A Trusted Information Sharing Project*

Syracuse University

Electrical Engineering & Computer Science

Shiu-Kai Chin, Polar Humenn, Thumrongsak Kosiyatrakul, Susan Older

Maxwell School of Citizenship and Public Affairs

Terrell Northrup, Stuart Thorson

*Partially sponsored by the CASE Center at Syracuse University – A Center for Advanced Technology in Information Technology sponsored by NYSTAR

Conclusions

- Sharing information in some cases is less about protocols and secure access control and more about establishing and maintaining *trust* between people and organizations
- Solutions rooted in engineering must be carefully integrated with solutions rooted in the social sciences
- Social science aspects predominate

Victims of Sexual Assault

"I would say that victims choose not to report for many reasons. Some of the most common reasons expressed are concerns for their privacy, the desire to return to their normal lives as soon as possible, concerns that they will not be believed, that attempts at criminal prosecution will be futile, and that the criminal process will actually put the victim on trial, leading to re-victimization. Some victims also fear reprisal from the offender."

Janet Epstein
Associate Director
Syracuse University R.A.P.E. Center

Our Project

- Produce a trusted system for sharing crime-related information between between SU's Dept. of Public Safety (DPS) and Syracuse Police Dept. (SPD)
- Focus on sexual-assault information reported by victims to SU's R.A.P.E. (Rape: Advocacy, Prevention, and Education) Center
- Status: Prototype CORBA-based system demonstrated, paper-based protocol for victims in development
  - Those authorized can access, those without denied
  - All access requests audited

Long-Range Vision

- Rigorously link concepts of trust in the social sciences to concepts of trust in computer science & engineering
  - *Trust* is domain specific
  - *System* includes humans and computers
  - *Complexity* arises out of size, cultural differences, unpredictability, and composition
- Hypothesis: The ability to rigorously relate societal notions of trust to engineering notions of trust enables policy makers, technologists, and citizens to better assess the trustworthiness of systems
- Starting point: relate computer science notions of *rights* and *access* to social-science notions of *rights*

An Interdisciplinary View

- Basic research on trust:
  - Philosophers: Annette Baier (delayed accounting), Thomas Scanlon (credible promises)
  - Formal methods: embedding into HOL theorem prover existing access control calculi (Lampson, Abadi, Burrows, Wobber, Howell, Kotz) based on modal logic to reason about rights, privileges, delegation, roles, and policies
  - Our extensions: incorporating RBAC and SARBAC (Scoped Administration of RBAC by Crampton) into the underlying Kripke model of principal calculus of Lampson, Abadi, et. al.
- Applied research on security standards:
  - Humenn: author of CORBA CSIv2 and ATLAS security standards
  - Humenn: one author of OASIS XACML v1.1: evaluation of credentials pertaining to access control
- Experiments: Trusted Info Sharing Project

This Talk

- Describe the project and what we have learned so far
- Briefly describe the engineering aspects
- Focus on underlying social-science principles
- Examine how the principles were instantiated in the project
- Observations and conclusions

1. Trusted Information Sharing Project

- Adapt the existing incident reporting system used by Syracuse University Department of Public Safety (DPS) to be electronically accessed by authorized personnel from the outside, such as the Syracuse City Police Department (SPD)
- Make this access adhere to security, and privacy laws/concerns, with a focus on sexual assault incidents

Principals

- SU R.A.P.E. (Rape: Advocacy, Prevention, and Education) Center
  - Information owners and victim advocates
- SU Department of Public Safety (DPS)
  - Interface between SU and police department
- Syracuse Police Department
  - Abused Persons Unit (APU)
- CASE Center: technologists
- Maxwell School: social scientists

