Tampere University

Yuhang Du

PRACTICAL OBFUSCATION FOR PRIVACY ON SOCIAL MEDIA PLATFORMS

Master of Science Thesis
Faculty of Information Technology and Communication Sciences
Examiners: Associate Professor Antonis Michalas
Doctoral Researcher Eugene Frimpong
April 2024

ABSTRACT

Yuhang Du: Practical Obfuscation for Privacy on Social Media Platforms
Master of Science Thesis
Tampere University
Information Security
April 2024

Based on the ongoing worries about privacy in the social media landscape, we introduce Obfuscure, an upgraded version of MetaPriv. This study focuses mostly on Facebook, meanwhile, it develops and evaluates a browser extension by using obfuscation techniques to protect users' online activities from social media's data collection and analytics practices. At the same time, Obfuscure introduces a user-friendly interface and multi-user support, making privacy protection more user-friendly and efficient. Through our test analysis, the results show that although Obfuscure is able to effectively protect user privacy from social media algorithms, it encounters limitations related to violations of community guidelines as well. From a long-term perspective, there is still a lot for us to work on in the development of Obfuscure. Apart from that, we hope to bring a better user experience and research value in the future by continuously improving and refining Obfuscure.

Keywords: Social Media, Social Networks, Data Obfuscation, User Experience, User Interface, Multi-User Capability, Privacy.

The originality of this thesis has been checked using the Turnitin OriginalityCheck service.

PREFACE

First of all, I would like to thank Professor Antonis Michalas for providing me with the opportunity to do research job in the NISEC group, also I am grateful for the guidance of ideas and constructive advice throughout the process especially when I was clueless about my research, as well as for actively following up and providing me with continuous support during the process.

I am also greatly grateful to Eugene Frimpong, who was very helpful in both research and providing emotional support. The path of research has taught me that research is majorly about recognizing and overcoming challenges. Even though the process may be "terrifying" from time to time, the effort of simplifying the problems has demonstrated that they are not as unachievable as they look like. Through their model, I have obtained more knowledge of what it is to be a successful researcher.

Last but not least, I would like to thank my parents and my friends, whose constant support is my stronghold in the moments of trouble. Their support has remained a steady source of power. Apart from that, being part of the NISEC team has brought me so many benefits, challenging my problem-solving skills and expanding my general knowledge.

Tampere, 23rd April 2024

Yuhang Du

CONTENTS

1. Introduction . . . 1
2. Related work . . . 3
3. Background and Preliminaries . . . 6
   3.1 Overview of Social Media . . . 6
      3.1.1 Relationship-based Social Networking Sites . . . 6
      3.1.2 Creative Social Networking Sites . . . 8
      3.1.3 Livestream Social Networking Sites . . . 10
      3.1.4 Discussion-based Social Networking Sites . . . 11
   3.2 Recommendation Systems . . . 13
   3.3 Preliminaries . . . 17
      3.3.1 Obfuscation . . . 17
      3.3.2 Web automation . . . 17
4. MetaPriv . . . 19
   4.1 High-Level Overview . . . 19
   4.2 Limitations . . . 22
5. System model and High-Level Overview . . . 23
   5.1 High-Level Overview . . . 24
      5.1.1 Registration . . . 25
      5.1.2 Login . . . 26
      5.1.3 Multi-user Support . . . 26
6. Implementation and results. . . . 28
   6.1 Client Design . . . 28
   6.2 Server Design . . . 29
      6.2.1 XAMPP . . . 29
      6.2.2 Database Design . . . 30
      6.2.3 Multi-threading . . . 31
   6.3 User Interfaces . . . 32
      6.3.1 MetaPriv's User Interface . . . 32
      6.3.2 Obfuscure's User Interface . . . 35
   6.4 User-friendliness: Comparing MetaPriv and Obfuscure . . . 37
   6.5 Multi-user Cases . . . 39
      6.5.1 Observations. . . . 41
   6.6 Limitations . . . 43
7. Conclusion and societal impact . . . 45

References 47

GLOSSARY OF ABBREVIATIONS

AI	Arti cial Intelligence
FB	Facebook
H	Hash
PIN	Personal Identi cation Number
SN	Social Networking
UI	User Interface
URL	Uniform Resource Locator

1. INTRODUCTION

In the digital era where social media platforms have revolutionized the social and communication culture, people get connected, communicated, and obtain information in a different way. Along with that, these platforms provide a wide set of options for social life interaction and information exchange, but on the other hand, the risk of a security breach is also extremely high. Massive internet users' data collection, processing and business use by social media platforms has caused stakeholders' concerns regarding data privacy and protection. In this paper, we will talk about an in-depth investigation of privacy threats on social media and also devise a creative solution to enhance data privacy with obfuscating strategies.

Nowadays, social media such as Facebook, Instagram and Twitter are everywhere gathering huge volumes of personal information about people. All the platforms rely on the information provided by users which is again used to customize the content, deliver ads and add a layer of interest to the users. Nevertheless, people's privacy is ignored as a result of this action at some point. Private data, browsing behaviors, and social communications are fully monitored, removed, and processed, usually without the consent of the user's permission or transparency. Furthermore, this excessive collection of personal data also violates privacy and it is likely that it will have a wider effect afterward concerning these issues including surveillance and data protection.

With the explosion of social media data collection methods, there is a desire for a tool that guarantees the privacy of user data without impacting or interfering with users' normal work. This thesis aims to address the above challenges by achieving the following objectives:

1. By looking into the actual data collection processes, major social media platforms use and highlight the essential points where users' privacy is being abused.

2. The tool should be developed in a practical way and called Obfuscure (a combination of "Obfuscate" and "Security") which uses data obfuscation mechanisms to prevent information correctly identi cation by social media applications.

3. With real-world scenario evaluation the tool's effectiveness is determined to ensure that it means privacy and also good user experience.

Privacy vs. Convenience: The Hardship Choices Between User Privacy And Convenience.: One of the core challenges in social media use is individuals have to make decisions between privacy and convenience. Apart from that, some users prefer a personalized and smooth web experience, which may be achieved by software data algorithms that optimize content delivery and human communication procedures. Thus, the more strongly the user feels satis ed and connected, the more attractive it becomes.

On the other hand, convenience comes with the price of privacy. Social networks are smarter and more customized for us than we could imagine, because the algorithm requires us to provide personal details. Through the collection of this personal information, the social network will then go through different machine model algorithms to accurately recommend related content to users. In fact, users often hang around social media to check their accounts, track their activities, analyze them and share them with others from time to time. As a result, it is easy to see the digital footprint that surrounds each other and is hard to erase. More seriously speaking, this type of monitoring may lead to a variety of shortcomings, ranging from identity theft to manipulation based on user information.

Privacy and convenience are the two main elements of this study, that is, how to achieve privacy while being user-friendly. By summarizing the privacy threats present on social media platforms and developing a user-friendly solution for privacy settings, this study contributes to the area of information security and provides a detailed analysis with a helping hand for the users to have increased control over their data. Apart from that, this research corresponds to the turning on obfuscation mechanism in an easy-to-install browser extension and proves whether it is possible that privacy can be enhanced by technical innovation.

Finally, our article, "Practical Obfuscation for Privacy on Social Media Platforms" attempts to bring together these two con icting things with a fresh perspective on the challenges and solutions of social media platforms' privacy protection.

2. RELATED WORK

With the development of technology, there are several large social media platforms such as Facebook and Instagram who are using various tracking methods to obtain information about users' activities so that they may push relevant content to users for acquiring pro t. In reaction to this phenomenon, and without breaking the terms and conditions of the regulations, researchers have created tools such as web browser extensions to assist users in improving their privacy in order to achieve a balance between the user's daily use and the desired privacy level.

Facebook Container [6], developed by Mozilla Firefox, is a Firefox-based browser extension that operates by storing a user's Facebook identity in a separate “container” that is isolated from everything else. Facebook's trackers and cookies are con ned to this "container" while the user uses Facebook within it, making it dif cult for Facebook to get access to the user's other actions through third parties. To be more speci c, when a user initially downloads the extension, three sites are included in the “container” by default: Facebook.com, Instagram.com, and Messenger.com. In this situation, when the user visits any of these sites, the extension will isolate the open tab as a “container” and distinguish it from the external active tab (at this point the user can notice there is a solid line at the top of the tab inside the “container”, so the user can tell if they are inside the “container” or not). Overall, the extension is relatively user-friendly for both frequent and occasional users, and it can assist separate Facebook's tracking behaviors to a certain extent as well, therefore enhancing user privacy. However, this tool has certain limitations. Although it can assist users in isolating Facebook's tracking behaviors, it cannot prevent Facebook from manipulating previously obtained data. Facebook can still access this data in its internal environment, such as the user's comments, likes, and other related activities on Facebook. In addition, if a user inputs a new address within the same “container” tab, the new address will be loaded directly as an external tab and the user will not be able to return to the previous page which is the Facebook container.

