NSF Trustworthy Computing Program: Selected Healthcare-related projects

Briefing for IFIP WG 10.4

14 January 2011

What is NSF?

- The National Science Foundation (NSF) is an independent federal agency created by Congress in 1950:
- "to promote the progress of science; to advance the national health, prosperity, and welfare; to secure the national defense…"
- Annual budget of about $6.9 billion (FY 2010)
- Funding source for approximately 20 percent of all federally supported basic research conducted by America's colleges and universities

How Does NSF work?

- NSF's task of identifying and funding work at the frontiers of science and engineering is not a "top-down" process.
- **NSF operates from the "bottom up,"** keeping close track of research around the United States and the world, maintaining constant contact with the research community to identify ever-moving horizons of inquiry, monitoring which areas are most likely to result in spectacular progress and choosing the most promising people to conduct the research.

NSF Organization

Mathematical and Physical Sciences (MPS)
Assist. Dir
Dr. Edward Seidel,

Biological Sciences (BIO)
(Acting) Assist. Dir.
Dr. Joann P. Roskowski

Geosciences (GEO)
Assist. Dir.
Dr. Timothy L Killeen

Computer and Information Science and Engineering (CISE)
(**Acting**) Asst. Dir.→ **Dr. Farnam Jahanian**
Dr. Peter Arzberger **Due Mar. 2010**

Engineering (ENG)
Assist. Dir.
Dr. Thomas W. Peterson,

Social, Behavioral, and Economic Sciences (SBE)
Assist. Dir.
Dr. Myron Gutman,

Education and Human Resource (EHR)
(Acting) Assist. Dir.
Dr. Jaon Ferrini-Mundy

Director:
Dr. Subra Suresh

Division of Computing & Communication Systems Foundations
Dr. Susanne Hambrusch

Division of Computer and Network Systems
Dr. Keith Marzullo

Division of Information and Intelligent Systems
Dr. Howard Wactlar

Office of Cyberinfrastructure (OCI)
(Acting) Director
Dr. Alan Blatecky

Office of Integrative Activities
Director
Dr.W. Lance Haworth

Office of International Science and Engineering
Director
Dr. Larry H. Weber

Office of Polar Programs
Director
Dr.Karl A. Erb

CISE Cross-Cutting Programs

Trustworthy Computing (TwC)

Network Science and Engineering (NetSE)

Smart Health and Well-being (SHB)

Healthcare-related research at NSF

- NSF active awards containing “healthcare” in title or abstract: 277 active awards, e.g.,
  - Result-Oriented Multidisciplinary Capstone Design to Aid Persons with Disabilities
  - Theoretical extensions to advance understanding of the impact of the awareness of death
  - CPS: Medium: Collaborative Research: Body Area Sensor Networks: A Holistic Approach from Silicon to Users
  - TC:Large:Collaborative Research:Anonymizing Textual Data and its Impact on Utility
  - ...
  - The Effect of Government Procurement of Pharmaceuticals
  - CAREER: Machine Learning Based Intelligent Image Annotation and Retrieval

Trustworthy Computing
FY10 Large Awards by topic

Proposal Title	Proposal keywords	NITRD Theme
TC: Large: Securing the Open Softphone (Crovella, BU)	Secure hardware; cryptography; authentication; privacy; incentive-based security; network security	Tailored Trustworthy Spaces (TTS)
TC: Large: Collaborative Research: Towards Trustworthy Interactions in the Cloud (Bestavros, BU)	Cloud computing; security; privacy; applied cryptography; mechanism design; and distributed systems	TTS/Cyber Economics (CE)
TC:Large:Collaborative Research:Anonymizing Textual Data and its Impact on Utility (Clifton, Purdue)	Privacy; Anonymity; Data Mining	TTS
TC:Large: Nudging Users Towards Privacy (Acquisti, CMU)	Privacy; information security; behavioral economics; soft paternalism; usability; machine-	CE
TC:Large: Self Protecting Electronic Medical Records (Rubin, JHU)	Electronic Medical Records (EMR), Attribute-Based Encryption (ABE), HIPAA compliance	TTS
TC:Large:Collaborative Research:Practical Privacy: Metrics and Methods for Protecting Record-level and Relational Data (Gehrke, Cornell)	Synthetic data; data privacy; data utility; disclosure; confidentiality; privacy-preserving data publishing	TTS

Trustworthy Computing FY10 Medium awards by topic

Proposal Title	NITRD Theme
1. WHISPER -- wireless, handheld, infrastructureless, secure communication system for the prevention of eavesdropping and reprisal (Dick, U Mich)	TTS
2. Dissemination and analysis of private network data (Miklau, UMass)	TTS
3. Securing JavaScript web applications via staged policy enforcement (Jhala, UCSD)	TTS
4. From statistics to circuits: foundations for future on-chip fingerprints (Schaumont, VT)	TTS
5. Experience-based access management for hospital information technology (Gunter, Illinois / Malin, Vanderbilt)	TTS
6. Pay-as-you-go: security and privacy for integrated transportation payment systems	TTS
7. Security and privacy preserving data mining and management for distributed domains (Ghafoor, Purdue)	TTS
8. Towards formal, risk-aware authorization (Lee, PSU)	CE,TTS
9. Foundations, architectures, and methodologies for secure and private cyber-physical vehicles (Savage, UCSD)	TTS
10. The impact of operating system on application robustness (Solworth, UIC)	TTS
11. Privacy and Declassification Policy Enforcement Framework (Winsborough, UTSA)	TTS
12. Higher-level Abstractions for Trustworthy Federated Systems (Myers, Cornell)	TTS

