A Trusted Information Sharing Project*

Shiu-Kai Chin[a] Polar Humenn[a] Thumrongsak Kosiyatrakul[a]
Terrell Northrup[b] Susan Older[a]
Stuart Thorson[b]
[a]Department of Electrical Engineering and Computer Science
[b]Maxwell School of Citizenship and Public Affairs
Syracuse University, Syracuse, New York 13244
http://www.ecs.syr.edu/faculty/chin

Key words: trust, interdisciplinary, information sharing, formal methods, social science, access control

1 Introduction

This project is part of an interdisciplinary research effort whose objective is to rigorously link concepts of trust in the social sciences to concepts of trust in computer science and engineering. Over the past two years, Thorson & Northrup (International Relations and Political Science), Older & Humenn (Computer Science), and Chin & Kosiyatrakul (Computer Engineering), have been collaborating on a variety of projects that explore notions of *trust* in complex systems, where the term "trust" is domain or discipline specific, the term "system" is broadly interpreted to include networks of both humans and computers, and complexity arises out of size, differences in culture, unpredictability, and composition. These projects include:

- Basic research on concepts of trust: (1) relating concepts of trust as understood by philosophers such as Annette Baier [Bai91] and Thomas Scanlon [Sca90] to notions of trust in computer science (Thorson, Older, Chin), and (2) creating a calculus for reasoning about access-control policies, delegation, roles, rights, privileges, and credentials modeled by a modal logic and implemented in a theorem prover [KOHC03, KOC01] (Older, Humenn, Chin, Kosiyatrakul).

- Applied research in credentials, access control, and secure information sharing: (1) participating on OASIS XACML[1] standards groups (Humenn) and developing a language with formal semantics to evaluate credentials as they pertain to access-control decisions [Hum03] (Humenn, Older, Chin), and (2) leading a nascent effort to develop and document organizational policies and practices and deploying secure information-sharing technologies to enable the Syracuse Police Department to pull information electronically from Syracuse University's Department of Public Safety's database related to sexual assaults (Thorson, Northrup, Humenn, Chin).

What we have learned from these collaborations is that establishing and maintaining trust depends on several components. From the social sciences, the following are necessary:

- *Extended empathy*, which our own work suggests is an important heuristic that people use to build trust in complex systems, by extending their understanding of motives and ethics to a group of people they may not know. Harré provides the example of "trusting" one's bank ([Har99], p. 259): "I trust my bank because I believe, without perhaps ever having formulated the thought explicitly, that it is staffed by honest and competent people."

- *Ecological validity* [Bru43], which provides a basis for trust because the systems and protocols used cover all the cases that could be encountered in "real life."

*Partially sponsored by the CASE Center at Syracuse University—a Center for Advanced Technology funded by the NY State Office of Science, Technology, and Academic Research (NYSTAR)

[1]Organization for the Advancement of Structured Information Standards eXtensible Access Control Markup Language, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

- *Delayed accounting*, which provides a basis for trust because when parties have earned a particular level of trust, resources do not need to be spent for a full accounting unless warranted by circumstances. This allows resources to be used to further the ends of the parties rather than on verifying their credibility [Bai91].

- *Credible promises*, which provide a basis for trust because successful discharging of promises and obligations is a cornerstone of establishing and maintaining trust [Sca90].

From computer science we have learned the following are also necessary:

- Precise descriptions of what authorities are recognized, the scope of each authority, how delegation of authority occurs (i.e., how representative or delegates are chosen), how credentials are interpreted, and how access-control decisions are made and accounted for. These provide a basis for trust because access control decisions can be analyzed precisely and designs can be verified for correctness [ABLP93, LABW92, WABL94].

- Protocols whose purposes and interpretations are precisely understood, which support trust through common interpretations that avoid misunderstandings [OC02].

- A means for independent verification when necessary, which supports trust by providing a means for accountability, error detection, and error correction when called for [KOHC03].

Our goal is to achieve a more precise understanding of how to rigorously relate notions of trust in political science to notions of trust in computer science. Doing so will move us towards the ability to field information systems that adequately account for the societal contexts in which systems operate. Our hypothesis is that the ability to rigorously relate societal notions of trust will enable policy makers, designers, and citizens to better understand if a particular system of computer networks, protocols, human organizations, policies and practices is trustworthy.

