

Received February 10, 2020, accepted February 24, 2020, date of publication February 28, 2020, date of current version March 11, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2977101

Social Media Users Send Promotional Links to Strangers: Legitimate Promotion or Security Vulnerability?

HONGZHOU YUE¹, SHUILONG HE¹, AND ZHENGHUI LIU^{2,3}, (Member, IEEE)

¹School of Computer and Information Technology, Xinyang Normal University, Xinyang 464000, China

²Henan Key Laboratory of Analysis and Applications of Education Big Data, Xinyang Normal University, Xinyang 464000, China

³Guangdong Key Laboratory of Intelligent Information Processing and Shenzhen Key Laboratory of Media Security, Shenzhen University, Shenzhen 518060, China

Corresponding author: Hongzhou Yue (yuehz@xynu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61602318, and in part by the Nanhu Scholars Program for Young Scholars of Xinyang Normal University.

ABSTRACT Nowadays, many users make money by publishing content on social media platforms. In order to attract users' attention, they often take measures to promote themselves. The security vulnerabilities in social media platforms may provide convenience for their user promotion work. We call this type of vulnerability the user promotion security vulnerability (UPSV). UPSV may cause unfair competition and endanger the interests of legitimate users and the social media platforms. Therefore it has great research significance to find and fix this vulnerability. In this paper, we propose a UPSV which widely exists in the function of sending messages to strangers of in-app chatting of many social media platforms. We first analyzed this vulnerability in some apps, and then YY app (China's largest live streaming platform) was chosen as the research object to verify the actual effect of the vulnerability on illegitimate user promotion. We took the method of promoting a target YY streamer through sending promotional links to viewers, and to improve promotion effect, we used the method of user preference learning to select viewers for promotion. The experimental results show that among the promoted viewers, more than 44% entered the target streamers' channels to watch live streaming, more than 21% followed the target streamers, and more than 13% gave gifts to the target streamers. It fully proves that this UPSV is real, exploitable and harmful, and we also proposed some fix suggestions to help the platforms to fix it.

INDEX TERMS Social media, user promotion, security vulnerability, in-app chatting, preference learning.

I. INTRODUCTION

With the development of social media app, more and more people use social media app for entertainment. For instance, users can use social media app to read news, watch videos, sing, make friends, etc., and it can be considered that social media app has greatly enriched people's lives [1]. Additionally, social media app can be used by a user not only for entertainment, but also for making money [2]. The commonly used methods to make money by social media include advertising, paid reading, commodity promotion, fans' donations, etc [3]. Social media has even become the main work platform for many freelancers. For instance, a large number of young

people in China are engaged in the work of live streaming, and receiving virtual gifts from viewers is a major way to earn money for them [4]. Advertising and paid product placement become the most common ways through which people make money on videos uploaded to YouTube [5].

We call a social media user who has money-making motive the profit-oriented user, or POU for short. Generally speaking, for each POU, more user attention means more potential revenue [6]. Therefore, most of the POUs will try to improve the quality of social media content, so as to attract more users' attention. However, it is not possible to rely only on good content to get high attention because no matter how good the content is, if the users do not know the existence of the content, or cannot find access to the content, then there will not be much users to pay attention to the content [7].

The associate editor coordinating the review of this manuscript and approving it for publication was Arianna Dulizia¹.

Therefore, if a POU wants to get more attention, he often needs to take measures to promote himself. The typical promotion methods that he can adopt include cross-promoting on different social media platforms and relevant forums, asking his network of friends to help him to promote, networking and forging connections with other POUs and organizations, etc. [8]. Besides, the social media platforms would also take measures to recommend excellent or potentially attractive content to users. The common recommendation measures include homepage recommendations, related item recommendations [9], recommendation notification [10], etc.

These promotion methods can indeed help a POU to promote his social media content, as long as he makes efforts to publicize his works, meanwhile improve the quality of the content in order to get platform's better recommendation. Furthermore, these promotion methods are usually not harmful to the social media platform and the other users, so we regard them as legitimate promotion methods. However, we have such a question, whether some POUs are not satisfied with these legitimate promotion methods, and use some more effective, labor-saving promotion methods which may be harmful to the social media platform and the other users? This is the main problem to be discussed in this paper.

We can think of several illegitimate promotion methods. For instance, a POU may obtain a large number of users' contact information (e.g., phone number, email address, etc.) through illegitimate methods [11], and send his social media links to each user by the contact information. A social media platform may expose the interface of notification push, through which a POU can send promotional links to the target users [12]. What's more, a POU may masquerade as a friend of the target user by the method of masquerade attack [13], and send promotional links to him. Illegitimate promotion methods may cause unfair competition, do harm to other POUs and the ordinary users, and damage the interests of social media platform. The security problem of illegitimate promotion of a social media platform may be caused by its own security weakness (e.g., leakage of users' privacy), or by other factors (e.g., private information trading). We regard the security weakness of a social media which can lead to illegitimate promotion problem as "user promotion security vulnerability" (UPSV).

In order to explore whether there exists UPSVs in popular social media apps, we analyzed a large number of social media apps and find a kind of UPSV which is applicable to numerous apps. This vulnerability exists in the in-app chatting function [14] of each vulnerable social media app, through which a POU can send promotional links to large numbers of strangers. In this paper, we did a security analysis on this vulnerability, and verified its harmfulness by the actual vulnerability exploitation. We also proposed some fix suggestions to help the platforms to fix the vulnerability.

The main contributions of this paper are as follows:

1) We introduced the concept of UPSV of social media, and analyzed its establishing conditions. In an era when social media content can create economic benefits for users, UPSV

may cause unfair competition and endanger the interests of legitimate users and the social media platforms. Therefore it has great research significance to find and fix this vulnerability.

2) We proposed a UPSV that widely exists in the in-app chatting function of many social media platforms, and did a security analysis on this type of vulnerability of some popular social media apps. Many apps have in-app chatting function, and in order to facilitate users to make new friends, most of them allow users to send messages to strangers. However, since many apps lack effective restrictions on the number of messages that users are allowed to send to strangers and effective content inspection of the messages, users can send a large number of promotional contents to the strangers. As a result, an illegitimate user can promote himself in this way. Therefore we consider that there exists UPSVs in these apps.

3) We choose YY app (China's largest live streaming platform) as the research object to verify the actual effect of UPSV on illegitimate user promotion, and proposed some fix suggestions. We did a detailed analysis on the UPSV that exists in the function of sending messages to strangers of in-app chatting of YY, and take the streamer as the promotion object to study the method of exploiting the vulnerability to promote a streamer to the potential viewers. In order to improve the promotion effect, we use a user preference learning method to select viewers for the target streamers, and sent promotional links to selected viewers. The experimental results show that our vulnerability exploitation method is feasible and effective, and also prove that UPSV is helpful for an illegitimate user to promote himself and harmful for the legitimate users and the social media platforms.

The remainder of this paper is organized as follows: We analyze the establishing conditions of UPSV and the existence of this vulnerability in in-app chatting function of several popular social media apps in Section II, and as one app of them, YY's UPSV is analyzed in Section III. In Section IV, we introduce the vulnerability exploitation method of YY, and the evaluations of our vulnerability exploitation method are given in Section V. We present the related works in Section VI, and give some vulnerability fix suggestions in Section VII. The conclusions and future works are given in the last Section.

II. USER PROMOTION SECURITY VULNERABILITY

A. ESTABLISHING CONDITIONS

This section we will discuss the establishing conditions of UPSV.

First of all, if a POU wants to send promotional links to the target users, he must first get a way to send information to the target users, and considering the promotion effect, the promotional information should be able to send to as many users as possible. There exists an important precondition here, namely, the POU must first be able to get a large amount of users' contact information (chatting accounts, phone number, email address, etc.) which is necessary for this way of sending

TABLE 1. Analysis of in-app chatting function of 10 apps.