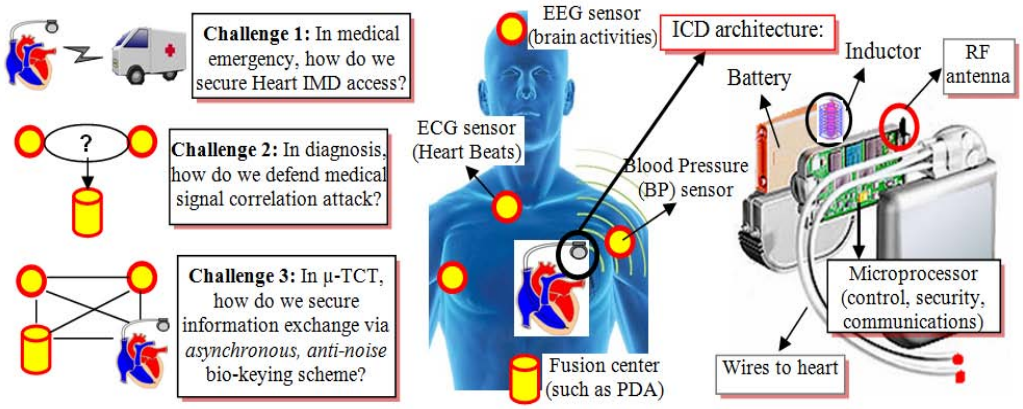
Selected Active TwC Healthcare-related Awards

1. NSF 0716455 Collab: CT-ISG: **Error-resistant, Accountable, RFID-assisted Wireless Sensor Networks for Elder Cardiac Tele-Healthcare**
   Start: 01-Aug-07, Fei Hu, U Alabama
2. NSF 0831244 CT-ISG: **Improving Security and Privacy in Pervasive Healthcare**
   Start: 01-Sep-08, Kevin Fu, U Mass
3. NSF 0712846 IPS: **Security Services for Healthcare Applications**
   Start: 01-Aug-07, Elisa Bertino, Purdue
4. NSF 0910842 TC: Large: **Trustworthy Information Systems for Healthcare IT**
   Start: 15-Jul-09, David Kotz, Dartmouth
5. NSF 0964392 CT: Collaborative Research: **Experience-Based Access Management (EBAM) for Hospital Information Technology**
   Start: 01-Apr-10, Carl Gunter, U Illinois
6. NSF 1010928 TC: Large: **Self Protecting Electronic Medical Records**
   Start: 01-Oct-10, Avi Rubin, Johns Hopkins
7. NSF 0716252 CT-T: MedVault – **Ensuring Security and Privacy for Electronic Medical Records**
   Start: 01-Sep-07. Doug Blough, Georgia Tech

Error-resistant, Accountable, RFID-assisted Wireless Sensor Networks For Elder Cardiac Tele-Healthcare

NSF #0716455:
Fei Hu Rochester Institute of Technology / U Alabama Tuscaloosa, with Yang Xiao, University of Alabama and others

- Goal: achieve an ultra-low-energy, medical-signal-adaptive security among medical sensors and implantable medical devices (IMDs)



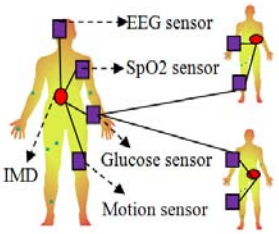
Approach / Progress

- Early work (2007)
  - studies of energy consumption of alternative crypto algorithms
  - collection architecture: sensors to cluster heads to gateway; all links encrypted
  - security analysis considers attacks on network components, including injection
- Recent work (2010): hardware implementation of NTRU lattice-based public key algorithm -- IEEE 1363.1, with trust modeling "Matryoshka" model
  - Secure heart IMD Emergency Access via Bi-directional Intentional Signal Interference;
  - Secure tele-cardiology diagnosis with the protection of medical data correlation;
  - Secure tele-cardiology data collection via asynchronous bio-keying based on Wavelet feature extraction

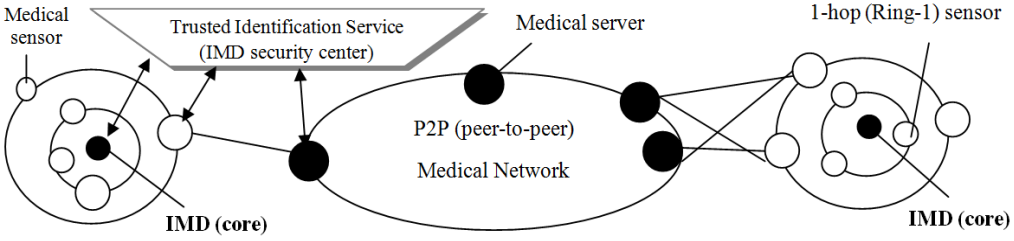
Project Outcomes




(1) RF Board (2) EKG sensor (3) EEG sensor (4) RFID



Proposed Matryoshka-based trust model (in implantable medical devices (IMDs) / medical sensor system) in a ring-shaped medical network topology



