Faceless: Decentralized Anonymous Group Messaging for Online Social Networks

Xiaoxiao Song, David Isaac Wolinsky, and Bryan Ford

Yale University

{xiaoxiao.song, david.wolinsky, bryan.ford}@yale.edu

Abstract

Social networks (SNs) enable physically distributed groups to communicate seamlessly. Unfortunately such communication can be easily mined by adversaries in attempts to breach users' privacy or suppress open discussion on sensitive topics. While anonymous posting can help protect users by hiding the link between individuals and the messages they post, existing anonymization schemes are centralized or vulnerable to well-known attacks. To offer stronger protection for free speech online, we propose a method for anonymous group communication using SNs called Faceless. Faceless leverages existing Internet-based SNs for convenience in managing groups and users' public identities, but augments these centralized services with a decentralized anonymous posting overlay offering provable anonymity guarantees, resisting even group infiltration and traffic analysis attacks.

Categories and Subject Descriptors D.4.6 [*Security and Protection*]

Keywords Social networks, anonymity, anonymous communication

1. Introduction

Online social networking (SN) sites such as Facebook and Twitter, and the group-oriented messaging features they provide, have become increasingly popular channels for online self-expression and discussion. When a user posts a message to a group, the SN normally makes public the identity of the message's sender, as is usually preferred. In discussions on sensitive or controversial topics or in political discussion by citizens of nations that lack freedom of speech, however, users often desire the ability to participate and post messages anonymously. Users often pursue this anonymity by creating SN accounts under pseudonyms, but this approach violates the policies of most SNs, leaving these users at risk of being unfairly silenced by their critics via "terms-of-use attacks" [6].

To address the demand for anonymous communication in SNs, GroupTweet[1], allows Twitter users to post messages to a group anonymously. While well-intended, the anonymity offered by such a service is difficult to measure, and it suffers the same fundamental security flaws as prior, centralized anonymization services such as Anonymizer[2]. Twitter or GroupTweet servers might log message submissions, revealing the true identity of a message's sender to repressive governments or other authorities that can exert political or economic pressure, to hackers that succeed in compromising any of the servers, or to system administrators with otherwise-legitimate access to the servers. Even if GroupTweet's centralized anonymization service remains uncompromised, traffic analysis or other "side-channel" techniques can enable an attacker to link a message with its sender. Many SNs publicly identify which members of a group are online at a given moment, for example, for the well-intentioned purpose of supporting instant messaging activities. An attacker can use this online information, however, to correlate the time particular group members were online or otherwise active on the SN and the time a particular message was posted anonymously. Long-term intersection attacks over multiple pseudonymous posts can further amplify such side-channel attacks [2].

To address these concerns, we introduce Faceless, a platform enabling members of a SN group to post messages anonymously with stronger security properties. With Faceless, users need not create SN accounts under false names and risk account shutdown due to terms-of-use violations. Instead, SN users can use their real names for casual (non-sensitive) interaction and online discussions. When they wish to participate in a more sensitive online discussion, however, users can post messages anonymously to SN groups via a *decentralized* anonymity network that Faceless provides, which hides the link between their real identity or SN account and the messages they post anonymously. Unlike the GroupTweet, Faceless's anonymizing network stands independently of the SN and provides strong, quantifiable and provable anonymity guarantees, even if some of the anonymizing servers are compromised and the adversary is capable of sophisticated traffic analysis attacks [4, 5].

2. System Architecture Overview

The Faceless concept, as shown in Figure 1, embodies the following two properties: First, some subset of group members can post to the group "wall". Second, only messages

[1] `http://grouptweet.com/`

[2] `http://anonymizer.com/`

SNS'12, April 10, 2012, Bern, Switzerland.
ACM 978-1-4503-1164-9/12/04.