As a starting point, we are exploring the relationship between computer-science notions of trust in the form of *rights and access* to the larger meaning of rights in political-science contexts. Our interest is to discover and develop the means to preserve the intended meaning of rights through several refinements, from the policy-maker's view to the engineer's implementation. We anticipate that there are many other points of intersection beyond the notion of rights.

As a means to further our research and to provide a public good, we are engaged in a trusted information-sharing project (TISP) with the Syracuse University R.A.P.E. (Rape: Advocacy, Prevention, and Education) Center, Department of Public Safety (DPS), and the Syracuse Police Department (SPD). The long-term purpose of this collaboration is to produce a trusted system for sharing crime-related information between DPS and SPD. The participants agree in principle that information sharing is a positive good for a variety of reasons, including the following:

1. If information can be securely shared across jurisdictions, then patterns of criminal behavior that cross those jurisdictional lines can be seen. This can assist in investigations.

2. Sharing of information, over time, adds to law-enforcement understanding of particular types of crimes. This greater understanding contributes to an enhanced ability to educate the public and to the prevention of crime.

3. What is learned about the development of such trusted systems has the potential for being transferable to other types of information-sharing projects.

The rest of this paper is organized as follows. In Section 2 we provide some details of the underlying network and the security protocols used. In Section 3 we give illustrative examples of how social-science notions of extended empathy, ecological validity, delayed accounting, and credible promises were manifested. We conclude in Section 4.

2 Engineering Details

The existing system that DPS uses is called the Aegis Public Safety System. Aegis records data on incidents and on the people involved in those incidents. It is the primary way in which officers, administrators, and department heads record, report, and perform analysis on information related to people, places, and incidents that occur within the university community. The system defines the SQL database tables and the form of the data that is stored. Security is based on password authentication between the Ageis user interface and the SQL database without any integrity or confidentiality protection.

In our prototype, we split up the DPS system logically into three major components, which we will classify as the back-end and two facades. The back-end

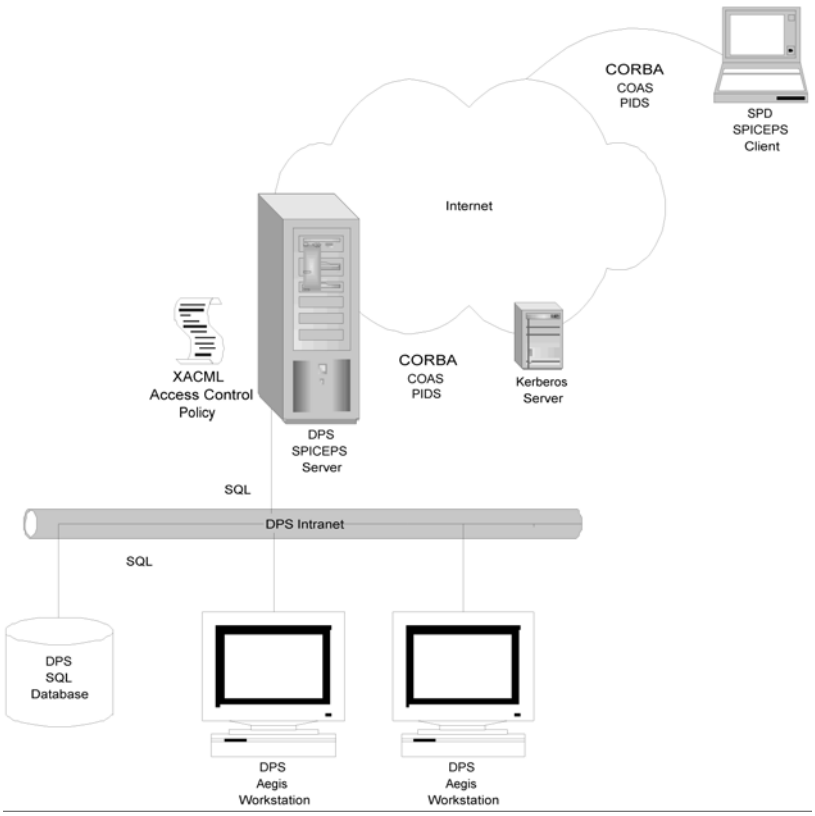

Figure 1: SPICEPS Network

consists solely of a SQL database running on a single server. The internal facade consists of the existing Aegis user interface. It accesses the SQL database through a direct network connection to the back-end on the DPS intranet.