TrackMeNot [21], an extension based on web browsers as well, primarily focuses on adding obfuscation to those search engines such as Google, Yahoo!, Bing, and AOL by automatically sending random search queries to those search engines. In other words, TrackMeNot is a browser add-on that operates in the background and regularly sends random search queries to the browser. These search terms are randomly selected from a list

that is prede ned with the aim of simulating the search behavior of real users. Throughout the process, it can be even more dif cult for those search engines to target the users' actual search data or information since it helps conceal the users' actual searches inside obfuscation searches. In the meanwhile, to better simulate user behavior, TrackMeNot uses a dynamic query mechanism to 'evolve' each client (uniquely) over time, parsing the results of its searches for 'logical' future query terms with which to replace those already used [19]. However, this extension was rejected by the Google store because they assumed “It violated several of the Chrome Web Store's Program Policies, such as providing an inaccurate description of its functionality or requesting permissions that it did not use [20].” The fact is that Google has 8.5 billion [8] searches per day and it keeps track of its users' search histories, so in this case, people might prefer to think about how private their search data is and how to stop search engines from using it maliciously to generate revenue or for other purposes.

Ghostery [9], compared to adding obfuscation directly on users' data, this extension is primarily designed as a tracker blocking tool to improve user privacy protection by blocking ad trackers, social media trackers, and more. With this tool, users have the exibility to block trackers on the website and even keep trackers on the site. Ghostery will also block ads and popups to prevent websites from collecting users' information for malicious purposes, apart from that, it helps speed up the page loading by reducing the number of resources that need to be loaded as a result of the blocking process. Regarding its core functions, one of them is to block trackers, Ghostery can detect and block any type of tracker, including ad trackers, social media trackers, analytics tools, and more, to help users avoid their online behaviors and preferences from being tracked by these tools. More precisely, it can automatically balance the loading functions of websites and privacy protection. Furthermore, Ghostery intelligently adjusts the number of trackers blocked based on the site's needs and the user's privacy preferences. For the current situation, most existing privacy protection tools focus on preventing trackers from collecting data rather than actively generating noisy data. This is mostly due to considerations for user experience and legal risk. Noise-generating methods may cause unnecessary data traf c, affecting the normal operation of the platform, and may even result in the permanent suspension of user accounts.

Here are some other tools we used as examples, such as FaceCloak [13], Scramble [1], TrackThis [7], and AdNauseam [11]. In general, these products seek to improve user privacy in various ways. FaceCloak, a Firefox extension, mainly protects user privacy by providing a fake version of user pro les such as birthdays and contact information. Meanwhile, the real data is encrypted and stored on another server and only the user's friends can get access to it if they have the extension installed on their machine. However, FaceCloak does not work with Facebook anymore due to changes made by Facebook to its website [12]. Scramble is a tool for social media that protects content from being seen

by unauthorized users or the platform itself by encrypting the information that users post on social media. Only authorized users can decrypt and view the original content. TrackThis is a project launched by Mozilla for confusing ad trackers by opening 100 tabs in the browser, and there are four identities for users to pick in order to trick the trackers, they are Hypebeast, Filthy Rich, Doomsday, and In uencer. After users choose their pro les, then TrackThis will mislead trackers by opening pages related to that identity. Last, AdNauseam is a Firefox plugin that aims to add obfuscation to browsing data in order to fool ad trackers, in this way, it works similarly to TrackMeNot and TrackThis. In terms of application objectives and methods, FaceCloak and Scramble focus more on protecting users' personal data and postings on social media by encrypting and replacing information, while TrackThis and AdNauseam confuse trackers by generating large amounts of fake data, the former by opening tabs and the latter by clicking on ads. In terms of user experience, FaceCloak and Scramble require the user's friends in the social network to use the same tool or method to access the encrypted content, which may limit their ease of use, while TrackThis and AdNauseam primarily affect the user's interactions with the ad tracker, with less impact on other users in the social network. In terms of application range, FaceCloak is speci c to Facebook, Scramble can be used for a variety of social media platforms, TrackThis and AdNauseam are widely used for ad tracking across the Internet. In conclusion, even though they have different focuses, all these tools achieve privacy through some form of data obfuscation or encryption designed to improve user privacy on the Internet. However, this behavior is often resisted by social platforms, which means that it can easily be seen as a violation of the rules.

Based on MetaPriv [2], this time we built an extension version of it, known as Obfuscure. The above-mentioned tools inspired us to work on the add-on extension based on the Firefox browser, thus making it more user-friendly. Obfuscure is designed to provide users with a higher level of privacy when using Facebook by simulating user interactions with Facebook, the inner principle is similar to TrackMeNot, which is to add obfuscation to the user account to maintain a balance between the actual use and user privacy. In our case, the personal data obfuscation technique is simply an automated process that creates noises by mimicking user behavior on Facebook, such as liking posts and nding relevant material. They may interfere with data analytics tools' tracking of a user's real interests and activities by automating these activities on the user's social media account through random or algorithmically generated behaviors based on speci c algorithms. On the other hand, using any automated tool to interact with social platforms almost always violates the terms of service of those platforms. At the same time, automated behaviors might trigger the social platform's security mechanisms, leading to account suspension or banning. This is also one of the problems we encountered during the development process.

3. BACKGROUND AND PRELIMINARIES

3.1 Overview of Social Media

Social media is an Internet-based communication platform that allows users to create and share content such as text, image, video, and audio over the Internet [14]. In other words, it is like a bridge that can easily connect people with their friends, family, and even strangers through the Internet, and at the same time, people can share their experiences, opinions, feelings, and pieces of their daily lives on different social platforms.

Nowadays, there are many different kinds of social media on the market. According to the different manifestations of social media, we have categorized them into four categories, they are: (i) Relationship-based social networking sites, (ii) Creative social networking sites, (iii) Livestream social networking sites, (iv) Discussion-based social networking sites. In the subsequent subsections, we will provide a high-level overview of each of the four categories of social media and show how they impact people from different perspectives.

3.1.1 Relationship-based Social Networking Sites

Relationship-based social networking sites are those online platforms that help build relationships between people or social groups, focusing on maintaining relationships with family, friends, and coworkers, such as those well-known online platforms: Facebook, Snapchat, and LinkedIn, which enhance human interaction and emotions.

Facebook is a social media outlet owned by Meta, founded in 2004 by Mark Zuckerberg and four other Harvard students [27]. Facebook focuses on the personal socialization of its users as well as the sharing of everyday content. It allows people to interact with friends or family by writing posts, commenting on posts, uploading photos, and joining different groups. First of all, users can see the posts made by their friends or people they followed on their homepage, and people can interact with their friends by commenting, liking, etc. underneath the posts. In addition, users can also create content in the form of text, images, or videos to share their lives or things they nd interesting with their friends. At the same time, users can send text and voice messages to their friends through Messenger, and even initiate voice and video calls (Messenger is a built-in Facebook chat program

that was initially available within the Facebook platform, but has since evolved into a stand-alone application). Apart from that, Facebook offers people the ability to watch videos, and these are categorized into ve groups based on different attributes: "For You," "Live," "Games," "Reels," and "Follows," which allows people to choose what they want to watch based on their needs. It is worth mentioning that Facebook's Marketplace, rst of all, it has two modes, they are "Personalized" and "Non-personalized". If a user chooses "personalized", Facebook will use the user's Facebook information to give the user full access to "Marketplace" features, such as messages and personalized lists; conversely, if the user chooses the latter, the user will not be able to experience the relevant features. Marketplace gives users a place where they can buy and sell commodities with other people, and even if the user is not inclined to trade at the moment, it serves as a " ea market" where people can hang out as much as they like. Overall, Facebook provides a place for people to interact with each other, where friends can share interesting content, and where people can trade items with other people through the Marketplace.