App	App type	Conditions for sending messages to strangers	Number limitations of messages	Can refuse to accept stranger's message?
WeChat	Messaging	Chatting by greeting function	No limitation	Yes
Sina Weibo	Microblog	Chatting freely	No limitation	Not followed user can be refused
Huajiao Live	Live stream	Chatting freely	No more than 20	Not followed user can be refused
Momo	Messaging	Chatting freely	No more than 10	Can turn off message reminder of stranger
YY Live	Live stream	Chatting by greeting function	No limitation	Can turn off message reminder of stranger
Douyin	Short video	Chatting freely	No limitation	Not followed user can be refused
Kuaishou	Short video	Chatting freely	No more than 10	Not followed user can be refused
Kg.qq	Karaoke	Chatting by private letter function	No limitation	yes
Changba	Karaoke	Messaging after following a stranger	No limitation	Not followed user can be refused
Kugou	Music & Live stream	Chatting freely	No limitation	Can turn off message reminder of stranger

information. We can think of many means to send information to the target users such as making use of the leaked users' phone numbers and email addresses, or the user communication function within a social app itself. Whatever promotion method is applied by a POU, it should be guaranteed that it is not easy to arouse users' disgust. A promotion way that is easy to arouse users' disgust may lead to the increase of complaint rate, thus affecting the promotion effect.

Furthermore, it should ensure that a POU can send out enough promotional links within an acceptable time. There is no doubt that a POU hopes sending out large amounts of promotional links spend as little time as possible, too much time spent will make the promotion work hardly to be carried out. But if the information disseminator (e.g., telecommunication operator, e-mail service provider or app service provider) takes restriction measures to limit the number of links that a POU can sent out within a specified time period, it is difficult to achieve good promotion effect. Therefore, it can be considered that only if there exists no effective restriction measures, a POU can successfully send a large number of promotional links to users in a limited time.

Last but not least, we consider that the promotional information sent out by a POU should not be blocked by the information disseminator due to illegitimate content. Some disseminators may adopt automatic content inspection mechanism to inspect the information sent by a user, and once the illegitimate promotional content is found, the content sending behavior of a POU may be blocked. Therefore, only in the absence of effective inspection mechanism can a POU successfully send promotion information to the target users.

In conclusion, we consider that the establishing conditions of UPSV can be summarized as follows:

Condition 1: The ways to send information to large numbers of target users can be obtained.

Condition 2: The number of promotional links sent through a specific method of sending information is not restricted strictly.

Condition 3: The content sent through a specific method of sending information is not inspected effectively.

These three conditions can be considered as the important conditions, and it can be considered that if a social media app satisfies these conditions, we think it has UPSV. Besides, we believe that other less important conditions should also be satisfied considering the effective exploitation of the vulnerability. For instance, we can think of two less important conditions: ① There exists an automatic way to send information. The promotion method is best to achieve automation, otherwise the human workload will make the promotion method difficult to implement. ② There exists a way for a POU to automatically analyze the users who may be interested in him, such as using a data mining or preference learning algorithm to analyze and select users. This can make the POU's promotion work be more targeted and efficient.

B. UPSV IN IN-APP CHATTING FUNCTION

According to our research, many social media apps have UPSVs in their in-app chatting functions. A user can send messages to a large number of strangers, and the message content is not effectively inspected. We selected 10 representative apps with more than 10 million users in China for analysis and the results are shown in Table 1.

It can be seen from Table 1 that all of the 10 apps allow a user to send messages to a stranger. Most of the apps allow users to send messages to strangers freely, that is to say, there is little difference between sending messages to strangers and to friends. There are also some apps treat sending messages to strangers and to friends differently. For instance, a WeChat user can only send messages to a stranger

by greeting function. The messages sent to a stranger by a YY user can only be displayed in the greeting message item. A Changba user needs to follow a stranger before sending messages to him. It can be also seen from Table 1 that almost every app sets the option (or the related option) of forbidding stranger's messages. However, the setting of this option is ineffective in defending UPSV because most of the users would not reject strangers' messages. Moreover, for a large social platform, the number of users that a POU can choose is large enough. Therefore, it can be concluded that all of the 10 apps satisfy Condition 1 of establishing conditions of UPSV.

Furthermore, we analyzed the number of messages that a user can send to strangers in each app. We found that only Huajiao Live, Momo and Kuaishou limit the number of messages that a user can send to strangers. They limit the number of messages a user can send to strangers up to 20, 10 and 10 per day respectively. On the contrary, the other 7 apps have no number limitations, but these apps generally use an implicit restriction measure, namely, if a user sends messages to too much strangers, his account may be banned by the platform because of being complained and reported by multiple users. However, this restriction measure is ineffective in defending UPSV because a POU may send promotional links by using multiple accounts. Moreover, a POU may apply the technique of automatic promotional links sending which is fast enough to ensure that all the promotional links are sent out before an account is banned. Therefore, it can be concluded that these 7 apps satisfy Condition 2 of establishing conditions of UPSV.







As for the inspection of illegitimate content, since a POU may adopt different forms of promotional links for different apps and the identification of illegitimate content by each app service provider is different, we did not make an in-depth study on whether the promotional links can be inspected effectively by each app service provider. However, through our analysis, we found that virtually none of the 10 apps do a strict inspection of the messages sent by users. Accordingly, it would not be difficult for a POU to construct promotional links that can bypass the interception of the platform.

In summary, it can be concluded that 7 of the 10 apps have UPSVs. We will take YY as an example to verify the existence and harmfulness of the vulnerability in the following sections, and the effective exploitation method of the vulnerability will be studied.

III. INTRODUCTION OF YY AND VULNERABILITY ANALYSIS

Through the analysis of Section II, we learned that YY's in-app chatting function has UPSV. For YY live streaming platform, a POU is a live streamer and the promotional link is the live streaming channel link. A live streamer can use the greeting function of YY in-app chatting to send his live streaming channel link to the strange viewers to promote himself. In this section, we will introduce YY platform and analyze this security issue.

TABLE 2. YY user identity level and clothes.

Clothes (male/female)	Color	Identity level
	purple	channel owner
	orange	channel general manager
	yellow	channel manager
	blue	member
	green	guest
	white	visitor

A. INTRODUCTION OF YY LIVE STREAMING PLATFORM

The YY live streaming platform provides users with live streaming viewing and sharing services. There are two different types of users in YY—streamer and viewer. The streamer uses YY platform mainly to gain profits through sharing live streaming, and the live streaming forms mainly include singing, playing games, chatting, DJ(Disc Jockey), storytelling, etc. The viewer uses YY platform mainly for entertainment through viewing streamers' live streaming, and the profits gained by the streamer mainly come from the virtual gifts given by viewers. Actually, there is no essential difference between the user accounts of streamer and viewer. A streamer can become a viewer if he accesses other streamer's channel to view live streaming, and a viewer can also become a streamer if he applies for the live streaming permission successfully.

A YY streaming channel is an URL address in which a streamer shares his live streaming, and for each YY channel, the identity of YY viewers on this channel can be classified into 6 levels, the classification of identity levels is shown in Table 2. The clothes icons on the first column of the table indicate the viewers' identity levels. In a channel, streamers with different identity levels will be shown different colors of clothes icons in front of their nicknames. The purple clothes represent the channel owner, namely the streamer himself, and each channel is owned by only one streamer. The orange and yellow clothes represent the channel managers, blue and green clothes represent the channel's ordinary viewers, and white clothes represents the channel's visitors. In a live streaming channel, the permissions of streamers of the six identity levels are successively reduced, and these permissions include user management, voice input, text input, etc. Visitors can be regarded as temporary viewers, which have the lowest permission and often be limited in text input.

Each YY user can have different identity levels in multiple channels, and a user's identity levels in each channel can be queried by any other user, which is not part of personal privacy. Fig. 1 shows the channel list of a user which is shown in his homepage. The identity level of a viewer in a channel is authorized by the streamer. The streamer authorizes



FIGURE 1. Live streaming channel list of a YY user.

a viewer’s identity level according to viewer’s contribution to the streamer and streamer’s favorable impression on the viewer. Generally speaking, those who make a greater contribution to the streamer will be authorized a higher identity level. Viewer’s contribution to the streamer is mainly reflected by the virtual gift giving. The virtual gift is purchased by the viewer with money and the different virtual gifts have different prices.

