NSF

TRUST
Team for Research in Ubiquitous Secure Technology

TRUST: Team for Research in Ubiquitous Secure Technology

TRUST Center Overview

Shankar Sastry
TRUST Director
Dean of Engineering, University of California, Berkeley

NAE GUIRR Meeting, Washington, Feb 2011

Berkeley UNIVERSITY OF CALIFORNIA
Carnegie Mellon
Cornell University
San José State UNIVERSITY
STANFORD UNIVERSITY
VANDERBILT UNIVERSITY

Outline

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

TRUST Overview

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 cybersecurity 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 2010-11

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

San José State
UNIVERSITY

STANFORD
UNIVERSITY

VANDERBILT
UNIVERSITY

Supporting Disciplines

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

TRUST Overview (cont.)

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/Diversity

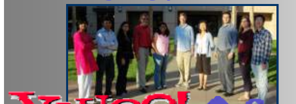
Curriculum development and teaching the next generation of computer / social scientists and engineers

TRUST Academy Online

Textbooks

INFORMATION SECURITY
Kenneth P. Birman
Reliable Distributed Systems
Technologies, Web Services, and Applications
Springer

SECuR-IT



YAHOO!
Sun microsystems
RAPPORT
ebay

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
- 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
TATA
TATA CONSULTANCY SERVICES
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 Research

Research Thrust #1: Financial Infrastructures

Scope and Objectives:

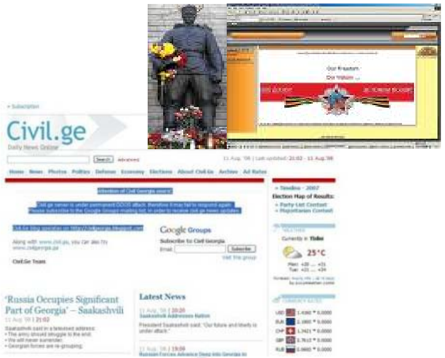
Trustworthy environment that links and supports commercial transactions among financial institutions, online retailers, and customers.

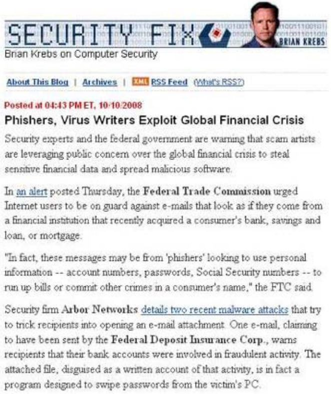
Fundamental Challenges:

- 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
  - 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 <u>and</u> 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





Brian Krebs on Computer Security

About This Blog | Archives | XML RSS Feed (What's RSS?)

Posted at 04:43 PM ET, 10/10/2008

Phishers, Virus Writers Exploit Global Financial Crisis

Security experts and the federal government are warning that scam artists are leveraging public concern over the global financial crisis to steal sensitive financial data and spread malicious software.

In an alert posted Thursday, the **Federal Trade Commission** urged Internet users to be on guard against e-mails that look as if they come from a financial institution that recently acquired a consumer's bank, savings and loan, or mortgage.

"In fact, these messages may be from 'phishers' looking to use personal information -- account numbers, passwords, Social Security numbers -- to run up bills or commit other crimes in a consumer's name," the FTC said.

Security firm **Arbor Networks** details two recent malware attacks that try to trick recipients into opening an e-mail attachment. One e-mail, claiming to have been sent by the **Federal Deposit Insurance Corp.**, warns recipients that their bank accounts were involved in fraudulent activity. The attached file, disguised as a written account of that activity, is in fact a program designed to swipe passwords from the victim's PC.

http://blog.washingtonpost.com/securityfix/

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

TRUST Research (cont.)

Research Thrust #2: Health Infrastructures

Scope and Objectives:

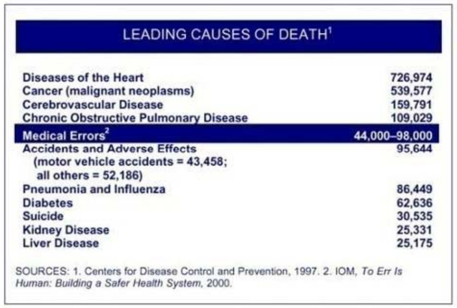
“Healthcare Informatics” that supports engaged patients, personalized medicine, and agile evidence-based care.

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

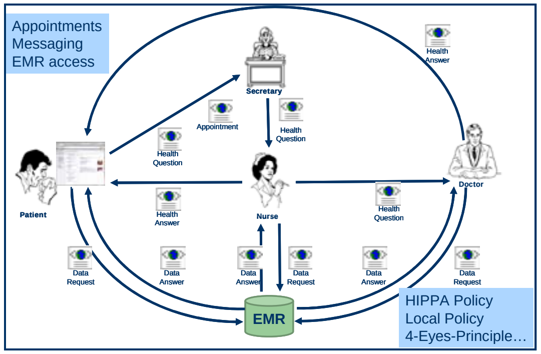
TRUST Research and Development:

- 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



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 (cont.)

Research Thrust #3: Physical Infrastructures

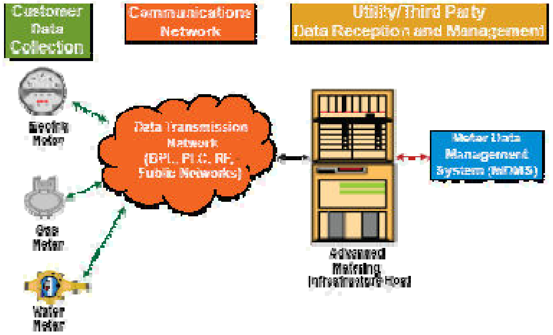
Scope and Objectives:

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

Advanced Metering Infrastructure


Customer Data Collection
Communications Network
Utility/Third Party Data Reception and Management
Electric Meter
Gas Meter
Water Meter
Data Transmission Network (BPL, PLC, RF, Public Networks)
Advanced Metering Infrastructure Host
Meter Data Management System (MDMS)

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 Education and Outreach

TRUST
Team for Research in Ubiquitous Secure Technology

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

Textbooks

Computer Security in the 21st Century
Information Security
Principles and Practice
Mark Stamp
Kenneth P. Birman
Reliable Distributed Systems
Technologies, Web Services, and Applications
Springer

…

Professional Development

ebay
RAPPORT
Sun microsystems
hp
salesforce
YAHOO!