Snapchat is a multimedia instant messaging social platform developed by Snap Inc. that focuses on picture and video sharing with friends, and its main feature is that after a picture or message is sent out, it can only be seen by other users for a short period of time, for example, a message will be deleted immediately after it has been read for 24 hours [31]. Unlike other social media, Snapchat does not have a homepage. Instead, the rst page that appears by default when a user opens Snapchat is the "Camera" page, which is similar to Instagram's built-in camera and allows users to take photos in real-time using its built-in camera and add lters or other actions to edit them. Snapchat's lter gallery is more powerful and informative than Instagram's. After taking a photo, users have the option to send the photo as a "snap" to their friends, and then users can go to the "Chat" to view the speci c content. In other words, this page can also be called the message list where users can interact with their friends. Interestingly, when a user sends a snap to a friend, the snap disappears immediately after the friend has viewed it once (the sender or receiver can also choose to save the snap so that it would not disappear); similarly, when a user sends a text message to a friend, the text message disappears immediately after 24 hours. Also, if the receiver takes a screenshot while viewing the snap, then the user receives a message such as "Alice took a screenshot!". In addition to the screenshot alert, there are similar alerts such as "Alice saved a snap in chat!". In addition to this, if the user chooses to share the location with friends, then on the "Map", the user can see the location information of himself and his friends, as well as the stories of nearby and friends' locations. Meanwhile, users can go through Snapchat's "Stories" to view stories posted by friends or recommended by Snapchat. Overall, Snapchat's burn-after-view feature and rich lter material provide users with a more private and relaxed way of sharing to a certain extent, increasing the fun of sharing among friends and improving user engagement.

LinkedIn was launched on May 5, 2003 by Reid Hoffman and Eric Ly [28]. It has a different focus than Facebook and Snapchat, as it is geared more towards the job market, helping people connect with companies or coworkers, explore career opportunities, and share knowledge of industry experiences. When users rst start using LinkedIn, they need to create a pro le, which includes a resume, educational background, work experience, professional certi cations, project experience, and so on. After that, users can see what the people or companies they follow have posted through the homepage, as well as participate in discussions about their industry or topics of interest. When it comes to LinkedIn's "My Network" section, it is like a work social circle where users can connect with acquaintances or colleagues as a way to expand their social circle. In addition to this, people can also express their personal opinions, views on the industry, and share knowledge in specialized elds by creating posts on LinkedIn. It is also worth mentioning that people can go through "Jobs" on LinkedIn to set their job search preferences and job recommendations to nd the right position for them. Apart from that, those companies, as job recruiters, can also go through LinkedIn to post relevant job listings. In conclusion, from a career development point of view, LinkedIn offers users the possibility to develop and expand their networks, which is certainly helpful for people who are looking for a job. From a reputation perspective, users or companies can also improve their professional reputation by sharing industry knowledge and insights.

3.1.2 Creative Social Networking Sites

Creative social networking sites such as Instagram, TikTok and Youtube, mainly focus on sharing visually oriented content such as images and videos, while these platforms enable users to showcase their creative content, such as TikTok's content publishers are called "TikToker", and YouTube's are called "YouTuber". The core of these platforms is to attract users' attention through visual effects such as images and videos, thus attracting users to share content and self-expression. These platforms are centered on attracting users' attention through visuals such as pictures and videos, which in turn attracts users and promotes content sharing and self-expression.

Instagram is owned by Meta, the same company as Facebook. It is a social software mainly used for sharing pictures, videos and other content, supporting both web and mobile versions. First of all, users can see the pictures or videos posted by the bloggers they followed on the homepage, and they can also interact with them by "liking", "commenting" and "sharing". In addition, people can choose to create their own story content and share it with their followers, then their followers are able to interact by leaving different reactions or comments when browsing the stories. It is worth mentioning that, compared with Facebook users who can only upload photos from albums to create new posts, Instagram users can directly use its built-in camera to take photos in real-time, and Instagram has a

rich library of lters, so that after taking a photo, users can edit the photo according to their own preferences, such as adding lters, music clips and so on. It is also because of this feature that Instagram attracts many younger users. In addition, Instagram offers private messaging, which allows users to interact directly with friends by texting, voice or video calling (unlike Facebook Messenger, Instagram interacts directly within the app, rather than switching to a separate app). In fact, people can use Instagram to explore content they may be interested in, as users can see creative content from a variety of bloggers recommended by Instagram based on the user's browsing history and more. One of the most interesting points is that Instagram allows users to post pictures, videos, and other visual-based content, but does not support sending text-only posts like Facebook. Apart from that, users can watch short video content on Instagram reels and interact with the video creators such as leaving comments and likes. For content creators, Instagram can help them increase the number of clicks on their content, improve visibility and gain more followers. For individuals, unlike Facebook, which focuses more on internal communication, Instagram focuses more on public communication, which promotes the desire to create and share, enhances the user experience, and builds social connections.

TikTok is a globally popular short-video sharing platform under the Chinese Internet company ByteDance, which is loved by young people [33]. First of all, TikTok provides users with a broad platform where people can not only watch videos, follow interesting TikTokers, but also interact with people by liking, reposting, and commenting on them. Meanwhile, people can choose to become a TikToker to create and publish their own video content, which can range from a few seconds to a few minutes in length. While watching, if a user is not interested in a video, they can reduce the push of related videos by selecting "Not Interested". In addition, people can also choose to switch between different modes to lter the videos they watch, for example, in "Following" mode, users can only see the content of the video bloggers they already followed, while in "For You" mode, users can see the videos that TikTok recommends to them. TikTok gives users the option of watching live streams as well, where people can comment, gift gift-giving to interact with TikToker. At the same time, people are able to receive videos or messages from their friends within TikTok, making it easy for people to quickly share videos and interact with their friends. In fact, while users watch videos, TikTok brings branding and social impact to sponsors and video creators. Sponsors can brand themselves through cooperation with video creators, while video creators can increase their visibility and gain value at the same time. What is more, popular content on TikTok often becomes a dominant trend in public life, with a signi cant impact on music and culture.

YouTube is Google's social media for online video viewing, and it supports a variety of different types of video content, including short videos, documentaries, movie trailers, live streams, video blogs (vlogs), live gaming, and more [37]. Users can select the videos they are interested in according to the different types of videos on YouTube, and people can

watch the current popular and attention-grabbing videos on YouTube through "Trending" to get a quick overview of what is going on around them in terms of trending events, pop culture, hot topics, or interesting stories from the world. In fact, the basic version of YouTube can satisfy the needs of most users, but the shortcomings may lie in the fact that users have to view advertisements before watching the video, and if the duration of the video is long, they will have to watch the advertisements during the watching time as well. On the other hand, if people subscribe to the premium version of YouTube, then they can enjoy a silky smooth ad-free experience while watching videos, meanwhile, YouTube also allows people to download relevant video content, background play and so on. Similar to other social media, YouTube allows users to interact with content creators through comments, likes and more. However, compared to Instagram and TikTok, YouTube does not support direct communication between users, such as sharing videos with each other or sending text messages. In addition, people can watch short videos on YouTube, similar to TikTok and Instagram Reels, which is called "Shorts". For YouTubers, YouTube provides a platform for them to showcase themselves to the outside world, allowing them to publish their own creative content and gain visibility, and if the videos they create have a certain level of popularity and views, the platform will give them back revenue based on the level of views they get. For the viewers, there is a wide range of video content on YouTube and everyone can be a video creator and share their lives, which in a way facilitates a two-way street.

3.1.3 Livestream Social Networking Sites

Live social media is social media that focuses on users sharing video content in real-time and interacting with it in real-time. On these platforms, users can interact with anchors by, for example, voting in real-time and sending comments in real-time. Real-time, interactivity and engagement are the distinguishing features of this form of social media, and provide users with a unique online social experience. Here we mainly talk about Twitch.

Twitch , founded in 2011 by Twitch Interactive, a subsidiary of Amazon.com, Inc., is a social media platform for live streaming of games, including eSports tournaments and individual game shows, as well as music, art and other content [34]. It is geared towards live-streaming viewers and creators. Regarding the version for live viewers, rst of all, users can subscribe to its paid version to go for an ad-free browsing experience, larger storage capacity, unlocking more emoticons, battery chat badges, etc. Twitch supports users to choose the type of live streams they want to watch, which is divided into ve main categories: "Games", "Esports", "Music", "IRL" and "Creative". While watching the live stream, users can post real-time comments and interact with the host via "Chat". Also, users can send gifts to the hosts via "Gift a Subscription", see "Top Gifters" and "Top Cheerers" in the "Leaderboard", which is more of a gifting leaderboard where the

top-ranked ones appear. Additionally, users can use the "Browse" to see Twitch's ranking of Twitch's recommended live streams based on view history or number of viewers from highest to lowest. On the other hand, when the mode switches to the creator mode, the content is different from the viewer mode. First of all, users can view various metrics on the homepage, such as "Chat" and "Streaming Health". At the same time, users can also view and manage their uploaded videos, if authors want to create new content, they can go ahead and choose whether to create "Stream Games" or "Stream IRL" based on their preferences. In this case, "Stream Games" is used for live gaming, while "Stream IRL" is used for the host's daily life. In addition, Twitch supports people to go through "Analytics" to view detailed data and various metrics of a live stream, such as viewer stats, watch time, and revenue. At this stage, authors can decide on possible next steps and clarify their self-positioning. Finally, "Channels" gives users the ability to manage their channels, such as editing pro les and adjusting channel settings. In short, Twitch provides a broad platform and personalized experience for viewers and live content creators, which to a certain extent promotes the popularity of eSports culture and inspires independent studios to develop games.