If a viewer has identity level (except visitor) in a streamer’s channel, he can easily find out and access the streamer’s channel by searching his channel list. Besides, a viewer follows a streamer can also facilitate the viewer to access the streamer’s channel, because when a viewer follows a streamer, the streamer’s channel will be shown in the viewer’s following list. What’s more, the platform will send notices to the viewer whenever the streamer in the following list starts sharing live streaming. Both following a streamer and having identity level in a streamer’s channel can be regarded as a viewer’s preference for the streamer, and they are independent of each other and have no correlation. If a viewer does not follows a streamer, he may still have identity level in the streamer’s channel, as long as he is willing to contribute for the streamer and is favored by the streamer. On the contrary, if a viewer follows a streamer and enjoy viewing the streamer’s live streaming, but does not contribute for the streamer, he may not has identity level in the streamer’s live streaming channel.

B. SENDING LIVE STREAMING CHANNEL LINK TO STRANGER

The promotional links sent from a streamer to the targeted viewers are in the form of direct message, namely the targeted viewers can receive the links like the ordinary instant messages. Fig. 2 is used to show how YY users send live streaming channel links to strangers. In Fig. 2, Bob and Alice are strangers and the process that Bob makes use of YY’s greeting function to send Alice a live streaming channel link is as follows:

- 1) Bob opened Alice’s homepage and chose the function “send message”.

- 2) The conversation window with Alice was opened and Bob sent Alice a live streaming channel link.
- 3) New message arrived at Alice’s account and a red dot began attaching to her in-app chatting window which could remind her to view the newly received messages.
- 4) Following the reminding of red dot, Alice clicked the greeting message item and viewed all the greeting messages, eventually she found a greeting message sent from Bob.
- 5) Alice viewed Bob’s message and found it is a live streaming channel link.
- 6) Out of curiosity, Alice entered into the live streaming channel corresponding to the link and watched the live streaming of a streamer.

C. VULNERABILITY ANALYSIS

First, we analyze whether YY has UPSV in terms of the establishing conditions of the vulnerability.

Through the in-app chatting function to send messages to the target viewers, an illegitimate streamer only needs to know the account numbers of the target viewers, and a large number of YY account numbers can be easily collected from the various websites of YY by the method of web crawling [15], or by the simple method of account number traversing. Therefore, Condition 1 is satisfied. In addition, YY platform does not limit the number of messages that a user can send to strangers and a streamer can send live streaming channel links to a large number of YY viewers in an acceptable time. Therefore, Condition 2 is satisfied. Finally, live streaming channel link is a frequent used form of information exchange between YY users which does not have the nature of external advertising, hence it is generally not intercepted as illegitimate content by the platform. Therefore, Condition 3 is satisfied. To summarize, it can be concluded that YY has UPSV.

Then, we analyze whether the vulnerability can be exploited in terms of user psychology.

From streamer’s point of view, a YY streamer earn money mainly depends on the virtual gifts given by YY viewers and he obviously wants more viewers to watch his live streaming so as to bring him more potential income. However, with the development of live streaming industry, the number of streamers is increasing, and the competition among YY streamers becomes more and more fierce. Lots of streamers cannot attract viewers not because of poor quality of live streaming, but because that they cannot find the right way to publicize themselves, which results in users unable to know the existence of their live streaming. Therefore, there is a strong demand for a streamer to take effective measures to promote himself, and the method of sending live streaming channel links to the target viewers by YY’s in-app chatting function can provide great assistance for him.

From viewer’s point of view, as the live streaming channel link is not a third-party advertisement, hence it is not often ostracized by the YY users. Driven by curiosity, YY users are inclined to click the live streaming channel links sent

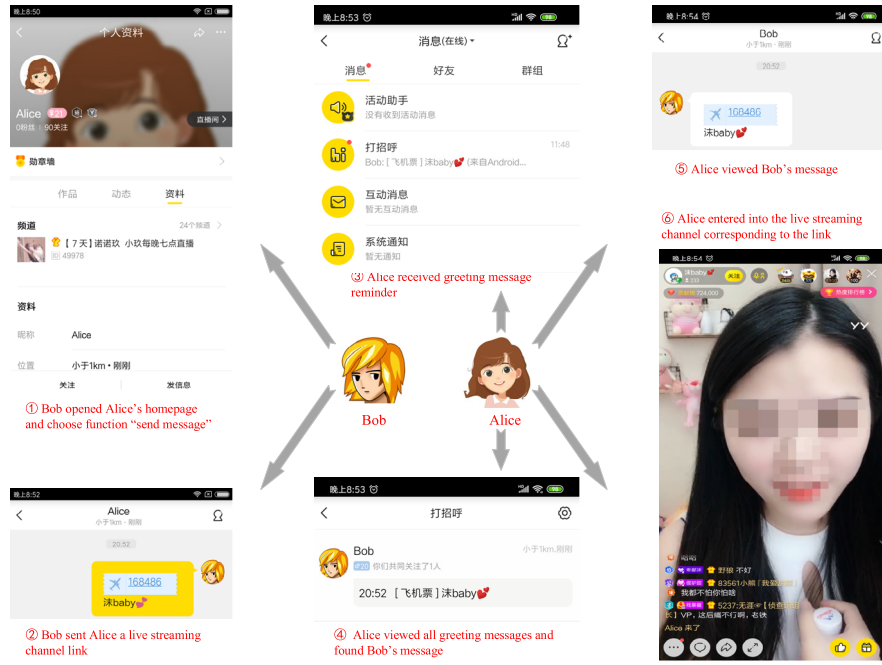


FIGURE 2. The process of YY users sending live streaming channel links to strangers.

by others. Furthermore, if the live streaming channel link is constructed reasonably, user complaint rate can be effectively controlled, which makes message sender's account not be easily banned due to low user complaint rate.

Therefore, it can be concluded that YY's UPSV can be exploited.

IV. VULNERABILITY EXPLOITATION OF YY

Using the vulnerability described in the Section III, an illegitimate streamer can send live streaming channel links to a large number of YY viewers. In this section, we will introduce the effective exploitation method of the vulnerability.

A. VULNERABILITY EXPLOITATION BASED ON HOOK MECHANISM

Our research found that a streamer can automatically send live streaming channel links to the target users through the hook mechanism [16], as shown in Fig. 3. The solid part in Fig. 3 is the original process of sending messages of YY app, while the dotted part is the new process after adopting hook mechanism. Before adopting hook mechanism, the app gets user's ID (short for UID) and messages from the user conversation program, and sends messages to the target user who is corresponding to the UID. After adopting hook mechanism, a UID set and the constructed message (i.e., live streaming channel link) to be sent are stored in the SD card, and the original method of reading UID and sending message are hooked. As a result, each UID is extracted from the UID set through the method of loop iteration, and the live streaming channel link is sent to each target user.

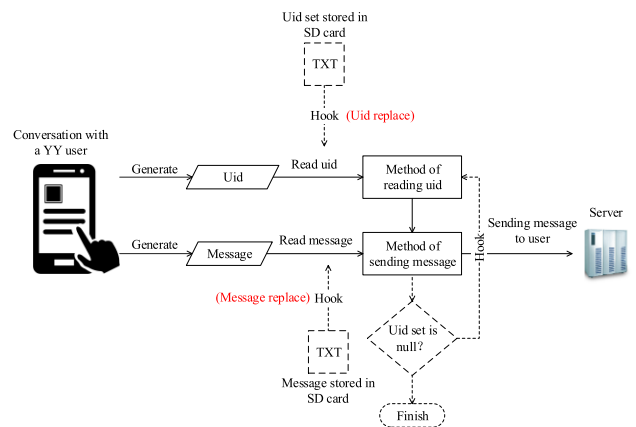


FIGURE 3. Sending messages automatically based on hook mechanism.

The automatic message sending method based on hook mechanism improves the efficiency of sending live streaming channel link, reduces the manual work, and makes the vulnerability exploitation be more feasible.

B. USER PREFERENCE LEARNING

If a streamer chooses users randomly for promotion, it will be definitely inefficient, while if the users who may be interested in the streamer can be selected by some methods, it will make the user promotion more effective. In this section, we propose a user preference learning method to screen users and make the user promotion be more targeted.