DISSEMINATION

TRUST Academy Online

https://tao.truststc.org

TRUST Security Seminar

DIVERSITY

San José State University

ALLIANCE FOR MINORITY PARTICIPATION

HBCU Summer Partnership

H&SS Information Systems
Carnegie Mellon

TRUST-REU

Center for Underrepresented Engineering Students
University of California, Berkeley

Women's Institute in Summer Enrichment

TRUST Education and Outreach (cont.)

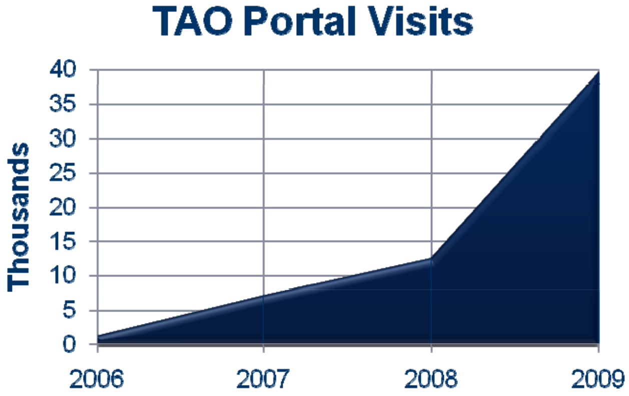
TRUST Academy Online (TAO)

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

TRUST
Courseware
Projects
Welcome to the TRUST Academy Online (TAO) Portal
Building Trustworthy Patient Portals
TAO Courseware
Security Technology
TRUST Courseware

- **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



TRUST Knowledge Transfer Partners

External Partners/Sponsors Support 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
TATA CONSULTANCY SERVICES

EADS

OAK RIDGE National Laboratory

TELECOM ITALIA

hp

QUALCOMM

United Technologies

Government Agencies

NSF

National Security Agency – United States of America

Air Force Office of Scientific Research – United States Air Force

DARPA

U.S. Department of Homeland Security

AFRL

International Collaborators

iCAST
International Collaboration for Advancing Security Technology

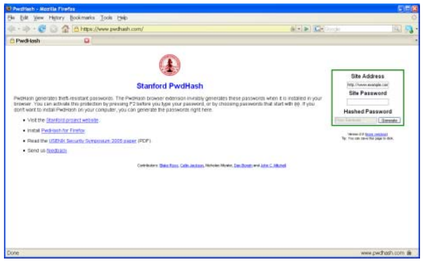
CSIT
CENTRE FOR SECURE INFORMATION TECHNOLOGIES

AMRITA-TIFAC CORE in CYBER SECURITY

* Including Microsoft's Trustworthy Computing Academic Advisory Board (Schneider, Mulligan Co-Chairs; Gligor member)

Engaging the Financial Community (cont.)

Early Knowledge Transfer in Web Security



PwdHash - Mozilla Firefox

https://www.pwdhash.com/

Stanford PwdHash

PwdHash generates theft-resistant passwords. The PwdHash browser extension invisibly generates these passwords when it is installed in your browser. You can activate this protection by pressing F2 before you type your password, or by choosing passwords that start with @@. If you don't want to install PwdHash on your computer, you can generate the passwords right here.

- Visit the Stanford project website.
- Install PwdHash for Firefox
- Read the USENIX Security Symposium 2005 paper (PDF)
- Send us feedback

Contributors: Blake Ross, Collin Jackson, Nicholas Miyake, Dan Boneh and John C. Mitchell

Site Address: http://www.example.com

Site Password:

Hashed Password: Generate

https://www.pwdhash.com/

PwdHash

- ❖ Web browser extension (Mozilla Firefox, IE 6/7)that transparently converts a user's password into a domain-specific password.
- ❖ User chooses passwords that start with a special prefix (@@) or by pressing a special password key (F2). PwdHash replaces the password with a one-way hash of the password/domain name. Target site sees domain-specific hash of the password, not the password itself.

SpyBlock - Mozilla Firefox

http://getspyblock.com/

SpyBlock

Stanford University

Abstract

Current phishing attacks focus primarily on stealing user credentials such as passwords. In response, web sites are deploying stronger authentication and backend analytics systems. These tools are designed to make it harder for phishers to extract value from stolen passwords. We anticipate that phishers will adapt in response. In particular, we expect to see huge growth in the use of a different type of botnet malware called a Transaction Generator or TG for short. A TG waits for the user to log in to his account at a site and then issues transactions on behalf of the user. We discuss a number of mechanisms by which TGs can hide their tracks so that users have no idea that fraudulent transactions were issued by their machine. We also describe a mitigation system, called SpyBlock, that can help reduce the damage caused by TGs.

Papers

- Collin Jackson, Dan Boneh, and John C. Mitchell
  Transaction Generators: Root Kits for the Web (pre-proceedings draft). To appear at HotSec '07.

Download

SpyBlock can defend against transaction generator malware. To use SpyBlock, you will need the following:

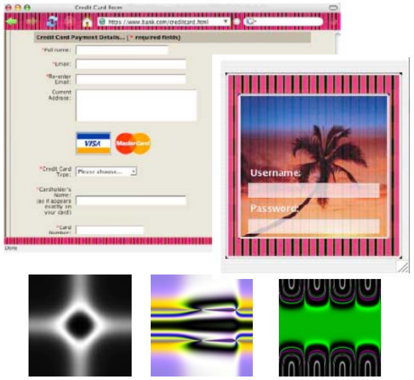
- Mozilla Firefox, a free, extensible, open source web browser.
- Windows Vista is the host operating system provider CardSpace, the identity selector.