3.1.4 Discussion-based Social Networking Sites

Discussion-based social networking sites are online discussion forums that support people to exchange experiences and share ideas online, like a free classroom with different groups where people can discuss, ask questions and share ideas with each other. It categorizes speci c groups of people and speci c topics, people can choose the corresponding topics to view the content of the posts, ask questions, talk about ideas, share experiences and communicate with each other. Reddit, Discord and Facebook group are typical examples.

Reddit is a large online forum where people can enthusiastically post and interact with each other. At the registration stage, users are asked to select their "interests", i.e. pick things the user would like to see in their home feed, and then select the appropriate communities and avatars. It is worth noting that people do not need to provide their real information to create an account here. In general, users can browse posts on topics they are interested in on their homepage and interact with them by voting for or against them, as well as by commenting and sharing. In addition, users can also access content in the "Popular" and "News" sections. Reddit's "Communities" are categorized by different topics giving users more opportunities to explore community content, and there are other categories such as "Popular Global Communities" and "Top Global Communities" for users to browse. Meanwhile, Reddit supports users to start new topics and chat with friends and group members. Users can receive push messages about events and other personal conversations as well. Overall, Reddit offers users a new way to socialize, as

its anonymity gives users less to worry about and allows them to nd people with similar interests faster and easier at times.

Discord is a social platform used by many gamers that allows people to interact through voice calls, video calls, and text messages, as well as joining different "servers" and interacting with "like-minded" people [26]. Discord enables users to see the activities on the servers they are on, as well as access different channels to interact with others based on their preferences, such as sending text messages and giving gifts. Speaking of gifts, different levels of gifts can unlock different features, such as a basic level that allows recipients to enjoy more stickers, personalized emojis, and larger le transfers, while higher levels of subscriptions give them access to superb chat. In addition, users can create their own "servers", where there are two different modes: "For me and my friends" and "For clubs or communities". Here, the administrator can set relevant rules to bind the community members and control the user's privileges. Undoubtedly, if a user receives an invitation link from someone, he/she can also join a server through this invitation link. Also, the user can explore other servers he/she may be interested in via "Explore", where the servers are classi ed into seven different types: "Games", "Music", "Education", "Science and Technology", "Communities", "Entertainment" and "Student Center". And Discord supports direct messaging between users and others, as well as the ability to interact with friends via text messages, voice calls and video calls. All in all, Discord offers a user-friendly platform that is not limited to game chatting, but also supports other forms of interaction such as video calling, offering unlimited potential for different communities.

Facebook group is a Facebook forum for community groups. Compared to Discord, Facebook group does not have as many features as Discord, for example, it does not support online video chat or voice chat. First of all, if a person wants to join a Facebook group, he/she needs to send a request to the group administrator, and after the administrator agrees, he/she can nally join the group. After this step, users can see what the group has posted before, and they can also see the number of views on the bottom left corner of the post, such as seen by 5. Apart from that, they can leave a comment on the post, like the post, or share the post via WhatsApp as well. Users can create a post by clicking on the icon in the bottom right-hand corner and choose to make it anonymous or not if they wish, and of course they can choose to create an "Event" to invite people to participate. Meanwhile, users can directly search to view related posts, Facebook group also provides different le types according to the content posted by the group, where users can see six categories, they are: "Reels", "About", "Photos", "Events", "Files" and "Albums". Users can click on different categories to view the posts they want to know more about. Overall, the Facebook group provides users with exible usage scenarios and promotes interactions between people.

In general, although these social media platforms have different focuses and purposes, their primary goal is to promote interaction between users and the platform by allowing

them to use the site's features as a way to improve user engagement and enhance the platform's in uence. In the next section, we will discuss Facebook and explain how Facebook's recommendation mechanism works from the perspective of its system model to provide accurate recommendations to users. In addition, in terms of user privacy, we aim to obfuscate the privacy of users when they use Facebook, and we intend to utilize noise to fool Facebook's recommendation system.

3.2 Recommendation Systems

As of March 2024, Facebook is the third most visited website in the world [29]. First, Facebook's recommendation mechanism and ad delivery are its core functions, which involve complex algorithms and strategies throughout the process to enhance the user experience and increase the effectiveness of ads. Regarding its recommendation mechanism, Facebook's platform is based on the algorithmic categorization of users' preferences, and it needs to understand and deduce what users are likely to be interested in, so as to display the pushed content on users' homepage, and provide advertisers with the ability to target users according to their different interest categories in the whole process. At the same time, Facebook uses continuous machine learning to achieve a more accurate push to the target group, based on the user's behavior on Facebook, such as the user's previous search history, liked the page to determine the user may be interested in the content and accurate push [25]. On the other hand, regarding Facebook's ad delivery mechanism, Facebook helps advertisers to accurately deliver to target groups of users from four aspects. First, Facebook utilizes user pro le information such as geographic location, age, gender and other user characteristics to directly connect advertisers with target users [22]. Secondly, Facebook analyzes and predicts the content that users may be interested in by using a large amount of user data through various machine models. After that, Facebook will carry out a speci c ad recommendation, for example, if the user has previously interacted with a website then Facebook will push the site's ads to the target user as well. Finally, during the delivery of a Facebook ad, advertisers are able to monitor in real-time how many people are reacting, commenting, sharing and clicking on it, and can use this data to improve their future campaigns. Meanwhile, Mark Zuckerberg, during the Meta's most recent earnings call, has pointed out that more than 20 percent of a person's Facebook and Instagram feed is now recommended by AI from people, groups or accounts they do not follow [15].

Next, we are going to discuss Facebook's recommendation system in detail. First of all, Meta has its own recommendation guideline, namely the "remove, reduce and inform". The main purpose of this strategy is to remove content that violates the community standards, reduce the spread of content that does not violate the community standards but is problematic in itself, and recommend people additional information [18]. This is to

ensure that its recommendation system works as expected, and delivers content that is meaningful and relevant to the user, while protecting the user from potentially sensitive or uncomfortable content. In this case, showing people relevant content can boost their user experience, for example, if someone frequently likes mountain biking content or belongs to a related group. In addition to this, Facebook may recommend record-breaking races or videos of cycling adventures shared by content creators. As well as recommending easy and healthy recipes for wilderness riding - this is because Facebook thinks that the user may also like the content because other users who share the same interests as the user like the post content and nd them useful [17]. To do this better and on a larger scale, Facebook has introduced Meta AI, which aims to nd optimal content for platform users by learning the nuances and showing people the most relevant posts out of tens of billions of possibilities [17]. Next, we will go into Meta AI on a higher level, starting with the fact that it is a research division focused on the development and study of deep learning and arti cial intelligence (AI) technologies. Meta AI's research efforts include MViT, XLM-R/XLM-V, and FLAVA/Omnivore.

Multi-scale Vision Transformer (MViT) , a model based on the Vision Transformer specifically designed to handle visual tasks with different scale features, such as image classi- cation, object detection, and segmentation [5]. It is like a "Superman" with supervision, seeing the big surface features of an object as well as the minutiae. The core of MViT lies in how it processes and understands the information in an image or video, and in particular how it constructs and utilizes spatio-temporal hierarchies of features. One of the most innovative aspects is its "Pooled Attention Mechanism", which pools projection queries, keys, and value vectors to reduce visual resolution, it is coupled with increasing channel dimensionality in order to construct hierarchies ranging from simple features at high visual resolution to more complex, high-dimensional features at lower resolutions. Figure 3.1 shows an example of multi-scale attention: the original input video is shown in the leftmost column; the second column from the left displays the video at a lower resolution; and the last four columns show the attention maps from the different heads of the MViT architecture, where the deeper layers are shown in the lower rows [16]. Regarding how MViT speci cally performs multiscale image analysis, rst, the original image is input into the model and divided into a number of chunks, such as the modules labeled 1, 2, 3, 4, etc., as shown in Figure 3.2, after which each chunk is processed at a different scale. Scale 1 is probably the closest to the original image and has a higher resolution. Scale 2 and scale 3 subsequently show progressively lower resolution. As the scale increases, the image blocks appear to become smaller and smaller. This indicates that the model is gradually shifting from focusing on details to obtaining a wider eld of view. C, H, and W in the gure represent the number of channels, height, and width, respectively. In this process, as we move down the scale, the height and width decrease (i.e., the visual resolution decreases) while the number of channels increases. This means that the model

Figure 3.1. Multi-scale attention maps [16]

Figure 3.2. MViT model for processing image information [5]

is shifting from focusing on the high-resolution details of the original image to focusing on higher-level, more abstract features (i.e., the number of "channels" increases) [5].

