Shade Privacy Network Online Social Networking Sites

Pranshu Kapoor
HMR Institute of Technology and Management
Department of CSE
New Delhi,

Ravinder Beniwal
HMR Institute of Technology and Management
Department of CSE
New Delhi,

Sanya Swain
HMR Institute of Technology and Management
Department of CSE
New Delhi,

Smriti Bhardwaj
HMR Institute of Technology and Management
Department of CSE
New Delhi,

Namrata Mishra
HMR Institute of Technology and Management
Department of CSE
New Delhi,

***Abstract*—Online social networks (OSNs) have become mainstream way of sharing media and information among friends, online. With ever increasing number of internet users, and in turn OSN users, there is an increase in risks related to user's privacy and security. There are three core privacy issues in today's OSNs, such as not asking for user's consent, not able to categorise data or friends on the basis of certain factors, and lack of easy-to-access one-window privacy settings. We have implemented Shade, a layered privacy framework containing three privacy layers that aims to address the three core privacy issues, and provide a solid foundation for OSNs. Shade is an online social network implemented on top of Shade for privacy-caring users. The three privacy layers present in Shade, through Shade, are Consent Layer, Data Categorisation Layer, and Friends Categorisation Layer. Each layer addresses one of the three core privacy issues.**

Keywords*—*Social Network, Privacy Issues, Security Issues, Privacy Analysis, Shade Privacy Framework, Shade Social Network

I. INTRODUCTION

An online social network (OSN) is a way of interacting with people you know in real life, or strangers with similar interests, and sharing information and media online.

With a rapid growth in the number of internet-connected devices in the last few years, OSNs have become the mainstream way of sharing information among your online friends. People share all sorts of personal information and media such as *photos*, *videos*, *phone number*, *address* etc.

Around 4 billion devices are connected to internet [1], and out of those 4 billion, 2 billion devices are on some sort of OSN [2]. While it is generally good to have people connected to internet, and in turn to OSNs, for a faster information transport, it imposes some risks on the users of OSNs.

Broadly, there are two types of risks imposed on users of OSNs:

- **Security risks:** Users when on an OSN, can get exposed to an insecure network via a third-party app or service. These insecure networks can affect user's device in many ways. Most popular of them being *virus*, *malware*, *spyware*, *phishing*, *Trojan* etc.
- **Privacy risks:** Privacy risks and security risks overlap in some areas like phishing, but there are areas that come under privacy risks only, such as not asking user for consent before storing their data, selling their data to third parties, leaking of sensitive yet plain data in large amounts, etc.

In this paper, we have addressed three core privacy issues in today's OSNs:

- User is not asked for consent before storing or sharing personal information.
- User is not able to categorise information based on risk factor, and is also not able to categorise friends into different groups for group specific posts.
- Privacy settings are scattered all over the place and are complex for an average user.

We have implemented an OSN called *Shade* based on our own *Shade Privacy Framework*. *Shade*addresses all the three core privacy issues mentioned earlier, and is a layered privacy framework containing three privacy layers to make users' online experience private and secure:

- Layer 1 ensures that users are asked for an explicit consent whether they want to share their *High-Risk Data* with OSN, or not, for analysis purposes.

- Layer 2 ensures that users' data is categorised into two different categories based on risk factor: *Low-Risk Data*and *High-Risk Data*.
- Layer 3 ensures that users' friends are categorised into four different categories based on comfort level: *Friends*, *Family*, *Acquaintances*, and *Public*.

Each layer adds up on privacy level of the previous layer, and makes user's online experience more secure and more private by many folds.

II. CONTENT

This section elaborates upon the basics of terminology discussed in this paper.

A. *Online Social Networks*

An online social network (OSN) is an online platform built for people to interact with their real-life friends, and also to meet like-minded strangers online.

People are able to share any sort of information online with their friends such as *photos*, *videos*, personal information like *phone number*, *home address*, etc.

OSNs are also used for real-time chats with friends. It is very useful as in the friends chatting with each other feel like they are sitting together, and having a real conversation, without anyone having to leave the comfort of their home.

