Emergence of Privacy Conventions in Online Social Networks

[Extended Abstract]

Mohammad Rashedul Hasan
University of North Carolina at Charlotte
Charlotte, NC 28223, USA
mhasan8@uncc.edu

ABSTRACT

Online social networks (OSNs) user data have a great commercial value to marketing companies, competing networking sites and identity thieves. With the emergence of new web technologies public developers are able to interface and extend the online websites services as applications. Proposing a fine-grained access control model for controlling application access to the OSN user data does not solve the problem of extension vulnerabilities. Because users might deny all the permissions or deny a subset of the permissions that might render the app non-usable. Moreover, it would be difficult for the app developers to design apps based on these diverse policy preferences. Therefore, it is important for the users to reach a consensus about the privacy settings of the apps they are interested about. My research goal is to design an agent-based approach that harnesses game theory and the dynamical properties of social network to facilitate agent reasoning for achieving optimal privacy conventions in the OSN and to develop decentralized learning mechanisms that facilitate controlled and fast convergence to optimal conventions.

Categories and Subject Descriptors

I.2.11 [**Distributed Artificial Intelligence**]: *Multiagent Systems*

Keywords

Online Social Network; Privacy Conventions; Game Theory; Network Dynamics; Multiagent Learning

1. INTRODUCTION

The emergence of new web technologies [7] has brought exciting opportunities as well as posed severe privacy risks for the users in online social networks (OSNs). These online sites and frameworks provide open platforms to allow the seamless sharing of profile data. This enables public developers to interface and extend the online websites services as applications (or APIs). For example, Facebook allows anyone to create software plug-ins that can be added to user profiles to provide services based on profile data. Similarly web browsers and smart phones allow users to install extensions and applications (apps) to extend their functionality. However, although these open platforms enable such advanced features, they also pose serious privacy risks.

For example, the OSN user data have great commercial value to marketing companies, competing networking sites, and identity thieves. In the last few years several extension vulnerabilities have been discovered, which include stealing cookies, key logging, expose confidential information, and hijack the local operating system [4]. Current state of the art systems notify the users when installing apps, and highlight a summary of the permissions requested by the application. Most frameworks have adopted an all-or-nothing policy, where a user is required to allow all the permissions requested by the application for installing it. Ideally, users should be able to take advantage of the available extensions while still having strong control on their data.

However, designing a fine-grained access control model for controlling application access to browser resources does not solve the problem as users are not experts and will probably overlook these policy settings [2]. Users might deny all the permissions or deny a subset of the permissions that might render the app unusable. In addition, from the app developers' perspective to design apps that will cater to all the possible privacy policy settings is a challenging task. Therefore, it is important for the users to reach a consensus about the privacy settings of the apps they are interested about.

My research goal is to design a multiagent framework that enables the users to reach to a consensus on a preferred set of privacy settings or **privacy conventions** so that the app developers could easily design their apps to target these small number of privacy conventions. Moreover, it would require the users to select only one of the privacy profiles instead of specifying their preference for each of the requested permissions. This would ensure security with minimum user intervention as well as allow the users to enjoy the advanced app features. I will show how the software agents recruited by the respective human users could leverage the (a) **evolutionary game theory** and the (b) **dynamic properties of the OSN** to converge into the preferred privacy conventions.

2. APPROACH

Figure 1 provides a high-level view of the proposed framework. We regard apps in a specific category as members from the same *app community* providing similar functionalities, thus expected to request a similar set of accesses.

Appears in: *Proceedings of the 12th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2013), Ito, Jonker, Gini, and Shehory (eds.), May, 6–10, 2013, Saint Paul, Minnesota, USA.*

In the beginning, users receive policy recommendations to decide whether an app would be harmful to install or not. For these app policy recommendations pattern mining technique [3] will be used to mine likely properties in an app category (step 1). Based on the policy recommendations, users would install apps and would propagate their app settings over the online communities in order to influence other users on their app policy settings (step 3). However, in the OSN this may result in diverse policy setting alternatives or privacy profiles and the number of profiles of a given category could be very large (step 4). Therefore, in order to converge to a minimum set of profiles or conventions, an agent based technique will be used where every user will recruit software agents that leverage game theory to negotiate rational privacy preferences with other agents on the users' behalf (step 5). Agents share the user's initial privacy settings and user application usage metrics in its neighborhood OSN community (step 6). Upon receiving this information agents are able to compare their utility gains and choose appropriate strategy by adopting shared privacy preferences that optimize the gain with minimum cost. To assist the agents to choose the appropriate strategy we propose using the OSN dynamic properties [5] and multi-agent learning algorithms [1] (step 7 and 8). For example, agents with conservative privacy inclinations [6] would be aided to allign with a group of other agents in their neighborhood that share the similar preferences.

