Augmenting Trust Establishment in Dynamic Systems with Social Networks

[Extended Abstract]

Brent Lagesse
Cyberspace Science and Information Intelligence Research Group
Computational Science and Engineering Division
Oak Ridge National Laboratory
lagessebj@ornl.gov

Mohan Kumar
Department of Computer Science Engineering
University of Texas at Arlington
mkumar@uta.edu

Svetha Venkatesh
Department of Computing
Curtin University
S.Venkatesh@curtin.edu.au

Mihai Lazarescu
Department of Computing
Curtin University
M.Lazarescu@curtin.edu.au

Categories and Subject Descriptors

C.2.0 [**General**]: Security and protection

General Terms

Security

1. INTRODUCTION

Social networking has recently flourished in popularity through the use of social websites. Pervasive computing resources have allowed people stay well-connected to each other through access to social networking resources. We take the position that utilizing information produced by relationships within social networks can assist in the establishment of trust for other pervasive computing applications. Furthermore, we describe how such a system can augment a sensor infrastructure used for event observation with information from mobile sensors (ie, mobile phones with cameras) controlled by potentially untrusted third parties.

Pervasive computing systems are invisible systems, oriented around the user. As a result, many future pervasive systems are likely to include a social aspect to the system. The social communtities that are developed in these systems can augment existing trust mechanisms with information about pre-trusted entities or entities to initially consider when beginning to establish trust.

An example of such a system is the Collaborative Virtual Observation (CoVO) system fuses sensor information from disaparate sources in soft real-time to recreate a scene that provides observation of an event that has recently transpired. To accomplish this, CoVO must efficiently access services whilst protecting the data from corruption from unknown remote nodes. CoVO combines dynamic service composition [14] with virtual observation [11] to utilize existing infrastructure with third party services available in the environment. Since these services are not under the control of the system, they may be unreliable or malicious. When an event of interest occurs, the given infrastructure (bus cameras, etc.) may not sufficiently cover the necessary information (be it in space, time, or sensor type).ă To enhance observation of the event, infrastructure is augmented with information from sensors in the environment that the infrastructure does not control.ă These sensors may be unreliable, uncooperative, or even malicious. Additionally, to execute queries in soft real-time, processing must be distributed to available systems in the environment. We propose to use information from social networks to satisfy these requirements.

In this paper, we present our position that knowledge gained from social activities can be used to augment trust mechanisms in pervasive computing. The system uses social behavior of nodes to predict a subset that it wants to query for information.ă In this context, social behavior such as transit patterns and schedules (which can be used to determine if a queried node is likely to be reliable) or known relationships, such as a phone's address book, that can be used to determine networks of nodes that may also be able to assist in retrieving information. Neither implicit nor explicit relationships necessarily imply that the user trusts an entity, but rather will provide a starting place for establishing trust. The proposed framework utilizes social network information to assist in trust establishment when third-party sensors are used for sensing events.

2. BACKGROUND

CSIIRW 2010 Oak Ridge, TN USA
Copyright 2010 ACM 978-1-4503-0017-9 ...$5.00.

Increase in network connectivity and the pervasive computing resources have led to more social applications of computing. Many applications focused on explicitly enhancing this social aspect in the form of social network websites [2, 4, 3, 1] have become popular in recent years. Much research has been conducted on analyzing or establishing trust in social networking sites [9, 7, 10], but little has been done on utilizing information in social networks to establish trust in other domains. Some trust models [23] include a social context in the model for establishing trust, but no system has focused on using social information to assist in the trust-establishment problem.

In this context, a social network is defined as the set of relations connecting multiple entities in a system. These relations may be either explicit or implicit. Explicit relations are stated as in a social networking websites such as Facebook [2] where people explicitly and mutually agree to be friends. Implicit relations are implied, often by context information or recurring mutual patterns, such as people that spend overlapping time in the same coffee shop on a regular basis. We propose to use this information as a starting point to bootstrap the trust establishment process.

Distributed trust is used in a wide variety of applications and in many forms. Distributed trust is used rather than traditional security mechanisms in systems where it is not feasible to centralize all security decisions to a monolithic system. Trust is often used in distributed systems such as Peer-to-Peer (P2P) systems [22, 15, 21, 17], service composition systems [6, 18, 5, 12, 8], and pervasive computing systems in general [13, 20, 19, 16]. We will demonstrate how social network information can be used to augment AREX[17], an adaptive trust mechanism used in CoVO, in this paper.