Most popular OSNs, today, are *Facebook*, *Twitter*, *LinkedIn*, etc. *Facebook* is also the most controversial of the lot for their data scandal with *Cambridge Analytica*[3].

B. *Online Risks*

With a rapid increase in the internet-connected devices, and in turn in the number of OSN users, the risks related to security and privacy of users also increase.

There are mainly two types of risks related to user's online activity:

- **Security Risks:** Risks related to user's exposure to insecure networks, or malicious software like *virus*, *malware*, *Trojan*, etc.

Virus, *malware*, *spyware* are malicious software which get downloaded on user's computer and steal or exploit personal information [4].

- **Privacy Risks:** Risks related user's personal information on OSNs, or elsewhere, such as *phishing*, *data breach*, etc.

Phishing is an online activity attempted by people with malicious intentions, to obtain sensitive information of users such as *username*, *password*, *bank details* etc [5].

Data breach refers to leaking of sensitive information of people without their consent. Large amounts of profiling information gets leaked, or stolen by hackers for malicious reasons [6].

Security risks and privacy risks overlap in some areas but we have mainly focused on privacy risks in this paper.

Privacy issues and *privacy risks* are two terms that are generally used interchangeably. In this paper, privacy risks refer to all the risks related user's privacy anywhere on the internet, and privacy issues are the three core privacy issues in today's OSNs.

The three core privacy issues in today's OSNs are:

- Users are not asked for an explicit consent while signing-up, whether they want their data to be shared with OSN, or not.

Users' personal data can be used to profile them and to provide them a personalised online experience. But today's OSNs do not ask for user's consent during sign-up, or at any point-of-time afterwards, before storing their data for profiling and analysis purposes, and selling their data to third parties for advertising purposes.

- Users' data is not categorised based on risk factor, and users' friends are not categorised based on comfort level.

OSNs do not categorise data into *Low-Risk Data* and *High- Risk Data*, and friends into *Friends*, *Family*, *Acquaintances*, and *Public*. This makes it hard for users to create and post audience-specific posts. The posts are either made for friends, or for public. There is no audience-specific solution available in today's OSNs.

- Privacy settings are scattered all over the place, and are complex enough for an average user.

OSNs make it very hard for average users to change privacy settings according to their taste. The settings are not present in one place, and are scattered place all over the place, that confuses users with all the possible permutations of best possible privacy settings.

III. SHADEPRIVACY FRAMEWORK

*Shade*is a layered privacy framework that aims to provide a solid foundation for OSNs. We have implemented *Shade* on top of the *Shade Privacy Framework*.

*Shade*contains three privacy layers, each adds up to the privacy level of the previous layer, and makes users' online experience more secure and more private, by many folds.

Each layer in the *Shade Privacy Framework* addresses one of the three core privacy issues addressed in this paper.

A. *Layer 1*

This layer is called the *Consent Layer*.

This layer addresses the first privacy issue that "*Users are not asked for an explicit consent while signing-up, whether they want to share their data with OSN, or not.*"

In this layer, users are asked for an explicit consent at the sign-up, whether they want to share their data with OSN, or not. Based on their choice, they are put into one of the two user pools:

- **Shaded Users:** Users who don't want their data to be shared with OSN, and in turn don't want their data to be used for a personalised experience, and by third parties for advertising purposes.
- **Unshaded Users:** Users who allow the OSN to gather their data including their personal information for profiling and advertising purposes, and in turn want a personalised experience.

B. *Layer 2*

This layer is called the *Data Categorisation Layer*.

This layer addresses the second privacy issue that "*Users' data is not categorised based on risk factor.*"

In this layer, user's data is categorised into two categories based on the risk factor:

- **Low-Risk Data:** This data can not be used for profiling purposes, and thus is invalid for advertising companies. Low-Risk Data includes *consent value*, *joining date*, etc.
- **High-Risk Data:** This data is sensitive. It can be used for profiling users, and thus is very valuable for advertising companies. This data can also be used for malicious reasons by hackers. High-Risk Data includes *posts* that can contain *phone number*, *address*, *bank details*, etc.

