TRUST:
Team for Research in Ubiquitous Secure Technologies
Overview

Shankar Sastry, PI and Dir.
Ruzena Bajcsy, Outreach Dir.
Sigurd Meldal, Education co-Dir.
John Mitchell, co-PI
Mike Reiter, co-PI
Larry Rohrbough, Executive Director
Fred Schneider, Chief Sci.
Mary Margaret Sprinkle, Project Manager
Janos Sztipanovits, co-PI and Education Co-Dir
Doug Tygar, Berkeley Dir.
Steve Wicker, co-PI

Carnegie Mellon · Cornell University · MILLS COLLEGE · San José State UNIVERSITY
SMITH COLLEGE · STANFORD UNIVERSITY · Berkeley · VANDERBILT UNIVERSITY

Second Year Review
March 19th, 2007

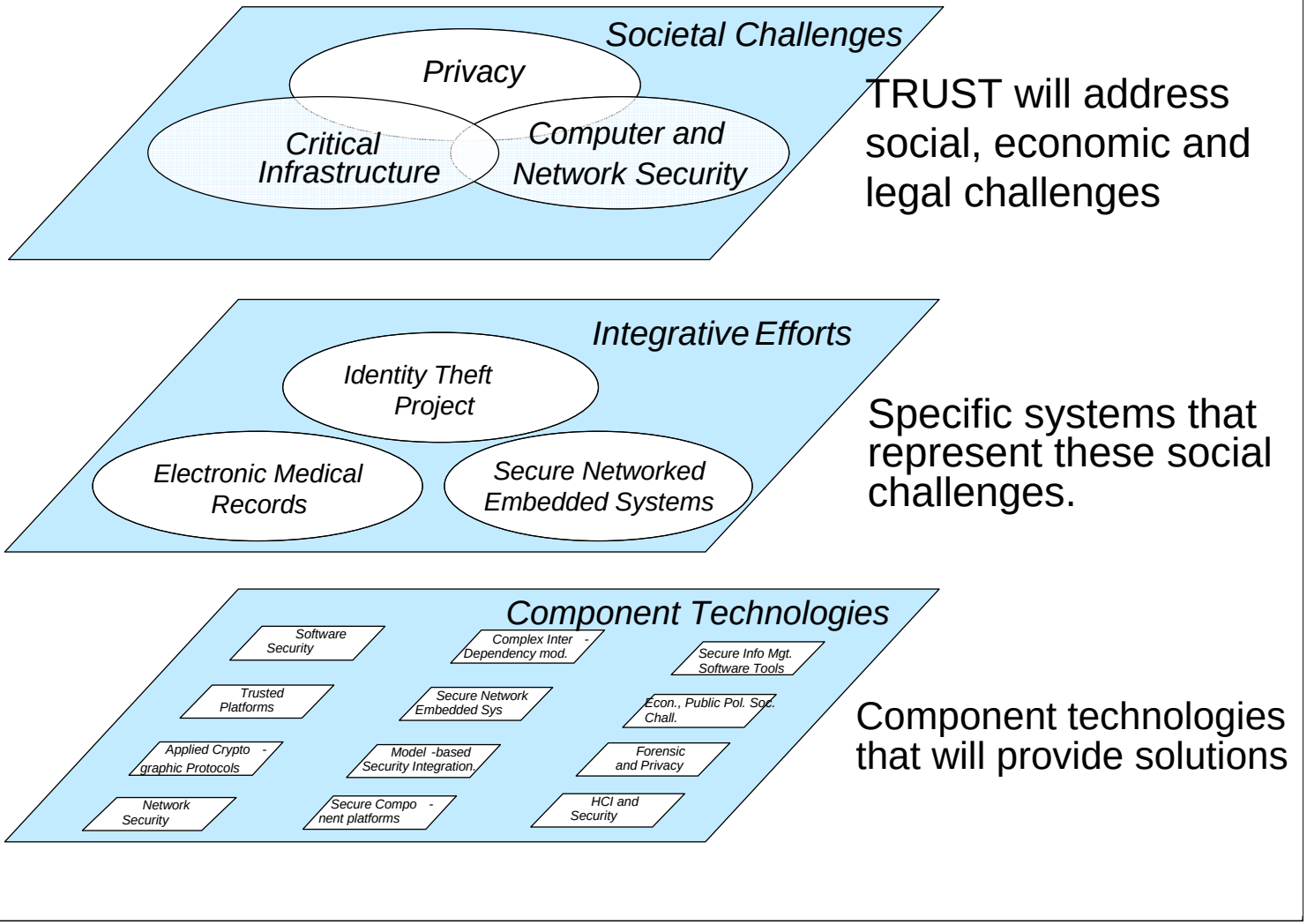
TRUST worthy Systems

- More than an Information Technology issue
- Complicated interdependencies and composition issues
  - Spans security, systems, and social, legal and economic sciences
  - Cyber security for computer networks
  - Critical infrastructure protection
  - Economic policy, privacy
- ***TRUST***: "holistic" interdisciplinary systems view of security, software technology, analysis of complex interacting systems, economic, legal, and public policy issues
- Trustworthiness problems invariably involve solutions with **both** technical and policy dimensions
- Goals:
  - Composition and computer security for component technologies
  - Integrate and evaluate on testbeds
  - Address societal objectives for stakeholders in real systems

Sample TRUST Events: April 06-Mar 07

- Next Generation SCADA: planning meeting, DC and final NITRD interagency workshop, Pittsburgh: Mar and Nov 2006
- AF-TRUST kickoff, DC June 2006
- TIPPI Workshop, Palo Alto June 2006
- SUPERB-TRUST, Berkeley SIPHER-TRUST, Vanderbilt June-Aug 2006
- WISE, Berkeley July 2006
- Capacity Building Program, Pittsburgh, July-Aug 2006
- TRUST External Advisory Board, Berkeley Aug 2006
- TRUST Fall Retreat, Pittsburgh, Oct 2006
- iCAST Collaboration with Taiwan kickoff: Pittsburgh, Berkeley, Oct 2006
- Unblinking; Conference on Visual Privacy, Berkeley, Nov 2006
- iCAST Conference, Taipei, Jan 2007
- House of Lords Select Committee, March 2007

TRUST Research Vision



TRUST will address social, economic and legal challenges

Specific systems that represent these social challenges.