XLM-R is a model that achieves state-of-the-art performance in cross-language comprehension through the use of self-supervised training techniques, primarily for comprehending and generating multilingual text. As people share their stories and thoughts on Facebook in over 160 languages, XLM-R becomes a key step in the process: no matter what language users are communicating in, XLM-R ensures that everyone has the best experience on the platform. First, since XLM-R is using self-supervised techniques and at the same time, it uses over 2TB of publicly available data for training. Also, it cleaned the CommonCrawl dataset containing texts in various languages to create a robust cross-language model. During the ne-tuning process, XLM-R uses labeled data in multiple languages to re ne the model to improve its performance, enabling the model to achieve state-of-the-art results on cross-lingual benchmarks. Overall, by using such a large number of datasets and optimizing downstream task performance through ne-tuning, XLM-R maintains cross-linguistic exibility while also providing a deep understanding of the nuances of each language [3].

FLAVA, rst of all, it is a foundational language and vision alignment model, which is capable of processing both linguistic and visual information, and enhances content understanding through joint pre-training of unimodal and multimodal data as represented in Figure 3.3. In FLAVA's pre-training process, the rst step is the input of data, here multimodal and unimodal pretraining data includes image-text pairs, unpaired images and unpaired text. After that, it enters into the pre-training phase, which is done by using the input data to perform the task. Finally, when the pre-training task is completed, the FLAVA

Figure 3.3. Overview of the FLAVA model pre-training and application process [24]

Figure 3.4. Flow of the Omnivore model for processing different types of visual data [10]

model can be applied to the three domains of visual recognition, language understanding, and multimodal reasoning, respectively. Through this process, the FLAVA model can be exibly applied to a variety of complex visual and linguistic tasks [24].

Omnivore is a single vision model for many different visual modalities, which is capable of handling many different visual tasks. The general processing ow represented in Figure 3.4 is: First, the input data types include image, video, and single-view 3D. For each type, rst, the data will be partitioned into many patches, and then these patches are converted into visual data through linear layers. After that, the data will be input into the Transformer model for understanding and process. Finally, the Transformer model outputs an embedding vector that can be used for e.g. classi cation, detection, or other visual understanding tasks [10].

In conclusion, based on the various models mentioned above, they allow Meta AI to fully understand the semantic meaning of content in different modalities (e.g., image, text, audio, or video), these systems utilize very large-scale attention models, graphical neural networks, and other techniques to understand people's behavioral preferences. AI systems like these tailor the experience at scale for each individual and enhance the user experience by continuously learning and anticipating to go to the user with accurate

recommendations.

3.3 Preliminaries

3.3.1 Obfuscation

Obfuscation, literally speaking, is the deliberate use of techniques to make things unclear or dif cult to understand in order to achieve an obfuscating effect. In the context of a software program, obfuscation means to protect trade secrets or intellectual property by obfuscating the programming code to make it dif cult to understand, as well as to prevent malicious attacks. From the perspective of data security, obfuscation usually refers to the condition that data becomes dif cult to understand and recognize without changing its core functionality, making it more dif cult for external attacks without affecting the functionality of the system. From a communications privacy perspective, obfuscation is used to prevent third-party attacks, such as eavesdropping and interception of information. However, obfuscation is controversial from a legal and ethical point of view, because it can be used as an unethical tool for malicious purposes, for example, the developer intentionally conceals the malicious behavior in the code, so from this point of view, we need to control the degree of obfuscation, and nd a balance between security and compliance with the ethics and laws.

In Obfuscure, we have also introduced the idea of obfuscation, here we are looking at it from the perspective of other data collectors such as social networks, by mixing real data with fake data (noise) to confuse the data collector. In this way, we protect the user's privacy in social networks by providing the user with a large amount of noise to confuse the social platform data collectors, in order to nd a balance between the user's privacy and the user's experience.

3.3.2 Web automation

Web automation is the process of automating tasks in a web browser through the use of software or scripting software. It involves automating interactions with websites, web applications, and web services by simulating user actions such as clicking buttons and navigating web pages [4]. In terms of application scenarios, it can be used rstly in automated testing, which is used in the software development process to test whether a web application functions as expected by simulating user behavior. Also, web automation can be used to capture data from websites, which can be used in areas such as market analysis. In addition, as mentioned earlier, web automation can be used to simulate user behavior to perform automated tasks, such as automatically logging into a website, submitting forms, and managing website content. These tasks can be automated to save time and reduce manual errors.

On the other hand, while automation tools bring convenience to development, there are also certain challenges and caveats. For example, when the layout and elements of a web page change, this may cause the automation script to fail, and it may also place an additional burden on the web server if the automation script is operated frequently. It is also worth noting that a large number of automated interactions can also violate a site's terms of service. During the development of Obfuscure, we encountered a similar problem when frequent logins to Facebook were seen as a violation of the community guidelines, which resulted in the blocking of the associated test account.

In MetaPriv's development, we used the Selenium framework, a comprehensive open-source project that provides a set of tools and libraries to support web browser automation. The project includes extensions to simulate user-browser interactions and a distribution server to extend browser distribution [23]. It also supports multiple browsers such as Firefox, Chrome, Safari, and Internet Explorer. MetaPriv was designed to simulate user behavior by invoking the Selenium automation tool to automate Firefox web driver instances to perform user interactions with Facebook.

4. METAPRIV

MetaPriv is a privacy tool based on simulating user interactions with Facebook. The tool utilizes obfuscation technology to protect the anonymity of users by generating "noise" through BOT to confuse Facebook's data pro ling algorithms. To be more speci c, this method fools Facebook into believing that the interactions generated by the BOT are actually generated by the real user, in this way, MetaPriv helps hide the user's actual interests to achieve the goal of protecting the user's privacy. Furthermore, MetaPriv works by using the BOT doing automated activities to simulate human interactions with Facebook to achieve the aim of not revealing the user's actual preferences, in other words, it reduces Facebook's accuracy in targeting ads and content customization.

Additionally, to verify that MetaPriv can help users improve their privacy over a certain period, MetaPriv was analyzed with both dummy and real accounts during a testing phase. The analysis of the results showed that after six weeks of operation, user privacy has been signi cantly improved. These tests proved that MetaPriv did a good job of hiding user behaviors. Observation and comparison of the content as well as advertisements that Facebook recommended to their users before and after MetaPriv was introduced showed that the noise generated by the BOT effectively disrupted the platform's effectiveness in pro ling user activities. Moreover, the tool has a promising future and is expected to be extended to other social media platforms such as Twitter and Instagram to popularize digital privacy protection. All in all, MetaPriv allows users to protect their data privacy while browsing Facebook. Meanwhile, MetaPriv also provides a platform for research to evaluate and validate the performance of different privacy protection methods, thus supporting the innovation and advancement of privacy technologies.

4.1 High-Level Overview

First, before we introduce the basic idea behind MetaPriv, we would love to explain some entities beforehand.