To implement this layer, *Shade* uses two different database, one for each category of data.

C. *Layer 3*

This layer is called the *Friends Categorisation Layer*.

This layer also addresses the second privacy issue that "U*sers' friends are not categorised based on comfort level.*"

In this layer, user's friends are categorised into three different categories based on the comfort level in real life:

- **Friends:** These are the friends of user. User can share any sort of information with them without having to worry about information misuse.
- **Family:** These are members of user's family and extended family. User can only share family-friendly information with them.
- **Acquaintances:** These are *acquaintances*, *colleagues*, and other casual friends of user. User can trust them with only certain amount of information.
- **Public:** These are any other people that are not user's friends, and visit user's profile with a public point-of-view. They can only see user's *Low-Risk Data* and *Public* posts.

IV. Implementation and Results

This section shows the implementation of *Shade* OSN based on our *Shade Privacy Framework*.

A. *Architecture*

Fig. 1 shows the basic block architecture of *Shade Privacy Framework*. *Shade* is based on this architecture. The framework has three layers, as mentioned earlier: *Consent Layer*, *Data Categorisation Layer*, and *FriendsCategorisation Layer*.

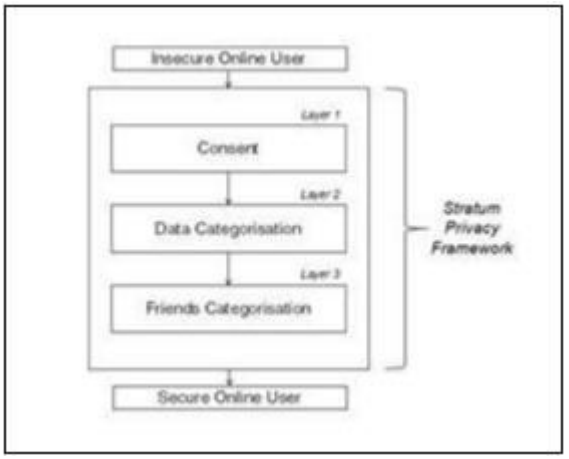

Fig. 1. Shade Privacy Framework Block Architecture

Technologies used in Shade are as follows:

- **Client-Side Technologies:** *HTML*, *CSS* and *JavaScript* for layout, design and front-end functionality, respectively.
- **Server-Side Techonologies:** *Node.js/Express*, *EJS*, *Mongoose*, and *Passport* for server-side logic, templating, database operations, and secure login system, respectively.
- **Database:** *MongoDB*

B. *Layer 1*

Layer 1, or *Consent Layer* is exercised during sign-up process. Users are asked for explicit consent on the sign-up page, whether they want to share their data with OSN, or not. Fig. 2 shows the sign-up page.

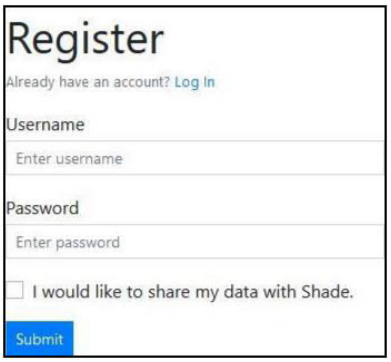

Fig. 2. Shade Sign Up Page

Fig. 3 shows selective fields of a user's data as stored in the database. It clearly shows whether the user has given consent to *Shade*, or not. *Shade* respects user's privacy, and doesn't go against user's will.

Fig. 3. Selective User Data

C. Layer 2

Layer 2, or *Data Categorisation Layer* is exercised at database level. Two different database are used to store users' data, one for each category of data.

*users*database is used to store users' *Low-Risk Data,* and *posts* database is used to store users' *High-Risk Data* i.e. *posts.*

Fig. 4 shows the two database used with *Shade.*

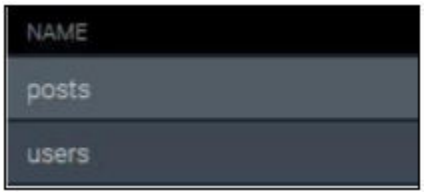

Fig. 4. Shade Database

D. Layer 3

Layer 3, or *Friends Categorisation Layer* is exercised through user's interaction with *Shade*.