File Edit View History Bookmarks Tools Help
Abstract Papers Download Related Staff
Done

http://www.getspyblock.com/

SpyBlock

- ❖ Web browser extension to reduce phishing by *Transaction Generators* (botnet malware) – code that captures user account information and generates fraudulent transactions after a user has logged into a website (e.g., online retailers, banks).
- ❖ Tool interacts with web browser and provides an authentication agent in a protected (VM) environment that works with user authentication programs (e.g., CardSpace in MS Vista) and provides a “transaction confirmation” capability.



Credit Card Form

https://www.bank.com/creditcard.html

Credit Card Payment Details... (* required fields)

*Full name:

*Email:

*Re-enter Email:

Current Address:

*Credit Card Type: Please choose...

*Cardholder's Name: (as it appears exactly on your card)

*Card Number:

Username:

Password:

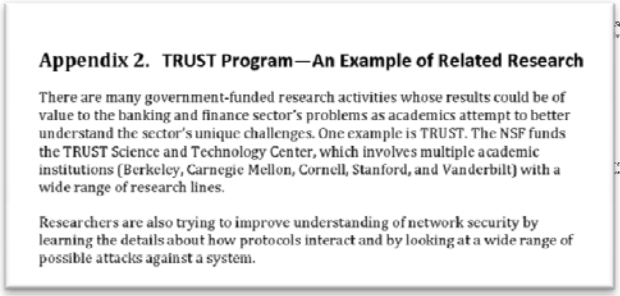
Dynamic Security Skins

- ❖ Security indicator based on user-defined images (versus programmer-defined indicators like SSL padlock icon). Images can be real photographs or randomly generated.
- ❖ Web browser “trusted window” includes the visual security indicator (image) and displays it at the point of login (username and password) entry so the user can not ignore it.

Engaging the Financial Community (cont.)

Government/Industry/Academia Workshop on Financial Infrastructure

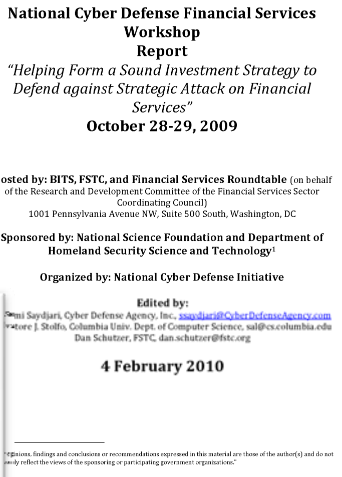
- National Cyber Defense Initiative
  - Vision: Over the next ten years, transform the cyber-infrastructure to be resistant to attack so that critical national interests are protected from catastrophic damage and our society can confidently adopt new technological advances
- National Cyber Defense Financial Services Workshop (Oct. 2009)
  - Government, Financial Industry, Academia participants
    - TRUST Investigators Mitchell, Birman organizers
  - Focus on high-impact, large-scale attacks on the banking and finance sector
  - Key Recommended Research Directions
    - Analytical Models
    - Collaborative Situational Awareness/Understanding
    - Resiliency
    - Authentication
    - **Leverage Research** →



Appendix 2. TRUST Program—An Example of Related Research

There are many government-funded research activities whose results could be of value to the banking and finance sector's problems as academics attempt to better understand the sector's unique challenges. One example is TRUST. The NSF funds the TRUST Science and Technology Center, which involves multiple academic institutions (Berkeley, Carnegie Mellon, Cornell, Stanford, and Vanderbilt) with a wide range of research lines.

Researchers are also trying to improve understanding of network security by learning the details about how protocols interact and by looking at a wide range of possible attacks against a system.



National Cyber Defense Financial Services Workshop Report

"Helping Form a Sound Investment Strategy to Defend against Strategic Attack on Financial Services"

October 28-29, 2009

Hosted by: BITS, FSTC, and Financial Services Roundtable (on behalf of the Research and Development Committee of the Financial Services Sector Coordinating Council)
1001 Pennsylvania Avenue NW, Suite 500 South, Washington, DC

Sponsored by: National Science Foundation and Department of Homeland Security Science and Technology[1]

Organized by: National Cyber Defense Initiative

Edited by:
mi Saydjari, Cyber Defense Agency, Inc., ssaydjari@CyberDefenseAgency.com
tore J. Stolfo, Columbia Univ. Dept. of Computer Science, sal@cs.columbia.edu
Dan Schutzer, FSTC, dan.schutzer@fstc.org

4 February 2010

pinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not ly reflect the views of the sponsoring or participating government organizations."

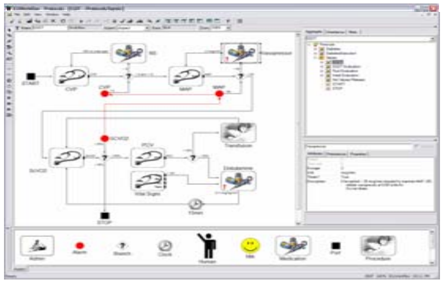
Full Report:
http://www.cyber.st.dhs.gov/docs/NCDI_FI_Workshop_Report.pdf

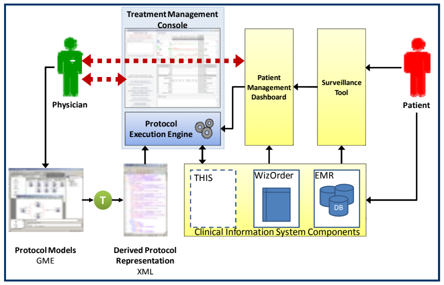
Engaging the Healthcare Community

STEEP: Sepsis Treatment Enhanced through Electronic Protocolization

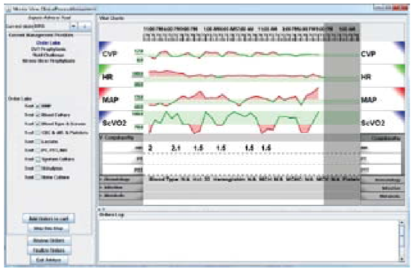
- **Hypothesis**
  - Electronic process management tool will increase adherence to *evidence-based practices*, improve objective *quality indicators*, and lead to *better clinical outcomes*.
- **Sepsis**
  - Common: ~750,000 cases/year
  - Deadly: ~25-35% mortality rate
  - Expensive: $17B/year (40% of ICU costs)
  - Treatable: Validated treatment protocols
- **Challenges**
  - Mathematically sound operational protocols, healthcare policies, and treatment guidelines
  - Protocol modeling language semantics
  - Protocol model validation /verification
  - 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.