Publications

Partial list of publications

- Fei Hu, Yang Xiao, Qi Hao, “Congestion-aware, Loss-Resilient Bio-monitoring Sensor Networking,” *IEEE Journal on Selected Areas in Communications (JSAC),* VOL. 27, NO. 4, MAY 2009. Pages 450-465.
- Fei Hu, Meng Jiang, Mark Wagner and Decun Dong "Privacy-Preserving Tele-cardiology Sensor Networks: Towards A Low-cost, Portable Wireless Hardware / Software Co-design ", *IEEE Transactions on Information Technology in Biomedicine*, VOL. 11, NO. 6, NOVEMBER 2007, Pages 617-627.
- Fei Hu, Qi Hao, Qingquan Sun, Marcin Lukowiak, Kyle Wilhelm, and Stanisław Radziszowski, Yao Wu, “Trustworthy Data Collection from Implantable Medical Devices (IMDs) via High-speed Security Implementation based on Industry Standard IEEE 1363,” *IEEE Transactions on Information Technology in Biomedicine, Vol 14, Issue 6, Pages 1397-1404, November 2010.*

Improving Security and Privacy in Pervasive Healthcare

NSF Award: CNS-0831244

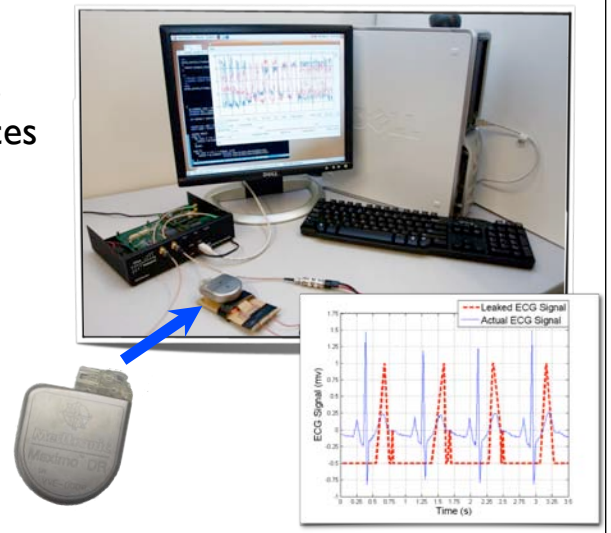
PI: Kevin Fu, UMass Amherst Computer Science

Goal: Discover ways to improve trustworthiness of wireless medical devices

Approaches:

- Zero-power security
- Security analysis
- Software radio
- Human subjects

IMD = Implantable Medical Device
ICD = implantable Cardioverter Defibrillator



Progress: Impact on Computing

Outstanding Paper award
IEEE Security & Privacy 2008

Awards and Recognition:

Outstanding Paper Award, IEEE Security and Privacy, 2009.
MIT Technology Review Magazine TR35 Innovator of the Year, 2009.
Sloan Research Fellowship, 2009.

Technology Transfer and Outreach:

Panel at Presidents Innovation and Technology Advisory Committee (PITAC), June 2010
FDA/FCC Workshop on Enabling the Convergence of Communications and Medical Systems, July 2010.
U.S. patent application filed on Zero-Power Security, 2009.

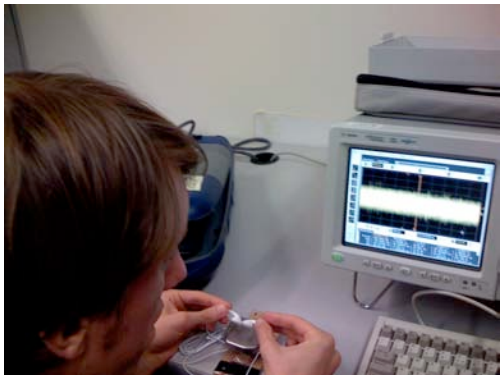
Selected Publications:

"Health information collaborative collection using privacy and security" by Molina et al. ACM Workshop on Security and Privacy in Medical and Home-Care Systems (SPIMACS), November 2009.
"Inside risks, reducing the risks of implantable medical devices: A prescription to improve security and privacy of pervasive health care" by Kevin Fu. CACM, 52(6), June 2009.
"Privacy of home telemedicine: Encryption is not enough" by Salajegheh et al. Journal of Medical Devices, 3(2), April 2009.
"Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses" by Halperin et al. IEEE Symposium on Security & Privacy, May 2008.
NOTE: simulation of human body with ground beef and bacon:

More at: http://prisms.cs.umass.edu/bibliography/kevin.php?val=all&format=display

PI: Kevin Fu, UMass Amherst Computer Science NSF Award: CNS-0831244

Progress: Impact on Public Health



Public Health Outreach:

"Headphones Can Disrupt Implanted Heart Devices" NPR All Things Considered, October 2009.
"A Heart Device Is Found Vulnerable to Hacker Attacks" New York Times, March 12, 2008.
"Heart-Device Hacking Risks Seen" Wall Street Journal, March 12, 2008.

Selected Publication:

"Clinically significant magnetic interference of implanted cardiac devices by portable headphones" by Lee et al.
Heart Rhythm Journal, October 2009.

PI: Kevin Fu, UMass Amherst Computer Science NSF Award: CNS-0831244

Open Medical Device Library

UMass Amherst Computer Science graduate research assistant Shane Clark sterilizes pacemakers and defibrillators to enable other researchers to experiment with innovative trustworthy computing mechanisms on medical devices.