We use two kinds of data to summarize a user's preference: streamers that a user follows and a user's identity levels in



FIGURE 4. Impression labels of a streamer.

each channel. We had introduced in Section III-A that both following a streamer and having identity level in a streamer’s channel can be regarded as a viewer’s preference for the streamer. These two data can be gotten in user’s personal homepage which shows user’s following list and channel list.

We use the impression label data to summarize the characteristics of a streamer. The impression labels of a streamer are generated by users’ evaluation and are the reflection of streamer’s characteristic. Fig. 4 shows an example of the impression labels of a streamer. Similarly, the impression label information of a streamer can be gotten in his personal homepage.

For these three kinds of data, methods we can use to get the data including HTTP packet sending and receiving, using hook mechanism, etc. We had developed a data acquisition program, which can automatically collect these three kinds of data.

The characteristics of streamers that the different users prefer are different, and the impression label can reflect the characteristics of the streamer. Therefore we can calculate a user’s preference for a streamer by calculating the user’s preference for the streamer’s impression labels. The specific methods are as follows:

We represent the set of streamers that user u follows as $S_u = \{a_{s1}^u, a_{s2}^u, \dots, a_{sn}^u\}$. The impression labels set of streamer a is represented as $B_a = \{b_1^a, b_2^a, \dots, b_n^a\}$. The set of streamers on whose live streaming channels user u has identity levels is represented as $T_u = \{a_{t1}^u, a_{t2}^u, \dots, a_{tm}^u\}$. The identity level of user u on streamer a ’s channel is represented as m_u^a . According to Table 2, there are mainly four identity levels in YY (except for the streamer and visitor): guest, member, channel manager and channel general manager. We use four integers 1, 2, 3 and 4 to represent these four identity levels respectively, and it can be considered that the larger the number is, the higher the identity level is.

There may exists three cases for user u prefers streamer a .
 Case 1: u not only follows a , but also has identity level on a ’s channel.

Case 2: u follows a , but has no identity level on a ’s channel.

Case 3: u has identity level on a ’s channel, but does not follow a .

We think that in these three cases, user u ’s preference levels for streamer a are different, so we need to treat

them differently when we calculate the preference value. For Case 1, we set a coefficient $\alpha (\alpha > 1)$, and it can be considered that u ’s preference value for all the streamers that satisfying Case 2 is α . For Case 3, we set a coefficient $\beta (\beta < 1)$, and it can be considered that u ’s preference value for all the streamers that satisfying Case 3 is $\beta \times$. For Case 1, it can be considered that u ’s preference value for all the streamers that satisfying Case 1 is $\alpha \times m_u^a$.

User u ’s preference for streamer a can be described as u ’s preference for the streamer with the impression label set B_a , and in order to calculate this preference value, we need to calculate u ’s preference for each impression label in B_a firstly. User u ’s preference for impression label b of streamer a can be calculated by Eq. (1):

$$XH_{u,a,b} = \begin{cases} 0 & a \notin S_u \cup T_u \text{ or } b \notin B_a \\ \alpha & a \in S_u, a \notin T_u, b \in B_a \\ \alpha \times m_u^a & a \in S_u \cap T_u, b \in B_a \\ \beta \times m_u^a & a \notin S_u, a \in T_u, b \in B_a \end{cases} \quad (1)$$

Then, user u ’s preference for impression label b can be calculated by Eq. (2):

$$XH_{u,b} = \frac{\sum_{a_i \in S_u \cup T_u} XH_{u,a_i,b}}{\sum_{a_j \in S_u \cup T_u} \sum_{b_k \in B_{a_k}} XH_{u,a_j,b_k}} \quad (2)$$

C. SYNONYM PROCESSING

We need to solve the problem of synonym when dealing with the impression labels. Although some impression labels are different, they may be synonyms with each other (e.g., “beauty” and “goddess”). We should treat these synonymous labels as the same because they can reflect the almost identical characteristics of a streamer. We use the synonym computation method based on HowNet [17] to calculate synonym which can judge whether two impression labels are synonyms. The process of the computation method is as follows:

First of all, we defined the similarity calculation of two impression label words as the maximum similarity between all of its concepts. For two words W_1 and W_2 , we suppose W_1 has m concepts ($C_{11}, C_{12}, \dots, C_{1m}$) and W_2 has n concepts ($C_{21}, C_{22}, \dots, C_{2n}$). Thus, the similarity of W_1 and W_2 can be calculated as Eq. (3).

$$sim(W_1, W_2) = \max_{i=1\dots m, j=1\dots n} \{sim(C_{1i}, C_{2j})\} \quad (3)$$

Then we need to calculate the similarity of two concepts. We define $sim_1(s_1, s_2)$ as the similarity of two concepts’ all the basic sememes, $sim_2(s_1, s_2)$ as the similarity of relational sememes and $sim_3(s_1, s_2)$ as the similarity of relational symbol sememes. We also define β_1, β_2 and β_3 as three weight coefficients which are adjustable and satisfy $\beta_1 + \beta_2 + \beta_3 = 1$ and $\beta_1 \geq \beta_2 \geq \beta_3$. The similarity of two concepts can be

calculated as Eq. (4).

$$sim(C_1, C_2) = \sum_{i=1}^3 \beta_i \prod_{j=1}^i sim_j(s_1, s_2) \quad (4)$$

Finally, we calculate the similarity of two sememes by Eq. (5). In Eq. (3), $dis(s_1, s_2)$ means the path length of two sememes s_1, s_2 in the sememe tree. ∂ is an adjustable parameter and represents the sememe path length when the similarity is 0.5. For the sememe path length calculation, we use the method of weighted sememe path length algorithm. Suppose there are n edges in the shortest reachable path between s_1 and s_2 in the sememe tree. $level(k)$ represents the level number of the parent node on the k -th edge in the tree structure, and the level number of the root node is set as 0. The sememe path length calculation algorithm are as Eq. (6) and (7).

$$sim(s_1, s_2) = \frac{\partial}{dis(s_1, s_2) + \partial} \quad (5)$$

$$dis(s_1, s_2) = \sum_{i=1}^n weight(level(k)) \quad (6)$$

$$weight(i) = \frac{m-1-i}{m-1} \cdot (1 + \sin(\theta \cdot i \cdot \pi/180)) \quad (7)$$

Through the above method, we can calculate the similarity of two impression label words. We set a threshold, for example, if the threshold is 60%, then we consider that impression label words with similarity more than 60% are synonyms. We define the synonym set of label b as $SIM_b = \{s_1^b, s_2^b, \dots, s_n^b\}$ and the synonym set of label set B_a as SIM_{B_a} which can be calculated as Eq. (8).

$$SIM_{B_a} = SIM_{b_1^a} \cup SIM_{b_2^a} \cup \dots \cup SIM_{b_n^a} \quad (8)$$

Therefore, user u 's preference value for streamer a can be calculated by Eq. (9). When we promote for a streamer, we can set a threshold, and if a user's preference value for the promoted streamer reaches this threshold, we will choose him as the targeted user for promotion.

$$XH_{u,a} = \sum_{b_k \in SIM_{B_a}} XH_{u,b_k} \quad (9)$$

V. EVALUATION

In Section IV, we introduced the vulnerability exploitation method of YY's UPSV. In this section, we will verify the feasibility of this vulnerability exploitation method through experiments. We took several streamers as the promotion objects, and sent live streaming channel links of the streamers to the target users which were chosen by the specified user selection method to analyze the actual effect of user promotion.

