

Traditional Group based policy management approach for online social networks

V.Surendra Reddy

Jagan's College of Engineering and Technology, Nellore

Abstract: - Privacy control mechanism based on policy frameworks that are rich in semantic web technologies to control information flow in social networking applications. The privacy control mechanism Provides users of the system better control while sharing information than the state of the art systems Combines dynamic user context, For instance, current time, current location or current activity of the user Online social networking is viewed by many as the next new paradigm in personal, professional and organizational networking and marketing. (Social media are the tools that people use to do social networking, such as Facebook, LinkedIn and Twitter.) The following sections first give a broad overview of the movement of social networking, including basics about each of the most popular tools. The next section describes how to use the tools for personal, professional and organizational networking and marketing.

I. INTRODUCTION

Online service providers, such as Facebook and Amazon, are beginning to collect various kinds of public and private data across the Web for the purposes of targeted marketing. A vast variety of data is collected about the user, and the current legal system has different legal standards for different kinds of data. This is problematic because the privacy policies against government and third-party intrusions are complex and confusing to the end user. To better protect consumers' privacy, all aggregated user data and online activities should be subjected to the same level of protection under a blanket privacy policy. Furthermore, we are proposing an accountability infrastructure for protecting consumer's online privacy. There are a lot of business marketing incentives to combine the data stored by these online services. Platforms have been introduced by these companies to better combine e-commerce and social networking. Currently, different kinds of data are protected under separate privacy policies and codes. The end user cannot predict how the data can be used by the government or third-parties, or how all their private information would be protected under the existing law.

II. BACKGROUND

Social networking sites are experiencing tremendous adoption and growth. The internet and online social networks, in particular, are a part of most people's lives. E-Market reports that in 2011, nearly 150 million US internet users will interface with at least one social networking site per month. E-Marketer also reports that in 2011, 90% of internet users ages 18-24 and 82% of internet users ages 25-34 will interact with at least one social networking site per month. This trend is increasing for all age groups. As the young population ages, they will continue to leverage social media in their daily lives. In addition, new generations will come to adopt the internet and online social networks.

III. OVERVIEW OF SOCIAL POLICY NETWORKING

The following links will give you a general understanding of social networking and its many uses, and will mention some of the most common social networking tools -- although the number of tools seems to be increasing daily. The following paragraphs in this Library topic give you more information about some of the most popular tools



Online social networking sites are experiencing tremendous user growth with hundreds of millions of active users. As a result, there is a tremendous amount of user profile data online, e.g., name, birth date, etc. Protecting this data is a challenge. The task of access policy composition is a tedious and confusing effort for the average user having hundreds of friends. In this paper, we propose a Policy Manager (PolicyMgr) Framework for social networks. PolicyMgr assists users in composing and managing their access control policies for objects posted to their profiles.

IV. GOOD PRACTICES FOR ONLINE SOCIAL NETWORKING POLICY

This social networking policy outlines five good practices for using the social networking tools employed by the Cost-Benefit Knowledge Bank. Following these practices will minimize risks to security and privacy that are inherent in any kind of communication. These guidelines suggest methods users of the Knowledge Bank can employ to meet record retention requirements and avoid copyright infringement and other legal risks. This policy also articulates the Terms of Service that users agree to when using the Knowledge Bank web site and its official outposts on other social networking services.



Good Practices for Online Social Networking

1. Know and follow your own organization's policies and guidelines.
2. Maintain an authentic online identity.
3. Treat all online activity as public activity.
4. Use strong passwords for your social media accounts.
5. Make a weekly transcript of your official social media activity.

4.1. Know and follow your own organization's policies and guidelines.

Find out if your employer has issued a policy for using online social media and networking sites, and make sure to follow those policies in your participation in the Knowledge Bank.

A number of state governments, including Massachusetts, Delaware, and North Carolina have issued policies specifically addressing use of online social media, as have government agencies at the federal, state and local levels, some nonprofit and educational institutions, and many companies. Most organizations, however, have yet to promulgate such policies.

If your organization does not have any explicit rules to guide your participation in online social networks, consult your organization's employee handbook, human resources or legal department for guidance on external communications and ethical standards. Even if your organization has adopted a social media policy, it may address only one form of social networking, or it may be primarily focused on using social media in relations with the public and the press, so you will still need to look to your employer's more general policies as a guide for your participation in the Knowledge Bank.

