Finding "Hidden" Connections on LinkedIn
An Argument for More Pragmatic Social Network Privacy

[Position Paper]

Jessica Staddon
PARC
3333 Coyote Hill Road
Palo Alto, CA 94304
staddon@parc.com

ABSTRACT

Social networking services well know that some users are unwilling to freely share the information they store with the service (e.g. profile information). To address this, services typically provide various privacy "knobs" that the user may adjust to limit access by content type or user identity. However, the main purpose of social networks, community building, is largely at odds with this, hence it is unsurprising that privacy breaches in social networks are increasingly discovered. We argue that this tension between social networking goals and privacy suggests that research efforts should be focused more on efficient methods for detecting privacy breaches in social networks and on building user awareness of privacy risks and the trade-off between privacy and utility. We support our argument with a simple method for discovering LinkedIn contacts ostensibly hidden by privacy settings. This method appears discoverable with a straightforward analysis of the LinkedIn system and its features (indeed, LinkedIn is likely aware of this method), however Linkedin's privacy instructions suggest to users that implementing a privacy setting will prevent such discovery.

Categories and Subject Descriptors

H.2.0 [**General**]: Security, integrity and protection

General Terms

Security

Keywords

Privacy, social network, LinkedIn, data mining, policy.

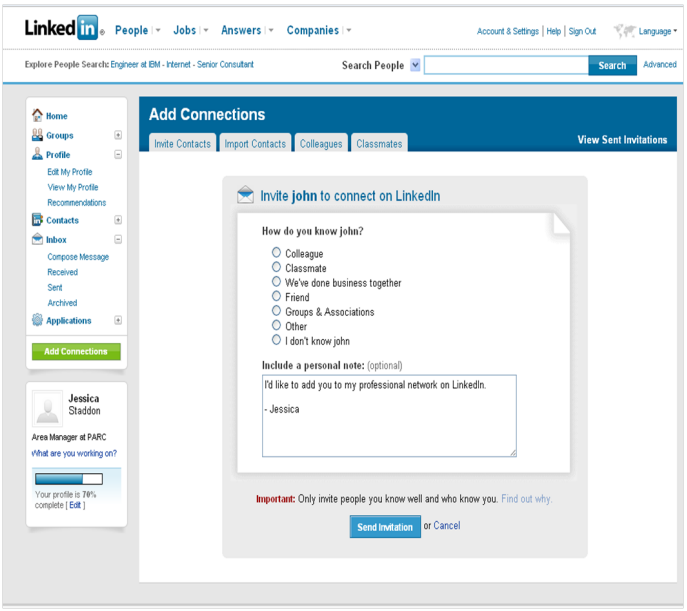

Figure 1: A user must select one of the above answers before inviting someone to be there LinkedIn contact; at least 3 of the categories ("Colleagues", "Classmates", "Groups & Associations") suggest that the inviter shares a profile attribute with the invitee. Note that at the bottom LinkedIn reinforces this by requesting that the user "only invite people you know well".

1. INTRODUCTION

For a variety of reasons (e.g. phishing and identity theft fears [12, 24]), many users are unwilling to freely share all the information they store with a social networking service and so such services commonly give users some ability to control their information. For example, Facebook [14] users can control who will be able to find them through Facebook's keyword search feature, and what information the searchers can see about them when they do find them through search. Adding to this, MySpace users can specify which users can see when they are online, and they can block access to their profiles by age or identity. In addition, many sites allow users to control what updates to their account are visible and by whom.

In addition to these various privacy features, social networking services provide tools serving what is their main goal: facilitating the formation of communities. To sup-

AISec'09, November 9, 2009, Chicago, Illinois, USA.

port this goal, many sites make suggestions for new contacts based on profile attributes, offer to mine email or text messaging history for contacts and support the creation of searchable groups within the social network. At a high-level, the community-building features make users of the service more intertwined and dependent. Users comment on each other's activities and may even develop similar attributes [4].

Clearly, the community-building goal is in direct conflict with privacy. Hence, well-intentioned though the privacy features may be, the existence of several privacy attacks [1, 2, 10, 12, 3] indicates they merely serve to placate privacy fears rather than providing actual protection. We believe that the prevalence of attacks stems from an inherent conflict between the utility of a social networking service and privacy. Hence, we argue that research should focus on efficient techniques for identifying privacy breaches in social networking services and communicating the trade-offs to users. In particular, the same network mining that is at the root of most attacks can, in conjunction with a model of the service, enable the detection of potential breaches and potentially enable metrics for gauging privacy risk.