A. USER SELECTION

Suppose that a is the streamer we want to promote, we choose users for a according to the process shown in Fig. 5: ① We choose users from the contribution lists of each live streaming channel online. If a user is in the contribution list of any

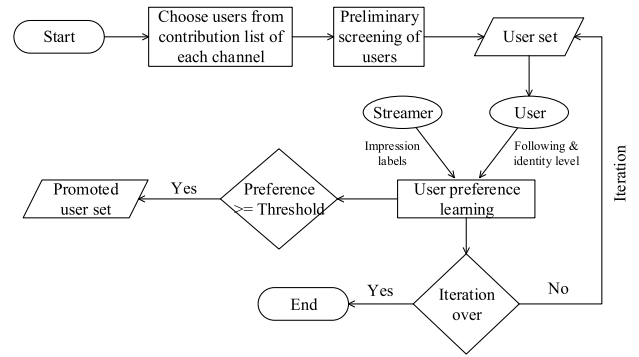


FIGURE 5. Process of selecting users.

streamer, it means that the user account is very active recently. Furthermore, it also means that the user is willing to give virtual gifts to their favorite streamers. ② We do a preliminary screening for the selected users. First, we exclude the users who have already followed a or have identity level on a 's channel. Second, the gender of users would be screened. If a is a male streamer, then we choose female users for promotion and vice versa. This is to follow the law of opposite sex attraction. Third, we select the users who log in YY within 30 minutes. This selection method is mainly to prevent the user from shutting down YY app due to fatigue caused by using YY for too long. We can query the last login time of a user through a function interface of YY mobile app, as shown in Fig. 6. ③ We use the method of user preference learning introduced in Section IV to calculate each user's preference value for streamer a . We set a threshold and when a user's preference value for a is greater than the threshold, we consider that the user may be interested in streamer a , and then the user would be added to the promoted user set.

B. USER PROMOTION AND EFFECT ANALYSIS

We chose a female streamer for experiment. Before the experiment, she was followed by 12784 YY users and had been engaged in live streaming for one year and three months. Her streaming time is from 8 p.m. to 11 p.m. every day. Within 5 days of the experiment, we finished the user selecting work before she started live streaming every day. We started to send her live streaming channel links to the selected users from the start of her live streaming. The number of links being sent increased day by day, namely, 1000 links were sent on the first day, 2000 links were sent on the second day, and 5000 links were sent on the fifth day. The selected users are not repeated each day, and we sent only one link to each selected user to avoid disturbing and offending them. We set α to 1 and β to 0.5, and the threshold of the preference value to 0.2.

Table 3 shows the overall results of the experiment. The third column of Table 3 shows the time needed to send live streaming channel links, and it can be seen that sending links takes very less time, for instance, it only takes 11.4 minutes to send 5000 links and only 2.3 minutes for 1000 links.

TABLE 3. Overall experimental results of sending promotion links for a streamer.

Day(th)	Number of links	Time spent sending links	Within 3 hours of live streaming			Number of users entering the channel within 1 day of the experiment
			Number of users entering the channel	Number of followers	Number of users giving gifts	
1	1000	2.3min	176	55	32	452
2	2000	4.6 min	339	92	71	887
3	3000	7.0min	570	122	92	1398
4	4000	9.1min	794	182	110	1880
5	5000	11.4 min	918	230	144	2347



FIGURE 6. Last login time of a YY user.

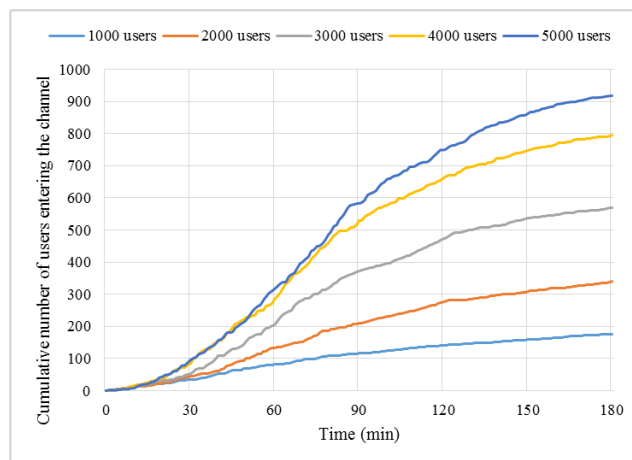


FIGURE 7. Distribution of cumulative number of users entering the live streaming channel.

Therefore, it can be considered that the speed of sending links is fast enough to avoid negative effects on user promotion.

We made statistics on the number of users entering the channel during the live streaming time of the streamer. The statistical method was applying hook mechanism to conduct a real-time information monitoring for the live streaming channel, and we only monitored the users who had been sent the promotional links. As for the other viewers entering the channel during this time, we do not count them. The statistical results are shown in the fourth column of Table 3. In the three hours of the live streaming, the number of users entering the channel accounted for 16% - 19% of the total number of users who had been sent links. We also made statistics on the number of users who followed the streamer and gave gifts to the streamer in 3 hours. The results are shown in the fifth and sixth columns of Table 3 respectively. The number of users who followed the streamer accounts for 21% - 32% of the total number of users who had been sent links, and the number of users who gave gifts accounts for 13% - 21%. These results prove that our promotion method is helpful for the streamer to increase fans and profits. Besides, in order to analyze the attractiveness of the promotional links to users more effectively, we extended the monitoring time to one day, and found that the number of users entering the live streaming channel in one day accounted for 44% - 47% of the total number of users who had been sent links. This proportion is close to one half and high enough, indicating that sending promotional links to the target users can really

attract users. We did not make statistics on the number of users who followed the streamer and gave gifts to the streamer out of the 3 hours of the streamer’s live streaming, because YY users are not allowed to do these behaviors during the non-streaming time of a streamer.

We also analyzed the time points when the users who had been sent links entered the live streaming channel within 3 hours of the streamer’s live streaming, and the results are shown in Fig. 7. This figure shows the cumulative number of users entering the channel at a given time point, and it can be seen from the figure that the number of users increased with time. Meanwhile, users entered the channel most frequently within 30 to 90 minutes after sending promotional links.

On the 5th day (5000 links were sent), we made statistics on the time users who had been sent links spent on watching live streaming within 3 hours of the streamer’s live streaming, and the results are shown in Fig. 8. In Fig. 8, the horizontal axis represents the time and the vertical axis represents the number of users who watched the live streaming for more than a specified time. From this figure, we can see that most of the users watched the live streaming for a very short time (mainly less than 20 minutes), it means that only a small number of users were really interested in the streamer and were willing to spend time watching her live streaming.

We also made segment statistics on the time users spent on watching live streaming, and the statistical results are shown in Table 4. The second column shows the cumulative number

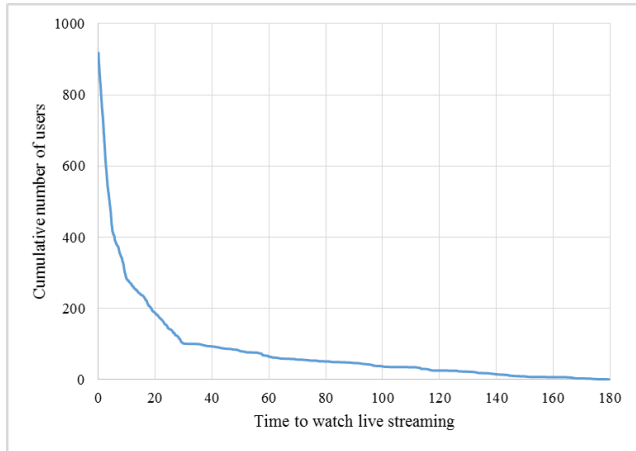


FIGURE 8. Cumulative time distribution of users watching live streaming.

TABLE 4. Segment statistics on time users spent on watching live streaming.

Time segment	Users number	Number of followers	Number of users giving gifts
>2.5 hours	9	9	6
2-2.5 hours	16	14	9
1.5-2 hours	21	16	12
1-1.5 hours	18	13	10
0.5-1 hours	37	16	19
20-30 minutes	86	32	33
10-20 minutes	95	25	32
5-10 minutes	132	37	16
3-5 minutes	155	35	5
<3 minutes	349	33	2

of users who watched the streamer’s live streaming for a period of time corresponding to the time segment shown in the first column. The third and fourth columns show how many users among the users showed in the second column followed the streamer and gave gifts to the streamer respectively. It can be seen from Table 4 that the number of users who watched the live streaming for more than 20 minutes only accounts for 20.37% of the total number of users entering the channel. In addition, it can also be seen from the distribution of the number of users who followed the streamer and gave gifts to the streamer that the users who watched the live streaming for longer time were more willing to follow the streamer and give gifts to the streamer.