4.2. Maintain an authentic online identity.

Your participation in online media gains credence and accountability when you are transparent about your true identity and your professional role and responsibilities. Be clear in your communications whether you speak for your employer or for yourself. Present yourself and the organization you represent honestly and openly. Healthy and positive functioning of online social networks and communities relies on authentic onymity of participants.

Make sure your identity can be verified in your contributions to online social networks. When you create accounts on social networks, include a link in your profile that leads to a web page with information about you, such as a staff listing or C.V. and update those pages with links back to your social network profiles. These reciprocal links validate your contributions and help promote accountability within the community. They also help prevent your or your organization's identity from being hijacked by a third party.

In representing yourself online, avoid exposing personally identifiable information (PII). Many social networks allow messaging within the network so you do not need to reveal your e-mail address or telephone number. If you choose to make your e-mail address or phone number public, make sure to use an official, work-related e-mail address and phone number.

If you represent yourself with a picture in an online profile, use a small, low-resolution photo, no more than 144 pixels in width and height. You do not want to use a high resolution photo that could be used by someone else to create fake identity credentials.

4.3. Treat all online activity as public activity.

Regardless of whether you are using a password-protected online environment or not, you should consider any contribution to a social network to be a public activity. Comments on web sites, ratings and recommendations, referrals, the information in your public profiles, Facebook updates and Twitter messages – these are all forms of communication you should remember are public. You should take care with private e-mail messages, as well.

Anything online can be copied and shared with others very easily. Even if you share something within what you believe is a closed network, it can be copied and shared by any other person in the network to people outside of that network. Make sure that anything you say online is something you would be comfortable sharing in public.

If you stick to your areas of expertise, are polite and constructive in your contributions, and maintain an authentic online identity, you will be able to safely participate in the Knowledge Bank community online.

4.4. Use strong passwords for your social media accounts.

A strong password is essential to maintaining your authentic online identity and safeguarding your and your organization's privacy and reputation. Strong passwords are:

- 8 or more characters in length;
- are composed of a mix of letters, numbers, and non-alphanumeric characters;
- do not include or mimic words that may be found in a dictionary; and
- are different for each account you create. (If one of your accounts is hacked, none of your others are at risk.)

Write down your passwords for different accounts on paper and keep this paper in a safe place only you can see, such as your wallet. It is a bigger risk to use weak passwords you can remember and not write down than to use strong ones that are written down in one place.

Avoid using public or friends' computers to log in to password-protected services. You do not control the settings and security of those computers, and cannot know how safe or secure those computers are. There is a risk of logging in to a site from an unsecure computer that your password could be stolen by a "malware" program even the owner doesn't realize has infected their computer.

You should avoid using unknown Wi-Fi networks for similar reasons.

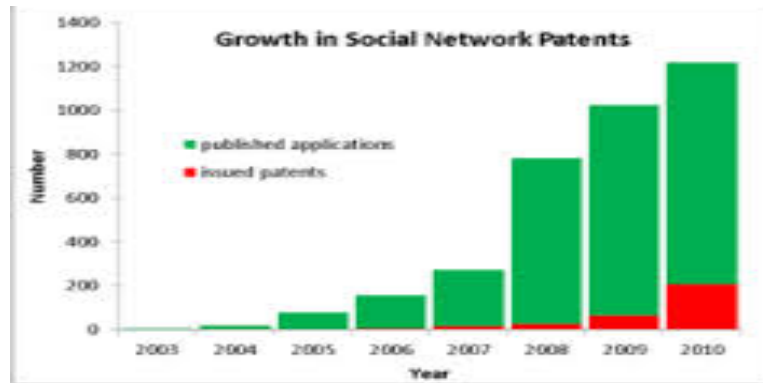
4.5. Make a comprehensive weekly transcript of your official social media activity.

Your organization's record retention requirements very likely apply to your participation in online social networking services. If that is the case, it is recommended that you save copies of your contributions to the Knowledge Bank. Copy and paste your comments, recommendations, e-mails, or other written activity on the Knowledge Bank site to a document (such as a Microsoft Word document) on your computer once a week. Alternately, you may use services such as Backup to automatically archive your social networking contributions. Their Threats to Privacy and a Proposal for a New Blanket Privacy Policy and Standard for Privacy Notices.