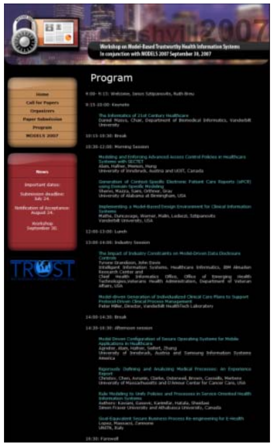

Treatment Management Console
Physician
Patient Management Dashboard
Surveillance Tool
Patient
Protocol Execution Engine
T
THIS
WizOrder
EMR
DB
Clinical Information System Components
Protocol Models
GME
Derived Protocol Representation
XML

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



Engaging the Healthcare Community (cont.)

- MOTHIS 2007 (Nashville) and 2008 (Toulouse)
  - International Workshop on Model-Based Design of Trustworthy Health Information Systems
  - ICSE workshop sequence on Health IT
  - Discussion on starting a new International Conference is in progress
- Dagstuhl 2009
  - Model-Based Design of Trustworthy Health Information Systems
  - 35 participants from US and EU
- Methods of Information in Medicine
  - Special Issue on Model-Based Design of Trustworthy Health Information Systems (2009)


Nashville 2007

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

Important dates:
Submission deadline: July 24
Notification of Acceptance: August 24
Workshop September 30

Program

9:00- 9:15: Welcome, Janos Sztipanovits, Ruth Breu

9:15-10:00: Keynote

The Informatics of 21st Century Healthcare
Daniel Masys, Chair, Department of Biomedical Informatics, Vanderbilt University

10:15-10:30: Break

10:30-12:00: Morning Session

Modeling and Enforcing Advanced Access Control Policies in Healthcare Systems with SECTET
Alam, Hafner, Memon, Hung
University of Innsbruck, Austria and UOIT, Canada

Generation of Context-Specific Electronic Patient Care Reports (ePCR) using Domain Specific Modeling
Sharvo, Mazza, Saini, Orthner, Gray
University of Alabama at Birmingham, USA

Implementing a Model-Based Design Environment for Clinical Information Systems
Mathe, Duncavage, Werner, Malin, Ledeczi, Sztipanovits
Vanderbilt University, USA

12:00-13:00: Lunch

13:00-14:00: Industry Session

The Impact of Industry Constraints on Model-Driven Data Disclosure Controls
Tyrone Grandison, John Davis
Intelligent Information Systems, Healthcare Informatics, IBM Almaden Research Center and
Chief Health Informatics Office, Office of Emerging Health Technologies,Veterans Health Administration, Department of Veteran Affairs, USA

Model-driven Generation of Individualized Clinical Care Plans to Support Protocol-Driven Clinical Process Management
Peter Miller, Director, Vanderbilt HealthTech Laboratory

14:00-14:30: Break

14:30-16:30: Afternoon session

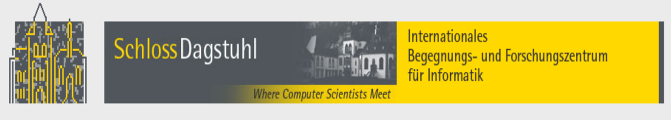
Model Driven Configuration of Secure Operating Systems for Mobile Applications in Healthcare
Agreiter, Alam, Hafner, Seifert, Zhang
University of Innsbruck, Austria and Samsung Information Systems America

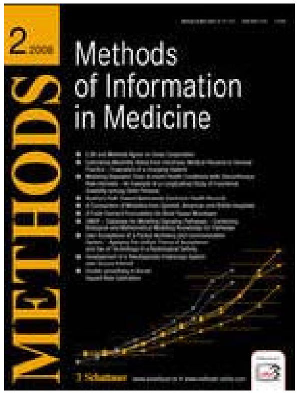
Rigorously Defining and Analyzing Medical Processes: An Experience Report
Christov, Chen, Avrunin, Clarke, Osterweil, Brown, Cassells, Mertens
University of Massachusetts and D'Amour Center for Cancer Care, USA

Rule Modeling to Unify Policies and Processes in Service Oriented Health Information Systems
Authors: Kaviani, Gasevic, Kaneddar, Hatala, Sheidaei
Simon Fraser University and Athabasca University, Canada

Goal-Equivalent Secure Business Process Re-engineering for E-Health
Lopez, Massacci, Zannone
UNITN, Italy

16:30: Farewell


Schloss Dagstuhl
Where Computer Scientists Meet
Internationales
Begegnungs- und Forschungszentrum
für Informatik


2 2008

Methods of Information in Medicine

METHODS

Schattauer

Engaging the SCADA Community

TRUST Leadership in Securing Critical Infrastructures

NITRD: EU-US Workshops on Security and Privacy of Wireless Sensor Networks (Washington, DC and Helsinki, Finland – 2006)

- Sastry and Wicker

NITRD: US-EU Workshops on Next Generation SCADA (Washington, DC, Pittsburgh, PA, Edinburgh, Scotland – 2007)

- Sastry, Sinopoli, and Krogh

VIKING: Major EU-IST project on security of SCADA systems with specific focus on smart grids and power systems (2009 – 2010)

- Sastry, Sinopoli

CPSWeek: First Workshop on Secure Control Systems at Cyber Physical Systems Week (Stockholm, Sweden – April 12, 2010)

