Consumer-Centric Protection for Online Social Networks

Raja Naeem Akram, Ryan K. L. Ko, and Tsz Fung Law
Cyber Security Group, Department of Computer Science,
University of Waikato. Hamilton, New Zealand
{rnakram, ryan}@waikato.ac.nz, tfl3@students.waikato.ac.nz

Abstract

Online Social Networks (OSNs) are a unique construct that is shaped by the advancement and availability of Internet technologies. A large portion of internet users make use of OSN services to share and celebrate their personal lives with friends and family. A substantial proportion of these shared experiences revolve around privacy-sensitive information. The OSN services handling privacy-sensitive information deploy state-of-the-art security and privacy-preserving mechanisms. However, these protections are, to a great extent, not consumer-centric: this is the main focus of this study. In this paper, we define the notion of Consumer-Centric Protection (CCP) for OSNs. In this proposal, the individual user controls how her data can be accessed by her contacts (e.g. friends and family members) and others, thus giving control of user data back to the rightful owner — the user. This work is still in progress and in this paper we present our preliminary results.

1 Introduction

In our societies, social structures define sets of social entities and their roles/responsibilities. Such formations are so fundamental to human societies that with the advent of any technological revolution in communication, it is inevitably translated into new means of communication. Examples include pen-pals using letters, telephones and internet chat.

The advent of the internet also introduced the concept of the cyber world and the constructs of the real world were then translated and in some cases reinterpreted. Among these structures were social networks that were translated into social networking sites. There are a number of social networking sites including Facebook, Google+, Twitter, Pinterest and LinkedIn, to name just a few. A large number of online users engage in one way or another with these social network sites, which are also called "Online Social Networks (OSNs)".

OSNs project themselves as human-centric services that facilitate the sharing and exchanging of life experiences. In most OSNs (e.g. Facebook, Google+) the user data resides on the network and providers use it to target their services to individual users [11]. In certain situations such sharing of information might be detrimental to the users' privacy and security [15, 22]. The openness and accessibility of the information on OSNs has created some unintended consequences, including employers or potential employers evaluating a job applicant's OSN profile. Furthermore, facial recognition technologies can be used to match an individual with his/her OSN profile [1, 29]. To provide a secure and privacy-preserving service, certain OSNs have updated their privacy policies. These steps are commendable; however, the security and privacy of the data is still placed in the hands of the consumers. If a user does not configure her privacy setting properly, she may end up sharing more than intended while maintaining a false sense of security. It is correct that applying default settings with strong privacy requirements is one potential solution; however, in our opinion a consumer-centric mechanism would empower the user more.

In this paper, we focus on a consumer-centric privacy mechanism that provides a seamless and least-interaction-based framework. The aim is to build a framework that does not require consumers to change their normal behaviour in terms of how they use the relevant OSN, and does not require any additional configuration/tasks to be performed by the consumer. As a case study, we base our development on Facebook: the rationale for choosing it was its top position in terms of number of total users and daily visits.

The proposed consumer-centric protection mechanism is based on state-of-the-art cryptographic mechanisms that secure the user's data before uploading it to the appropriate OSN. To do so, we have proposed an additional layer between the web browser at the user's end and OSN interface (website). This additional layer takes care of all security- and privacy-related tasks in a seamless manner. Only the authorised entity, the data owner[1] can decrypt it. The en-

[1]Data Owner: In this paper, the data owner is referred to as the user or entity who uploads the data on an OSN.

cryption and decryption process is completely hidden from the user and she does not even realise that such an operation is taking place, thus meeting our seamless integration requirement.

The key contributions of the paper include but are not limited to: 1) Giving control of data to users, not to any centralised authority (i.e. OSN operator), 2) A seamless framework that does not require users to change their behaviour to use their preferred OSN, 3) A consumer-oriented privacy framework that encrypts all user activities like sending text messages, status updates, and uploading images, 4) A secure key sharing mechanism to enable only authorised users to view the information (i.e. messages and images).

