CSU Stanislaus (HSI)
CSU San Bernardino (HSI)
San Francisco State University
San Diego State University (HSI/MSI)
San José State University (TRUST)
Carnegie Mellon University (CyLab)
UC Berkeley (TRUST)
Colorado State University
Drexel State University
Mt. San Antonio College (HSI)
Jackson State University (HBCU/MSI)
Howard University (HBCU/MSI)
Fisk University (HBCU/MSI)
Mills College
Tuskegee University (HBCU/MSI)
Polytechnic University of Puerto Rico (HSI)
Inter American University of Puerto Rico (HSI)
Virginia State University
Youngstown State University

CDSIA: Curriculum Development in Security and Information Assurance

Curriculum Development in Security and Information Assurance (CDSIA) at San José State University. The 4th CDSIA 2011 held April 29, 2011.

2010 → 36 participants 2011 → 60 participants

- **Objectives:**
 1. **Reach out** to the California State University system, HSI/HBCUs and to other universities whose mission is focused on work-force preparation and undergraduate education
 2. **Share** material and support structures developed by the TRUST partners
 3. **Strengthen** the TRUST-related community of educators, and
 4. **Facilitate** the education of members of underrepresented communities in the domain of secure technologies.

- **Target Student Audiences**
 1. The **broad population** of educated individuals – general education
 2. The **designers of our future** – STEM discipline students
 3. The **future domain specialists** – BS and MS IT discipline students

The TAO Portal: URL <http://www.tao.truststc.org/>



The screenshot shows the TRUST Academy Online (TAO) Portal homepage. At the top, there is a navigation menu with links for Home, Projects, Courseware, News, Survey, Site Map, Accessibility, Contact, Join, and Log in. A search bar is located on the right side of the header. The main content area features a large TRUST logo with a yin-yang symbol in the letter 'O'. Below the logo, there are two main sections: 'Courseware' with an icon of a stack of books, and 'Projects' with an icon of a wind turbine and a solar panel. A 'NEWS' sidebar on the right lists recent updates, including 'Portal now implements OAI-PMH' (02-21-2008), 'New site survey available' (12-11-2007), 'Profile metadata has changed' (12-10-2007), and 'Live TRUST news feed available' (10-21-2007). A 'Welcome to the TRUST Academy Online (TAO) Portal' message is displayed in a white box, followed by a paragraph describing the portal's purpose. The footer contains copyright information for 2008 TRUST STC and design credit to ProTotus at ISIS, Vanderbilt.

Home Projects Courseware News Survey Site Map Accessibility Contact Join Log in advanced search...

TRUST

HOME

Courseware

Projects

NEWS

- Portal now implements OAI-PMH 02-21-2008
- New site survey available 12-11-2007
- Profile metadata has changed 12-10-2007
- Live TRUST news feed available 10-21-2007

More news...

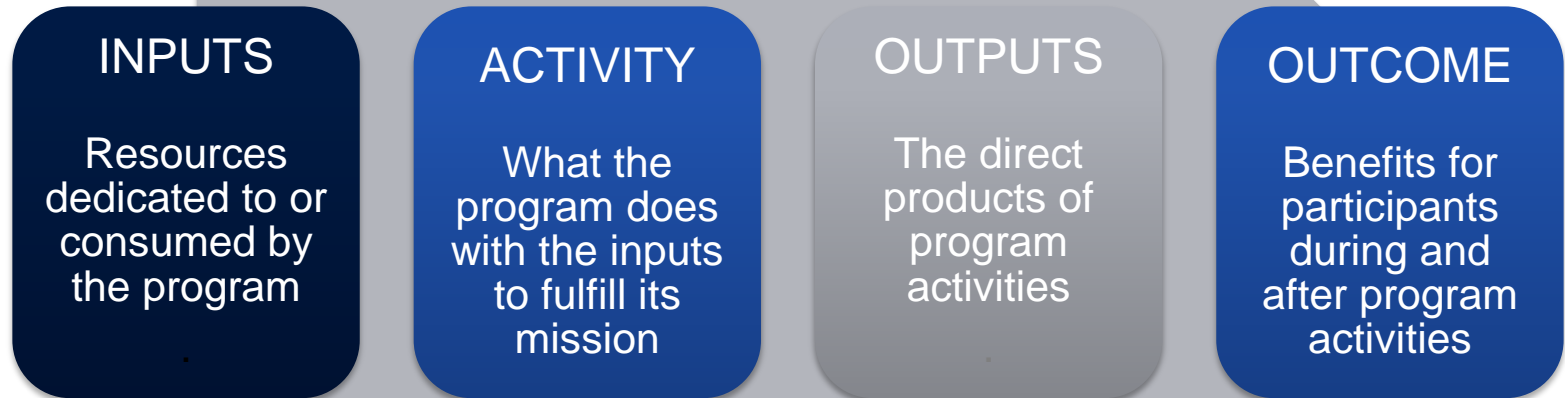
Welcome to the TRUST Academy Online (TAO) Portal

TAO supports online community outreach for TRUST, an NSF Science and Technology Center. TAO Project Profiles share the stories of individual TRUST projects and provide access to related resources. TAO Courseware Profiles disseminate sets of learning materials contributed by TRUST investigators, institutions, and partners.

© 2008 TRUST STC Design by ProTotus at ISIS, Vanderbilt.

Evaluation, Outcomes and Tracking

Summary of Program Outcomes Model



The purpose for evaluation is to understand the degree to which the project goals are being met and to monitor and improve project effectiveness along the way in an effort to help reach those goals.

Significant attention will be paid to gathering and tracking longitudinal data so that we can document overall impact of engagement with and support of TRUST on participant educational and career choices.

- **Priming the Pipeline.** Leverage TRUST programs across partner institutions and multiple communities: undergraduate to the professorate and beyond-- TRUST REU, SECUR-IT, WISE, CDSIA, TAO and pending CE21, CI-TEAM and RET.
- **Collaborations** will leverage and expand current programs as well as create new undergraduate research opportunities– e.g., USC's Information Sciences Institute (ISI).
- **SECuR-IT** Expand program to 30 interns with 10+ industry partners. Scale program to include **Financial** Infrastructures at **Cornell** and **Health** Infrastructures at **Vanderbilt**.
- **CDSIA** will draw in community colleges and broaden participation.
- **Trust Academy Online.** Building an outstanding archive of cyber security and trustworthy systems learning materials, program resources, and technical seminars and be recognized as the primary source in cyber security research and academic program support.