Lessons Learned: Needed are

Engineering

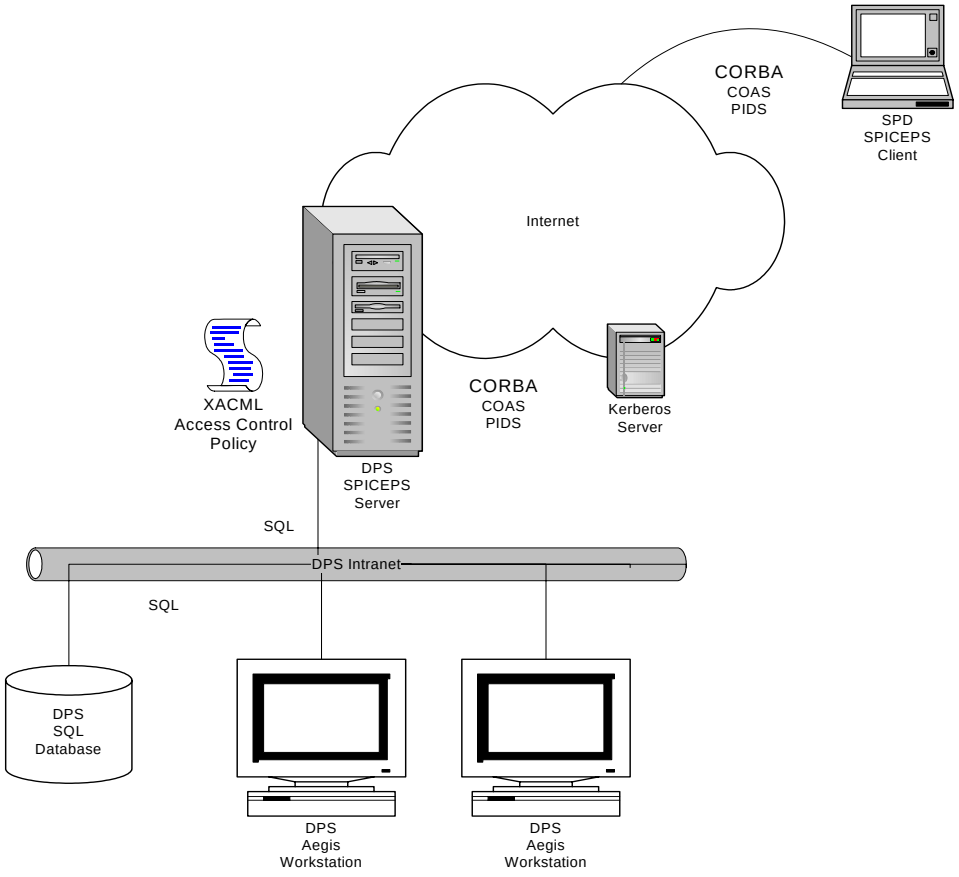
- Precise descriptions of scopes of authority, delegation, credentials, access-control decisions
- Common understanding of protocols
- Means for independent verification

Social Science

- **Extended empathy**: extension of person's understanding and ethics to a new group
- **Ecological validity**: coverage of all cases encountered in "real life"
- **Delayed accounting**: postpone accounting to allow use of resources
- **Credible promises**

2. Engineering Details

- Policy written in XACML v 1.0
- Access control enforced by CORBA secure ORB CSIv2
- Secure sessions via Kerberos



Data

- Data on incidents and people spread across several SQL DB tables
- Data modelled as COAS (Clinical Observation Access Service) observations and PIDS (Person IDentification Service) identities
- Interfaces consistent with COAS and PIDS

3. Social Science Principles Supporting Trust

- *Extended empathy*: people sometimes extend their understanding of motives and ethics to people they may not know
- *Ecological validity*: systems and protocols cover all “real life” cases
- *Delayed accounting*: resources used to further ends of principals rather than on verifying credibility

These are paraphrases. Read the full text

Promises, Scanlon

- *Principle M (no manipulation):* not misleading someone to do something they might not otherwise do
- *Principle D (due care):* not misleading someone to a false expectation about what you will or won't do
- *Principle L (loss prevention):* if someone will suffer a significant loss if you don't do something they expect you to do, then you must take reasonable steps to prevent that loss
- *Principle F (fidelity):* you will do what you say you will do, particularly when you have given assurances to this effect

4. Application of Principles

- R.A.P.E. Center staff are trusted advocates for victims. They must come to trust TISP in order for them to offer TISP as an option to victims
- Due diligence by Center staff has focused on being reasonably assured that Scanlon's four principles are satisfied
  - Principle M: Getting victims to disclose
  - Principle D: Making sure Center staff are not legally compelled to disclose by engaging in TISP
  - Principle L: Making sure victims' identities are shielded
  - Principle F: Precisely and accurately understanding TISP protocols, technology, limitations, and consequences

Extended Empathy

- Established by reaching a consensus as to why sharing sexual-assault information is a positive good
  - Assisting investigations, better understanding of this type of crime leading to enhanced education, lessons learned can be applied to other information-sharing projects
- Initially feasible because DPS Chief Marlene Hall was trusted by all principals
  - She was able to articulate to each group the value of the project and the shared motivations.