1.1 Structure of the Paper

In section 2, we briefly discuss OSNs and associated security and privacy issues. This section also looks at the existing work in the field of OSN data privacy and how it compares to the proposed framework in this paper. Section 3 provides a rationale for the consumer-oriented privacy-preserving framework proposed in this paper, along with the requirements for the proposed framework and a generic architecture. In section 4, we describe the implementation of our framework to provide consumer-oriented privacy. Finally in section 5 we conclude the paper and provide future research directions.

2 Online Social Networks

In this section, we briefly introduce OSNs and discuss the related security and privacy issues. The section concludes with the discussion of existing solutions that provide data control in OSNs.

2.1 Brief Introduction

The phenomenon known as OSNs began with the first well-known site called `SixDegrees.com` [21], which implied the potential to connect any two users in the world. The upsurge in OSNs began in 2003 [21] when sites like LinkedIn, Facebook, YouTube and Twitter offered their services to online consumers. The advent of OSN sites has had a profound effect on both business and popular culture [8].

The main objective of the OSNs was to foster closer connections and collaborations between individuals who are either in a social network in the real world or who are part of an online community. This objective brought a unique set of risks and challenges; nevertheless, consumers have flocked to these services in large numbers and usage is still growing at a phenomenal rate [18]. A pivotal role in this proliferation is played by the accessibility and ease with which a user can share his or her information and gain a sense of relationship and intimacy with friends and family on an OSN [12].

A huge amount of personal information is being shared by OSN users and the OSN operators can use this information to target their customers or shape their services according to customers' requirements [14]. With the advent of smartphones, a new dimension to OSNs was created that targets the more tech-savvy customers. There is a multitude of smartphone applications, provided by traditional OSNs like Facebook and Twitter, along with smartphone-based OSN providers like Snapchat and WeChat. In this paper, we will focus only on the traditional OSNs; however, the proposed framework in its generic architecture could also be deployed as part of the smartphone-based OSNs.

User-generated data is crucial for both the user and respective OSN business models. However, the architecture and roles around this user data are vague. Both the user and the OSN can simultaneously assume the role of data controller (owner) and data processor [11]. The architecture and associated services of an OSN are provisioned and maintained by the OSN operator, which can then qualify as a data controller for the user's data (account and usage data) after the user's consent [28]. The OSN operator can use this information for commercial benefits. In contrast, the user can qualify as the data controller for the personal data which (s)he publishes on the OSN, such as pictures, videos and messages. For such data, the OSN should be merely the data processor, which stores and publishes the user data.

However, the oversimplified explanation of how data is managed by an OSN as presented above might not be correct in many situations. There are a number of OSNs and their respective privacy policies declare that the operator has the right to use the user's (uploaded) data for their own commercial purposes [11]. The wide range of services that facilitate real-time communication and exchange of data (images, videos, and messages, etc.), and the security and privacy concerns around such data have emerged as a critical issue [24]. Such concerns are discussed at various levels including by industry, academia and even governments [14]. We will discuss these concerns succinctly and examine the existing proposals for potential solutions to such concerns.

2.2 Security and Privacy Issues

The security and privacy concerns regarding OSNs stem from the lack of a strong track record for protecting users' privacy [17]. If a user makes a misconfiguration or the OSN does not provide a robust privacy management facility, it is difficult to protect a user's data from being copied and used for nefarious purposes [7]. The privacy risks associated with user data on the OSN include but are not limited

to:

1) Loss of control of data (storage, access, and dissemination) 2) No control of how such data is used by third parties 3) Potential for identity theft

In addition to the above list, there are other concerns about the privacy of the data as highlighted by social phishing. In social phishing, a malicious user can learn about a user through his or her OSN profiles/information and then try to use this information to again access to or advantage from the user's friends, family or colleagues. The personal information presented online can also be used by online crooks, stalkers and bullies [2]. There are also instances in which information available on OSNs used to spy on citizens or foreigners [16].