We support our belief that the process of breach identification can be made more efficient with a simple method for reconstructing privacy-protected networks in LinkedIn [15]. This method can be easily discovered with an analysis of LinkedIn's functionality (and indeed the weakness is known to at least one blogger [22], and probably LinkedIn, as well) yet LinkedIn's privacy instructions lead the reader to conclude that the available privacy setting prevents such a leak. At best, there appears to be a communication failure between LinkedIn and its users.

2. RELATED WORK

We provide examples of contact discovery in LinkedIn, despite privacy protections. One motivation for our attack is the desire of phishers to improve the credibility of phishing messages by referring to contacts of the user target [12, 24]. Many far more sophisticated social network privacy attacks have already been discovered (see, for example, [2, 1, 3, 10, 25]).

The LinkedIn example illustrates the challenge of presenting privacy policies in user-understandable form and in reconciling policies with the user's own privacy concerns. These issues have been studied, particularly in the context of P3P policies, in [20, 19].

The database privacy community has recently made great strides in developing a formal and pragmatic model of privacy [6]. These ideas are clearly valuable in the context of social networks but do require adaptation to accommodate the interdependent nature of social networks as well as to allow the preservation of network utility.

Social network analysis is a long-standing research area (see, for example, [21, 11, 9]) however this work generally does not focus on privacy.

3. AN EXAMPLE

LinkedIn allows users some control over how easily their contacts are viewed. In particular, LinkedIn offers the following guidance to users who have selected the contact privacy setting [16]:"*Right now, your connections list is hidden from your other connections. If you would like to allow your trusted friends and colleagues to browse your connections list, click here.*"

It is very tempting to interpret this text as indicating that if user A is a contact of user B and user A selects the privacy setting described above, then no one will be able to tell that A and B are contacts. This is not the case. In particular, LinkedIn's search tool will still reveal the relationship. In addition, if A and B share a profile attribute (as is encouraged by LinkedIn, see figure 1) then this relationship is made easier to discover; for example, a contact of A's searching on the attribute shared with B will likely find B and discover the relationship, even with the privacy setting. This suggests a simple algorithm for discovering a user's contact list:

- Input: A login to user account, S, and a contact of user S, denoted T. We often call S the "attacker" and T the "target".
  1. From T's profile extract attributes from the employment fields labeled "Current" and "Past", and the "Education" field.
  2. Enter each attribute into the keyword field in LinkedIn's search tool [17].
  3. For any returned user, V, labeled "2nd" click on the "shared connections" region (if present) and look for a listing of T. If the "shared connections" region isn't present, click on V's name to see their profile and look in the "How you're connected to" region for a listing of T. If a listing of T is found in either region, add V to a set, C_T.
- Output: The set of discovered contacts, C_T.

An impedance to this process is the size of the searcher's own network. A large network will tend to lead to more hits for a given search, thus making the contacts of a target user harder to find. Adding to this is the fact that LinkedIn limits query results to 100, for free accounts. One remedy to this is the use of artificial LinkedIn accounts, that is a user establishes an account, links to a single other user (the target), mines their contacts and then simply removes the contact and initiates contact with a new target. By LinkedIn policy, the contact who is removed is not notified of this action and so is unlikely to notice the targeting. This leads us to a variant on the above approach that uses such artificial nodes (also called "Sybil" [5, 23] nodes); such nodes are easy to create On LinkedIn with a valid email account as only the attacker or other Sybils, need to connect to a Sybil. We describe below how Sybil nodes can be leveraged in conjunction with the method.

SYBIL EXTENSION FOR 3RD DEGREE ATTACKS. If user T above begins to receive phishing emails from their contacts, they are likely to start searching for the culprit amongst their first degree contacts. Hence, if the attacker is a third degree contact, then the attacker is harder to find as the group of third degree contacts is much larger and T has far less information about them, in particular, T does not know the complete path to a third degree contact.

Our contact discovery method cannot be implemented exactly as described by a third degree attacker because they cannot complete step 3; LinkedIn does not supply this information for 3rd degree contacts. However, with the use

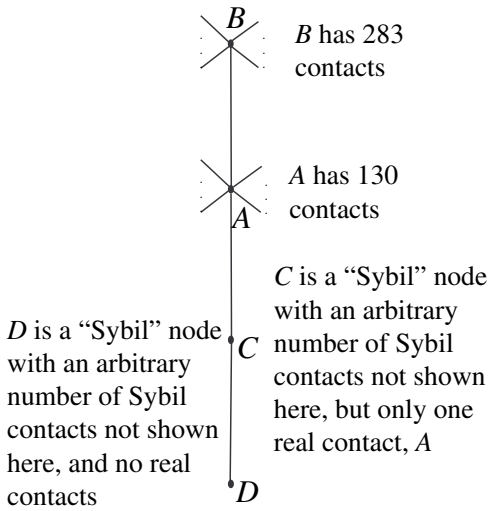

Figure 2: Nodes A and B represent 2 genuine LinkedIn users with 130 and 283 contacts, respectively. A is linked to Sybil node C which in turn is linked to Sybil node D. Nodes C and D may be linked to an arbitrary number of additional Sybil nodes (not shown in the picture) if desired.

of Sybil nodes this becomes unnecessary. The attacker simply ensures that any Sybil node attributes are different from those of the target, then any third degree contacts returned by a search query must correspond to a contact of the target T.