Component technologies that will provide solutions

TRUST Second Year Portfolio

- Integrative Research Project Themes
  - Secure Network Embedded Systems (Wicker, Mulligan leads)
  - Identity Theft, Phishing, Spyware and Related Issues (Mitchell, Tygar leads)
  - Electronic Medical Records (Sztipanovits, Bajcsy, Eklund leads)
  - Trustworthy Systems (Wagner, Aiken, Reiter leads)
  - Network Security (Joseph, Birman leads)
  - Seedling Topics
- Integrative Education Project Themes (Ed/Outreach Director Kristen Gates)
  - TRUST Academy Online (TAO: Sztipanovits, Meldal leads)
  - Education Community Development (EDC Meldal lead)
  - Outreach (OUR Bajcsy lead)

Network Embedded Systems: Open Experimental Platform

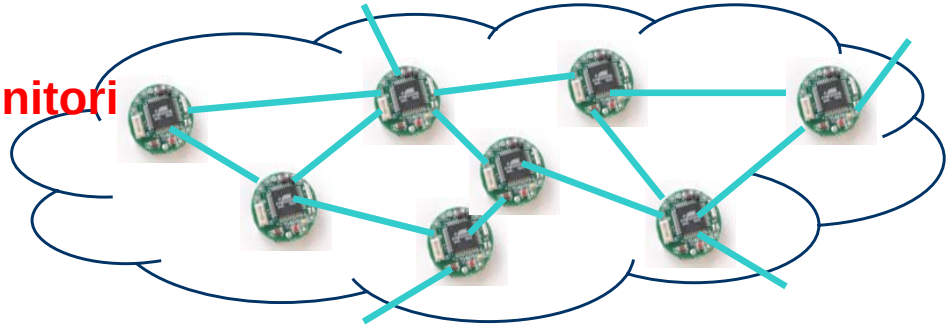
- Focused on low power
- Sleep - Majority of the time
  - Telos: 2.4μA
  - MicaZ: 30μA
- Wakeup
  - quickly to process and return to sleep
  - Telos: 290ns typical, 6μs max
  - MicaZ: 60μs max internal oscillator, 4ms external
- Process
  - Get your work done and get back to sleep
  - Telos: 4MHz 16-bit
  - MicaZ: 8MHz 8-bit
- TI MSP430
  - Ultra low power 1.8 V
    - 1.6μA sleep
    - 460μA active
- Standards Based
  - IEEE 802.15.4, USB
- IEEE 802.15.4
  - CC2420 radio
  - 250kbps
  - 2.4GHz ISM ban
- TinyOS support
  - New suite of radio stacks
  - Pushing hardware abstraction
  - Must conform to std link
- Ease of development and Te
  - Program over USB
  - Std connector header
- Interoperability
  - Telos / MicaZ / ChipCon

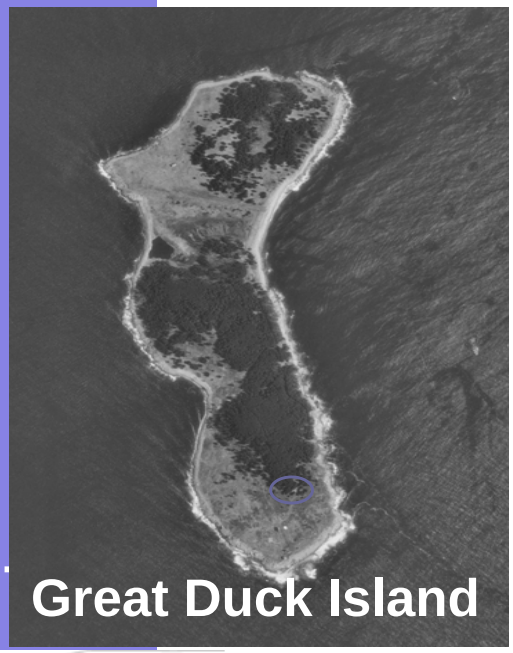
UCB Telos

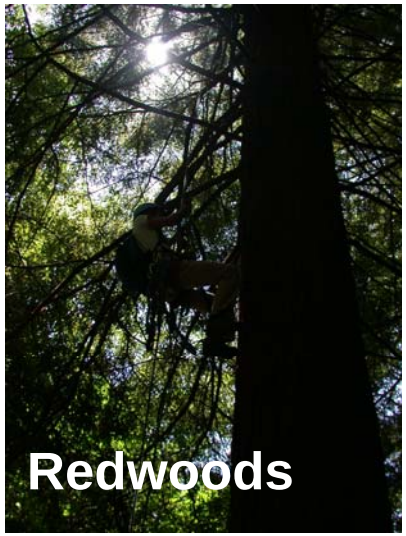
Xbow MicaZ

Ubiquitous Instrumentation

- **Understanding phenomena:**
  - **Data collection for offline analysis**
    - **Environmental monitoring, habitat monitori**
    - **Structural monitoring**