Disclosing information on OSNs cannot be curbed: it is difficult to convince users to stop using OSNs or limit the information that they share. A large portion of OSN users do understand the privacy risks but still use the sites either because of lack of strong privacy protection tools or the idea that such information cannot be used in any damaging way [9]. An important point to note is that information shared over an OSN is more or less permanent and making it disappear or removing it is potentially a difficult proposition [19]. Users will keep on sharing information and there will be the potential for breaches by different actors in the OSN ecosystem.

There is a misconception that most OSN users are not interested in data privacy [13]. In this paper, the notion of privacy is defined as control over the access, flow and usage of user data uploaded on OSNs. The user who is uploading the data should be helped to exercise his/her rights over his/her data. This is the main objective of this paper and the proposed framework. Furthermore, in the context of this paper we assume all three entities (Service Providers, Other Users, and Third-Party Applications) to be less than trustworthy.

3 Consumer-Centric Protection for Online Social Networks

In this section we discuss the rationale behind our proposal, along with the design challenges faced. Finally, the section ends with a succinct description of the proposed framework and why we selected Facebook for our PoC.

3.1 Rationale for Consumer-Centric Protection

A large number of online users have opted in to various OSNs and most of these OSNs are based on a centralised architecture. Therefore, our choice of target OSN type was based on deployment and consumer population.

In centralised OSNs, proposing a mechanism that requires modifications to the deployed architecture is attractive and can be argued to provide a more robust solution. However, in most cases, achieving this in real terms is close to impossible. Therefore, we chose to provide an OSN-independent solution. This even included the option of creating an application for the OSN provider.

The rationale behind a consumer-oriented solution is to empower the user, the main driving force of any business and especially of OSNs. Users have the most at stake in the OSN ecosystem, as it's their data and in certain situations leakage of it would be detrimental to their privacy and possibly even their physical security. This provides a strong reason to design a solution that is aimed at the users but at the same time does not require them to change their activity patterns. Modifying how a user performs mundane tasks usually either ends up being ignored or else the user just opts out of it: an example of this is the secure email and (smartphone) online messaging services [3].

Furthermore, when designing consumer-oriented solutions, the proposal should require minimal interaction on the user's part and accomplish most of the security- and privacy-related operations seamlessly in the background [4]. Therefore, the proposal not only has to provide a robust, scalable, secure and privacy-preserving architecture but it also has to be a lightweight mechanism that performs most of the tasks with minimal user interaction.

3.2 Requirements for Consumer-Centric Protection

In this section we propose the fundamental requirements for the proposed framework. These requirements are by no means an exhaustive list, but should be taken as the initial set of requirements at the current stage of the work on consumer-oriented protection.

3.2.1 User's Personal Space Privacy

The user's personal space on the OSN refers to their profile, messages (e.g. status updates) and images. This requirement demands that information present on the personal space of the user should only be accessible[2] to the users and to entities as defined by the users.

3.2.2 User's Communication Privacy

Individual users might communicate with their contacts using OSN services. All such communications should be protected and only the intended recipients should be able to access the information.

[2]Accessibility in this context means access to the understandable (plaintext) information and not the encrypted information.

3.2.3 Privilege to Reveal and Control

Finally, users should have total control over their information. This total control extends to not only include users' friends and family but also OSN providers.

The generic architecture of our proposal is discussed in the next section, followed by the rationale for why we choose Facebook to be the host OSN for our PoC.

3.3 Proposed Architecture for Consumer-Centric Protection

The proposal is required to be a seamless and least-interaction solution. For this reason we are proposing a thin and lightweight layer called "Consumer-Oriented Protection (COP)" to be added to the traditional model of the OSN. Figure 1 shows a reference architecture for an OSN with the proposed COP layer.