- Sastry, Sinopoli, Sztipanovits

Idaho National Lab: Second Symposium on Security and Resilience of SCADA (Idaho Falls, Idaho – August 2010)

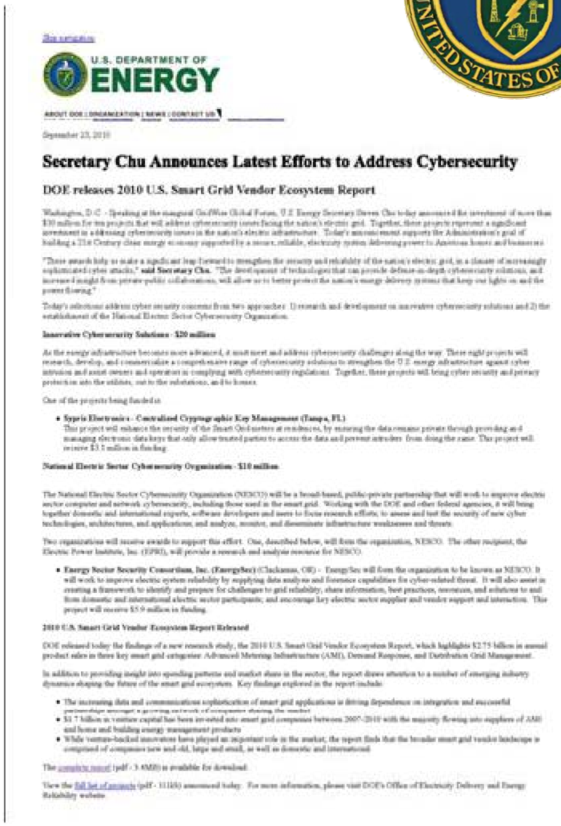
- Karsai, Sastry, Sinopoli, Wicker

Engaging the SCADA Community (cont.)

National Electric Sector Cybersecurity Organization Resource (NESCOR)

- Enhance collection and dissemination of threat and vulnerability information to industry.
  - Challenges to grid reliability, resiliency, and security.
  - Assist in developing strategies to protect the energy infrastructure.
- Develop strategies to protect the electric infrastructure.
  - Review and utilize NIST, NERC, and other cybersecurity requirements, standards, and results and identify gaps in cybersecurity capabilities.
- Support electric infrastructure reliability and cyber security solutions development.
  - Develop testing methodologies and facilitate performance of testing to review emerging security technologies in labs and pilot projects.
  - Participate in testing with electric sector stakeholders as well as conducting tests in EPRI's testbed.

EPRI | ELECTRIC POWER RESEARCH INSTITUTE


Skip navigation
U.S. DEPARTMENT OF ENERGY
ABOUT DOE | ORGANIZATION | NEWS | CONTACT US

September 23, 2010

Secretary Chu Announces Latest Efforts to Address Cybersecurity

DOE releases 2010 U.S. Smart Grid Vendor Ecosystem Report

Washington, D.C. - Speaking at the inaugural GridWeek Global Forum, U.S. Energy Secretary Steven Chu today announced the investment of more than $30 million for ten projects that will address cybersecurity issues facing the nation's electric grid. Together, these projects represent a significant investment in addressing cybersecurity issues in the nation's electric infrastructure. Today's announcement supports the Administration's goal of building a 21st Century clean energy economy supported by a secure, reliable, electricity system delivering power to American homes and businesses.

"These awards help us make a significant leap forward to strengthen the security and reliability of the nation's electric grid, in a climate of increasingly sophisticated cyber attacks," **said Secretary Chu.** "The development of technologies that can provide defense-in-depth cybersecurity solutions, and increased insight from private-public collaborations, will allow us to better protect the nation's energy delivery systems that keep our lights on and the power flowing."

Today's selections address cyber security concerns from two approaches: 1) research and development on innovative cybersecurity solutions and 2) the establishment of the National Electric Sector Cybersecurity Organization.

Innovative Cybersecurity Solutions - $20 million

As the energy infrastructure becomes more advanced, it must meet and address cybersecurity challenges along the way. These eight projects will research, develop, and commercialize a comprehensive range of cybersecurity solutions to strengthen the U.S. energy infrastructure against cyber intrusion and assist owners and operators in complying with cybersecurity regulations. Together, these projects will bring cyber security and privacy protection into the utilities, out to the substations, and to homes.

One of the projects being funded is:

- **Sypris Electronics - Centralized Cryptographic Key Management (Tampa, FL)**
  This project will enhance the security of the Smart Grid meters at residences, by ensuring the data remains private through providing and managing electronic data keys that only allow trusted parties to access the data and prevent intruders from doing the same. This project will receive $3.1 million in funding.

National Electric Sector Cybersecurity Organization - $10 million

The National Electric Sector Cybersecurity Organization (NESCO) will be a broad-based, public-private partnership that will work to improve electric sector computer and network cybersecurity, including those used in the smart grid. Working with the DOE and other federal agencies, it will bring together domestic and international experts, software developers and users to focus research efforts, to assess and test the security of new cyber technologies, architectures, and applications, and analyze, monitor, and disseminate infrastructure weaknesses and threats.

Two organizations will receive awards to support this effort. One, described below, will form the organization, NESCO. The other recipient, the Electric Power Institute, Inc. (EPRI), will provide a research and analysis resource for NESCO.

- **Energy Sector Security Consortium, Inc. (EnergySec)** (Clackamas, OR) - EnergySec will form the organization to be known as NESCO. It will work to improve electric system reliability by supplying data analysis and forensics capabilities for cyber-related threat. It will also assist in creating a framework to identify and prepare for challenges to grid reliability, share information, best practices, resources, and solutions to and from domestic and international electric sector participants; and encourage key electric sector supplier and vendor support and interaction. This project will receive $5.9 million in funding.

2010 U.S. Smart Grid Vendor Ecosystem Report Released

DOE released today the findings of a new research study, the 2010 U.S. Smart Grid Vendor Ecosystem Report, which highlights $2.75 billion in annual product sales in three key smart grid categories: Advanced Metering Infrastructure (AMI), Demand Response, and Distribution Grid Management.