PI: Kevin Fu, UMass Amherst Computer Science NSF Award: CNS-0831244

Interoperability, Privacy, and Security (IPS): Security Services for Healthcare Applications

NSF 0712846
PI: Elisa Bertino (*bertino@cs.purdue.edu*)
Purdue University

Goals

To investigate concepts and solutions for security services for healthcare applications with focus on three different classes of services:

- *digital identity management*
- *authentication management*
- *access control*

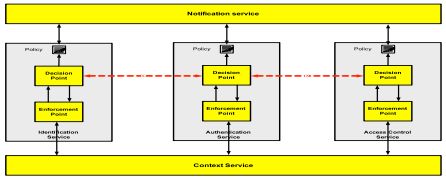
Approaches

Use of high-level declarative policies for service configuration, including novel policy languages for authentication, digital identity management, and access control

•Novel access control models and languages defined as extension of the well-known RBAC paradigm and their deployment in different contexts, including multidomain systems and streaming data

•Use of encryption techniques for access control and identity verifications

Security Pipeline



Main Results

•**FENCE** - a novel mechanism for continuous enforcement of access control policies in streaming environments
Application: patient monitoring

•**P-RBAC** - a privacy-aware RBAC system
Application: ensuring privacy for health-care data

•**VeryIDX** – a system for the privacy-verification of identity attributes based on the use of zero-knowledge proof protocols
Application: e-prescription

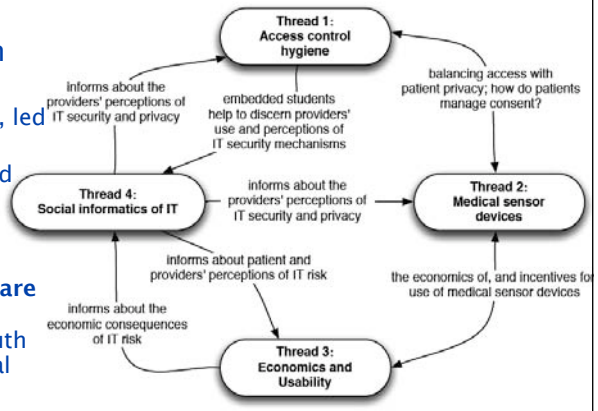
•**Multi-domain privacy-aware RBAC** – an RBAC system supporting inter-operation among multiple domains
Application: federation of healthcare providers

•Evaluation criteria for privacy policies in Personal Health Record systems

Trustworthy Information Systems for Healthcare (TISH)
PI: David Kotz, Dartmouth

- Goal: Drive innovation in information-sharing technology that ensures security and privacy while addressing the pragmatic needs of patients, clinical staff, and healthcare organizations to deliver efficient, high-quality care.

- **Approach:** Multidisciplinary team focusing on 4 research "threads".
  - **Access control in clinical settings**, led by Sean Smith (CS)
  - **Mobile healthcare (mHealth)**, David Kotz and Tanzeem Choudhury (CS)
  - **Economic and risk models**, Eric Johnson (Business)
  - **Social informatics of IT in healthcare organizations**, Denise Anthony (Sociology) and Ann Flood (Dartmouth Institute of Health Policy and Clinical Practice)



- **Scope:** Electronic Health Records (EHR), Personal Health Records (PHR), and mobile healthcare technologies (mHealth)

Outreach, Workshops, etc.

- Workshop
  - Securing IT in Healthcare (SITH), May 2010: 17 scholars, clinicians, and industry experts met with Dartmouth team members to address three challenges for IT in HC
    - 1) security and usability of mHealth technologies; 2) security and usability of EHRs; and 3) understanding of privacy and security risks of (1) and (2) to stakeholders
- Seminars
  - Two doctoral seminars (two sessions each) on the impact of implementing EMRs
  - One three-session seminar on EMRs considering the balance of need for access with the concern of privacy
  - One seminar on the state of the art of authentication in healthcare
- Speakers
  - Several experts invited to talk as part of ISTS speaker series and Health Policy Faculty Workshops
- Student Involvement
  - 8 graduate students, 10 undergraduates

Publications and Presentations

- Publications
  - **2011**
    - "Will HITECH Heal Patient Data Hemorrhages?" Proceedings of HICSS-44, International Conference on System Sciences, IEEE Computer Society.
    - "A threat taxonomy for mHealth privacy." Proceedings of the Workshop on Networked Healthcare Technology (NetHealth '11), IEEE Computer Society.
  - **2010**
    - "Information Security Failures and Security Investments in the Healthcare Sector," Proceedings of the Workshop on Information Security & Privacy (WISP10).
    - "Problematic Assumptions about Patients, Doctors and Healthcare," Proceedings of the Security and Privacy in Medical and Home-Care Systems Workshop (SPIMACS).
    - "What's Wrong with Access Control in the Real World?", IEEE Security and Privacy.
    - "Dr. Jekyll or Mr. Hyde: Information Security in the Ecosystem of Healthcare", 1st USENIX Workshop on Health Security and Privacy. HealthSec '10.
    - "Is Bluetooth the right technology for mHealth?", HealthSec '10.
    - "On Usable Authentication for Wireless Body Area Networks", HealthSec '10.
    - "Can I access your Data? Privacy Management in mHealth", HealthSec '10
    - "Institutional and Market Forces in Organizational Change: HIPAA Compliance in Acute Care Hospitals" Presented at the American Sociological Association Annual Meeting.