AREX is an adaptive security mechanism that is designed for highly dynamic systems as it does not rely on collaboration to establish trust. AREX uses a game theoretic approach to motivate attackers to attack less often. It also does not suffer the same vulnerabilities as reputation mechanisms, such as vulnerability to intermittent connectivity, startup/traitor attacks, and being highly connected to malicious entities. The downside is that in large systems, such as performing collaborative virtual observation in a major urban area, AREX adapts to the system slowly. Social network information will be incorporated into AREX and thereby overcome performance issues caused by large systems.

3. DESIGN

This section introduces the Social Augmentation Framework for utilizing relations in social networks to bootstrap trust algorithms. It also describes the application of this framework to collaborative virtual observation.

3.1 Social Augmentation Framework

This section describes the Social Augmentation Framework as shown in Figure 1 and the interactions of each component. The Social Augmentation Framework consists of three components: Social Networks, Translations, and Trust Mechanisms.

3.1.1 Social Networks

Social Networks are a set of data sets of social connectivity information that are available to the system. These may take the form of web-based social networking sites, contact lists in a cell phone, or databases of traffic information that can be mined for links.

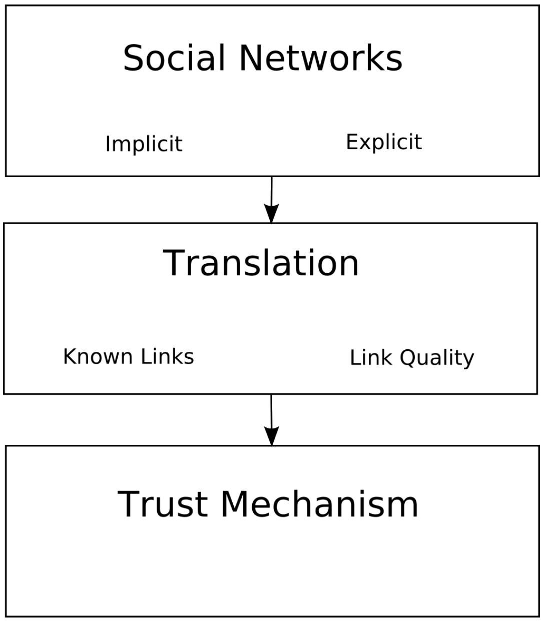

Figure 1: Social Augmentation Framework

3.1.2 Translation

The Translation component is responsible for translating information from the Social Network into a usable form for the Trust Mechanism. This may be as simple as identifying connected nodes or as complicated as analyzing connections to provide initial values for nodes to the trust mechanism. The Translation component also is responsible for resolving nodes in the social network into addressable nodes in the system.

3.1.3 Trust Mechanism

The Trust Mechanism requests initial information to assist in bootstrapping the request for trust computations. Additionally the Trust Mechanism can make requests to the Translation component to augment current calculations.

3.2 Social Augmentation of CoVO

Collaborative Virtual Observation (see Figure 2) involves utilizing resources from pre-existing infrastructure in addition to opportunistic access from services and resources available in the environment such as cell phone cameras and processors. Observations made by these resources are then stitched together using available services based on variables such as time and space. The result is a virtual observation of events that can be accessed in soft real-time. To accomplish this though, the resources and services from the environment must provide valid services; otherwise, the resulting virtual observation may be worse than would be the case with just the available infrastructure. Existing trust mechanisms do not achieve the soft real-time requirements in dynamic environments in which collaborative virtual observation is performed; however, by augmenting trust mechanisms with social information, the performance of the trust mechanism can be enhanced to meet the requirements in many cases.