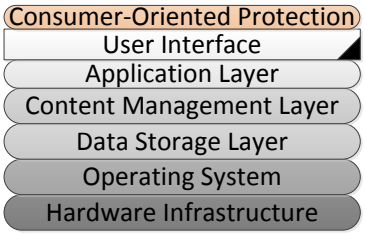

Figure 1. Reference Architecture of an OSN with Proposed COP Layer

The basic components of an OSN are constructed over the hardware infrastructure and the underlying operating system. The data storage layer deals with different storage technologies to support a reliant and robust architecture. The content management layer is where most of the OSN management services are deployed and this layer deals with the user/data management, access control and content aggregation. On top of this layer is the application layer that provides user-oriented services like searches, music, videos and photo rendering. The user interface is the layer that a user directly interacts with and it is in most cases the website of the OSN. Our proposed layer sits on the top of the user interface without requiring any change to it. It should be implemented as a transparent layer and from the users' point of view they should be directly interacting with the user interface. However, before the user interface transfers information to the application layer the COP will enforce the user's protection policies.

From an operational point of view, the user interface is presented to the user via a web browser. Therefore, the most suitable place for our proposal to be implemented is at the web browser. Therefore, the proposed COP is implemented as an add-on to the web browser that observes the user's activities and for data where a privacy policy has to be enforced, it interrupts these data transfers and treats the data accordingly.

There are three main protection operations that the COP preforms: encrypting and decrypting data and key exchange. In addition, from an operational point of view the COP also retrieves the user's contacts and any groupings defined on the OSN (e.g. user groups on Facebook). As a design ideology we opted for not storing user's contacts to any server, including the COP's server[3].

Facebook is the top OSN provider by far in the market. The total number of active users and unique visitors to Facebook makes it the major market leader [18]. For this reason we chose Facebook for our initial PoC. Although in this paper we are only discussing the Facebook implementation, in future we would like to extend it to other major OSNs.

4 Consumer-Centric Protection for Facebook

In this section we very briefly discuss the current state of the PoC for the COP proposal based on Facebook.

4.1 Initial Implementation

As our initial PoC implementation, we developed an add-on for the Firefox browser. This add-on represents the COP layer depicted in Figure 1. The browser add-on interrupts status update, message sent and image upload events. After intercepting these events, the add-on then encrypts these data values accordingly. For encryption we are using Advance Encryption Standard (AES) in Cipher-Feedback Mode (CFM) and Galois/Counter Model (GCM). For key share mechanism, we have currently implemented ECC based encryption/decryption mechanism. The AES keys used to encrypted data is embedded with the data encrypted with the public key of the intended recepient. Similarly, when a user browses a Facebook page and there are some items that are encrypted, the add-on automatically detects them. It then decrypts them and displays them to the user. In all this process of encryption and decryption the user is not actively involved. The user only has to enable the encryption of different data types (e.g. status update, messages and images).

Figure 2 shows the before and after situation when a user updates his or her status on Facebook. When the user clicks the "Post" button or presses "Enter," the add-on captures the data (in this case the "Testing Status") and encrypts it. The

[3] In its current stage of the PoC, the COP proposal is based on a completely decentralised architecture. However, further experiments and evaluation are required to decide which architecture would be most suitable for the COP proposal.

Figure 2. Status update message before and after encryption

encrypted value is displayed to the user. A point to note is that on the next page refresh or after a certain amount of time, the encrypted status will be displayed to user as plaintext as shown in Figure 3.

Figure 3 also shows that when a user comments on a status update, message or an image, the add-on interrupts the data and encrypts it.

Figure 3. Comments before and after encryption

As with previous operations, in Figure 4 a user is uploading images to Facebook. The add-on interrupts the uploading processing and encrypts the image before transferring it to the OSN server.

All of the operations discussed in this section are performed by the add-on in a seamless manner. We do not modify the OSN interface. The only implementation is done as part of the browser add-on.