- User: $U := f u_1; u_2; : : : ; u_n g$ is the set of all users registered on Facebook. Each user u_i is uniquely identi ed within the range $i \ 2 \ [1; n]$. Additionally, each user has their attributes represented by the set $A_i \quad A$. [2]
- Attributes : The set of attributes within a social network (SN) is represented by

Figure 4.1. High-level overview of the BOT's functionality [2]

$A := \{a_1, \ldots, a_m\}$, referred to as the attribute space. Each attribute characterizes a particular interest of a user u_i, such as "u_i likes cooking". [2]

- User Real and Noise Attributes : Consider a user u_i associated with an attribute set A_i. Elements in A_i could be generated by the BOT or the authentic user activities. The set of attributes in A_i from genuine user activities is represented by $A_i^r \subseteq A_i$, whereas the set of attributes generated by the BOT is shown as $A_i^n \subseteq A_i$. [2]

MetaPriv's basic idea is to hide Facebook's perception of a user u_i by blending u_i's original attributes A_i^r with some noise attributes A_i^n. To achieve this goal, a BOT is used to communicate with the social network as u_i. As for the optimal privacy coverage, the BOTS' activity should be equal to or greater than the amount of traf c generated by u_i genuine interactions. [2]

If a user u_i signs up on Facebook (FB) for the rst time, then their attributes set A_i is empty initially. After registration and starting to use Facebook, the user u_i begins to generate activities by liking posts, commenting, watching videos, and so on. During the process, Facebook would collect these user activities and analyze them to create a list of user attributes that shows u_i's interests for accurate recommendations in the future. In our work, we consider these attributes to be real and represented by the set $A_i^r \subseteq A_i$. After this, the set A_i is used by Facebook to personalize the content to the target u_i. This is how the social network gets a clear picture of u_i's interests, thus, enabling it to provide tailored content accurately. However, we want to protect user privacy from social networks to provide more anonymity for people. To this end, MetaPriv was developed, a tool designed to help users disguise their real interests to the social network. MetaPriv operates on a straightforward principle: it generates noises on behalf of a user, and the

attributes are attached to the set A_i^n which characterizes the noise mentioned before. This strategy is implemented by the BOT, a core component of MetaPriv whose functionality is shown in Figure 4.1. [2]

Figure 4.2. MetaPriv's Work ow

Next, we will explain the steps of the BOT process:

1. The BOT necessitates entry to user u_i's account, which can be achieved through one of two methods: The user u_i can directly supply their login details, or the BOT can retrieve the necessary data from the browser pro le directory—this is the concealed folder located within the user's system directory that houses web browser cookies and other related data.
2. After the BOT secures entry to the user's account, it needs a collection of keywords produced by another component of MetaPriv, intended to function as noise attributes. Yet, the keyword generator mandates an initial seed keyword, which the user is obliged to provide at the outset.
3. The user speci es their preferred privacy setting, which essentially corresponds to the degree of convenience and advantages they are prepared to forgo for enhanced privacy protection. Practically, this setting dictates the consistent degree of obfuscation applied to the account.
4. Ultimately, the BOT repeatedly carries out a sequence of actions shown in Figure 4.1.

Overall, the entire process of MetaPriv is divided into two steps as represented in Figure 4.2. Next, we will describe them step by step:

1. Interactions between the user and the BOT : First, users are supposed to enter their password to log in to MetaPriv. After successful authorization, users will send a request to the BOT by clicking "Start Bot Process", then the BOT will execute relevant commands to complete the corresponding operation.
2. Interactions between the BOT and social media : When the user makes requests to the BOT to execute relevant actions, the BOT will initially authenticate into the user's Facebook account using the credentials saved in the local le. After that, the

BOT will generate noise with Facebook by random liking posts, videos, and so on, based on the received user's privacy level and seed keywords.

4.2 Limitations

Although MetaPriv can help users improve their privacy on Facebook within an effective period, it still has certain limitations. Next, we will discuss the limitations of MetaPriv from different aspects.

- Single-user Design : MetaPriv is a single-user architecture system and it limits its suitability for providing privacy to multiple users. This restriction is inef cient i.e. the BOT can only serve one person.
- User Interface and Usability : The user interface of MetaPriv is very primitive and user-unfriendly. First, its set-up process requires the user con gures a Linux environment and installs relevant resources. This may reduce the usability of the systems to users, especially to those who do not have a technical background, limiting the system's implementation in the hands of the users.
- Security Issues : MetaPriv stores user data locally, which can be a big threat to its security, especially once the local le is compromised. This can make user data vulnerable to attack and may lead to unauthorized access.
- Inappropriate Content : MetaPriv may accidentally like or comment on content that is not in line with the user's values, therefore, it may put the user in awkward situations at some point.
- Limitations of Word and Noise Data Generation : MetaPriv's word generation is limited since we realized that some words or topics are considered inappropriate by Facebook and this could lead to content deletion or account blocking. Apart from that, the generation of noise data is limited as well. The constraint can have a negative impact on obfuscation's ef ciency primarily in those scenarios when various noise data is crucial in preserving privacy.

Based on these limitations, we introduce Obfuscure, an upgraded version of MetaPriv to resolve the limitations discussed above. In the next chapter, we will discuss the system model of Obfuscure as well as a high-level overview of it to demonstrate where exactly it has been improved compared to MetaPriv.

5. SYSTEM MODEL AND HIGH-LEVEL OVERVIEW

In this chapter, we will analyze the system model of Obfuscure , the improved version of MetaPriv, which consists of ve entities: (i) Client, (ii) User, (iii) Server, (iv) BOT, and (v) Social Network (SN). Each entity is designed to play a key part in maintaining the privacy of the user, and together, they provide the user with the convenience and security of networking.

- Client : The client is a Firefox browser-based extension. It is the gatekeeper and the main way for users to interact with Obfuscure's features. The client handles the authentication process and ensures secure communication with the server. It is designed to create an easy-to-use interface that allows users to determine their desired level of privacy and what seed keywords to generate relevant noise around to obfuscate.
- User : Let $U := f u_1; u_2; : : : ; u_n g$ be the set of all users bene ting from the functionalities of Obfuscure through the client. Each user u_i is uniquely identi ed by their user_id within the range $i \ 2 \ [1; n]$. Each user u_i operates independently, ensuring that actions executed by one user do not interfere with the processes of another. Obfuscure is designed with a strong user focus; this includes setting a user attribute pro le that encompasses privacy considerations, allowing users to tailor the system to meet their speci c privacy needs.
- Server : The server is the principal component, which synchronizes the data interactions between the client and BOT. It executes user requests, controls obfuscation algorithms, and veri es that user privacy settings are appropriately employed. In addition, the server design allows it to serve several user requests, keep user data secure as well as properly communicate with BOT for enforcement of obfuscation policies.
- BOT: The BOT is a key element that resides on the server, which acts as a user proxy in the social network. It does this through the simulation of actual user activities based on the obfuscation parameters supplied by the client. Through noise generation and creating an impression of real social activities, the operation of the BOT confounds the digital pro le of the user. Hence, the SN cannot derive an accurate model of the user data.

- Social Network (SN) : De ned as a graph $G = (U; R)$, this graph consists of vertices that represent users from a set U. The edges in this graph denote the relationships between these users and are de ned by the set R, which is a subset of $\{\{u; v\} \mid u; v \in U \text{ and } u \neq v\}$.

5.1 High-Level Overview

This section discusses Obfuscure from a high-level overview of how each component in Obfuscure works together to help users achieve privacy on Facebook. First of all, Obfuscure not only solved the limitations of its predecessor, but also brought new features that made using the tool in multi-user systems considerably safer and more user-friendly.

Overall, the entire process is divided into four steps. Next, we will explain them step by step:

1. Interactions between the user and the client : Each user corresponds to their respective client. The user rst logs in to the client through the Firefox browser plug-in. During this process, users are supposed to enter their username, password, and PIN to log in to the client. After successful authorization, users can adjust their privacy level and seed keyword settings directly through the client interface.
2. Interactions between the client and the server : Once the client receives sessions from the user (i.e., the user sets all desired parameters), each client sends a corresponding con guration request to the server. During this process, the server receives and manages each user's session separately, and processes multiple requests at the same time through multiple threads to avoid interference or session con icts.
3. Interactions between the server and the BOT : After the server processes the request corresponding to each user, the server talks to the BOT to execute relevant commands to complete the corresponding operation.
4. Interactions between the BOT and social media : After the server sends commands to the BOT to perform relevant operations, rst of all, the BOT automatically logs in to the user's Facebook account by using the credentials stored on the server. Afterward, the BOT simulates the user's interactions with Facebook through automated behaviors such as liking posts, watching videos, etc. based on the received user's corresponding privacy level and seed keywords. In this way, it confuses Facebook with the user's real activities and interests by generating such noises.

In general, Obfuscure ensures user privacy due to the collaboration of those entities, including interactions of users, clients, server, BOT, and social media platforms represented in Figure 5.1; that is, users can remain in a safe and user-friendly environment as well as nd a balance between social media and user privacy.

Figure 5.1. Obfuscure's Work ow

5.1.1 Registration

In the following two sections, we would like to introduce Obfuscure's registration and login process in a detailed view to explain how they exactly ensure user privacy along the way. As we mentioned before, during the interactions between the user and the client, the user is supposed to complete the registration and login process. First, we will discuss the registration process a bit.

Initial Setup：

- Extension Download：Users are supposed to download the Obfuscure plugin from Firefox if they want to use the extension.
- Registration Interface：A new user is expected to register an Obfuscure account via the registration page, which is straightforward and user-friendly, guiding the user through the essential steps to safely input their credentials.