V. SOCIAL NETWORKING AND FACEBOOK

Web sites like MySpace, Facebook attract millions of users a year, and people ranging from teens to elders are signing up to use the online social networking services around the world. All these different services have a common theme—the social networks combine people from all around the world who share similar interests and friends. These social networking Web sites provide ways for members to communicate with each other, and give Web space for users to post information about themselves. These Web sites provide a low cost and convenient way for consumers to stay connected with the members of the Web site. These online social networking platforms also allow user to publish and control content about them easily. The databank of digital information has also helped users better and more quickly find information about others around the world. In 2005, MySpace has exceed Google's page views on the internet, and is expected to continue growing (Rosenbush, 2005). Besides helping users stay in touch with their friends, these Web sites now provide other services like media entertainment, shopping, job search, and many more. These Web sites continue to expand their services to attract more users to sign up, and continue to entice their existing users use the services more.

Facebook started as a social networking Web site for college students, and has opened up for public registration in 2006. The Web site offers basic social networking services such as ways to add other members as your friends. In addition, the Web site allows user to join networks and groups that share the same interest and views. Users can also share unlimited photos with their friends. Facebook also facilitates communications by allowing users to send messages to each other, and post messages on each other's profiles. Friends can also post events and invite guests on Facebook. Facebook also provide a bulletin board for users to sell and buy products from each other. More interestingly, Facebook has an open platform that software developers can use to create new applications on Facebook. New applications range from horoscopes to ways to arrange an itinerary for a vacation with your friends. Developers range from college coders looking for a fun project to companies looking for ways to take advantage of the mass distribution on Facebook.



VI. MAJOR SOCIAL NETWORKING TOOLS

Blogging

A blog is an online journal of information about a certain topic. The blogger, or owner of the blog, writes or publishes regular "posts," or articles, about the topic. Posts vary in size from 100 words to 1,000 depending on the nature of the topic. The posts might be published once a month or even once a day, depending on the blogger's time and energy for the blog.

A blog is a powerful means for the blogger to establish relationships with stakeholders by sharing his/her opinions and expertise on a regular basis. Stakeholders could include, e.g., customers, investors, employees, community leaders, collaborators and suppliers. The stakeholders read the blog posts to learn more about the topic and even more about the blogger

LinkedIn

LinkedIn is sometimes described as a "social networking service for adults". It's a very useful tool for quickly informing people about your professional experiences, skills and interests. You also can use LinkedIn to conveniently network with others who have similar backgrounds and interests. Compare LinkedIn to Facebook, below, which tends to be about more informal topics, such as personal background, interests, family, hobbies, friends, etc. Facebook People can join Facebook to share information about themselves or their organization. Information about themselves tends to be rather informal -- more so than LinkedIn. Organizations increasingly use Facebook as a public relations tool, to inform the public about the organization.

MySpace

MySpace is a social networking site for people to share information especially about themselves. Users of social networking often compare Facebook and MySpace and have strong feelings about which one is best.

Twitter

Twitter is a social networking site that allows the author to quickly share messages, or tweets, of up to 140 characters and with huge numbers of people. While 140 characters might seem quite limiting, an increasing number of people and organizations use Twitter to share opinions and even to advertise products and services. Some news organizations use Twitter to quickly broadcast up-to-the-minute news items.

YouTube

YouTube provides a forum in which people can show videos about a broad range of subjects, including about themselves and their organizations. The videos usually include audio/sound, so YouTube is a very quick, convenient, low-cost way to broadcast information about yourself and your organization. It's viewed by millions of people.