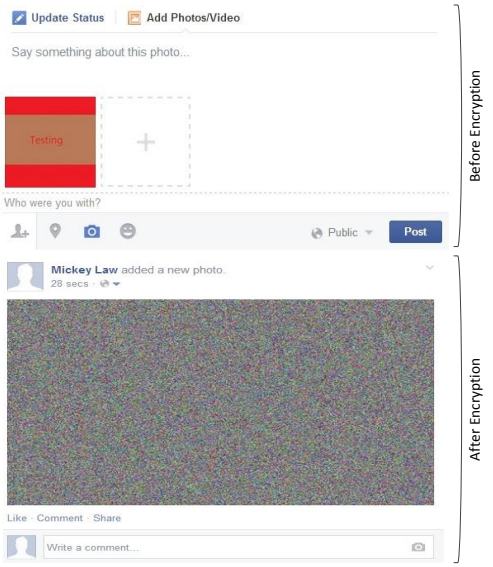

Figure 4. Images before and after encryption

4.2 Challenges Ahead

In the current iteration, we have implemented the encryption, decryption and basic key share. The basic key share is peer-to-peer in which the key is only shared in one-to-one relationships. What this means is that a user can communicate securely with only one user at a time. The key share is achieved by embedding the key sharing information in the communicated data (messages and images). However, at present we are working on key sharing in one-to-many relationships. There are multiple ways we can achieve this that include using a group key, via a centralised server (i.e. potentially a key distribution server: COP Server) or a decentralised architecture. We have to perform extensive evaluation before selecting a suitable solution. Furthermore, we are trying to optimise the add-on in a manner that imposes minimal performance penalties. In future work, we would also like to evaluate our proposal for security and robustness. Finally, we would like to port the add-on to other browsers with support for additional OSNs.

5 Conclusion

The privacy of user data is of paramount importance and it has received, to some extent, the necessary attention from academics, the public, industries and governments. However, the missing link in all the efforts is that most of the solutions are built from an architecture point of view that is not centred on the consumer, who is, ironically, the entity whose data all of the solutions are trying to protect. A potential reason for this might be that users are considered to be either the weakest link or not technically sound enough

to carry out complex security-related tasks. However, we consider that security does not always have to require an active interaction with the users. It can be built as a seamless, lightweight and least-interaction mechanism. Therefore, to provide a consumer-oriented protection for users on OSNs, we have proposed a framework in this paper. The COP framework is implemented as a web browser add-on that intercepts users' actions and if required, enforces the privacy policy. The enforcement of the privacy policy is completed seamlessly and does not require the user's input. The proposed framework emphasises that user behaviour and OSN interfaces should not be required to fit the operations of the COP. In fact, it should be the other way around, where the COP should be implemented in a way that supports user behaviour and the OSN interface. The proposal in this paper is research in progress and we are highly confident that this proposal can be polished and refined to provide an effective and robust data privacy system for OSN users.

References

[1] A. Acquisti, R. Gross, and F. Stutzman. Faces of Facebook: Privacy in the Age of Augmented Reality. USA, August 2011. Blackhat.

[2] R. G. . A. Acquisti. Information Revelation and Privacy in Online Social Networks (The Facebook case). 2005.

[3] R. N. Akram and R. K. L. Ko. End-to-End Secure and Privacy Preserving Mobile Chat Application. In D. Naccache and D. Sauveron, editors, *Workshop in Information Security Theory and Practice (WISTP'14)*, IFIP LNCS, Crete, Greece, June 2014. Springer.

[4] R. N. Akram and K. Markantonakis. Rethinking the Smart Card Technology, Invited Paper. In T. Tryfonas and I. Askoxylakis, editors, *16th International Conference on Human-Computer Interaction*. Springer, June 2014.

[5] M. Backes, M. Maffei, and K. Pecina. A Security API for Distributed Social Networks. In *NDSS*. 2011.

[6] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin. Persona: An Online Social Network with User-defined Privacy. *SIGCOMM Comput. Commun. Rev.*, 39(4):135–146, Aug. 2009.