In addition to providing insight into spending patterns and market share in the sector, the report draws attention to a number of emerging industry dynamics shaping the future of the smart grid ecosystem. Key findings explored in the report include:

- The increasing data and communications sophistication of smart grid applications is driving dependence on integration and successful partnerships amongst a growing network of companies sharing the market.
- $1.7 billion in venture capital has been invested into smart grid companies between 2007-2010 with the majority flowing into suppliers of AMI and home and building energy management products.
- While venture-backed innovators have played an important role in the market, the report finds that the broader smart grid vendor landscape is comprised of companies new and old, large and small, as well as domestic and international.

The complete report (pdf - 3.8MB) is available for download.

View the full list of projects (pdf - 111kb) announced today. For more information, please visit DOE's Office of Electricity Delivery and Energy Reliability website.

Engaging the Government Community

TRUST
Team for Research in Ubiquitous Secure Technology

Security Policy and Advising + Leadership in Scientific Studies

U.S. House of Representatives

- Armed Service Committee: Schneider testified at hearing *Private Sector Perspectives on Department of Defense Information Technology and Cybersecurity Activities* (Feb. 2010).
- Committee on Energy and Commerce : Hoofnagle testified at hearing *Exploring the Offline and Online Collection and Use of Consumer Information* (Nov. 2009).
- Committee on Science and Technology: Schneider testified at hearing *Cyber Security Research and Development* (June 2009).

Office of Science and Technology Policy

- Hoofnagle provided written comments to the OSTP inquiry about use of cookies on Federal Government websites (July 2009).

Department of Defense

- AF SAB: Sztipanovits led summer study *Defending and Operating in a Contested Cyber Domain* (2008-2009).
- DSB/DDR&E: Schneider member of DSB and served on DDR&E ad hoc summer study *Cyber Security Technology Initiatives* (2010).

National Institute of Standards and Technology

- Schneider member of Information Security and Privacy Advisory Board (ISPAB) and Bajcsy member of Visiting Committee on Advanced Technology (VCAT) (2009-2010).

National Security Agency

- TRUST (Berkeley, CMU, Cornell, Stanford) “Science of Security” initiative (2009-2010).

Engaging the Government Community (cont.)

AF-TRUST-GNC (Air Force TRUST for GIG/NCES)

- Objective
  - Advance the state-of-the-art in cyber-assurance to address key trust- and QoS-related properties throughout the lifecycles of large-scale Air Force infrastructure associated with the Global Information Grid (GIG) and Network Centric Enterprise System (NCES).
- Research Areas
  - **Time-Criticality/Quality of Service** – Technologies compatible with COTS solutions that achieve scalable quality of service. Existing web services standards in use for GIG/NCES platforms don't focus on Air Force system needs of rapid response, scalability, bandwidth guarantees, fault-tolerance, and the ability to function under stressful conditions and over connections with strange properties (e.g., bursty loss, latency issues, route flaps).
  - **Information Assurance with Legacy Applications** – Research to achieve confidence in extremely complex systems-of-systems environments with interconnecting legacy applications by providing protection against malfunctioning components, predicting behavior in difficult conditions, and reasoning despite uncertainty, conflicting data.
  - **Secure Service Discovery/Mediation** – Tools that support the dynamic discovery requirements of military systems that often need to "discover" information sources securely despite enormous challenges (e.g., connectivity, bandwidth) and when systems may be mutually distrustful.
- Funding
  - PRET – $3.85M for 4 years (2006-2010)

Engaging the International Community

Recent International Partnerships and Collaborators

- **EU (EC-IST) Major Project VIKING**
  - Modeled after TRUST with focus on security of physical infrastructures: power, SCADA, process control, wireless infrastructures. Partners: Royal Institute of Technology, Stockholm (KTH), TU Berlin, Ericsson, ABB, Swedish power companies, ... Sastry is spending sabbatical with VIKING in Stockholm, sponsoring the first EU-US workshop on Secure Control Systems during CPS Week in Stockholm, April 2010.
- **Indian National Cybersecurity**
  - Amrita-TIFAC Core on Cybersecurity project coordinated through Ministry of S&T: plans to develop a Master of Advanced Studies to be offered to IT industry in India.
- **Italian National Project on Cybersecurity**
  - Modeled on TRUST coordinated by Finmeccanica: SELEX-IT with GWU for policy studies.
- **Centre for Secure Information Technologies (CSIT)**
  - National UK research center at Queen’s University Belfast modeled on TRUST (£30M funding over five years).
  - Investigating Data Security, Network Security, Wireless Security, and Intelligent Surveillance Systems.

Engaging the International Community (cont.)

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

iCAST

International Collaboration 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*

Engaging the International Community (cont.)

iCAST Success: Secure Wireless Overlay Observation Network (SWOON) Testbed

Testbed Overview

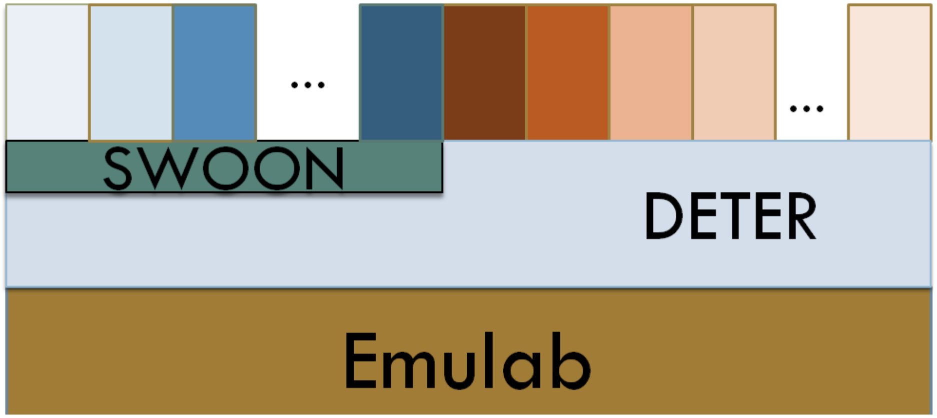
- ❖ First wireless security testbed
  - Attacks contained & observed
  - Comprehensive & flexible
- ❖ An emulation-based testbed (not simulation)
  - WSN, WiFi, WiMAX, Wired Networks
- ❖ Network topology dynamically adjusted