As an illustration of the above algorithm we conducted a small experiment on the network shown in Figure 2. This network consists of the author (A), a contact of the author (B), and 2 nodes created just for this experiment, C and D. C is connected to A in addition to D and D is only connected to C[1] We launched "first-degree" contact discovery attacks in which C attempted to recover the contacts of A and A attempted to recover the contacts of B. We also launched "second degree" contact discovery attempts in which C attempted to recover the contacts of B and D attempted to recover the contacts of A. Each attempt used the above algorithm with the difference that in the second degree case we look for "3rd" in step 3 (rather than "2nd") and we do not get complete network path information so we simply add any 3rd degree connection to the set of potential contacts. In all the experiments both A and B had the privacy setting in their account set to not share contacts as described in the introduction. The results are summarized in Table 1.

These experiments demonstrate the ease with which contacts are discovered by first-degree contacts if the user's network is "strong", meaning they share attributes with many of their contacts. That is, a strong network allows the method to achieve high recall[2]. In addition, perfect precision[3] is achieved because LinkedIn provides confirmation of the contact path.

Note that recovering contacts in this way does involve some work. The number of LinkedIn queries is small, on the order of the number of user attributes (possibly augmented to include variations on the phrasing of an attribute, e.g. "MIT" and "Massachusetts Institute of Technology"[4]), but it is then necessary to sift through the 100 results (in the case of a free account), clicking through many of the results to confirm the target contact is there. Hence, a maximum of 100×(number of user attributes) Web pages need to be reviewed. However, if the goal is merely to acquire *some* attributes (as may suffice in phishing, for example) then the attacker can merely stop when enough contacts have been discovered. In addition, given the existence of cheap outsourcing today via Amazon's Mechanical Turk [18], this attack can potentially scale.

4. SOLUTION DIRECTIONS

Since strong privacy properties run the risk of diminishing the utility of the network, we advocate the development of more efficient methods for identifying potential privacy breaches together with approaches toward promoting user-awareness of the risks. We highlight two areas for research, privacy-oriented analysis and modeling of networks and data mining-driven privacy metrics.

Privacy-Oriented Modeling and Analysis. Today's social networks share similar features and so it may be possible to construct a skeleton model of a social networking service that can be easily extended to capture each particular service. The model can then be formally analyzed to identify potential privacy breaches, for example, breaches stemming from conflicts between privacy settings amongst contacts (e.g. [25]) seem potentially identifiable with such an analysis.

Attacks relying on information outside the social network (see examples in [6]) are unlikely to be detected with such an approach and so an interesting question is how to represent such outside information in the model. There may be detectable patterns in previous breaches that yield heuristics that have the same effect as explicitly modeling outside knowledge. Or conversely, deviations from "normal" social network use may be sufficient to flag attempted breaches.

Data Mining-Driven Privacy Metrics.As the LinkedIn example shows, it can be difficult to clearly communicate privacy risk to users. What the LinkedIn page says is accurate, the list of contacts is not viewable, however it leaves out the fact that much of the list of contacts is easily discovered. Hence, we suggest that a notion of the work associated with discovering a piece of information (e.g. a contact) is what needs to be communicated to the user for privacy reasons.

This information might also inform the design of the network, that is, mechanisms might be put in place to ensure

[1]An arbitrary number of Sybil nodes may be connected to C and D to make them appear more typical in the network, but ideally any attributes those nodes have would be different from those of A and B to avoid diluting search results.

[2]Recall is the fraction of true contacts that our method finds.

[3]Precision is the fraction of discovered contacts that are true contacts.

[4]However, Linkedin handles some of this for you, so only a minimum amount of manual augmentation is needed.