Publications and Presentations

- Publications
  - **2010** (continued)
    - "The Status of Health IT in the U.S. Healthcare System: Implications for Security, Privacy and Quality" Invited Talk Pitney Bowes 6th Annual Conference on Information Security and Communication.
    - "Healthcare Data Hemorrhages: Inadvertent Disclosure and HITECH_" Proceedings from the IEEE Symposium on Security and Privacy.
    - "Activity-aware ECG-based patient authentication for remote health monitoring", Proceedings of the International Conference on Multimodal Interfaces and Workshop on Machine Learning for Multi-modal Interaction (ICMI-MLMI).
  - **2009**
    - "A Privacy Framework for Mobile Health and Home-Care Systems", Proceedings of the Security and Privacy in Medical and Home-Care Systems Workshop (SPIMACS).
    - "HIPAA Compliance in Home Health: A Neo-Institutional Theoretic Perspective", SPIMACS.
    - Sara Sinclair, "Meta-Observations from an Outsider's Study of Clinical Environments", SPIMACS.
    - "HIPAA Compliance: An Institutional Theory Perspective" in Proceedings of the 15th Americas Conference on Information Systems.

CONTACT:

- Website: http://www.ists.dartmouth.edu/projects/healthit_security/tish/index.html
- Email: contact.tish@dartmouth.edu
- Phone: 603.646.0700
- PI: kotz@cs.dartmouth.edu

EBAM: Experience Based Access Management for Healthcare

NSF #0964392:
Carl A. Gunter, University of Illinois
Brad Malin, Vanderbilt University
David Liebovitz, Northwestern University

Identity and Access Management (IAM) in Health Care Organizations (HCOs)

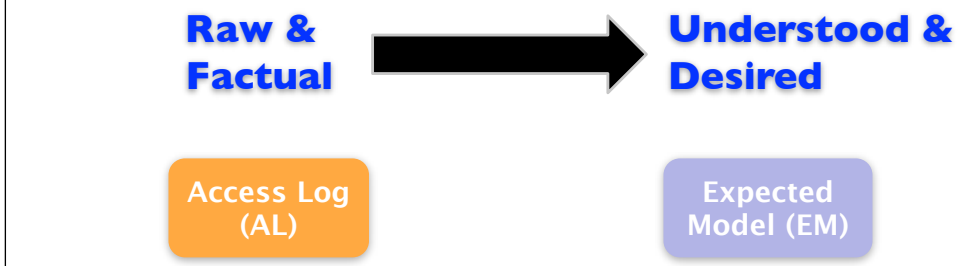
- IAM is a critical enterprise functions
- Systems have been successful: RBAC, DTM, ABAC, etc. but
- **More focus on process is needed**
- Want something like SE Waterfall, Spiral, or WRSPM Models

- Least Privilege management in Health Care Organizations (HCOs) is a good case study

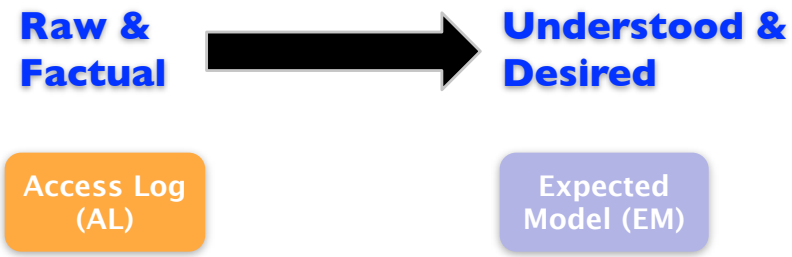
  Complex workflow

  Routine emergencies
- Break the glass case study: 54% of 99,352 records over-ridden by 43% of the 12,258 authenticated users