DETER/SWOON - TW

- ❖ Used by more than 80 organizations
- ❖ System re-engineered for reliability/ease of use
- ❖ Taiwan testbed in Hsin-Chu

Motivation and Approach

- ❖ Wireless security is important
  - Applications move to wireless networks
- ❖ Testing wireless security is hard
  - Infrastructure: big & expensive & contains attacks
- ❖ SWOON
  - First wireless testbed
  - Emulation (not simulation)
  - WSN, WiFi, WiMAX, Wired Networks
- ❖ Built on DETER
  - DETER supports only wired network
  - SWOON supports both wired & wireless network



Summary

- TRUST addresses challenge of building trustworthy systems
  - Multi-disciplinary team addressing fundamental cyber security and infrastructure problems inherently broader than the expertise of any single investigator.
  - Center projects have the breadth to incorporate privacy, legal, and policy issues.
- TRUST matches faculty expertise with problems of national interest
  - Top down and bottom up planning to pick areas
  - Renewal and assessment of performance on key integrative projects: center creates flexibility to do this
- TRUST has earned credibility, and influence
  - Industry (Security, Software, OEM/Vendors, Banking/Finance, Healthcare, Power, SCADA, Buildings, …)
  - Government (S&T Agencies, National Labs, Federal/State Lawmakers)
  - Military (Operational Needs, R&D, Studies)
  - Research Community (New Workshops and Conferences)

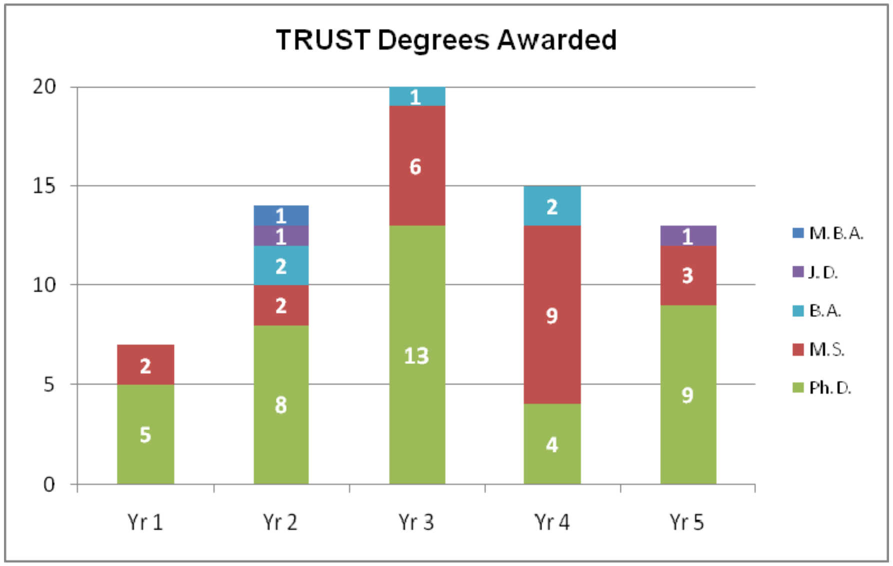
BACK UPS

TRUST Education and Outreach (cont.)

TRUST
Team for Research in Ubiquitous Secure Technology

HRD: Contributing to Pipeline of Security Researchers and Practitioners

- TRUST Degrees Awarded
  - Total of **69** graduates across partner institutions (2005 to date).
  - Average of **14** TRUST graduates per year with a peak of 20 graduates in Year 3 (2007-2008).
  - Variety of degrees/programs.
- TRUST STC Graduate Students
  - Graduates in a diverse set of fields: Academia, IT/Technology, Startups, Research, Law, …
  - Many directly leveraging TRUST.
- TRUST REU Undergraduates
  - Exposure to security topics, grad school environment, and research experience a positive influence in pursuing advanced degree.
  - 12 of 28 2006-2009 participants earned grad degree or in grad school.



Sameer Pai
Ph.D., ECE (Cornell , 2008)
Technical Advisor
Ropes & Gray

Marjan Aslani
B.S., EE (George Washington, 2009)
Summer 2008 TRUST-REU
First year Ph.D. EE student at Stanford

San José State University
Polytechnic University Puerto Rico
Stanford University
Berkeley University of California
Penn University of Pennsylvania
USC
The University of Wisconsin Madison

TRUST Knowledge Transfer (cont.)

Industry: Adoption/Use of Center Research Results by Commercial Partners

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

Electronic Medical Records

- Model-Based Trustworthy Health Information Systems (MOTHIS) 2007 & 2008 and Dagstuhl 2009: US and EU technologists + medical/legal/policy experts
- 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.

My Health at Vanderbilt
MOTHIS 2007
Nashville 2007
Workshop on Model-Based Trustworthy Health Information Systems
In conjunction with MODELS 2007 September 30, 2007
Schloss Dagstuhl
Where Computer Scientists Meet
Internationales Begegnungs- und Forschungszentrum für Informatik
Vanderbilt Home Care
Hearts and Minds at Home
TELECOM
PINE

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)

Privacy and Security Risks of RFID

Privacy and Security Risks of RFID Technology

<u>Goal</u>: Assess the privacy and security risks of RFID by exploring end-user comprehension of real and perceived risks

EVOLVING USES:

- Identification
  - *US e-Passport (2006)*
  - *PASS card (2008)*
  - *Enhanced drivers' licenses (Washington State, 2008)*
- Transit
  - *Automated tolls: EZ-Pass, FasTrak*
  - *Transit cards (in US: NYC, Atlanta, Bay Area), widespread in Europe*
- Payment
  - *Asia and EU: hybrid transit/payment cards*
  - *US: credit cards*

UNITED STATES OF AMERICA
PASSPORT CARD
PASS
The Enhanced Driver License and ID Card
WASHINGTON
PASSPORT
By land or by sea, Washington's passport alternative is faster, it's cheaper and it fits in your wallet.