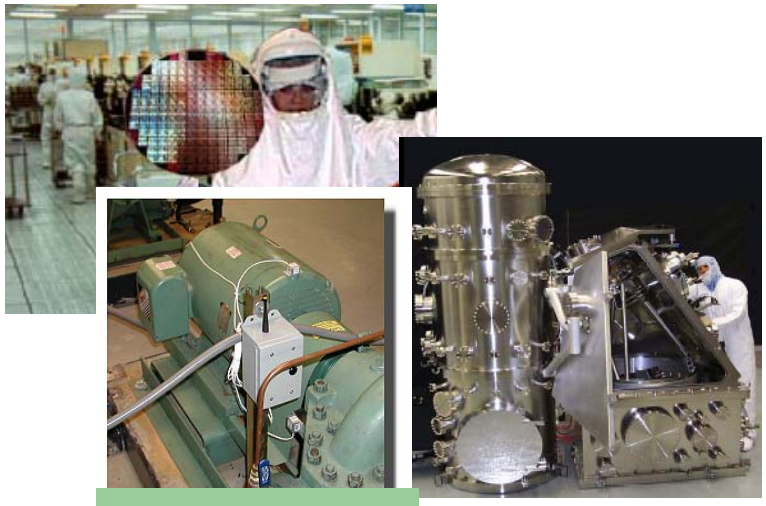




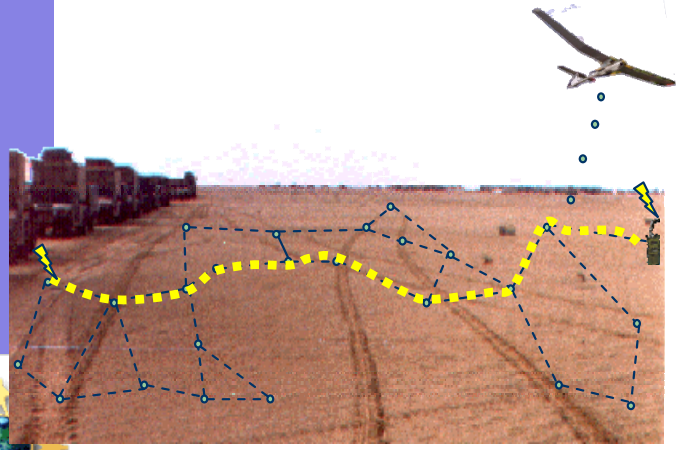


Sensor Webs Everywhere

- Understanding phenomena:
  - Data collection for offline analysis
    - Environmental monitoring, habitat monitoring
    - Structural monitoring
- **Detecting changes in the environment:**
  - **Thresholds, phase transitions, anomaly detection**
    - **Security systems, surveillance; health care**
    - **Wildfire detection**
    - **Fault detection, threat detection**



Intel Research

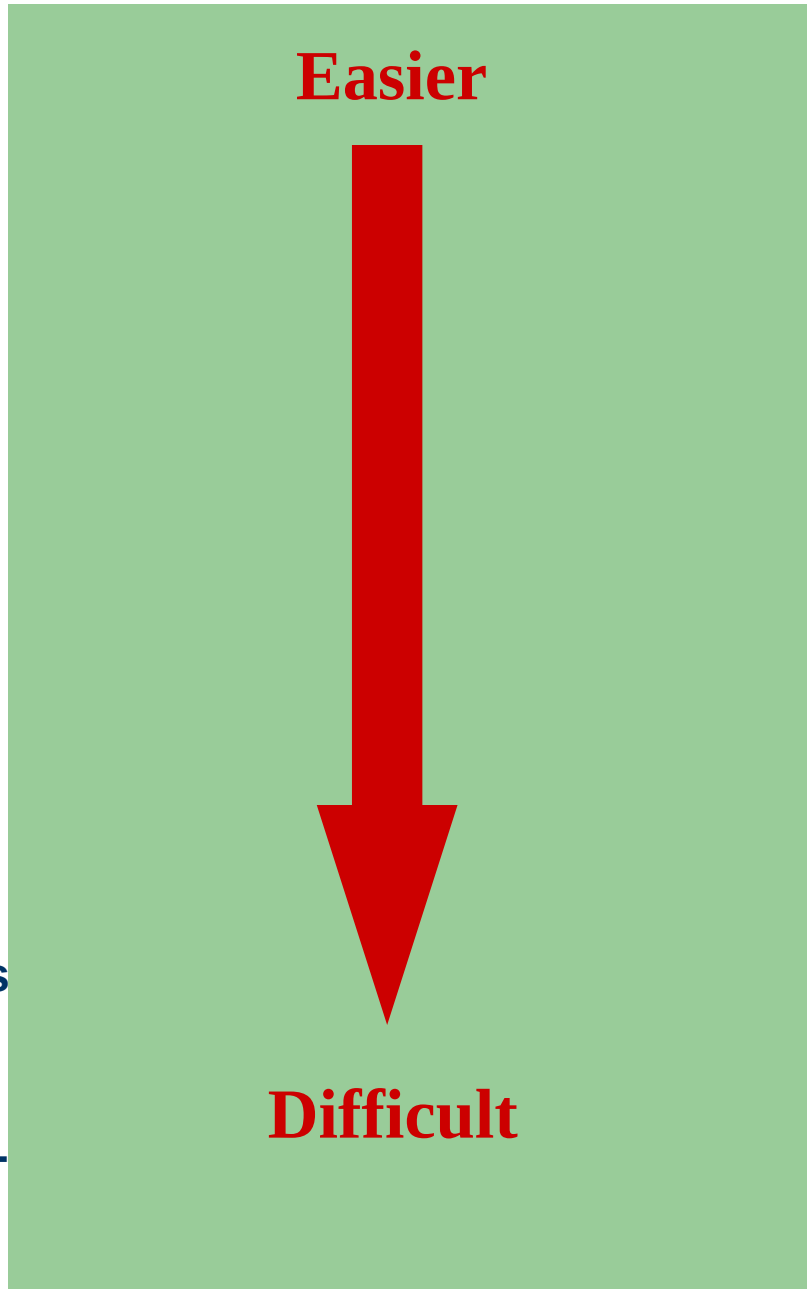


Fire Response

Health Care

Networked Embedded Systems Applications Taxonomy

- Understanding phenomena:
  - Data collection for offline analysis
    - Environmental monitoring, habitat monitoring
    - Structural monitoring
- Detecting changes in the environment:
  - Thresholds, phase transitions, anomaly detection
    - Security systems, surveillance
    - Wildfire detection
    - Fault detection, threat detection
- **Real-time estimation and control:**
  - **Traffic control, building control, environmental control**
  - **Manufacturing and plant automation, power grids SCADA networks**
  - **Service robotics , pursuit evasion games, active surveillance, search-and-rescue, and search-and-capture, telemedicine**