Access Logs Versus Expected Model

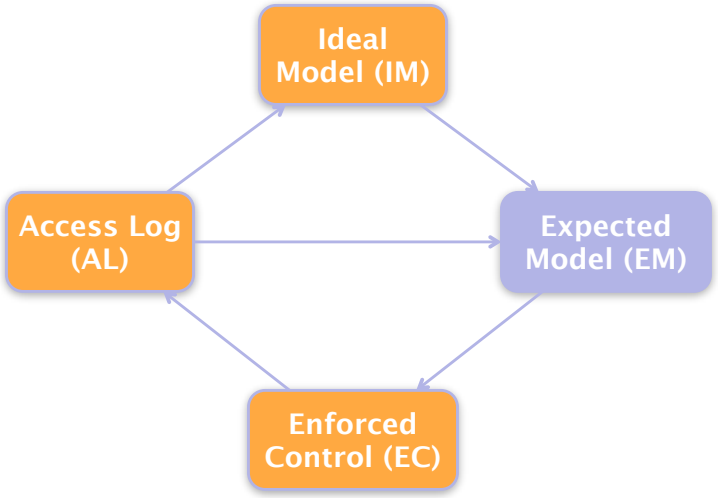


Access Logs Versus Expected Model

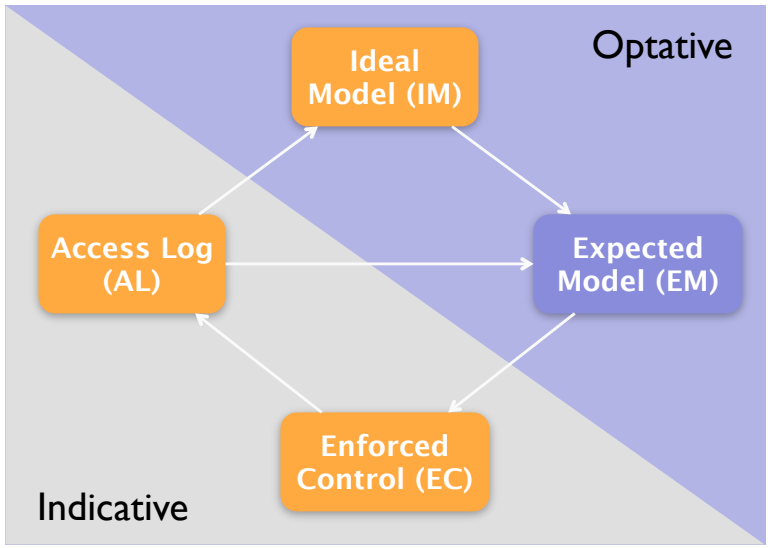


E **Experience**
B **Based**
A **Access**
M **Management**

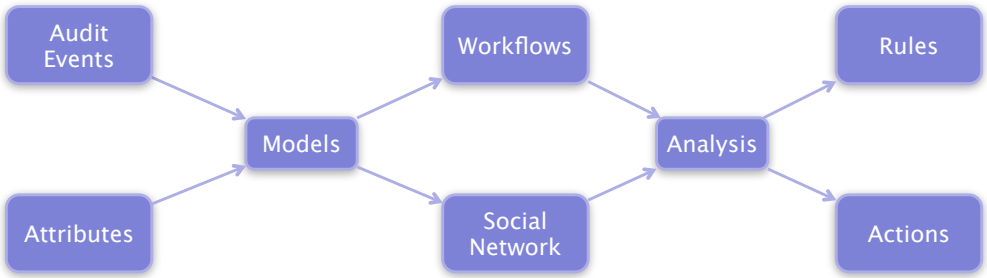
EBAM Cycle


Ideal Model (IM)
Access Log (AL)
Expected Model (EM)
Enforced Control (EC)

EBAM Moods


Optative
Ideal Model (IM)
Access Log (AL)
Expected Model (EM)
Enforced Control (EC)
Indicative

An EBAM Approach: Access Rules Informed by Probabilities (ARIP)



Discussion

- Related work: SPAM filters, intrusion detection
- Scope of applicability: applications that can tolerate some false negatives or positives
- Demand: new products appearing for risk mitigation in HCOs, what will be their engineering and scientific foundation?
- Technologies: supervised or unsupervised learning? other feedback avenues, viable measures
- Challenge and Opportunity: Health Information Exchange (HIE)

Maritza, Scout

Self Protecting Electronic Medical Records

NSF 1010928
Aviel D. Rubin, Johns Hopkins University
October, 2011 – September, 2015

Problems:

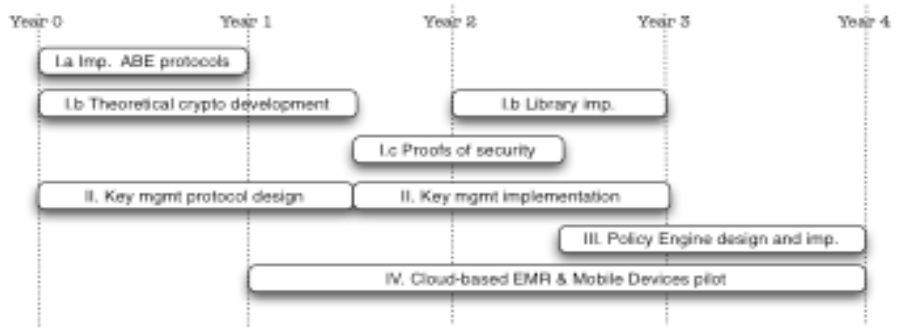
- Current Electronic Medical Records (EMRs) not self-protecting
  - Typically records only protected by transport layer protocols
- Access control is online only
  - Policy server must be online and available to make access control decisions
  - Availability issues: e.g. natural disaster or database crash
- Provider-centric environment
  - EMR systems are geared towards providers
  - Patients have little if any access to their records
  - PHR providers must be fully trusted
- Records are not well protected
  - E.g. at JHMI, approx 8,000 clinical employees have access to all the records for all the patients.
- Many regulations; few specific guidelines
- Complexity of access policies
- Complexities of log files
  - Regulations require keeping track of things; but good luck finding something

Approach

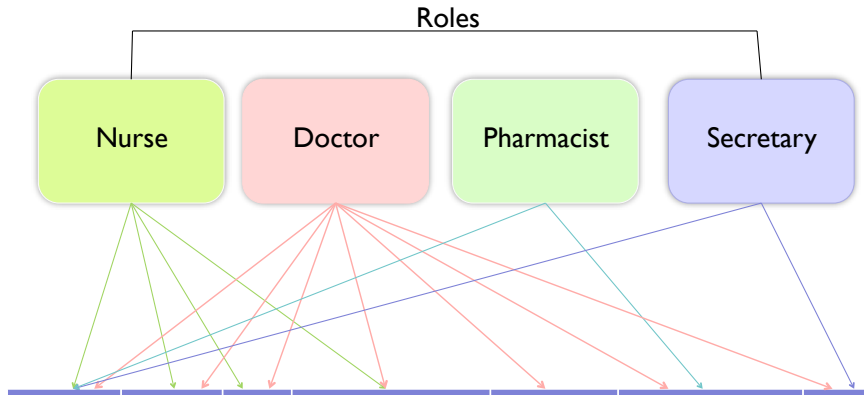
- Use Attribute-based encryption* (ABE) to create “self protecting” encrypted records
- Use role-keys & content-keys for access control
- Provide user-control and user-ownership of EMRs
- Use automation in policy generation from CCRs
- Enable offline access to EMRs w/out compromising security
  - Important in case of natural disaster
  - Network outage
  - Major weakness of today’s system
- Store records security in untrusted storage, i.e. cloud