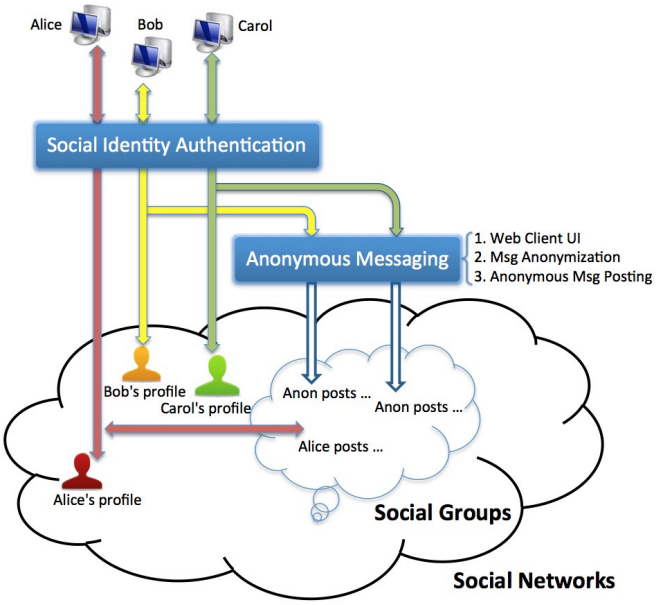

Figure 1. Faceless System Architecture

submitted into the anonymity network by members of a group should be posted to the group "wall." Within this domain, we describe two models. The simple approach limits access to an anonymity network to members of a SN group, where any member of that group can post a message. But we also envision more complex environments, where both practicality and anonymity benefit from a larger aggregation of groups, wherein many SN groups (amongst other applications) use a single anonymity network and use ring signatures [7] to limit message submission to group members.

Faceless builds on the following three technologies:

Social Identity Authentication: When a user interacts with a Faceless client for the first time, they enable Faceless access to their SN identity, a common constraint for all SN applications. Faceless can leverage this connection to authenticate with other members or services.

Anonymous Messaging: In order to remove the linkability between a message and the original submitter of the message, Faceless relies on an anonymity network.

Social Group: Message boards enable efficient group communication. By utilizing the integration within SNs, members can easily identify and authenticate members, and by pushing messages through the anonymity network can enable anonymous group communication leveraging SNs.

In our proposed system, we envision a user will download and run a Faceless application. Upon starting, users will be navigated to a web site hosted locally, where they will select their SN of choice and enter their credentials for that SN. The user will be presented a screen listing the various groups for which they have membership. For each of the user's group, recently posted messages as well as a box to post messages will be visible. In the background, Faceless uses information embedded within the SN and other sources to establish connectivity to a decentralized anonymity network, such as Tor [3] or Dissent [1]. When a member posts a message to the group, Faceless will choose the appropriate recipient who will actually do the anonymous post and transmit the message. When that member receives the message, it will be posted both on the SN website as well as be visible from within the Faceless client. Because Faceless client utilizes a service styel approach, users can leave it running transparently in the background, contributing to the groups anonymity set size.

At this point in time, our work has focused on the practicality of this approach. We have chosen Dissent [1] as the anonymity network due to its strong anonymity guarantees and we are focused on making Facebook the first Faceless supported SN due to its ability to embed information into profiles as well as third-party authentication techniques.

3. Conclusion and Future Work

In this paper, we have shown a model for anonymous group communication in members of SN groups called Faceless. While our implementation remains a work in progress, we have described a foundation that ensures its practicality and utility. For future work, we plan on considering the impact of anonymity group aggregation, mitigating denial of service attacks, and considering the applicability of membership concealing overlays.

References

[1] H. Corrigan-Gibbs and B. Ford. Dissent: accountable anonymous group messaging. In *17th ACM conference on Computer and communications security*, pages 340–350, Oct. 2010.

[2] G. Danezis and A. Serjantov. Statistical disclosure or intersection attacks on anonymity systems. In *Information Hiding*, May 2004.

[3] R. Dingledine, N. Mathewson, and P. Syverson. Tor: the second-generation onion router. In *13th USENIX Security Symposium*, 2004.

[4] P. Mittal et al. Stealthy traffic analysis of low-latency anonymous communication using throughput fingerprinting. In *18th ACM Conference on Computer and Communications Security*, Oct. 2011.

[5] S. J. Murdoch and G. Danezis. Low-cost traffic analysis of Tor. In *Security and Privacy*, May 2005.

[6] D. O'Brien. Google+, real names and real problems, Jan. 2012. `http://www.cpj.org/internet/2012/01/google-real-names-and-real-problems.php`.

[7] R. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In *ASIACRYPT*, Dec. 2001.