VII. POLICY NETWORK ONTOLOGY

- Integrates Rein and AIR policy ontology
- Rein policies to provide access control and AIR policies to provide justification to the inferences made
- Policies specified using N3 rules and Turtle.
- CWM, a forward chaining rule engine
- Pychinko, a forward chaining rule engine, written in Python, that implements Rete algorithm and allows for efficient processing of very large rule bases
- Supports a significant subset of the math, string, time and logic built-ins

VIII. PRIVACY POLICY FOLLOWS DENY-ACCESS APPROACH

It specifies authorization logic. Authentication is performed separately in the system. What information user is willing to share Location information with accuracy level

- With whom
 - Friends
 - Group of friends

```
@forAll REQ, LOCATION, WHO, USERID.
{
  REQ a rein:Request.
  REQ rein:resource LOCATION.
  ?T a TeachersGroupStuff.
  ?R a UserStuff; log:includes
  {
    LOCATION a tu:Location;
    USERID a tu:Userid
  }.
  REQ rein:requester WHO.
  ?T a TeachersGroupStuff; log:includes
  {
    [] t:member [ session:login USERID ]
  }.
  LOCATION loc:equalTo :UMBC .
  WHO :requestTime ?time.
  "" time:localtime ?localTime.
  ?localTime time:dayOfWeek ?day.
  ?day math:notlessthan "1".
  ?day math:notgreaterthan "5".
  ?localTime time:hour ?dtime.
  ?dtime math:notlessthan "9".
  ?dtime math:notgreaterthan "18".
} => { WHO loc:can-get LOCATION }.
```

- Under what conditions
- Day and time of the week
- Location of the user, specifying the area in which user can be seen
- Accuracy level of the location information
- Example policies can be :
 - Share my location with teachers on weekdays only if I am in the university campus and only between 9 am and 6 pm
 - Share exact location with members of family group all the time, in all locations
 - Do not share my location if user is at any of the sensitive locations
 - Do not share my activity status with teachers on weekends
 - Share my activity status with only close friends

```
@forAll REQ, ACTIVITY, WHO, USERID.  
{  
  REQ a rein:Request.  
  REQ rein:resource ACTIVITY.  
  ?TG a TeachersGroupStuff.  
  ?R a UserStuff; log:includes  
  {  
    ACTIVITY a tu:Activity;  
    USERID a tu:Userid  
  }.  
  REQ rein:requester WHO.  
  ?TG a TeachersGroupStuff; log:includes  
  {  
    [] t:member [ session:login USERID ]  
  }.  
  WHO :requestTime ?time.  
  "" time:localtime ?localTime.  
  ?localTime time:dayOfWeek ?day.  
  ?day math:matches "0".  
  ?day math:matches "6".  
} => { WHO act:cannot-get ACTIVITY }.
```

- User shares her protected resources and defines the privacy preferences
- System follows pull mechanism. All the different types of information sharing activities among participants are established by the privacy control module in the system.
- Whenever any participant makes a query, it is sent to the privacy control module which in turn processes the query by reasoning over the policy networks associated with the resource, and returns the valid answer to the query.

IX. CONCLUSION

I introduced two approaches to improving privacy policy management in online social networks. First, I presented an approach, leveraging proven clustering techniques that assists users in grouping their friends for policy management purposes. Our approach demonstrated reduced grouping times and improvements in ease of use over traditional group based policy management approaches. Second, I introduced same-As Policy Management, which leverages a user's memory and opinion of their friends to set policies for other similar friends. Our visual policy editor uses friend recognition and minimal task interruption to obtain substantial reductions in policy authoring times. In addition, same-As Policy Management was positively perceived by users over traditional group based policy management approaches.

X. FUTURE ENHANCEMENT

I presented an approach, leveraging proven clustering techniques that assists users in grouping their friends for policy management purposes. Our approach demonstrated reduced grouping times and improvements in ease of use over traditional group based policy management approaches. Second, I introduced same-As Policy Management, which leverages a user's memory and opinion of their friends to set policies for other similar friends.

REFERENCES

- [1]. Accoria. Rock web server and load balancer. <http://www.accoria.com>.
- [2]. Amazon Web Services. Amazon Web Services (AWS). <http://aws.amazon.com>.
- [3]. V. Cardellini, M. Colajanni, and P. S. Yu. Dynamic load balancing on web-server systems. IEEE Internet Computing, 3(3):28{39, 1999.
- [4]. L. Cherkasova. FLEX: Load Balancing and Management Strategy for Scalable Web Hosting Service. IEEE Symposium on Computers and Communications, 0:8, 2000.
- [5]. F5 Networks. F5 Networks. <http://www.f5.com>.
- [6]. R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, and T. Berners-Lee. Hypertext transfer protocol { http/1.1. In IETF RFC 2616, 1999.
- [7]. Google Inc. Google App Engine. <http://code.google.com/appengine/>.