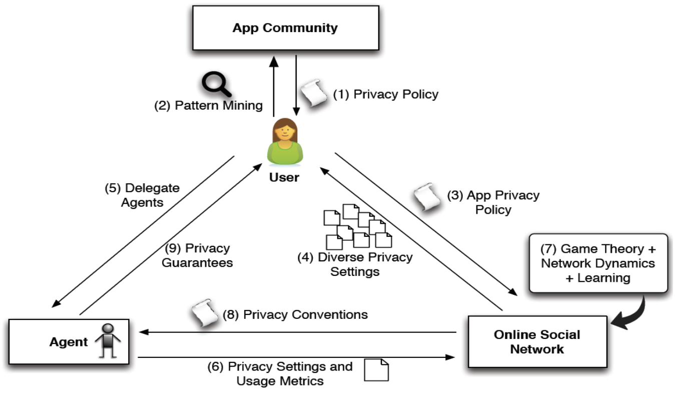

Figure 1: Emerging privacy conventions in online social network

The dynamics of the convergence of privacy conventions will be captured using an **evolutionary game theory** framework where an agent strategy (a privacy profile) is *evolutionary stable* if, when the whole network community is using this strategy, any small group of users using a different strategy will eventually converge over multiple iterations. We capture this idea in terms of numerical payoffs where an **agent's payoff** for adopting an alternative action in defined based on the utility associated with that action and what the other agents adopt. Both the utility and cost function for the game will be computed using metrics collected from the user statistics (based on experiments with actual app data).

Given a user's initial privacy settings, user application usage metrics, and local social network characteristics, the agent iteratively plays a privacy setting game and tries to find out appropriate strategies that would lead to a preferred privacy convention. To assist the agents in choosing the appropriate strategy I will use the OSN dynamic properties. However, agents' partial knowledge of the OSN structure could lead to frontier effects (FE) that results in a convergence into multiple sub-conventions [1]. FE arise when there is a stable barrier that separates the sub-conventions from each other leading to suboptimal equilibriums. In my preliminary work (see section 3) [5], I used agent attributes and dynamical properties of the network to resolve subconventions. I will extend this approach by using other network features such as the degree-degree correlation, link weight, assortativity etc. for the convergence. In addition to this, I will determine appropriate **multiagent learning** algorithms [8] to optimize privacy settings automatically over time.

3. PRELIMINARY RESULTS

We have developed a decentralized coalition emergence approach in a multiagent system operating on large scale-free networks [5]. Agent interactions with their immediate neighbors are captured by an iterated Prisoner's Dilemma game and we enable the agents to exploit the complex network dynamics to facilitate the convergence into a sustainable single coalition. Agents use the node coupling strength and payoff of their single-hop neighbors to join/form coalitions. We show that a single coalition emergence process is enhanced when the topological insights are embedded into the agent partner selection strategy. Instead of assuming a given pre-established network platform, our agents dynamically choose their interaction partners to form the network. Using a computational model we have performed extensive simulations and have shown that both increased degree-heterogeneity and clustering facilitates the emergence of a sustained single coalition over various types of scale-free networks.

4. REFERENCES

[1] S. Abdallah. Using a hierarchy of coordinators to overcome the frontier effect in social learning. In *AAMAS*, pages 1381–1382, 2012.

[2] A. Acquisti and J. Grossklags. Privacy and rationality in individual decision making. *IEEE Security and Privacy*, 3(1):26–33, 2005.

[3] R. Agrawal and R. Srikant. Fast algorithms for mining association rules in large databases. In *VLDB '94*, pages 487–499, 1994.

[4] S. Bandhakavi, S. T. King, P. Madhusudan, and M. Winslett. Vex: vetting browser extensions for security vulnerabilities. In *USENIX Security*, pages 22–22, 2010.

[5] M. R. Hasan and A. Raja. Emergence of multiagent coalition by leveraging complex network dynamics. Technical Report DAIR-2013-001, 2013.

[6] P. Kumaraguru and L. F. Cranor. Privacy indexes: A survey of westin's studies, 2005.

[7] T. O'Reilly. What Is Web 2.0. "http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html", September 2005.

[8] D. Villatoro, J. Sabater-Mir, and S. Sen. Social instruments for robust convention emergence. In *IJCAI*, pages 420–425, 2011.