

A Social Networking-Based Access Control Scheme for Personal Content

Kiran K. Gollu[†], Stefan Saroiu[†], Alec Wolman[‡]

[†]University of Toronto and [‡]Microsoft Research

1 Motivation

Personal media continues to drive the growth of home computing and consumer electronics. Equipped with various appliances, home users continue to create enormous quantities of photos, home videos, song collections, or blog pages. This new landscape has led to new challenges facing home users – managing their personal data, searching it to find objects of interest, and sharing it with family and friends.

These challenges have motivated the emergence of new class of web sites and applications such as MySpace, Flickr, YouTube, and Google calendar to help users manage and share their personal content online. However, there is a mismatch between people’s needs for sharing personal content and what today’s online applications offer. Most sharing sites restrict their users to a specific type of content. While sharing personal content warrants the need for restricting access, most sites (e.g., Flickr, YouTube) offer only two very simple access control policies. People can either enumerate all the site-specific userids who should have access or they can make the content publicly available to anyone. In addition, users must now create and maintain several copies of their social network: one for each online site. They must ask their friends and families to register userids on each site serving their personal content.

Our work presents a social networking-based access control scheme suitable for online sharing of personal media. Our goals are:

1. To present the design of the access control scheme that is centered around social relationships.
2. To illustrate how using social relationships to express access control policies is a new and powerful paradigm for controlling the sharing of personal data online by presenting three diverse applications.

2 A Social Networking-Based Access Control Scheme

In our scheme, users need to manage a single social network that can be stored in an address book on their own machines. This eliminates the need to manage many, site-specific social networks online. A personal identity is a pair of a public key and a private key. People communicate their public keys securely with their social networks through out-of-band mechanisms.

Our scheme introduces two new concepts:

Social Attestations: A social attestation is a piece of data that certifies a social relationship. Unlike capability-based models [1, 2], attestations do not include access rights. An attestation has four fields: an issuer, a recipient, a social relationship between two parties, and a relationship key. For

example, LinkedIn could issue an attestation to Bob certifying that Alice added Bob to her LinkedIn social network. Bob could prove his relationship with Alice to anyone who trusts LinkedIn. Attestations can be exchanged securely over insecure channels such as email, HTTP or chat.

Social Access Control Lists (ACLs): A social ACL contains an owner’s public key, the public keys of all people who can access the object (similar to traditional ACLs), and a social relationship. To access an object, people must either have their public key listed in the social ACL, or they must present an attestation issued to them by the owner certifying the relationship listed in the ACL.

3 Applications

In all the three applications below, our scheme uses the same set of attestations to control access.

Google Calendar: The sharing policies used by most of today’s online calendars are very restrictive. For example, the Google calendar allows sharing all information or just free/busy information with others. Instead, in our scheme, people can use social attestations to enforce fine-grained access control to different views of their calendars. They can publish different views of their daily schedules depending on the social relationship.

Social BitTorrent: Despite the immense growth of user-generated content, most online sharing systems are ill-suited for the needs of personal content. People still resort to email, and hosting websites to share personal photo albums. Instead, a peer-to-peer file-sharing system, such as BitTorrent, augmented with our access control scheme could serve as an ideal delivery vehicle for personal multimedia content. We implemented a prototype of our access control scheme in BitTorrent. We are planning to demo our new BitTorrent client.

Social Firewalls: In many scenarios, filtering based on IP addresses, port numbers, or protocol types is not sufficient for controlling access to resources behind a firewall. For example, organizations want to allow their employees to remotely access internal machines from any location, no matter what their IP addresses are. Instead, with our scheme, firewalls could implement access policies based on social relations. To bypass a firewall, a remote user must present a social attestation certifying the relevant social relationship.

References

- [1] R. Geambasu, M. Balazinska, S. D. Gribble, and H. M. Levy. Homeviews: Peer-to-peer middleware for personal data sharing applications. In *Proc. of SIGMOD International Conference on Management of Data*, Beijing, China, June 2007.
- [2] P. J. Keleher, N. Spring, and B. Bhattacharjee. Chit-based access control. Technical Report CS-TR-4878, University of Maryland at College Park, 2007.