A Typical Industrial Facility: 40+ years old, $10B infrastructure

~2 Square Miles

1400 Employees

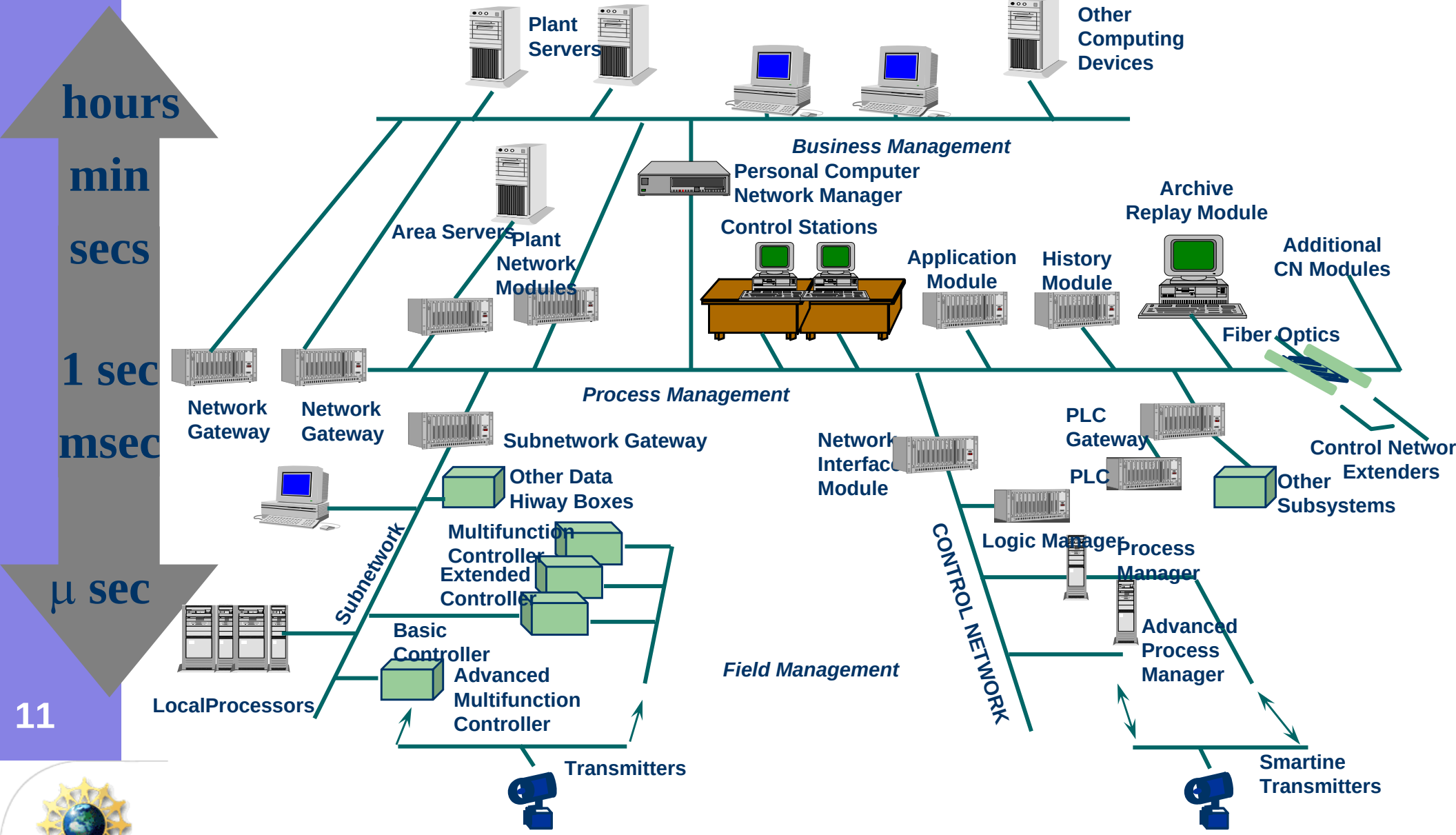
Operating Budge
$200M+/year

Primary products
Chlorine, Silica, Caustics

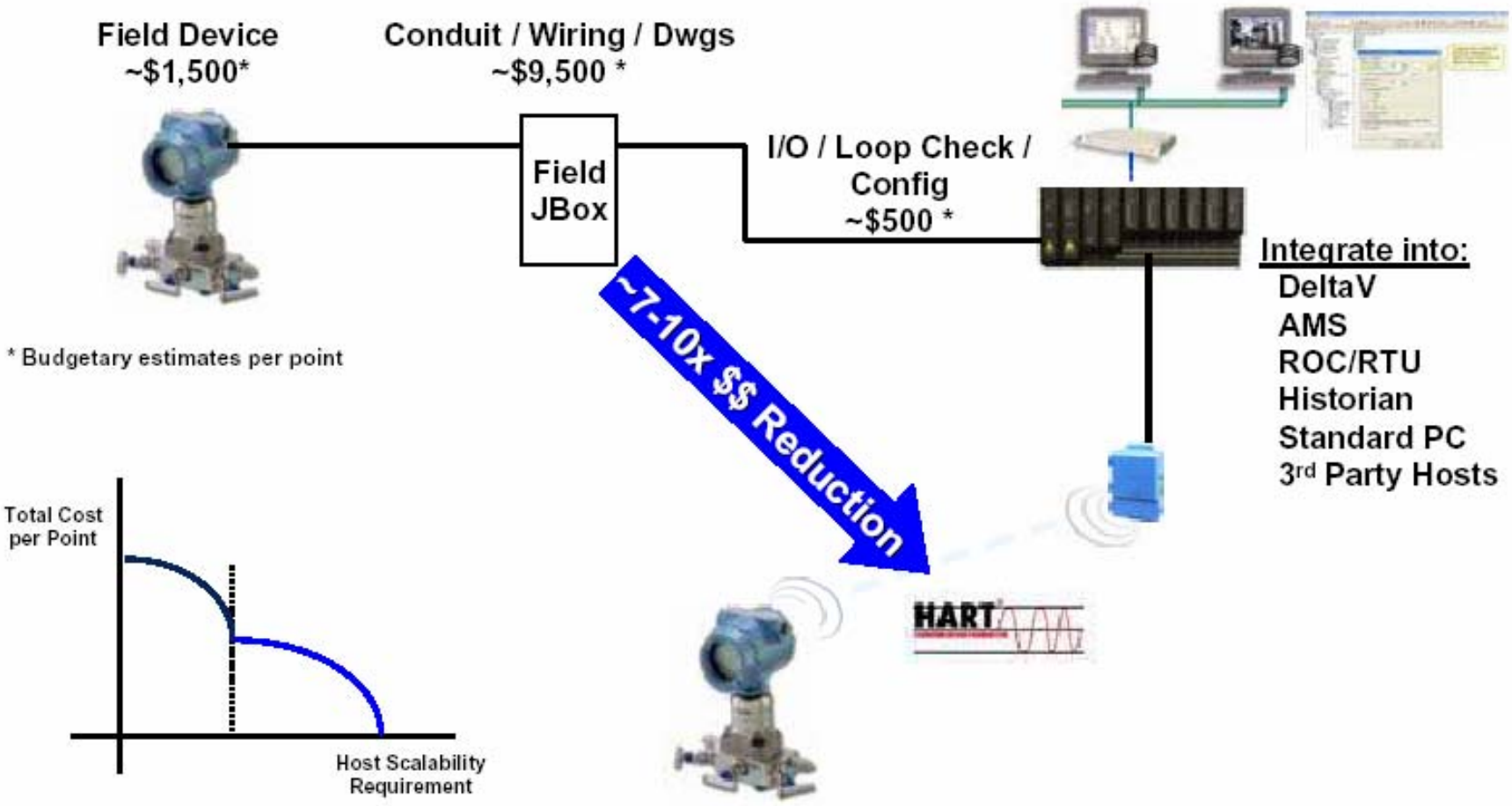
Highly profitable facility

DHS, OSHA, EP
compliance

The Plant: A Complex Environment



A Shift In Total Data Acquisition Cost Will Drive A New Asset Management Paradigm



Therefore, Self Org Nets Are Proving to be More Reliable, Easier to Use, & Cost Effective

Wireless HART (Self Organizing Networks)

Measurement	*	Communication	*	Data Management	=	99.99%
100%		99.99%		100%		

Traditional Point-to-Point Wireless (Proprietary)

Measurement	*	Communication	*	Data Management	=	~64%
~90%		~70%		~99%		

The overall system can only be as strong as the weakest link

Key Transition of WSN into SCADA

- Next generation SCADA will consist of wireless sensor networks: Emerson, Honeywell, Chevron count on ease of deployment
- Wireless sensor networks have grown to a $ 40 B business (Forrester) in the course of the last year. Secure SCADA is a key research and transition area from TRUST
- Next years: from SCADA to HVAC to automotive to security to embedded in the environment ubiquitously.

Sensor Networks in Public Places

- Protecting Infrastructure
  - Opportunities for embedding sensor networks
    - Transportation
    - Water and Fuel
    - Power Grid
  - TRUST is emphasizing development of supporting technology for randomly distributed sensors
- Buildings
  - Combine surveillance with energy control
  - Integrate into building materials
- Open Spaces (parks, plazas, etc.)
  - Combine surveillance with environmental monitoring
  - Line-of-sight surveillance technologies

Privacy Workshop

- "Exploring the Privacy Implications of Trustworthy Systems" - October 2006
- Two-day workshop for TRUST graduate students
- Researchers presented their work to TRUST faculty and nationally-recognized privacy-policy experts
  - **Kevin Bankston**, Electronic Frontier Foundation
  - **Janlori Goldman**, Health Privacy Project
  - **Jim Dempsey**, Center for Democracy and Technology
- Workshop identified privacy issues within students' research, and brainstormed on future interdisciplinary collaborations.