The other facade exposes a set of network interfaces to the outside world on the Internet. It consists of a set of server applications that access the back-end and provide a read-only object-based interface to the stored incident data. These applications also implement a guard that moderates access to the data.

The external facade consists of secure CORBA (Common Object Request Broker Architecture) server applications. These services are built with Adiron's Secure ORB (Object Request Broker) using Wedgetail's GSS (General Security Services) Kerberos implementation, which provides authentication and confidentiality for CORBA-based requests. This software allows a CORBA-server implementation to get authentication information about the client making the request. We call the server that provides this external facade the DPS SPICEPS (Secure Privacy and Interoperable Collaborative Electronic Public Safety) server. People at SPD will access DPS data with a SPICEPS client. Kerberos provides the network security through the Internet for the queries in the form of message integrity and confidentiality (encryption) along with authentication between the SPD SPICEPS client and the DPS SPICEPS server. Figure 1 is a diagram of the SPICEPS network.

The OMG (Object Management Group) standards that are employed are the Clinical Observation Access Service (COAS) and the Person Identification Service (PIDS). We used these two standards to model the data as well as to provide access. The COAS uses its "observations" to describe the "incident" data, while the PIDS uses its "identity" and "traits" to describe the people involved in an incident.

These standards are used with a custom GUI (graphical user interface) client that accesses the COAS and PIDS interfaces securely. This client is a Java-built client using Adiron's secure ORB implementation to get the accessibility to the COAS and PIDS interface using Kerberos authentication.

Even though the Microsoft SQL Server, which is used at DPS, can provide authentication and confidentiality protection with Microsoft's special version

of Kerberos, the SQL protection model is not sufficient to protect the DPS data to our requirements. Most SQL access policy is based on a simple access control list for each row in a table, listing the people that may see the row or see certain columns of that row. Incidents in Ageis are stored across several relational tables, so this kind of policy becomes problematic to implement. Instead we make use of a newly accepted OASIS standard for an access-control language, called the eXtensible Access Control Markup Language (XACML).

The XACML standard allows us to write access policy that is not restricted to row/column security, but is written in a general language in which policy may be based on "attributes" of the data bring protected, as well as identifying attributes of the client. For instance, before revealing a person's identifying information, the PIDS service must take into account the type of incident they are involved in, such as a victim of a rape. In the Aegis SQL database, the person's identity information is kept in a different table. So, it would be difficult for a row/column security model enforce such a policy at the database level. We model a "subject" of an incident as a person involved with an incident, so that we may be able to attribute the type of incident and type of subject (e.g., victim, perpetrator, etc.) to the identity.

Calls for XACML policy evaluations occur at various points of requests for information within the CORBA servers. Access is controlled not only at the CORBA interfaces but also by checking the ability to execute requested operations. Aggregate queries also must adhere to the policy. For instance, a query that asks for a specific incident may be explicitly denied. When that incident is part of an aggregate query that was selected on some attribute—such as the type of incident—that incident must be removed from the information that is returned.

SPICEPS models the data of the DPS database differently than its stored model (i.e., beyond a simple table) in order to protect the data according to privacy concerns. The external front end of the SPICEPS system consists of an interface that brokers access requests to the DPS data. SPICEPS moderates access to that information based on attributes of the information, such as the incident type of an incident subject. Along with those attributes it also makes its access decision based on attributes of the authentication of the requesting client, which are provided by Kerberos.

3 Social-Science Aspects

To appreciate the social-science aspects of this project we start by describing the SU R.A.P.E. Center's relationship with its clients and some of the chief concerns of its clients. Information already collected through the R.A.P.E. Center, or that might be collected with the help of the R.A.P.E. Center, is particularly sensitive. Clients of the R.A.P.E. Center, most of whom come to the Center because they have experienced sexual assault, are often only willing to come forward if they trust that their privacy is protected and that they retain control over the information they provide. A variety of policies dictate that the R.A.P.E. Center cannot share any victim information without the victim's permission. At times, a victim who does not want to report an incident to law enforcement may wish to provide information that could serve to help with an investigation or in some way contribute to preventing future sexual assaults. TISP provides an opportunity for information to be provided while assuring the protection of the client's privacy and anonymity.