A logged-in user can connect with other user by opening other user's profile, and connecting with other user as a *Friend, Family,* or *Acquaintance.*

Fig. 5 shows the three connection options on other user's profile as seen by a logged-in user.

Fig. 5. Connection Options

A logged-in user can then select *Friends, Family, Acquaintances,* or *Public* as audience during posting to create an audience-specific post, or a public post.

Fig. 6 shows the four audience options during posting.

Fig. 6. Audience Options During Posting

Layer 1 ensures user is asked for consent before accessing personal data.

Level 2 ensures data is properly categorised into two categories based on the risk factor.

Layer 3 ensures friends are categorised to ensure proper audience selection at the time of posts. All the three layers combined ensure that user's online experience on *Shade* is more secure and private than ever.

V. Conclusion and Future Scope

OSNs have become mainstream way of communicating online. People share their *photos*, *videos*, and other personal information like *address* and *phone number*, among friends. It's the responsibility of OSNs to protect the massive amount of data being generated by their users, everyday.

Unfortunately, in hope of better money, today's OSNs are ignoring privacy and security measures, which is responsible for data breaches like *Facebook - Cambridge Analytica Data Scandal* [7].

We identified three core privacy issues with today's OSNs, and built a new OSN called *Shade* which is based on our *Shade Privacy Framework*. *Shade*is a layered privacy framework with three layers: *Consent Layer*, *Data Categorisation Layer*, and *Friends Categorisation Layer*. Each layer addresses one of the three core privacy issues, and makes *Shade*a very solid foundation for an OSN.

We hope to keep incorporating new features into *Shade* to combat the ever changing online threats.

References

[1] World Bank Open Data, "Individuals using the Internet (% of population),"https://data.worldbank.org/indicator/IT.NET.USER.ZS.

[2] Statista, "Number of monthly active Facebook users worldwide as of 2nd quarter 2018 (in millions)," https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide.

[3] The Guardian, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach," https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[4] Malwarebytes, "All about malware," https://www.malwarebytes.com/malware.

[5] Phishing.org, "What Is Phishing?,"http://www.phishing.org/what-is-phishing.

[6] Norton by Symantec, "What is data breach?", https://us.norton.com/internetsecurity-privacy-data-breaches-what-you-need-to-know.html

[7] Vox, "The Facebook and Cambridge Analytica scandal, explained with a simple diagram," https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram.

[8] F. Persia and D. D'Auria, "A Survey of Online Social Networks: Challenges and Opportunities," Proc. IEEE International Conference on Information Reuse and Integration (IRI), 2017, pp. 614-620.

[9] ShailendraRathore, Pradip Kumar Sharma, Vincenzo Loia, Young-SikJeong, Jong Hyuk Park, "Social network security: Issues, challenges, threats, and solutions," Proc. Elsevier Information Sciences 421, 2017, pp. 43-69.

[10] Michael Fire, Roy Goldschmidt, and Yuval Elovici, "Online Social Networks: Threats and Solutions," Proc. IEEE Communication Surveys & Tutorials, Vol. 16, No. 4, Fourth Quarter, 2014, pp. 2019-2036.

[11] Xi Chen and Katina Michael, "Privacy Issues and Solutions in Social Network Sites," 2012.

[12] RachaAjami, Noha Ramadan, Nader Mohamed, and Jameela Al-Jaroodi, "Security Challenges and Approaches in Online Social Networks: A Survey," Proc. IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.8, 2011.

[13] K. Singh, S. Bhola, and W. Lee, "XBook: Redesigning Privacy Control in Social Networking Platforms," Proc. 18th Usenix Security Symp. (SSYM 09), Usenix Assoc., 2009, pp. 249–266.

[14] Aaron Beach, Mike Gartrell, and Richard Han, "Solutions to Security and Privacy Issues in Mobile Social Networking," Proc. International Conference on Computational Science and Engineering, 2009, pp. 1036-1042.