This symbol means you can make Visa payWave payments at merchants displaying this symbol.

Look for the payWave symbol on the front of the card.

CONCERNS WITH RFID

Privacy

- Data - when static, data can be linked to individuals
- User Awareness - may not realize object contains a transponder
- Signaling - object may not notify user when data is read

Security

- Tracking/Hotlisting - both real time as well as database compilation
- Eavesdropping/Skimming - reading without knowledge or consent
- Cloning - tag data can be copied/cloned and reused

Increasing Ubiquity

- More tags and more readers builds a ubiquitous infrastructure
- More opportunities for surreptitious reads in public places

Government Use

- Often no choice with government-issued ID (e.g., e-Passport)
- Poor understanding by government officials of what RFID is, how it works, and implications of use

Home health Care: CareNet

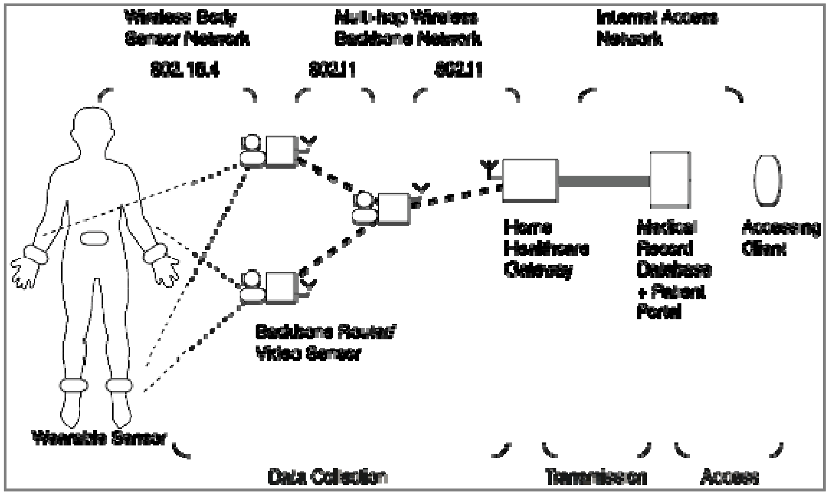
CareNet Body Sensor Network

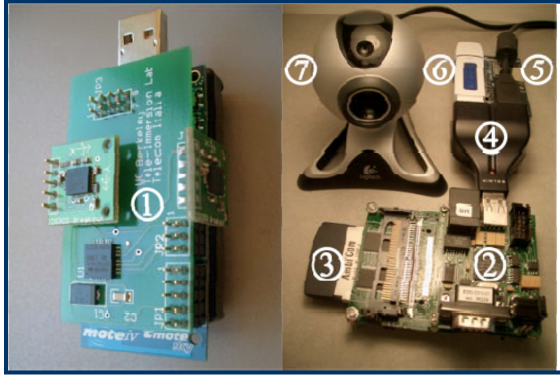
Vanderbilt Home Care

Hearts and Minds at Home

Secure Sensor Network System for Assisted Living in the Home

- Designed to ensure *integrity*, *availability*, and *confidentiality* of medical data and system information.
- Must provide *reliable*, *real-time*, *QoS-aware*, and *high-fidelity* patient data delivery capability.


Wireless Body Sensor Network
802.15.4
Multi-hop Wireless Backbone Network
802.11
802.11
Internet Access Network
Home Healthcare Gateway
Medical Record Database + Patient Portal
Accessing Client
Backbone Router/ Video Sensor
Wearable Sensor
Data Collection
Transmission
Access



① Sensor Mote
② Stargate
③ 802.11 CF Card
④ USB Hub
⑤ Base Station Mote
⑥ USB Storage Disk
⑦ Video Camera

- Two-tier wireless network for sensing, data forwarding, and image capturing.
- Scalability and optimization of 1st tier devices for wearability and 2nd tier devices for higher processing and bandwidth.

TRUST Knowledge Transfer (cont.)

TRUST
Team for Research in Ubiquitous Secure Technology

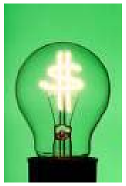
Government: Technology + Policy Advising

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

- CEC: Privacy of residential demand-response systems
- FTC: Identity management practices
- Data Breach Notification: California SB 1386 → 39+ states
- DHS: Privacy and security vulnerabilities of RFID
- USAF, NSA, DoD: Science of Security & Cyberwarfare
- US House: Science of Security & research in trustworthy systems

[illegible]



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*
- Led to establishment of CSIT (Queens U, Belfast)

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
£16.50 (inc VAT in UK)

HL Paper 165-I

Taiwan Science & Technology Advisory Group

- Review STAG panel investigating Taiwan's "Information-Communication Security" capabilities, August 2009
- Topics: global competitiveness, industry, education, e-government/e-commerce, health/medical

行政院科技顧問組
Science and Technology Advisory Group of Executive Yuan

TRUST Knowledge Transfer (cont.)

DoD / IC / Other: 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) for Network Centric Enterprise Systems (NCES)
- Time-criticality/quality of service with COTS and web services
- Legacy application/system-of-system information assurance

DHS/DARPA/NSF

- Desire for large-scale cyber network testing & evaluation
- Expand Berkeley/USC-ISI cyber testbed (DETER/DIPLOMAT/SWOON) architecture
- Leverage experimentation experience of TRUST DETER team for SCADA and wireless
- NSF/DHS *National Cyber Defense Financial Services Workshop* (Oct. 2009)

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 Science Board / DDR&E Advisory Board (2009)
- Science of Security (2009-10)