C. AFFECTING FACTORS FOR PROMOTION

In Section V-B, we studied the user promoting effect for a streamer. In this section, we will study the user promotion effect for multiple streamers. The promotion effect may be affected by many factors, but we mainly consider the following factors:

Factor 1: Number of followers. The number of followers of a streamer can reflect his popularity from the side, so the

attractions of streamers with different number of followers may be different, and then promoting for them may have different promotion effects.

Factor 2: Different impression tags. Streamers with different personalities may have different attractions to users, and the most direct embodiment of streamer’s personality is the impression label. Therefore, promoting for streamers with different impression labels may have different promotion effects.

For Factor 1, we chose 10 streamers with a certain gap in the number of followers, and each of them had a live streaming time of no less than 3 hours per day. We sent 1000 live streaming channel links for each streamer respectively, and monitored the changes happened in the channel within 3 hours of each streamer’s live streaming. The statistical results are shown in Table 5. The second column of Table 5 shows the number of followers of each streamer before the experiment, and the third column shows the number of users that entered the channels within 3 hours of each streamer’s live streaming. It can be seen that the number of users that entered each channel has no obvious regularity. However, the mean time of users watching live streaming is increasing with the increase of the number of initial followers, and so is the number of new followers, which indicates that the streamer with more followers is more attractive to users. On the contrary, when the number of followers of the streamers changes, the number of users giving gifts does not show an obvious regularity, which indicates that no matter how attractive the streamer is, there is no significant difference in the number of users willing to give gifts. We speculate that the number of users giving gifts may be related to the communication and interaction between the streamer and the viewer. Although the live streaming of the popular steamer is more wonderful and attractive to the users, the users are only willing to watch his live streaming and not willing to give gifts due to his less communication with them, while the less popular streamer is just the opposite. It can be considered that whether users are willing to give gifts reflects a kind of human relationship.

For Factor 2, we made a statistical analysis of the impression labels during the process of promoting for streamers, and analyzed the attractiveness of different impression labels to users. The methods are as follows: 100 streamers were chosen to promote, and 1000 promotional links were sent for each of the streamers. In order to exclude the influence of the number of followers on the promotion effect, the streamers we chose have the number of followers ranging from 8000 to 10000. From the previous experiment, we can see that there is no obvious regularity for the number of users entering the channel, which is not related with the attractiveness of the streamers themselves, only related with the curiosity of the user. Therefore, we did not discuss the number of users entering the channel in this experiment. For the different impression labels, we need to compare the following proportions: η_1 , the proportion of users following the streamer to the users entering the channel; η_2 , the proportion of users giving

TABLE 5. Experimental results of sending 1000 promotion links for 10 streamers.

Stream er Id	Number of followers before experiment	Number of users entering the channel	Mean time to watch live streaming (min)	Number of new followers	Number of users giving gifts
1	1520	187	15.91	45	36
2	2843	168	16.07	47	38
3	6864	194	16.11	51	42
4	8565	159	16.20	43	35
5	12855	201	17.85	52	39
6	20504	167	17.60	59	33
7	32638	175	18.32	66	39
8	50156	186	19.07	72	37
9	81296	158	19.10	69	42
10	115493	195	20.18	86	38

gifts to the users entering the channel. When calculating the proportions η_1 and η_2 , we did not calculate for each impression label independently, but calculate for the synonym sequence of impression labels. Since it can hardly ensure that the monitoring time of each of the 100 streamers reaches 3 hours, we only monitored the changes happened in the channel within one hour of each streamer’s live streaming. If a streamer’s live streaming time was less than an hour, we monitored until the end of his live streaming.

The proportions η_1 and η_2 are calculated as follows: For the synonym set SIM_b of label b , if there are n streamers $a_1, a_2, a_3, \dots, a_n$ among the 100 streamers have labels in SIM_b . The number of users entering their channels during the monitoring time were $e_{a1}, e_{a2}, \dots, e_{an}$ respectively; the number of users following the streamer were $f_{a1}, f_{a2}, \dots, f_{an}$ respectively, and the number of users giving gifts were $g_{a1}, g_{a2}, \dots, g_{an}$ respectively. Then, the calculation method of the proportions η_1 and η_2 of the label set SIM_b are shown in Eq. (10) and (11):

$$\eta_1 = \frac{\sum_{i=1}^n f_{ai}}{\sum_{i=1}^n e_{ai}} \tag{10}$$

$$\eta_2 = \frac{\sum_{i=1}^n g_{ai}}{\sum_{i=1}^n e_{ai}} \tag{11}$$

The statistical results are shown in Table 6, which lists the top ten synonym sets of impression labels. From the table, we can see that the synonym set “amusing, funny man, comedy king” has the highest attractiveness to users, and the number of users willing to follow and give gifts is the largest. It indicates that the live streaming with the style of humorous and funny has a high attractiveness to users. The second-place synonym set is “powerful singer, sounds of nature, music spirit”, which means that the good singing streamer has great attraction to users. What’s more, it can also be seen that the appearance of the streamer is also an important factor for attracting users. For instance, the 4th, 5th and 7th-place synonym sets in Table 6 are mainly used to describe the good

TABLE 6. The attraction of different impression labels to users.

Synonym set of impression labels	Proportion of users following the streamer (η_1)	Proportion of users giving gifts (η_2)
逗比(amusing) 搞笑(funny man) 喜剧天王(comedy king)	45.93%	37.65%
实力唱将(powerful singer) 天籁之音(sounds of nature) 音乐精灵(music spirit)	44.20%	36.25%
唠嗑(chatting) 段子手(talkative person) 段友(talkative friend)	43.53%	35.90%
颜值担当(beautiful face) 颜值即正(fine face)	42.87%	36.06%
女神(goddess female) 美丽动人 (beautiful and moving) 甜美(sweet girl)	42.62%	34.56%
公主气质(princess temperament) 清纯(pure girl) 小清新(little pure girl)	41.54%	33.15%
帅气(handsome) 男神(gold male) 小鲜肉(fresh male) 青蛙王子(frog prince) 型男(stylish man)	40.52%	33.30%
温文尔雅(gentle) 温柔(tender)	39.22%	31.19%
暖男(warm hearted man) 居家好男(good family man)	39.13%	29.03%
萌娃(cuddly person) 软萌萌 (ladylike and cuddly) 萌舞(cuddly dancer)	38.36%	29.18%

appearance of a streamer, which indicates that the streamers with a good appearance also has a high attractiveness to users. It can be concluded from Table 6 that the number of users who give gifts to a streamer is generally less than the number of users who follow him, and it can be considered that the number of users who give gifts to a streamer increases with the increase of the number of users who follow him.

VI. RELATED WORK

As our work is studying the security problem of user promotion, therefore we first discuss about the related works that relevant to the security problems that caused by illegitimate user promotion.

With the rapid growth in the number of social media users, more and more organizations and individuals use social media platforms for commercial promotion. Several researchers studied the illegitimate promoting campaigns existed in the social media platforms and proposed methods to detect promoter accounts and promotional campaigns. Li *et al.* [18] used the method of relational classification based on typed Markov Random Fields (T-MRF) to identify user accounts that are involved in promotion on social media platforms. Kuang *et al.* [19] studied the problem of what strategies can improve promotional effectiveness on social media platforms, they proposed a method based on Propensity Score Matching (PSM) to evaluate the effect of each promotional strategy. Jiang [20] proposed a classification method called SocAdDet based on the SVMs to identify different advertising strategies and detect the social promoters. Ferrara *et al.* [21] designed a machine learning framework capable to detect promoted campaigns and separate them from organic ones in their early stages. Zhang *et al.* [22] proposed a URL-driven framework to detect both spam and promotion campaigns. The key point of the framework is how to measure the similarity between accounts' purposes of posting URLs. Liu *et al.* [23] found that many crowdsourcing website users collusively manipulate deceptive questions and answers (Q&As) for promoting a target (product or service) in the activities of Community Question Answering (CQA), and proposed a unified framework to tackle the challenge of detecting collusive spamming activities of CQA. Aswani *et al.* [24] proposes a hybrid approach for identifying the spam profiles by combining social media analytics and bio inspired computing. These related works exposed many illegitimate promotion problems in social media platforms and contributed to the detection and defense of illegitimate user promotion behaviors. However, unlike our works, they did not distinguish profit-oriented users from ordinary users in social media platforms, and did not consider the security issue of profit-oriented users promoting social media contents to ordinary users to gain economic benefits. In addition, none of these works pay attention to the UPSV which widely exists in the function of sending messages to strangers of in-app chatting of many social media platforms.