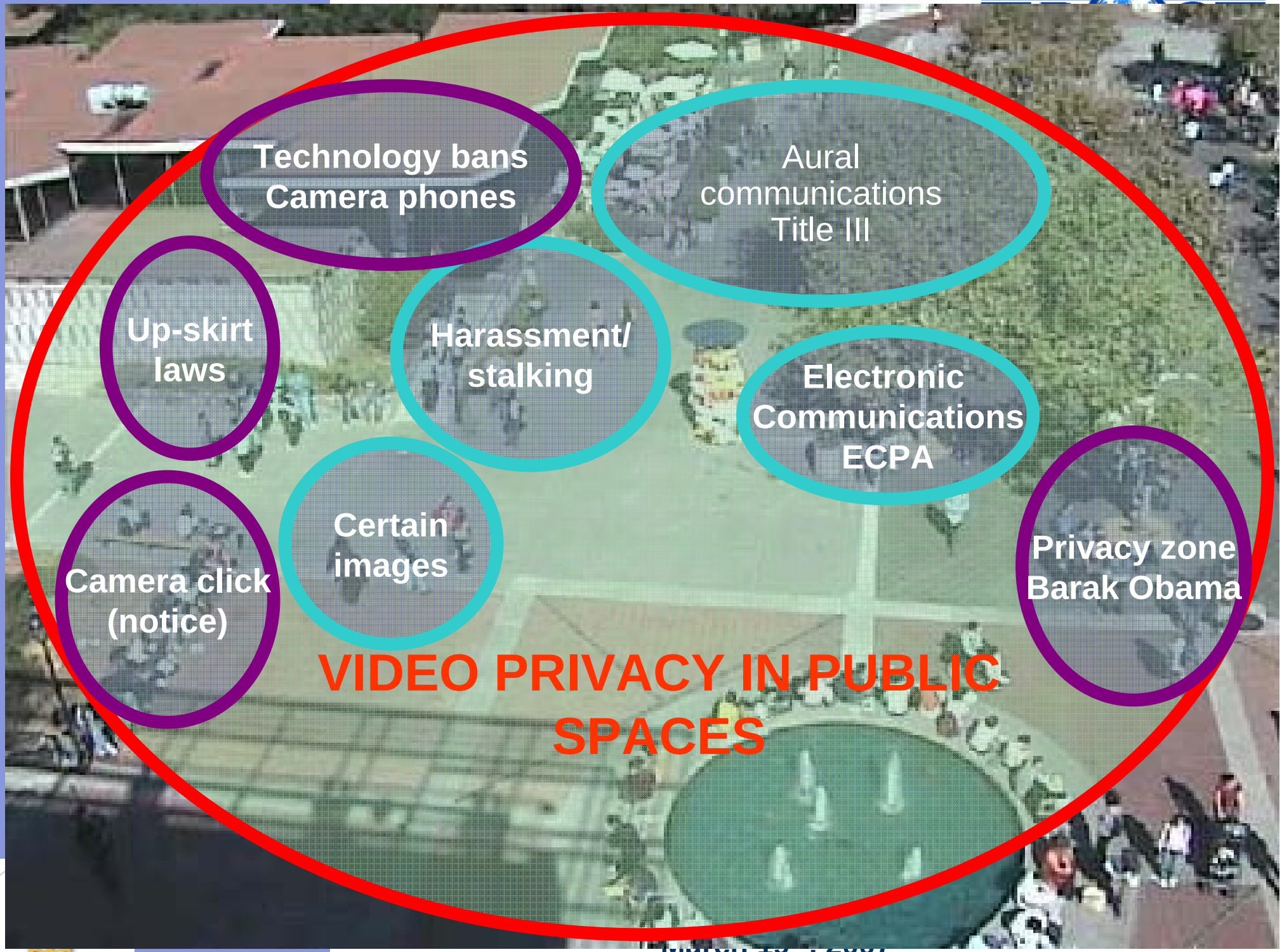
Visual Privacy Symposium

- "Unblinking: New Perspectives on Visual Privacy in the 21st Century"
- Symposium discussed the implications of increased network surveillance, cameras in public places, and public policy responses to this technology
- Participants included US and international experts in art, law, engineering, psychology, architecture, urban planning, sociology, human rights

Respectful Cameras: Background

- New class of Robotic Cameras since 9/11/2001
  - $20,000 -> Under $1,000
  - Static -> Pan, tilt, zoom (21x)
- UK - 3 Million Outdoor Cameras
- Now Deploying in Large US Cities, such as San Francisco: working with City IT manager


LOCAL TIME
CAPTURE IMAGE


Technology bans
Camera phones
Aural communications
Title III
Up-skirt laws
Harassment/ stalking
Electronic Communications ECPA
Certain images
Camera click (notice)
Privacy zone
Barak Obama
VIDEO PRIVACY IN PUBLIC SPACES

Objective of Respectful Cameras

PHISHING and Spyware Impact Stats

- Phishing (February 2007 numbers)
  - 3.5 million Americans gave up sensitive information in 2006, 84 % jump from previous year
  - Targets: Banks, credit card companies, Web retailers, online auctions (E-bay) and mortgage companies,11,976 unique sites in May 2006, financial services 92% of sites.
  - Total money lost $ 2.8 B
- ID Theft (March 2007 numbers)
  - 15 million Americans for year ending July 2006
  - Average loss $ 2357 per person in 2006 compared with $ 1408 in 2005
- Spyware: Software that collects personal information from you without your knowledge or permission
  - 15 percent of enterprise PCs have a keylogger
  - Number of keyloggers jumped three-fold in 12 months
  - 50 % of crashes caused by spware (Microsoft Watson)
  - Dell, HP, IBM: Spyware causes ~30% of calls
  - Estimated support costs at $2.5m+ / day
- Chris Hoofnagle testimony to Senate Finance Committee March 21st
  - Problems with estimates: high estimates $ 100s of B, low estimates $ 10s of B, owing to methodology
  - Require Financial institutions to disclose comprehensive data?
  - Numbers will show increase of synthetic identity theft, help germinate anti-identity theft market

Source: Gartner Research, Webroot's SpyAudit, Sophos
Concerns about methodology: self reported/phone interviews

TRUST client side tools

- PwdHash: (Computer World 2006 Horizon Award!)
  - Browser extension for strengthening pwd web authentication
- Dynamic Security Skins: (Start Up spin off)
  - Allows a remote web server to prove its identity using a photograph to create trusted path
- SafeHistory and SafeCache: (WWW '06)
  - Firefox extension that blocks (adaptive) super-phish attacks
- SpyBlock:(http://www.getspyblock.com)
  - Spyware/Malware protection using virtual machines
- Newer Work
  - Minesweeper, Panorama: malware detectors
  - BotSwat: Bot-net zombie detection system
  - Web Server timing attacks: Spear Phishing

Tech Transfer from Phishing Work

- SpoofGuard: Huge Number of News Articles!!
  - Some SpoofGuard heuristics now used in eBay toolbar and Earthlink ScamBlocker.
- PwdHash
  - RSA Security (www.pwdhash.com)
  - Initial integration into IE completed
  - Hope to convince IE team to embed natively in IE
- SpyBlock
  - Available at http://getspyblock.com/
  - Relevant companies: Mocha5, VMWare
  - Dialog with companies concerned with transaction generators
  - Free version (source code) running on Firefox
- Dynamic Security Skins
  - Start Up by Rachna Dhamija
- SafeHistory:
  - Microsoft, Mozilla.
  - Available at www.safehistory.com

Integrative testbeds:
Cyber Defense Technology and Experimental Reseach Network: DETER

- Lack of experimental infrastructure
  - Testing and validation in small to medium-scale private research labs
  - Missing objective test data, traffic and metrics
- Create reusable library for conducting realistic, rigorous, reproducible, impartial tests
  - For assessing attack impact and defense effectiveness
  - Test data, test configurations, analysis software, and experiment automation tools
- 400 PCs: vendor neutral: Real Systems, Real Code and Real Attacks
  - Nodes can be used as clients, routers, servers
  - Study rare events

CyberStorm: DHS Exercise, Sept 06

- Exercise in Feb 06, Report released September 06: controlled environment to exercise coordinated cyber incident response to largest and most complex attack to date on multiple critical infrastructures: energy, financial and telecom
- Over 100 public and private agencies from over 60 locations and 5 countries, DETER testbeds used to simulate some of the attacks.
- Findings Released to Federal Agencies, 30 private sector companies for defense and recovery efforts.
- DHS has decided to pick up NSF-DHS funded DETER testbed and make it an operational longterm testbed DECCOR starting Oct 1, 2006. Available to all TRUST researchers
- Joseph (Berkeley) and van Renesse (Cornell) are building an additional node at Cornell using an AF DURIP and are making it available to AFRL-IF, Rome Labs for cyber warfare defense exercises for command and control and other tactical networks.

Key Findings of Cyber Storm

- Interagency Coordination Mechanisms
- Contingency Planning and Risk Assessment: Roles and Responsibilities
- Correlation of Multiple Incidents between private and public sectors
- Exercise Program
- Coordination between entities of cyber incidents
- Common Framework for Response and Information Sharing
- Strategic Communications and Public Relations Plan
- Improvement of Process, Tools and Technology; especially SCADA!