Security Features：

- PIN Code Input：During registration, the user is asked to create a PIN code to act as an extra layer of security.
- Encryption and Storage：As shown in Figure 5.2, by combining the hashed values of the Obfuscure's password and the user PIN code, Obfuscure creates a more practical encryption key to protect user data from potential attacks. Furthermore, the database of Obfuscure does not store the user's PIN code, it only stores the essential user data and they are all encrypted. In other words, even if Obfuscure's database got compromised, the attacker still cannot get access to the user account since he is not able to get the user's PIN code.

  Non-storage of PIN Code：As we mentioned earlier, the PIN code is not stored in Obfuscure's database. This method reduces the threat of user data leakage even if the database is violated.

Figure 5.2. Key generation process

5.1.2 Login

The login process mainly deals with user authentication to ensure the right user can securely get access to the platform and use the service.

Authentication :

- User Credential Veri cation : When users are trying to log in to Obfuscure, they are required to input their username, Obfuscure's password, and PIN code. The system then veri es these inputs by recalculating the hashes and attempting to decrypt the data with the generated key.
- Key Matching : The security mechanism is based on the correct match of the keys generated (registration and login) ensuring that only the right user accesses their data.
- Access Control : If the user enters the right credentials, the user data will be successfully decrypted and the user will be granted access to their account; alternatively, if one of those credentials is entered incorrectly, the request will be refused to against unauthorized access.

5.1.3 Multi-user Support

To address the limitation that MetaPriv only supports single-user use, we upgraded Obfuscure to support multiple users to effectively use the BOT resources and increase user ef ciency.

Multi-threading Implementation :

- Multi-threading Support : Obfuscure supports multi-threading, each user starts a new thread when they log in to Obfuscure, and different threads would not interfere

with each other.

- Isolated Processes ：Each user corresponds to their unique user_id to ensure the BOT can process different activities due to their user_id. In this way, it can help keep one user's activities from affecting another's.

6. IMPLEMENTATION AND RESULTS

With the ever-changing online privacy situation, MetaPriv provides a way for users to improve their privacy on social networks through automation. However, MetaPriv is not user-friendly, as the user has to set up a Linux environment and download the necessary repositories, which might be unacceptable for people with no technical background. In this chapter, we will discuss the implementation and results of Obfuscure, and then compare them with MetaPriv.

6.1 Client Design

As we mentioned in Chapter 5, the client of Obfuscure is a Firefox browser-based extension shown in Figure 6.1. The Obfuscure plug-in is mainly used to interact with the user and consists of three parts as represented in Figure 6.2: JavaScript, HTML, and manifest.json.

- JavaScript : In charge of response and interaction with web content, and can control the behavior of pop-up elements in plug-ins, providing users with instant feedback and interactive functions.
- HTML: Responsible for the styles of the plug-in to bring a straightforward visual experience to users and present a layout where users can interact with Obfuscure functions.
- manifest.json : It is the core part of the browser extension. In this le, we de ne the basic metadata about the extension, such as its name, version, and required permissions.

Figure 6.1. Client of Obfuscure

Figure 6.2. Plug-in Design

6.2 Server Design

First of all, regarding the server of Obfuscure, we use XAMPP as the local server environment. Next, we would love to introduce XAMPP a bit to explain what it is and how it works.

6.2.1 XAMPP

XAMPP is an open-source free, multi-platform web server solution stack package. It is developed by an international team of volunteers known as Apache Friends. It mainly consists of an Apache HTTP Server, MariaDB database, and interpreters for scripts written in the PHP and Perl programming languages. The XAMPP interface has been made exible to allow for the use of almost all web server deployments. Apart from that, the package is highly convenient for developers who need an easy and reliable platform to test web applications locally before deploying them to a live server. [36]

Next, we will talk about the key components of XAMPP that we have used during the implementation of Obfuscure:

Figure 6.3. XAMPP control panel

Figure 6.4. users table

- Apache HTTP Server : A high-performance and popular web server that processes requests and delivers web content on the internet or local networks.
- MySQL: An open-source relational database management system, which is quite popular as it stores and retrieves data for web applications [30].
- PHP: A server-side scripting language that was initially created for web development but is used as a general-purpose programming language as well.

XAMPP was used as the local server environment for the development as well as testing of the backend aspects of the application, including databases and server-side scripts of Obfuscure.

6.2.2 Database Design

The database design plays a crucial role in our implementation. In our system, we have three tables in total, they are: (i) users, (ii) stats, and (iii) settings.

- users : As shown in Figure 6.4, this table includes usernames and passwords of Obfuscure, as well as users' Facebook credentials which are fb_email and fb_password.
- stats : As shown in Figure 6.5, this table includes keywords as well as those words generated by the BOT, stats_data which is the summary of the dashboard data, and the user_id corresponding to each user.
- settings : As shown in Figure 6.6, this table includes seed keywords that are set by each user, the percentage which is the desired privacy level of each user, as well as the user_id corresponding to each user.

Figure 6.5. stats table

Figure 6.6. settings table

6.2.3 Multi-threading

In operating systems, multi-threading allows multiple threads to share the same process's resources, each of those threads is isolated from each other and executed independently [32]. In our work, we used multi-threading to implement multi-user cases, each user has their own thread, and different threads are isolated from each other, enabling more ef cient execution of complex processes as well as ensuring each user's experience is uninterrupted.

- User-speci c Threads : Each user's interactions with Obfuscure are handled in separate threads as shown in Figure 6.7. To ensure our multi-threading would not be interrupted by other activities, we created an extra Python le, namely bot.py to execute threads-related activities. Since each user corresponds to their own user_id, whenever they try to log in to their account, the BOT will start a new thread due to their user_id. The activities of each user will be operated in a separate thread. In this way, it allows simultaneous operations across different user accounts without interference, where each thread manages the session and operations for one user.

Bene ts of Multi-threading :

- Improved Scalability : Through multi-threading, Obfuscure can effectively manage

Figure 6.7. Multi-threading

concurrent user sessions without wasting any resources.

- Reliability : Isolating users in separate threads prevents the situation when one thread has a problem, for example, an error or pages do not load as expected, from in uencing other threads.

The implementation of multi-threading in Obfuscure signi cantly improves the platform's ability to manage users. Each thread acts as an independent agent, which is allowed to execute operations and manage data without affecting the performance or experience of other users. This approach not only improves ef ciency but also user satisfaction by providing an uninterrupted service.

6.3 User Interfaces

In the eld of human-computer interaction, the user interface (UI) is where human-machine interaction occurs, and in general, user interface design aims to produce a user interface that makes it simple, ef cient, and enjoyable for the user to operate the machine (user-friendliness) in a way that produces the desired results [35]. Regarding security applications, it is even more important for such products to achieve an intuitive user interface to ensure that the user feels con dent and not overwhelmed when dealing with the settings. In this section, we will provide an in-depth comparison between MetaPriv and Obfuscure.

6.3.1 MetaPriv's User Interface

MetaPriv has a simple interface with useful features. The initial user login page of MetaPriv represented in Figure 6.8 is rather minimal, users can access the main interface of the platform after inputting their MetaPriv password. Additionally, the interactions between the end-user and the tool are limited as well.

As we can see from Figure 6.9, above a set of application features, there is an eye-catching instruction showing the user how to use the tool properly. Also, there is a slider that offers the option to choose how many posts to like per day, thus the user's privacy level, which allows users to manage the number of likes per day while they are using MetaPriv.

Figure 6.8. MetaPriv Login

Figure 6.9. MetaPriv Main Panel

In addition, the interface informs the user that detailed documentation is available in the GitHub repository and provides resources that the user can utilize to deepen their understanding or get help when troubleshooting.

Key operational features include:

A slider labeled "Posts per day (max):" allows users to set preferences for the maximum number of posts they can interact with. The slider is equipped with a numeric indicator for precise adjustment.

Below the slider are several available action buttons:

- Reset Seed Keyword : Resetting a new seed keyword is easy and people can do this by clicking on the button represented in Figure 6.10.
- Keyword Statistics: This provides the user with an analysis of the keywords used to generate the noise as represented in Figure 6.11.
- Denoiser Input : As shown in Figure 6.12, this part works similarly to a lter to prevent generated noise from appearing in the user's main feed on Facebook.
- Start Bot Process : Initiates the obfuscation process, in keeping with the explanatory text provided above.

Overall, MetaPriv is a privacy tool, which is simple in form but detailed in function, providing a center to the main features of the tool. However, it might be problematic since the only thing that stands out is the functionality, without any additional cosmetic considerations.