[7] D. Boyd. Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence. *Convergence: The International Journal of Research into New Media Technologies*, 14:13, Feb. 2008.

[8] D. M. Boyd and N. B. Ellison. Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication*, 13(1), 2007.

[9] L. Brandimarte, A. Acquisti, and G. Loewenstein. Misplaced Confidences: Privacy and the Control Paradox. In *WEIS*, 2010.

[10] L. A. Cutillo, R. Molva, and T. Strufe. Privacy preserving social networking through decentralization. In *WONS 2009*.

[11] P. V. Eecke and M. Truyens. Privacy and Social Networks. Computer Law & Security Review*, 26(5):535 – 546, 2010.*

[12] G. H. ENISA. Security Issues and Recommendations for Online Social Networks. Technical report, 2007.

[13] A. Felt, P. Hooimeijer, D. Evans, and W. Weimer. Talking to strangers without taking their candy: isolating proxied content. In L. Stein and A. Mislove, editors, SNS*, pages 25–30. ACM, 2008.*

[14] H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen. Security Issues in Online Social Networks. Internet Computing, IEEE*, 15(4):56–63, July 2011.*

[15] R. A. Greene. Personal Details of New UK Spy Chief on Facebook. Online, July 2009.

[16] G. Greenwald and E. MacAskill. NSA Prism program taps in to user data of Apple, Google and others. Online, June 2013.

[17] S. F. Gurses, R. Rizk, and O. GÃijnther. Privacy Design in Online Social Networks: Learning from Privacy Breaches and Community Feedback. In ICIS*, 2008.*

[18] J. Heidemann, M. Klier, and F. Probst. Online social networks: A survey of a global phenomenon . Computer Networks*, 56(18):3866 – 3878, 2012. The {WEB} we live in.*

[19] G. Hull, H. Lipford, and C. Latulipe. Contextual gaps: privacy issues on Facebook. Ethics and Information Technology*, 13(4):289–302, 2011.*

[20] S. Nilizadeh, S. Jahid, P. Mittal, N. Borisov, and A. Kapadia. Cachet: A Decentralized Architecture for Privacy Preserving Social Networking with Caching. In CoNEXT, ACM, 2012.

[21] G. Pallis, D. Zeinalipour-Yazti, and M. Dikaiakos. Online Social Networks: Status and Trends. In A. Vakali and L. Jain, editors, Studies in Computational Intelligence*, Springer, 2011.*

[22] J. Plunkett and N. Payne-Frank. Ex-Conman Frank Abagnale Warns How Facebook Users Risk Identity Theft - Video. Online, March 2013.

[23] A. Shakimov, H. Lim, R. Caceres, L. Cox, K. Li, D. Liu, and A. Varshavsky. Vis-a-Vis: Privacy-preserving online social networking via Virtual Individual Servers. In COMSNETS, 2011.

[24] D.-H. Shin. The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. Interacting with Computers*, 22(5):428 – 438, 2010.*

[25] A. Simpson. On the Need for User-defined Fine-grained Access Control Policies for Social Networking Applications. In Proceedings of the Workshop on Security in Opportunistic and SOCial Networks*, SOSOC '08, pages 1:1–1:8, New York, NY, USA, 2008. ACM.*

[26] K. Singh, S. Bhola, and W. Lee. xBook: Redesigning Privacy Control in Social Networking Platforms. In SSYM, USA, 2009.

[27] A. C. Squicciarini, H. Xu, and X. L. Zhang. CoPE: Enabling Collaborative Privacy Management in Online Social Networks. J. Am. Soc. Inf. Sci. Technol.*, 62(3):521–534, Mar. 2011.*

[28] B. Van Alsenoy, J. Ballet, A. Kuczerawy, and J. Dumortier. Social networks and web 2.0: are users also bound by data protection regulations? Identity in the Information Society*, 2(1):65–79, Dec. 2009.*

[29] Y. Welinder. A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks. Harvard Journal of Law and Technology*, 26(1), July 2012.*