Social augmentation assists with the trust computations

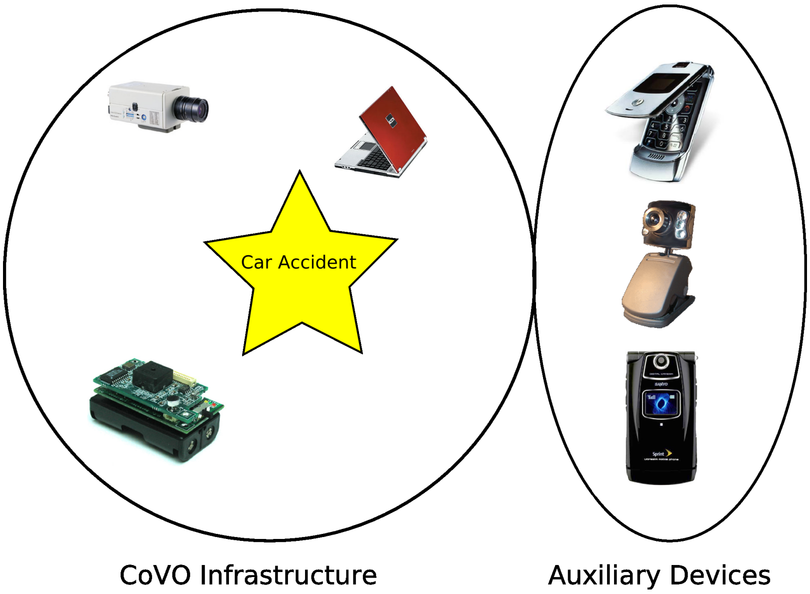

Figure 2: CoVO Example

to achieve soft real-time performance for CoVO. It utilizes implicitly formed social networks based on patterns derived from the observation of bluetooth signals by mobile nodes. The physical presence of an entity provides an implied social network since the entity is connected in terms of physical presence in a place in the society. An assumption contributing to this decision is that if a node consistently appears in a particular area for a long period of time that it is more likely to stay in the area while it is needed. For example, if a node is consistently in the Computer Science Department building for about 6 hours a day from Monday through Friday, there is a strong chance that it will remain in the area to provide its service during that regular pattern. An argument can be made that forming a consistent physical pattern is of high cost to an attacker and may be less likely, but just because a social network is used, it does not imply that there is trust between the nodes, just that the trust mechanism will augment its approach with information from the social network. Therefore, an actively malicious node would still have to undergo the same calculations from the trust mechanism as it would without the social network, just at a higher cost to itself.

Available nodes that are expected to remain in the area based on previous traffic patterns mined from the traffic databases seed the trust calculation process. The seeding is made possible by the translation component which selects a predetermined number of socially-connected nodes to use in the initial trust computation of the trust mechanism. The translation component also maintains a list of bluetooth addresses so that the trust mechanism can communicate with those devices. AREX-based adaptive trust mechanisms are used for resources access and service composition. Such trust mechanisms work best in smaller systems, so operating on a city-wide basis can slow the adaptation of the mechanism. The initial seeding from the social network provides the trust mechanism with the ability to reliably operate on a much smaller scale and provide similar reliability in less time.

4. CONCLUSION

In this paper, we take the position that social network information can be utilized to enhance the convergence time of adaptive security mechanisms used in pervasive computing. We introduces a framework for augmenting collaborative applications in large dynamic environments with social network information. The framework enhances security mechanisms by providing a foundation based on social aspects to begin establishing trust. From a broader perspective, this approach underscores the fact that social information can be effectively utilized to establish trust in large dynamic environments when third party contributions are critical to the collaborative efforts despite the associated uncertainties.

The work presented in this paper will be extended to examine several other trust mechanisms and identify classes of mechanisms that can be improved by social network information. Furthermore, we will examine defense mechanisms against unreliable nodes in the social network, both in a generalized sense and for specific applications. Finally, we will explore adaptive mechanisms for automatically adjusting the preferences for the social network, both in bootstrapping into new systems and in augmenting currently running systems

Acknowledgements

Prepared by Oak Ridge National Laboratory, P.O. Box 2008, Oak Ridge, Tennessee 37831-6285, managed by UTBattelle, LLC, for the U.S. Department of Energy under contract DE-AC05-00OR22725.

The work presented in this paper was partially supported under US National Science Foundation Grant ECCS 0824120.

5. REFERENCES

[1] Blogger, July 2009. `http://www.blogger.com`.

[2] Facebook, July 2009. `http://www.facebook.com`.

[3] Linkedin, July 2009. `http://www.linkedin.com`.

[4] Twitter, July 2009. `http://www.twitter.com`.

[5] Massimo Bartoletti, Pierpaolo Degano, and Gian Luigi Ferrari. Enforcing secure service composition. In *CSFW '05: Proceedings of the 18th IEEE workshop on Computer Security Foundations*, pages 211–223, Washington, DC, USA, 2005. IEEE Computer Society.