From a social science standpoint, a key concern for clients is the explicit promise that their information, identity, and circumstances will be protected from unauthorized disclosure. Clients want to avoid being forced to come forward in legal proceedings. If the promise is credible to R.A.P.E. Center clients, then clients are more likely to authorize disclosure of their information through the DPS to the SPD.

People who come to the R.A.P.E. Center as clients place their trust in the Center. Specifically, clients look to Center staff to advise them of their options and expect Center staff to act as their advocates. Center staff, acting as liaisons between victims of sexual assault and other agencies such as DPS and the Abused Person's Unit of SPD, are placed in a position of promising that victims' information will be properly handled.

Scanlon's paper *Promises and Practices* [Sca90] addresses some necessary conditions for people to trust promises. Scanlon as a philosopher and social scientist has postulated that the following principles are necessary for preserving credibility and trust:

> *Principle M (no manipulation)*: "In the absence of special justification, it is not permissible for one person, A, in order to get another person, B, to do some act, x (which A wants B to do and which B is morally free to do or not do but would otherwise not do) to lead B to expect that if he or she does x then A will do y (which B wants but believes

A will otherwise not do) when in fact A has no intention of doing y if B does x, and A can reasonably foresee that B will suffer significant loss if he or she does x and A does not do y." [Sca90] pp. 202–203

Principle D (due care): "One must exercise due care not to lead others to form reasonable but false expectations about what one will do when there is reason to believe that they would suffer significant loss as a result of relying on those expectations." [Sca90] p. 204

Principle L (loss prevention): "If one has intentionally or negligently led someone to expect that one will follow a certain course of action x, and one has reason to believe that that person will suffer significant loss as a result of this expectation if one does not follow x, then one must take reasonable steps to prevent that loss." [Sca90] p. 204

Principle F (fidelity): "If (1) A voluntarily and intentionally leads B to expect that A will do x (unless B consents to A's not doing x); (2) A knows that B wants to be assured of this; (3) A acts with the aim of providing this assurance, and has good reason to believe that he or she has done so; (4) B knows that A has the beliefs and intentions just described; (5) A intends for B to know this, and knows that B does know it; and (6) B knows that A has this knowledge and intent; then, in the absence of some special justification, A must do x unless B consents to x's not being done." [Sca90] p. 208

In our experience, the "due diligence" performed by R.A.P.E. Center staff centered around understanding the policies, procedures, mechanisms, and *people* involved with TISP well enough so they could feel reasonably assured of satisfying Scanlon's four principles. It is this assurance that will eventually enable the Center staff to offer TISP as an option to victims.

The TISP project to date has evolved roughly along the lines of (1) establishing the basis for *extended empathy* [Har99], where people extend their understanding of motives and ethics to a group of people they may not know; (2) establishing *ecological validity* [Bru43], by identifying all the cases that could be encountered in cases of victims reporting a sexual assault; and (3) *delayed accounting* [Bai91] by allowing access to resources without having to perform a complete accounting of actions taken or resources used to demonstrate how the SPICEPS system could work to securely share sexual assault information in ways that protect victims' rights. We touch briefly on these three areas in the following paragraphs.

The basis for extended empathy was established by reaching a consensus as to the reasons why sharing information about sexual assault is a positive good. These reasons are stated at the end of Section 1. The starting point for this process was the initial trust placed in the Chief of the Department of Public Safety, Marlene Hall, by the R.A.P.E. Center staff, Engineering and Computer Science staff, Maxwell School staff, and the Syracuse Police Department. Chief Hall was able to articulate to each group the value of the project and the common motivations shared by all.

The basis for ecological validity was established through the efforts of Terrell Northrup who served as a "go between" or interpreter between Lt. Rebecca Thompson of SPD's Abused Persons Unit, Janet Epstein, Associate Director of the R.A.P.E. Center, and Dessa Bergen-Cico, Dean of Students. Northrup's efforts served to understand in detail the protocols used by the R.A.P.E. Center, the information it gathered, and its obligations to its clients. Similarly, Northrup's efforts led to an understanding of the operations of the Abused Persons Unit. In combination, this led to a preliminary understanding of the policy and legal issues and to the design of a prototype (paper-based) information-sharing protocol between the R.A.P.E. Center and DPS as a first step.