* ABE: a user’s keys and ciphertexts are labeled with sets of descriptive attributes and a particular key can decrypt a particular ciphertext only if there is a match between the attributes of the ciphertext and the user’s key

Plan


Year 0
Year 1
Year 2
Year 3
Year 4
I.a Imp. ABE protocols
I.b Theoretical crypto development
I.b Library imp.
I.c Proofs of security
II. Key mgmt protocol design
II. Key mgmt implementation
III. Policy Engine design and imp.
IV. Cloud-based EMR & Mobile Devices pilot

ABE: Medical Records Example



Name	BP	Age	Height/	Disease	Prescriptions	Billing
Hubert	120/80	21	6'3" / 190lbs	Diabetes	Insulin	$120/mo.
Marie	170/110	40	5'8"/ 175lbs	Heart	Blood Pressure	$220/mo.
Samantha	100/65	18	5'3"/110lbs	Anemic	/	$80/yr.
…						

ABE: Medical Records Example

Nurse

"Nurse", "JHMI", "Part-Time", "General", "January2012"

Example…

("Doctor" V "Nurse" V "Pharmacist", "Secretary" V "Pharmacist") ^ ("Contract Date < Jan2011")

("Doctor" V "Nurse") ^ ("Full-time" V "Part-time" V "Temporary") ^ "Contract Date<Jan2011"

Name	BP	Age	Height/	Disease	Prescriptions	Billing
Hubert	120/80	21	6'3" / 190lbs	Diabetes	Insulin	$120/mo.
Marie	170/110	40	5'8"/ 175lbs	Heart	Blood Pressure	$220/mo.
Samantha	100/65	18	5'3"/110lbs	Anemic	/	$80/yr.
…						

ABE: Medical Records Example

Example…

Secretary

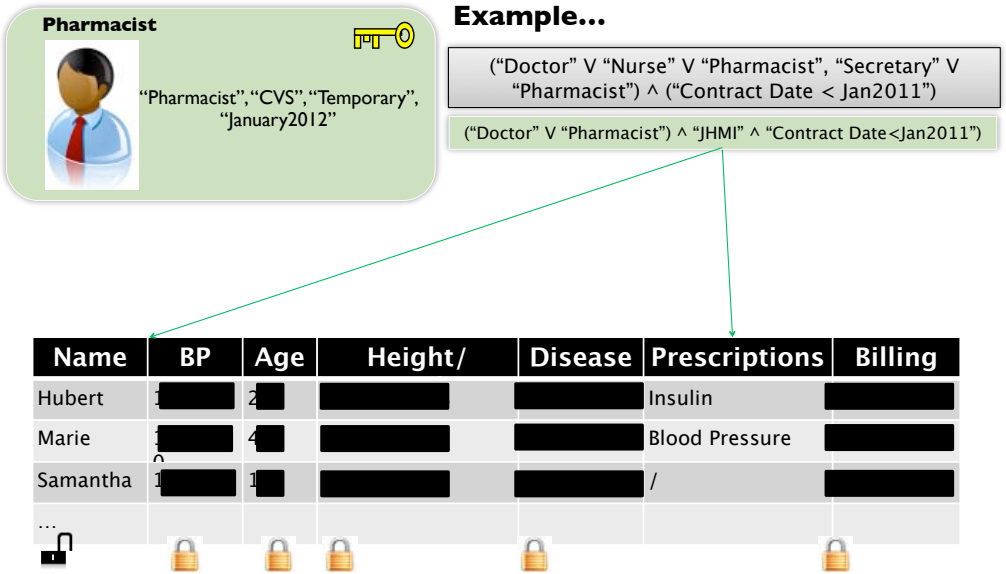
"Secretary","JHMI","Full-Time", "February2012"

("Doctor" V "Nurse" V "Pharmacist", "Secretary" V "Pharmacist") ^ ("Contract Date < Jan2011")

("Doctor" V "Secretary") ^ "JHMI" ^ "Contract Date <Jan2011"

Name	BP	Age	Height/ Weight	Disease	Prescriptions	Billing
Hubert	1[redacted]	2[redacted]	[redacted]	[redacted]	[redacted]	$120/mo.
Marie	1[redacted]	4[redacted]	[redacted]	[redacted]	[redacted]	$220/mo.
Samantha	1[redacted]	1[redacted]	[redacted]	[redacted]	[redacted]	$80/yr.
…						