Education Objectives

Combine push (bottom-up) and pull (top-down) strategies to maximize impact

- Engage new generation of researchers and instructors in advanced research
- Generate learning material (learning modules, course syllabi, textbooks, broader curricula) and extract best of breed from existing learning material
- Effective Disemination Solutions (on-line repositories, summer schools, center-wide seminar series)
- Establish Broad Educator Communities (through summer schools, WISE, conference participation)

Education Plans

- Learning Material Development
  - Each research project generates teaching modules
  - Curriculum Needs Assessment by Industry CSO group
  - Senior/Masters level security course for specialist CS majors
  - Senior level courses for non CS Engineering majors
  - CS course modules throughout CS curriculum for non specialist CS majors
  - News story driven seminar: yesterday's science, today's science, and tomorrow's technology
- Interdisciplinary curriculum for training next generation of science and technology policy makers in trustworthy systems
  - explore privacy implications (CSOs)
  - study the effect of policy on privacy (CPOs)
  - translate research for policymakers (briefing policy makers)

Briefing Policy-Makers

- Federal Trade Commission
  - Participated in “Protecting Consumers in the Next Tech-ade” sessions on:
    - Computing Power and How it Will be Used in the Marketplace of the Next Tech-ade
    - Communicating with Consumers in the Next Tech-ade : The Impact of Demographics and Shifting Consumer Attitudes
    - New Products - New Challenges
  - Presented at “Negative Options Workshop” regarding effect of “short-notices” for consumers before installing software
- Department of Homeland Security
  - Testified before DHS Security Data Privacy and Integrity Advisory Committee.
- California Energy Commission
  - Held seminar for Commissioner Rosenfeld on security and privacy concerns re: “demand response” energy systems
  - Working with CEC to facilitate their access to data for energy forecasting & conservation in a way that protects privacy

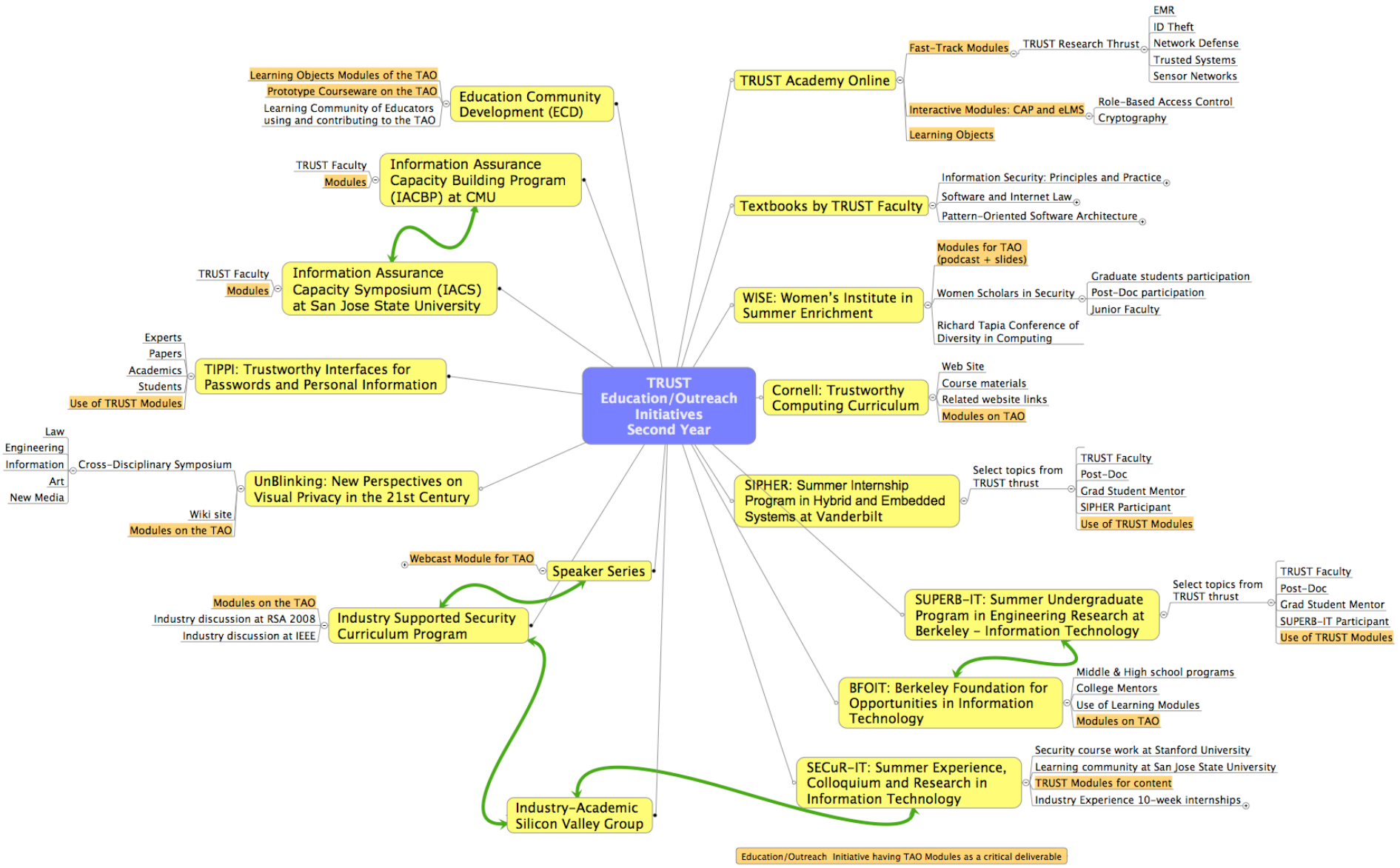
Briefing Policy-Makers (contd.)

- Invited to testify before Senate Subcommittee on Terrorism, Technology & Homeland Security
- Briefed House and Senate on TRUST
  - Offices of Senators Feinstein, Boxer, Rockefeller, Webb
  - Senate and House Committees on the Judiciary
  - Offices of Representatives Lofgren, Lee, Eshoo
- Participated in the Congressional Internet Caucus's "State of the Net" conference.