Malicious advertisement is also a typical illegitimate user promotion problem that was studied by many researchers which can mainly cause the following security problems: malware, scamming, spam, frauds, etc. [25], and lots of detection methods to detect malicious advertisements were proposed. For instance, Li *et al.* [26] found that hundreds of top ranking Web sites were threatened by malvertising and proposed a new detection tool called MadTrace to detect malvertising activities. Zarras *et al.* [27] studied the security advertisements of large number of web advertisements and found that the deficient filtering mechanisms makes ad exchange be more prone to serving malicious advertisements. Alghamdi *et al.* [28] analyzed the problem of social spam advertisements and proposed the detection models using combined features of URLs and OSNs (Online

Social Networks), and the user profiles and posts were also used to enhance the detection of malicious behavior. Auter and Fine [29] found that attack advertising on social media sometimes can act as an important measure used by a politician to compete with his opponent on an election campaign. Gimenes *et al.* [30] found that the low-valued user-product recommendation in some mobile apps can lead to the security problems of illegitimate promotion, and proposed the method of using vertex-centric asynchronous parallel processing of bipartite graphs to detect illegitimate promotion. Zhang [31] proposed the deep learning algorithms based on lexical features which can be used for classifying and visualizing the advertisements to detect the malicious advertisements. These related works contributed to solving the security problems caused by malicious advertisements. The security problem of illegitimate user promotion of social media platform we studied can also belong to the category of malicious advertising. However, none of these related works studied this security problem and concerned that a profit-oriented social media user may take illegitimate measures to promote himself to other users of the same social media platform to gain economic benefits.

Besides, as the illegitimate promotion method we analyzed is making use of the function of sending messages to strangers in a vulnerable social media app, therefore we discussed the related works regarding the security problems of app's chatting function, especially the messaging apps which are mainly used by users for chatting. Schrittwieser *et al.* [32] analyzed 9 popular mobile messaging and VoIP apps, and found that most of them have security vulnerabilities which allow attackers to hijack accounts, spoof sender-IDs or enumerate subscribers. Mueller *et al.* [33] revealed that most of the mobile messaging apps did not solve the problem of privacy implications, and the security and privacy features were generally existed on the new version of apps, while the older version of apps were usually threatened by old and even new vulnerabilities. Dudheria [34] found that most of the mobile messaging apps are vulnerable to MitM attack and proposed the corresponding attack scenarios, and an app's features and design choices are the key to defense MitM attack, rather than the end-to-end encryption technology. Botha *et al.* [35] studied the built-in security and privacy features of several messaging apps, and made some recommendations and practice advisements for users on the safe use of these apps. These related works revealed the security problems that exist in the messaging apps or app's chatting function. However, none of them focus on the illegitimate user promotion problems like our works.

VII. VULNERABILITY FIX SUGGESTIONS

UPSV of social media platform may cause unfair competition, do harm to illegitimate POUs and the ordinary users, and damage the interests of social media platform. In order to help the social media app manufacturers to fix this security vulnerability, we put forward some vulnerability fix suggestions:

First of all, the manufacturers should reduce the communication channels between a user and strangers in their social media apps. There are two communication channels that a user can use to communicate with strangers: transmitting information by social media app itself and by other means (e.g., phone number, email address, etc.). For the first channel, the manufacturers need not only to close the unnecessary communication functions between non-friend users, but also to strengthen the user relationship verification, so as to prevent malicious users from using the communication functions between friend users to send messages to strangers. For the second channel, manufacturers should try to protect users' contact information from being disclosed. They should not only prevent the user information stored in the servers from being stealing by attackers by means of network attack, but also prevent users from directly exposing their contact information on their personal homepages.

Furthermore, if an app has to open some communication functions between non-friend users due to the function needs or user experience needs, the manufacturer must strengthen the management of users' communication behavior, restrict the number and inspect the contents of the messages. For instance, for the UPSV that exists in the function of sending messages to strangers of in-app chatting revealed in this paper, we put forward the following two vulnerability fix suggestions:

1) Restrict the number of messages that users are allowed to send to strangers in a certain period of time effectively. The manufacturers cannot merely rely on the users to reject strangers' messages through the function provided by app to prevent this security vulnerability, because most of the users would not turn off the option of receiving messages from strangers, and a malicious POU can still find a large number of target users for promoting himself. Therefore, the manufacturers should use automated methods to limit the amount of messages users can send to strangers. When the amount reaches a certain threshold, the behaviors of users sending messages to strangers should be prohibited.

2) Inspect the contents of the messages that a user sends to the strangers automatically. Measures should be taken to prohibit users from sending any form of promotional links or other promotional information. The automated method, rather than the manual method to inspect message content should be used, because the speed of manual inspecting is generally too slow to deal with the automated vulnerability exploitation of UPSV.

Last but not least, the manufacturers should build a complete UPSV detection and emergency response mechanism, which could monitor the user behavior of social media platform comprehensively and discover and prevent illegitimate user promotion behaviors timely. They should also be able to respond quickly and find the exact UPSVs through users' illegitimate behaviors accurately, and fix the security vulnerabilities timely.

VIII. CONCLUSION AND FUTURE WORK

In this paper, we proposed the concept of UPSV of social media platform. The UPSV that exists in the function of sending messages to strangers of in-app chatting of many social media apps was analyzed. We take YY which is China's largest live streaming platform as our research object, and the illegitimate promotion method of promoting for a streamer through sending promotional links to strangers by YY's in-app chatting function is proposed. We used the method of reference learning based on impression label to select YY users, which can effectively improve the promotion effect. The experimental results show that the vulnerability exploitation method of YY's UPSV we used is feasible and effective.

However, there exists several limitations in this paper. The main limitation is that we chose a famous Chinese social media app (YY) to verify the harmfulness of UPSV, which may not be popular enough to be familiar to more people outside China. What's more, we concentrated on studying the UPSV in only one social media app, rather than more popular apps. In the future work, we will choose more popular social media apps especially the world famous apps to study their user promotion security problems. We will also try to explore more kinds of UPSVs in social media apps, and help more manufacturers to fix UPSVs to promote the safe and healthy development of social media platforms.

REFERENCES

- [1] A. M. Kaplan and M. Haenlein, "Users of the world, unite! The challenges and opportunities of social media," *Bus. Horizons*, vol. 53, no. 1, pp. 59–68, Jan. 2010.
- [2] M. Ye, "Analysis on the profit mode of post-modernized new media communication," in *Proc. 1st Int. Symp. Econ. Develop. Manage. Innov. (EDMI)*, Hohhot, China, 2019, pp. 566–569.
- [3] S. Xia, "A study on the profit model of we media in China," *Global Media J.*, vol. 15, no. 28, p. 1, Apr. 2017.
- [4] *The Rise Of Live-Streaming in China*. Accessed: Nov. 5, 2019. [Online]. Available: <https://www.beyondsummits.com/blog/rise-live-streaming-china>
- [5] *YouTube Business Model | How Does YouTube Make Money?* Accessed: Nov. 5, 2019. [Online]. Available: <https://www.feedough.com/youtube-business-model-how-does-youtube-make-money/>
- [6] Y. Liang and W. Shen, "Fan economy in the chinese media and entertainment industry: How feedback from super fans can propel creative industries' revenue," *Global Media China*, vol. 1, no. 4, pp. 331–349, 2016.
- [7] M. Pennacchiotti and S. Gurumurthy, "Social media user recommendation system and method," U.S. Patent 9 466 071, Oct. 11, 2016.
- [8] *Ways to Grow Your Twitch Channel in 2019*. Accessed: Nov. 5, 2019. [Online]. Available: <https://gleam.io/blog/twitch-growth/>
- [9] Y. Yao and F. M. Harper, "Judging similarity: A user-centric study of related item recommendations," in *Proc. 12th ACM Conf. Recommender Syst. (RecSys)*, Vancouver, BC, Canada, 2018, pp. 288–296.
- [10] J. E. Bostick, J. J. M. Ganci, and S. K. Rakshit, "Location aware photograph recommendation notification," U.S. Patent 9 716 827, Jul. 25, 2017.
- [11] Y. Li, Y. Li, Q. Yan, and R. H. Deng, "Privacy leakage analysis in online social networks," *Comput. Secur.*, vol. 49, pp. 239–254, Mar. 2015.
- [12] Z. Xu and S. Zhu, "Abusing notification services on smartphones for phishing and spamming," in *Proc. USENIX Conf. Offensive Technol.*, Bellevue, WA, USA, 2012, pp. 1–11.
- [13] S. J. Stolfo, M. B. Salem, and S. Hershkop, "Methods, systems, and media for masquerade attack detection by monitoring computer user behavior," U.S. Patent 9 311 476, Apr. 12, 2016.
- [14] *What is In-App Chat?* Accessed: Nov. 5, 2019. [Online]. Available: <https://www.pubnub.com/learn/glossary/what-is-in-app-chat/>