(X,Y)	Distance from X to Y	Recall, Free Account	Recall, Premium Account	Precision, Free Account	Precision, Premium Account
(A,B)	1	.37	.72	1	1
(C,A)	1	.78	.79	1	1
(D,A)	2	.78	.79	1	1
(C,B)	2	.01	NA	.19	NA

Table 1: Each row describes the success X has in discovering Y's contacts using our method. For these calculations we assume C and D are not connected to any additional Sybil nodes, although they could be with the amendment that those nodes not share any attributes with A or B so as to not dilute the search results. Premium precision and recall are not available for the last experiment because we have not paid for that level of service from LinkedIn. We can provide those numbers in the 3rd row because the lack of contacts of the Sybil nodes implies that any contacts we discover are true contacts.

that more sensitive information is more work to obtain akin to the way work has been suggested as a spam deterrent [7]. The work necessary for most social network privacy breaches has a mining aspect (e.g. mining of user profiles). In some cases (e.g. the LinkedIn example) it is correlated with attributes of the user's own network. For example, in the LinkedIn example, privacy breaches are more difficult for users with large networks. This suggests that one way to ensure some level of privacy is to allow the user more extensive use of the service as their network grows (e.g. higher query limits). Determining how to do this while still meeting the community building goals of the network is a research challenge.

5. CONCLUSION

We have added to the existing pool of social network privacy breaches, a very simple method for breaching LinkedIn's contact privacy. The simple nature of the attack supports our argument that many attacks may be detecting through a formal modeling of network and an analysis focused on privacy. In addition, we suggest that given the tension between network and utility and privacy, a more pragmatic approach that leverages data mining and potentially other AI tools to *calibrate* the difficulty of an attack is an effective way to communicate risk to users.

6. REFERENCES

[1] L. Backstrom, C. Dwork and J. Kleinberg. Wherefore art thou r3579x? Anonymized social networks, hidden patterns and structural steganogrpahy. *WWW 2007*.

[2] J. Becker and H. Chen. Measuring privacy risk in online social networks. *Web 2.0 Security & Privacy 2009*.

[3] J. He, W. Chu and Z. Liu. Inferring Privacy Information From Social Networks. *IEEE International Conference on Intelligence and Security Informatics*, 2006.

[4] D. Crandall, D. Cosley, D. Huttenlocher, J. Kleinberg and S. Suri. Feedback effects between similarity and social influence in online communities. *KDD 2008*.

[5] J. Douceur. The Sybil attack. *First International Workshop on Peer-to-Peer Systems, 2002*.

[6] C. Dwork. Differential privacy: A survey of results. *Theory and Applications of Models of Computation.*, April, 2008.

[7] C. Dwork, A. Goldberg, and M. Naor. On memory-bound functions for fighting spam. *In Advances in Cryptology - CRYPTO 2003*, volume 2729 of Lecture Notes in Computer Science, pages 426-444. Springer, 2003.

[8] A. Felt and D. Evans. Privacy protection for social networking platforms. *Web 2.0 Security & Privacy 2008*.

[9] L. Freeman. *The Development of Social Network Analysis.* Vancouver: Empirical Press, 2006.

[10] R. Gross and A. Acquisti. Information revelation and privacy in online social networks (the Facebook case). *WPES 2005*.

[11] L. Izquierdo and R. Hanneman. *Introduction to the formal analysis of social networks using Mathematica.*

[12] T. Jagatic, N. Johnson, M. Jakobsson and F. Menczer. Social Phishing. *Communications of the ACM*, October, 2007.

[13] G. Lebanon, M. Scannapieco, M. Fouad and E. Bertino. Beyond k-Anonymity: A Decision Theoretic Framework for Assessing Privacy Risk. *Privacy in Statistical Databases 2006*.

[14] http://www.facebook.com

[15] LinkedIn. http://www.linkedin.com

[16] http://www.linkedin.com/static?key=pop/pop_more_browse_connections

[17] http://www.linkedin.com/search

[18] Amazon's Mechanical Turk. https://www.mturk.com/mturk/welcome

[19] M. Prabaker, J. Rao, I. Fette, P. Kelley, L. Cranor, J. Hong and N. Sadeh. Understanding and capturing people's privacy policies in a people finder application. 2007 Ubicomp Workshop on Privacy.

[20] R. Reeder, P. Kelley, A, McDonald and L. Cranor. A user study of the expandable grid applied to P3P privacy policy visualization. WPES 2008.

[21] J. Scott. *Social Network Analysis: A Handbook*. Sage Publications, 2000.

[22] Socrata blog entry, October 10, 2008. Do you hide your LinkedIn connections? http://blog.socrata.com/2007/10/10/do-you-hide-your-linked-in-connections/

[23] S. Webb, J. Caverlee and C. Pu. Social Honeypots: Making friends with a spammer near you. *CEAS 2007*.

[24] J. Widman. Go phish! How to guard your privacy on Facebook. *PCWorld*, May 1, 2009.

[25] E. Zheleva and L. Getoor. To join or not to join: The illusion of privacy in social networks with mixed public and private user profiles. *WWW 2009*