Delayed accounting was illustrated by the fact that CASE Center staff member Polar Humenn eventually was given complete access to the DPS Aegis Public Safety system. An initial level of trust was achieved by Marlene Hall as DPS Chief and Shiu-Kai Chin as CASE Center Director where each vouched for the trustworthiness of their staff. Higher levels of trust were achieved through a continuing set of technical meetings involving Polar Humenn and Donna Adams, DPS Associate Director of IT. This degree of access was necessary to successfully demonstrate a prototype of the SPICEPS system.

4 Conclusion

TISP is an ongoing project. The SPICEPS prototype demonstration successfully showed that the system does in fact deny access to sexual assault information to unauthorized people as well as granting access to those with proper authority. Demonstrating the technology has been crucial for R.A.P.E. Center staff to envision what is possible in terms of secure informa-

tion sharing. In some ways, this has been the easiest part of the project.

From a computer science and engineering standpoint, what is interesting is the possibility of formalizing some of the social-science aspects of the project. For example, Scanlon's four principles deal with beliefs and possible outcomes. As the access control calculus of Lampson and Abadi [ABLP93, LABW92, WABL94] is based on a modal logic, we may be able to formalize specific instances of the four principles in specific contexts.

The more time-consuming part has been the establishment of extended empathy, ecological validity, and delayed accounting that has led to the construction of a memorandum of understanding (MOU) that succinctly and accurately details the objectives, policies, and procedures of TISP. At this point a second draft is in circulation with all parties committed to move forward. It may be that developing trusted systems may require, or be facilitated by, a pre-existing climate of trust between subsets of the people who will ultimately construct and vouch for the new system.

Finally, we acknowledge that there are limits to the assurances that we can provide to victims of sexual assault. As we cannot control the actions of defense attorneys (nor are we suggesting we should), we cannot guarantee that under *no circumstances* will victims who authorize sharing of their information with law enforcement be totally free from being legally compelled to come forward. All we can do is limit the risk of exposure to victims who desire to remain anonymous by anticipating as many of the legal issues as is possible and by implementing security as best we can.

References

[ABLP93] Martin Abadi, Michael Burrows, Butler Lampson, and Gordon Plotkin. A calculus for access control in distributed systems. *ACM Transactions on Programming Languages and Systems*, 15(4):706–734, September 1993.

[Bai91] Annette C. Baier. Trust. The Tanner Lectures on Human Values, Princeton University, May 6–8, 1991.

[Bru43] E. Brunswick. Organismic achievement and environmental probability. *The Psychological Review*, 50(3):255–272, 1943.

[Har99] R. Harré. Trust and its surrogates: psychological foundations of political process. In M.E. Warren, editor, *Democracy & Trust*, pages 249–272. Cambridge University Press, 1999.

[Hum03] Polar Humenn. The formal semantics of xacml – draft. available at http://lists.oasis-open.org/archives/xacml/200310/msg00094.html, October 2003.

[KOC01] Thumrongsak Kosiyatrakul, Susan Older, and Shiu-Kai Chin. Formal analysis of X.509 certificates. In *International Joint Conferences on Automated Reasoning IJCAR-2001*, pages 113–127. Workshop W3 Verification (VERIFY'01), 2001.

[KOHC03] Thumrongsak Kosiyatrakul, Susan Older, Polar Humenn, and Shiu-Kai Chin. Implementing a calculus for distributed access control in higher order logic and HOL. In V. Gorodetsky, L. Popyack, and V. Skormin, editors, *Computer Network Security: Second International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security*, volume 2776 of *Lecture Notes in Computer Science*, 2003.

[LABW92] Butler Lampson, Martin Abadi, Michael Burrows, and Edward Wobber. Authentication in distributed systems: Theory and practice. *ACM Transactions on Computer Systems*, 10(4):265–310, November 1992.

[OC02] Susan Older and Shiu-Kai Chin. Formal methods for assuring security of protocols. *The Computer Journal*, 45(1):46–54, 2002.

[Sca90] Thomas Scanlon. Promises and practices. *Philosophy and Public Affairs*, 19(3), Summer 1990.

[WABL94] Edward Wobber, Martin Abadi, Michael Burrows, and Butler Lampson. Authentication in the Taos operating system. *ACM Transactions on Computer Systems*, 12(1):3–32, February 1994.