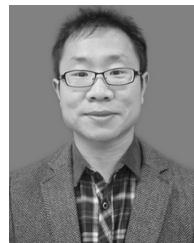
- [15] C. Jensen, C. Sarkar, C. Jensen, and C. Potts, "Tracking Website data-collection and privacy practices with the iWatch Web crawler," in *Proc. 3rd Symp. Usable Privacy Secur. (SOUPS)*, Pittsburgh, PA, USA, 2007, pp. 29–40.
- [16] Q. Tang, W. Zhang, X. Li, and B. Wang, "X-prcaf: Xposed based protecting cache file from leaks in Android social applications," in *Proc. 3rd Int. Conf. Trustworthy Syst. Their Appl. (TSA)*, Wuhan, China, Sep. 2016, pp. 17–22.
- [17] X. Zhu, R. Ma, L. Sun, and H. Chen, "Word semantic similarity computation based on hownet and cilin," *J. Chin. Inf. Process.*, vol. 30, no. 4, pp. 29–36, 2016.
- [18] H. Li, A. Mukherjee, B. Liu, R. Kornfield, and S. Emery, "Detecting campaign promoters on Twitter using Markov random fields," in *Proc. IEEE Int. Conf. Data Mining*, Brighton, U.K., Dec. 2014, pp. 290–299.
- [19] K. Kuang, M. Jiang, P. Cui, and S. Yang, "Steering social media promotions with effective strategies," in *Proc. IEEE 16th Int. Conf. Data Mining (ICDM)*, Barcelona, Spain, Dec. 2016, pp. 985–990.
- [20] M. Jiang, "Catching social media advertisers with strategy analysis," in *Proc. 1st Int. Workshop Comput. Methods CyberSafety (CyberSafety)*, Indianapolis, IN, USA, 2016, pp. 5–10.
- [21] E. Ferrara, O. Varol, F. Menczer, and A. Flammini, "Detection of promoted social media campaigns," in *Proc. 10th Int. AAAI Conf. Web Social Media*, Cologne, Germany, 2016, pp. 563–566.
- [22] X. Zhang, Z. Li, S. Zhu, and W. Liang, "Detecting spam and promoting campaigns in Twitter," *ACM Trans. Web*, vol. 10, no. 1, pp. 1–28, Feb. 2016.
- [23] Y. Liu, Y. Liu, K. Zhou, M. Zhang, and S. Ma, "Detecting collusive spamming activities in community question answering," in *Proc. 26th Int. Conf. World Wide Web (WWW)*, Perth, WA, Australia, 2017, pp. 1073–1082.
- [24] R. Aswani, A. K. Kar, and P. Vigneswara Ilavarasan, "Detection of spammers in Twitter marketing: A hybrid approach using social media analytics and bio inspired computing," *Inf. Syst. Frontiers*, vol. 20, no. 3, pp. 515–530, 2018.
- [25] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, "Beyond blacklists: Learning to detect malicious Web sites from suspicious URLs," in *Proc. 15th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining (KDD)*, Paris, France, 2009, pp. 1245–1254.
- [26] Z. Li, K. Zhang, Y. Xie, F. Yu, and X. Wang, "Knowing your enemy: Understanding and detecting malicious Web advertising," in *Proc. ACM Conf. Comput. Commun. Secur. (CCS)*, Raleigh, NC, USA, 2012, pp. 674–686.
- [27] A. Zarras, A. Kapravelos, G. Stringhini, T. Holz, C. Kruegel, and G. Vigna, "The dark alleys of madison avenue: Understanding malicious advertisements," in *Proc. Conf. Internet Meas. Conf. (IMC)*, Vancouver, BC, Canada, 2014, pp. 373–380.
- [28] B. Alghamdi, J. Watson, and Y. Xu, "Toward detecting malicious links in online social networks through user behavior," in *Proc. IEEE/WIC/ACM Int. Conf. Web Intell. Workshops (WIW)*, Omaha, NE, USA, Oct. 2016, pp. 5–8.
- [29] Z. J. Auter and J. A. Fine, "Negative campaigning in the social media age: Attack advertising on facebook," *Political Behav.*, vol. 38, no. 4, pp. 999–1020, May 2016.
- [30] G. Gimenes, R. L. F. Cordeiro, and J. F. Rodrigues-Jr, "ORFEL: Efficient detection of defamation or illegitimate promotion in online recommendation," *Inf. Sci.*, vol. 379, pp. 274–287, Feb. 2017.
- [31] X. Zhang, "A deep learning based framework for detecting and visualizing online malicious advertisement," M.S. thesis, Academic Unit Fac. of Comput. Sci., Univ. New Brunswick, Fredericton, NB, Canada, 2018.
- [32] S. Schrittwieser, P. Frühwirth, and P. Kieseberg, "Guess who's texting you? Evaluating the security of smartphone messaging applications," in *Proc. NDSS*, San Diego, CA, USA, 2012, pp. 1–9.
- [33] R. Mueller, S. Schrittwieser, P. Fruehwirt, P. Kieseberg, and E. Weippl, "Security and privacy of smartphone messaging applications," *Int. J. Pervas. Comput. Commun.*, vol. 11, no. 2, pp. 132–150, Jun. 2015.
- [34] R. Dudheria, "Assessing vulnerability of mobile messaging apps to man-in-the-middle (MitM) attack," *Int. J. Comput. Netw. Inf. Secur.*, vol. 10, no. 7, pp. 23–35, Jul. 2018.
- [35] J. Botha, W. C. Vant, and L. Leenen, "A comparison of chat applications in terms of security and privacy," in *Proc. 18th Eur. Conf. Cyber Warfare Secur.*, Coimbra, Portugal, 2019, p. 55.



HONGZHOU YUE received the B.S. degree in information management and information system from the Dongbei University of Finance and Economics, Dalian, China, in 2010, the M.S. degree in computer science and technology from Dalian Maritime University, Dalian, in 2013, and the Ph.D. degree in information security from Xidian University, Xi'an, China, in 2017. He is currently a Lecturer with the School of Computer and Information Technology, Xinyang Normal University, Xinyang, China. His research interests include the mobile app security, Android system security, and social network security.



SHUILONG HE received the B.S. degree in automation engineering from the Liaoning Institute of Technology, Jinzhou, China, in 2006. He is currently pursuing the M.S. degree in computer science and engineering with Xinyang Normal University, Xinyang, China. He was a member of the Henan Cryptography and Information Security Innovative Technology Team. His research interests include the Internet information security and cryptography application.



ZHENGHUI LIU (Member, IEEE) received the B.S. degree from Luoyang Normal University, Luoyang, in 2005, the M.S. degree from Xinyang Normal University, Xinyang, Henan, China, in 2010, and the Ph.D. degree in information security from Southwest Jiaotong University, Chengdu, in 2014. He held a postdoctoral position with the College of Information Engineering, Shenzhen University, Shenzhen, China. His current research interest includes multimedia forensics and security.

• • •