[6] John Buford, Rakesh Kumar, and Greg Perkins. Composition trust bindings in pervasive computing service composition. In *Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops*. IEEE Computer Society, 2006.

[7] James Caverlee, Ling Liu, and Steve Webb. Socialtrust: tamper-resilient trust establishment in online communities. In Ronald L. Larsen, Andreas Paepcke, José Luis Borbinha, and Mor Naaman, editors, *ACM IEEE Joint Conference on Digital Libraries*, pages 104–114. ACM, 2008.

[8] Dipanjan Chakraborty, Filip Perich, Anupam Joshi, Timothy W. Finin, and Yelena Yesha. A reactive service composition architecture for pervasive computing environments. In *PWC '02: Proceedings of the IFIP TC6/WG6.8 Working Conference on Personal Wireless Communications*, pages 53–62, Deventer, The Netherlands, The Netherlands, 2002. Kluwer, B.V.

[9] Catherine Dwyer, Starr R. Hiltz, and Katia Passerini. Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. In *Proceedings of the Thirteenth Americas Conference on Information Systems*, August 2007.

[10] J. Fogel and E. Nehmad. Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, 25(1):153–160, January 2009.

[11] Stewart Greenhill and Svetha Venkatesh. Virtual observers in a mobile surveillance system. In *ACM Multimedia 2006, 23-27 October, Santa Barbara, USA*, 2006.

[12] Xiaohui Gu, Klara Nahrstedt, and Bin Yu. Spidernet: An integrated peer-to-peer service composition framework. In *HPDC '04: Proceedings of the 13th IEEE International Symposium on High Performance Distributed Computing*, pages 110–119, Washington, DC, USA, 2004. IEEE Computer Society.

[13] Lalana Kagal, Jeffrey Undercoffer, Filip Perich, Anupam Joshi, and Tim Finin. A security architecture based on trust management for pervasive computing systems. In *Grace Hopper Celebration of Women in Computing*, October 2002.

[14] Swaroop Kalasapur, Mohan Kumar, and Behrooz Shirazi. Dynamic service composition in pervasive computing. *IEEE Transactions on Parallel and Distributed Systems*, 18(7):907–917, 2007.

[15] Sepandar D. Kamvar, Mario T. Schlosser, and Hector Garcia-Molina. The Eigentrust algorithm for reputation management in P2P networks. In *WWW*, pages 640–651, 2003.

[16] Brent Lagesse, Mohan Kumar, Justin Mazzola Paluska, and Matthew Wright. Dtt: A distributed trust toolkit for pervasive systems. *Pervasive Computing and Communications, IEEE International Conference on*, 0:1–8, 2009.

[17] Brent Lagesse, Mohan Kumar, and Matthew Wright. AREX: An adaptive system for secure resource access in mobile P2P systems. In *Eighth International Conference on Peer-to-Peer Computing*, pages 43–52. IEEE Computer Society, 2008.

[18] Bhaskaran Raman, Sharad Agarwal, Yan Chen, Matthew Caesar, Weidong Cui, Per Johansson, Kevin Lai, Tal Lavian, Sridhar Machiraju, Zhuoqing Morley Mao, George Porter, Timothy Roscoe, Mukund Seshadri, Jimmy S. Shih, Keith Sklower, Lakshminarayanan Subramanian, Takashi Suzuki, Shelley Zhuang, Anthony D. Joseph, Randy H. Katz, and Ion Stoica. The SAHARA model for service composition across multiple providers. In *Pervasive '02: Proceedings of the First International Conference on Pervasive Computing*, pages 1–14, London, UK, 2002. Springer-Verlag.

[19] Geetanjali Sampemane, Prasad Naldurg, and Roy H. Campbell. Access control for active spaces. In *ACSAC*, pages 343–352. IEEE Computer Society, 2002.

[20] Giovanna Di Marzo Serugendo. Trust as an interaction mechanism for self-organising systems. In *ICCS*, 2004.

[21] Kevin Walsh and Emin Gün Sirer. Experience with an object reputation system for peer-to-peer filesharing. In *NSDI*. USENIX, 2006.

[22] Li Xiong and Ling Liu. Building trust in decentralized peer-to-peer electronic communitties. In *International Conference on Electronic Commerce Research*, 2002.

[23] Li Xiong and Ling Liu. Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Transactions on Knowledge and Data Engineering*, 16(7):843–857, 2004.