ABE: Medical Records Example

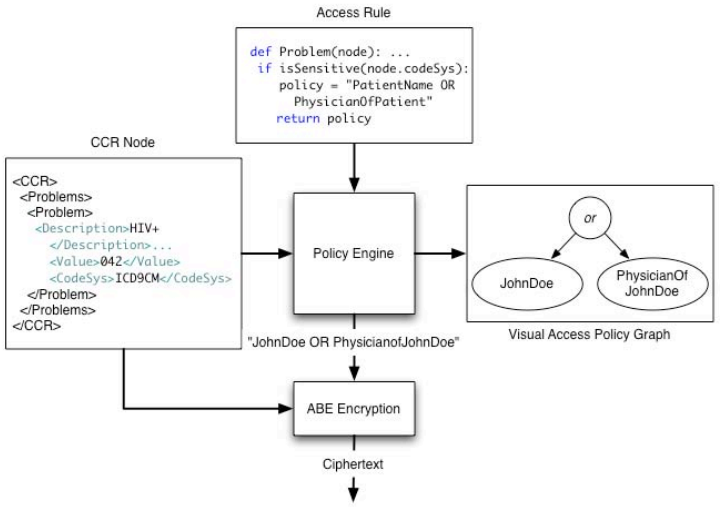


Automatic policy generation

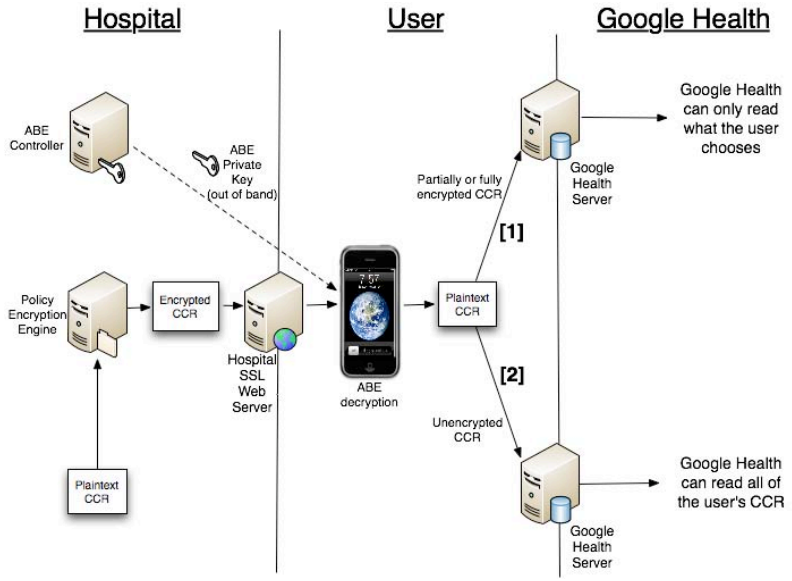
- Define list of access rules
  - Who should access what kind of data
- Scan a CCR
  - Look for keywords that match access rules
- Generate a policy graph that can be input to ABE engine
- Produce visualization of policy
  - Sanity check: e.g. very good at identifying typos

- Meant as a heuristic
  - Leverages repetitive, menial task that computers are good at
  - Human uses this as a starting point

Policy Engine

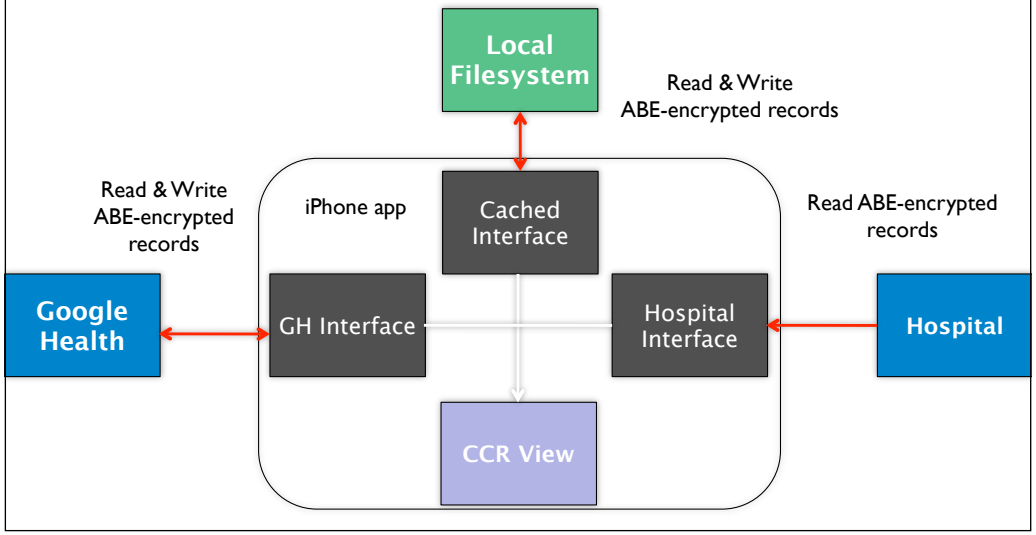


Architecture



Mobile Architecture

- Extensible Framework (multiple interfaces)
- Reusable components (CCR view)



iHealthEMR app

- Developed UI to allow users to authenticate and navigate their records
  - Navigation-based architecture creates “drill down” effect

Accomplishments (so far)

- Designed and implemented an ABE scheme for EMRs
- Developed a preliminary ABE code library
  - Ported code to the iPhone
- Began design and development of automatic policy engine
  - Developing tool chain for encryption/decryption of records
- Developed a Mobile app to allow patients to access their ABE-encrypted medical records offline and UI to view records.
  - App allows patients to download/upload their encrypted records to Google Health.
  - App allows users to locally store their ABE encrypted records.
- Publications:
  - contribution to two basic crypto papers with medical records applications (TCC ‘11, PKC ’11)
  - Applied paper in submission to ACNS ’11.

How to Find out More about Current NSF Research Awards

- www.nsf.gov/awardsearch
- Many search options available
  - Trustworthy Computing = Prog. Element 7795
- Results include abstract of award and PI-email
- Can be downloaded to spreadsheet

Thank You

Carl Landwehr
Program Director
Trustworthy Computing Program
National Science Foundation
clandweh@nsf.gov