Figure 6.10. Reset Seed Keyword

Figure 6.11. Keyword Statistics

Figure 6.12. Denoiser Input

Figure 6.13. Obfuscure Login

6.3.2 Obfuscure's User Interface

The user interface of Obfuscure is a signi cant improvement over MetaPriv's predecessor, providing users with a smoothly designed, modern, and familiar navigation environment.

Login Page Interface : As shown in Figure 6.13, the login page of Obfuscure presents a clean and straightforward entry point for users.

- Input Fields : It has three elds with distinct entries for 'Username', 'Password', and 'PIN', which help in the security process by the need to use a two-factor of authentication.
- Registration Link : The primary link for a new user is 'Register' displayed at the bottom part of the page, prompting users to register if they do not have an account with Obfuscure.

Post-Login Interface : As shown in Figure 6.14, the user is taken to this interface immediately after logging in.

- Privacy Settings : The user interface allows the user to select their expected level of privacy from a list of provided options and displays a drop-down menu asking the user how vague they would like their account to be.
- Keyword Input : The user can input "Keyword" in the eld, and de ne or change the seed keyword used to generate the noise, thus giving the obfuscation process the exibility to map the user's interests.
- Action Buttons : The user interface has different action buttons with descriptive labels such as "Save Keywords", "Login Facebook" and "Logout MetaPriv" to help users familiarize themselves with the site faster.

Figure 6.14. Obfuscure Settings

Figure 6.15. Obfuscure Main Panel

Main Panel Interface : As shown in Figure 6.15, the main panel of Obfuscure is where the user can control the core functionality.

- Statistical Dashboard Access : Users may access a more detailed interface via the "Stats Dashboard" button, where users can analyze detailed noisy data about privacy settings over time.
- Logout Options : Users are given the option to log out after logging in, by clicking on the "Logout Facebook" button, users can log out of their Facebook account and end the BOT process. Logging out of the current Obfuscure account can be done by clicking on the "Logout Obfuscure", the whole process is easy to do.

Keyword Statistics Interface : As shown in Figure 6.16, Obfuscure's statistics dashboard demonstrates the amount of noise data.

- Graphical Representation : A bar graph de nes interactions across different keywords such as 'Spring', 'bound', 'adhere' etc using different color scales. The graph differentiates activities such as 'Liked pages', 'Liked posts', 'Watched videos', and 'Liked videos' with distinct colors, providing a clear visual summary of the obfusca-

Figure 6.16. Obfuscure Dashboard

tion impact.

- Navigation : A simple 'Back' button is included below the graph, allowing users to return to the main panel without hassle.

Comparative Analysis of Obfuscure's Interfaces : The concept of design strategy of Obfuscure's user interface is the thoughtful design strategy oriented at user experience:

- Attractive Interface design : Compared to MetaPriv, Obfuscure has a more appealing interface design, with a uni ed design, color scheme, and button style across different panels and pages to provide a uni ed user experience.
- Enhanced Security Measures : Obfuscure improves user privacy by adding a PIN code authentication instead of the regular username/password authentication.

In conclusion, Obfuscure's interfaces have been designed based on user-oriented, focusing on ease of use and user privacy. The emphasis on the user interface design not only increases satisfaction but also the regular use of the tool, therefore, Obfuscure provides better privacy management on social media platforms.

6.4 User-friendliness: Comparing MetaPriv and Obfuscure

Ease of use is a crucial feature of every software application, especially when it comes to tools like MetaPriv which deals with sensitive privacy settings. This section presents the comparison of MetaPriv with Obfuscure about user-friendly.

MetaPriv : MetaPriv's interfaces are fairly primitive and featureless, offering only core functionalities with minimal attention to design or guide interactions. While the interface layout is very simple, there is far less feedback and support for users in terms of navigation, so it may not be as user-friendly for new users. The lack of detailed tutorials during the installation and con guration process can be daunting for those users without a technical background.

Obfuscure : Obfuscure is a Firefox browser extension, which was designed with user-friendliness to ensure an easy installation and smoother use. In a real-world scenario, people can download Obfuscure from the Firefox browser, and we simpli ed the installation process in comparison to MetaPriv's Linux con guration requirements.

- Ease of Installation : Downloading and installing Obfuscure can be done simply and it provides a chance for those users who do not have a technical background to use.
- Registration and Setup : If the user is new to Obfuscure, then the user is required to create an Obfuscure account, which includes three elements; a username, a password, and a PIN code. The process of account creation is pretty clear, with the input of the PIN code providing an extra layer of security authentication.
- Personalized Settings : After logging in, the user can set up the desired level of privacy and seed keyword. The settings are stored in the database and automatically lled for the next session, hence there is no need to con gure the same preferences repeatedly.
- Automated Interaction : The server-side BOT reacts to the corresponding user preferences by generating noises that simulate user activities on Facebook. It continuously performs this feature by generating new keywords related to the seed keyword input by the user, resulting in creating a new noise generation process with a more advanced level of automated behavior.
- Intuitive Interface and Controls : The interface of Obfuscure is user-oriented, it consists of understandable labels, buttons, and a visually appealing dashboard. The extension enables users to navigate easily around it with a clear option to log out either from Facebook or the Obfuscure completely.

Comparative Analysis : Compared to MetaPriv, Obfuscure is developed with a higher satisfaction to the user's requirements and expectations. Obfuscure's user interface not only allows for simpler and visually appealing interactions but also adds ef ciencies to improve user experience. Furthermore, the added functions of logout of Obfuscure and Facebook provide the user with a more controllable platform.

From MetaPriv to Obfuscure, the user-friendliness has been signi cantly improved. From start to end, Obfuscure is designed to help improve the interactions between the user and the platform. The improvements demonstrate MetaPriv's transformation from a privacy tool to an appealing, user-friendly extension that allows users to manage their privacy in social media with more ef ciency.

6.5 Multi-user Cases

Obfuscure is multi-user oriented, unlike MetaPriv's predecessor, which is single-user oriented. The improvement of Obfuscure is remarkable because it ts the actual life situation where a privacy tool should be able to serve multiple users with speci cally personalized interactions. This section analyzes the usability and performance of Obfuscure in multi-user cases.

Multi-user Login : In the testing phase, we did the experiments by logging into two different user accounts simultaneously. For user 1, we rst chose privacy level for 30% and the seed keyword was "Flower", and we analyzed the data for 5 hours. For user 2, we chose the same privacy level and set the seed keyword as "Swimming". Furthermore, except for running these accounts for 30% as the privacy level, we did another round in which the privacy level was increased to 50%.

First, we would like to discuss the results when the privacy level was 30%:

- User 1: The seed keyword we chose for user 1 was "Flower", then when we started the process to keep it continuously running for 5 hours. After 1 hour, the amounts of Liked pages, Liked posts, Watched videos, and Liked videos became [52, 9, 0, 0]. After 2 hours, the results changed to [54, 11, 4, 2]. Then the BOT kept running and after 3 hours, the results increased to [56, 12, 4, 2]. After 4 hours, the results became [89, 21, 4, 2]. After 5 hours, it became [106, 23, 11, 3].
- User 2: The seed keyword for user 2 was "Swimming", then the BOT started generating noises related to "Swimming" afterward. After 1 hour, the results became [32, 13, 1, 0]. After 2 hours, the results changed to [40, 15, 10, 6]. Then after 3 hours, the keyword results became [40, 15, 17, 8]. After 4 hours of running, the results signi cantly increased to [80, 23, 17, 8]. After 5 hours, the results turned to [90, 25, 25, 11].

Next, we will discuss the results of the two users when the privacy level was 50%:

- User 1: While the seed keyword remained the same as before, after running for 1 hour, the results of those four elements were [8, 5, 13, 9]. After 2 hours, the results became [34, 16, 13, 9]. Additionally, after 3 hours, the results changed to [54, 24, 13, 9]. After 4 hours, the results of raised to [98, 33, 13, 9]. After 5 hours, amounts of those four elements changed to [113, 34, 15, 9].
- User 2: The seed keyword of user 2 remained the same but we increased the privacy level up to 50%. After 1 hour, the amounts of those elements were [61, 12, 0, 0]. After 2 hours, the results changed to [77, 14, 4, 2]. While the BOT was generating noises for this keyword, the results became [87, 15, 9, 5]. After 4 hours, the results of raised to [136, 23, 11, 7]. After 5 hours, it became [136, 23, 15, 8].

Figure 6.17. Interactions After 1 Hour

Figure 6.18. Interactions After 2 Hours

Figure 6.19. Interactions After 3 Hours