Ecological Validity

- Established by Terrie Northrup acting as “interpreter” between Lt. Becky Thompson of SPD’s APU, Janet Epstein Assoc Director or R.A.P.E. Center, & Dessa Bergen-Cico, Dean of Students
- Outcomes: precise understanding of R.A.P.E. Center protocols, information it gathers, and obligation to its clients
- Similar level of understanding of APU operations
- Policy and legal issues affecting Center
- Preliminary paper-based information sharing protocol between DPS and Center

Delayed Accounting

- Illustrated by fact that CASE staff member Polar Humenn had complete access to DPS Aegis Public Safety System
- Initial lower trust level established by Hall & Chin vouching for their respective staff
- Built and maintained by Humenn and Adams of DPS over a series of technical meetings

5. Observations & Conclusions

- It may be possible to formalize some of Scanlon's principles using modal logic
- There are limits to the assurances we can provide to victims
- It may be that developing trusted systems may require that a pre-existing climate of trust exist between subsets of people who will construct or vouch for the system

Conclusions

- Sharing information in some cases is less about protocols and secure access control and more about establishing and maintaining *trust* between people and organizations
- Solutions rooted in engineering must be carefully integrated with solutions rooted in the social sciences
- Social science aspects predominate

Backup Slides

Existing System

- AEGIS™ Incident Reporting System
  - Frontend:
    - AEGIS™ Client Software provides a GUI to entering and examining incident data.
  - Backend:
    - All AEGIS data is stored on a Microsoft SQL Server
- AEGIS™ Software
  - AEGIS™ software is client software that directly manipulates database tables through SQL.
- Exporting AEGIS™ to SPD requires opening up SQL to the open network is therefore, not sufficient for our security concerns.

Solution System Architecture

- Wrap existing AEGIS™ SQL database tables
  - Use middle tier that provides guarded access to DPS information outside of DPS.
- Develop clients that access the information through the middle tier.
- Use industry standards (OMG, OASIS)
  - Clinical Observation Access Service (COAS)
  - Person Identification Service (PIDS)
  - Common Object Request Broker Architecture (CORBA)
  - Secure CORBA (CSIv2)
  - Kerberos
  - eXtensible Access Control Markup Language (XACML)

Information View

- Incidents are modelled as COAS “observations”.
- A Subject of an Incident (Person) is modelled as a PIDS “identity”.
- A subject is uniquely tied to the incident in which he/she appears because access policy must mitigate the release of people involved in certain incidents, such as rape..
- Access Policy is written to explicitly deny or filter out observations and traits of identities that are not allowed to be seen by a certain requester of the information.

Computational View

- The COAS and PIDS integrated CORBA interfaces follow the their respective data models.
- Kerberos provides authentication identifiers.
- Use of CORBA interfaces allows easy integration of CORBA security CSIv2 and GSS-Kerberos.
- XACML provides the vehicle to write access policy based on the requester's Kerberos identifiers and the data model.

Engineering View

- Servers
  - Hardware
    - Microsoft SQL Server holding AEGIS database.
    - Linux Debian PC as middle tier.
  - Functionality
    - Modified COAS and PIDS from Los Alamos National Laboratory's Telemed Project on the Linux PC
- Clients
  - Custom Java built GUI providing secure, authenticated access to the COAS and PIDS interfaces
- Security
  - Adiron.com Secure ORB SL3 (Secure CORBA based infrastructure) and XACML Access Decision Engine.
  - Kerberos (Standard MIT Kerberos Distribution)

Clinical Observation Access Service (COAS)

- The COAS standard is a CORBA interface description allowing the organization of information that is based on a data model of “observations”.
- This standard provides different interfaces for the access and management of observation data.
- Observations are related to people, which is defined by the Person Identification Service (PIDS).
- As all data is input by DPS officials using the AEGIS system, we merely use the “access” interfaces outside of DPS.

Person Identification Service

- The Object Management Group (OMG) PIDS standard is a CORBA interface for the organization identifying information about persons.
- This standard provides a set of interfaces for the access and management of identities, and their identifying “traits”.
- As all data is input by DPS officials using the AEGIS system, we merely use the “access” interfaces outside of DPS.