Education Plans (Continued)

- Dissemination Structure
  - TRUST Academy Online (TAO) leveraging repository based infrastructure technologies developed by VanTH ERC: CAPE/eLMS
  - Summer and Winter Educational Retreats and Summer School
  - TRUST textbook series
- Education Community Development
  - Making re-targetable courseware
  - Establishing broad community of educators that utilize resources provided through infrastructure
  - Teaching the teachers

Education and Outreach Initiatives, 2nd Year



OUTREACH Strategy

We are engaged in two kinds of outreach activities:

- Structured Outreach Activities:
  - WISE
  - SUPERB
  - SIPHER
  - BFOIT
  - Capacity Building Program
  - AMP
- Educational Outreach Activities:
  - Stanford Computer Security Course for industry professionals,
  - Berkeley, Cornell efforts to educate government professionals
  - TRUST Outreach efforts with Smith, Mills

Structured Outreach

- BFOIT - Berkeley Foundation for Opportunities in Information Technology http://www.bfoit.org/
  (Nurturing underrepresented high school students and their teachers in TRUST areas: Bajcsy, Sastry personal participation and fund raising.)

- SUPERB-IT-TRUST - Summer Undergraduate Program in Engineering Research at Berkeley - Information Technology http://www.eecs.berkeley.edu/Programs/ugrad/superb/superb.html
  (Increased number of under-represented students by 4)

- SIPHER - Summer Internship Program in Hybrid and Embedded Software Research http://fountain.isis.vanderbilt.edu/fountain/Teaching/
  (Increased number of underrepresented students by 2)

- Pennsylvania Area HBCU Outreach - Historically Black Colleges and Universities http://is.hss.cmu.edu/summer.html
  (Increased number of underrepresented students by 5)

Structured Outreach (Contd.)

- CMU CyLab Capacity Building Workshop
  - http://cylab.cmu.edu/default.aspx?id=2146
- Trustworthy Interfaces for Passwords and Personal Information: TIPPI workshop at Stanford
  - http://crypto.stanford.edu/TIPPI/
- WISE The Women's Institute in Summer Enrichment
  - http://trust.eecs.berkeley.edu/wise/
- AMP Alliance for Minority Participation
  - http://www.science.sjsu.edu/Default.htm

.

TRUST SUPERB 2006
Student Final Presentations

see also: trust.eecs.berkeley.edu/superb

Supervisor: Mike Eklund

Faculty Advisors: Shankar Sastry, Ruzena Bajcsy

Second Year Review
March 19th, 2007

TRUST SUPERB Summary

- 6 projects carried out by TRUST SUPERB Program in the Summer of 2006 (Mentors in parentheses):
  - Implementation of an Electronic Medical Record System
    - Sonny Hernandez, USC (Arsalan Tavakoli)
  - Camera Networks & Computer Vision for Healthcare Applications
    - Jamie Webb, University of Missouri-Rolla (Marci Meingast)
  - Design of Distributed Tracking System for Camera Networks
    - Jessica Jimenez, University of Puerto Rico (Edgar Lobaton)
  - Empirical Robustness Analysis of Wireless Connectivity In Sensor Network Deployments
    - Tonmoy Bhattacharjee, SUNY at Stony Brook (Phoebus Chen)
  - Time Synchronization Attacks/Countermeasures in Sensor Networks
    - Jocelyn Adams, Brown University (Tanya Roosta)
  - Towards Proactive Health Monitoring: Location-based statistical behavior modeling
    - Kaseima Frye, NCSU (Songhwai Oh)

IACBP+TRUST Expansion

- July 5-21, 2006 at the Distributed Education Center (DEC) at CMU targeted at Security Educators at HBCU. HSI
- Program run by Dr. Dena Tsamitis, Exec. Dir. IACBP
  - Detailed lectures in Security Engineering (from text book of the same name)
  - Topics include intrusion detection, firewalls, systems design, intrusion tolerant design, biometrics, computer ethics and society, visualization
  - Curriculum Development primers and discussion
  - CERT Curriculum Discussion
  - CISCO network security boot camp
  - Conference (SOUPS) Research preparation
- This year 9 participants: Spellman (2), Cal State-Dominguez Hills, Fullerton, LA, Northridge (5), Oakwood, Alabama A &M: 2 department chairs and 4 women
- SJSU to join CMU in offering IACBP from 2007 (Sigurd Meldal): supplemental NSF funding won!
- Will increase size and scope (doubling in 2007)

WISE-Center Outreach

- Women's Institute in Summer Enrichment (WISE): 1 week residential summer program in 2006 at Berkeley campus to bring together women (but it is not restricted to women only!) from all disciplines interested in TRUSTed systems
- Format has professors from across the country come to Berkeley to teach power courses in several disciplines, including computer science, economics, law, and electrical engineering.
- Format rigorous classes in the morning, and hands-on experiments and team-based projects in the afternoons.

Recruitment and Composition of the WISE program

- Applications for summer 2006 were posted on the website :http://trust.eecs.berkeley.edu/wise/
- Our tuition fee for summer 2006 was set to $1,500 -- applicants with financial need may request a fee waiver on the application form.
- 20 participants was selected from a nationwide applicant pool of young women and men who have demonstrated outstanding academic talent
- 19 out of the 20 participants in 2006 were women
- 13 graduate students (11 PhD + 2 MD), 4 Asst. Profs., 3 Assoc. Profs. 2 Af Am + 1 Hispanic Am.
- Speakers include Feigenbaum (Yale), Irvine (Naval Postgraduate School), Wright (Stevens), Xue (Vanderbilt), Fahmy (Purdue), Lerner (Berkeley Law), Wing (CMU), Sastry, Raghavan (Berkeley).

SUMMARY

- TRUST has been successfully launched, now in boost phase for research, education, outreach programs
- Hallmark of TRUST: Grand Challenge Projects
  - Large Integrative Projects
    - Identity Theft, Phishing, Spyware Defenses
    - Secure Network Embedded Systems
    - Trustworthy Systems
    - Secure Electronic Patient Records Portal
    - Network Defense
  - Education: Large Projects
    - Repositories: Evaluation using Learning Theory
    - Modules for existing courses
    - TRUST Summer School
  - Outreach: Comprehensive
    - BFOIT, SUPERB, SIPHER
    - Capacity Building Program for HBCU/HSI
    - WISE outreach to women researchers