COMPUTERS & SECURITY XXX (2015) 1–9

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Design and analysis of enumeration attacks on finding friends with phone numbers: A case study with KakaoTalk

Eunhyun Kim [a], *Kyungwon Park* [a], *Hyoungshick Kim* [a,*], *Jaeseung Song* [b]

[a] *Department of Computer Science and Engineering, Sungkyunkwan University, Republic of Korea*
[b] *Department of Computer and Information Security, Sejong University, Republic of Korea*

ARTICLE INFO

Article history:
Received 13 December 2014
Received in revised form
21 March 2015
Accepted 18 April 2015
Available online xxx

Keywords:
Finding friends with phone numbers
Enumeration attack
Information leakage
Privacy
Instant messaging
KakaoTalk

ABSTRACT

Users' phone numbers are popularly used for finding friends in instant messaging (IM) services. In this paper, we present a new security concern about this search feature through a case study with KakaoTalk which is the most widely used IM in Korea. We demonstrate that there are multiple ways of collecting victims' personal information such as their (display) names, phone numbers and photos, which can be potentially misused for a variety of cyber–criminal activities. Our experimental results show that a user's personal data can be obtained automatically (0.26 s on average). The results also indicate that a large portion of KakaoTalk users (72.8%) have used real or real-like names in their profiles, which means that our discovered enumeration attacks seem to be practically dangerous. To mitigate these attacks, we present three countermeasures including a misuse detection system that can discover abnormal application activities within a certain time-window.

1. Introduction

Instant messaging (IM) has become a popular communication service for people who want to stay in touch with their family, friends and business colleagues since there is no cost (or low cost) to use IM services other than an Internet data plan that most users already have for their smartphones or PCs. However, IM services (e.g., WhatsApp, iMessage and Skype) have become the target of continuous cyber attacks such as spam, phishing and the misuse of personal data due to their growing popularity. For example, spammers might want to create rogue user accounts to effectively share their advertisements with IM users.

In this paper, we particularly focus on the discussion of security concerns raised by the friend search (or recommendation) feature with phone numbers, which are used in many IM services by default. This feature provides a sufficiently convenient way for managing IM friends but according to our research it can introduce new and significant privacy risks; an attacker might collect IM users' personal data such as their accounts, names, phone numbers and even photos. Those personal data can be potentially misused for various cyber criminal activities such as spam, phishing and rogue accounts — it can be beneficial for spammers to collect real phone numbers used by someone together with associated users' real name. We note that user

* *Corresponding author*. Tel.: +82 31 299 4324.
E-mail address: hyoung@skku.edu (H. Kim).
http://dx.doi.org/10.1016/j.cose.2015.04.008
0167-4048/

accounts can be collected with only the phone numbers associated them.

As a case study, we analyze the security of this feature in KakaoTalk (http://www.kakao.com/talk/en) which is the most widely used IM service in Korea. Once this friend search feature is enabled, the newly added phone numbers from the address book in a user's mobile phone are periodically uploaded to the KakaoTalk server in order to maintain the list of the user's friends up to date by automatically registering friends based on their KakaoTalk accounts associated to the added phone numbers. This automatic process is based on the intuition that address book contacts in a mobile phone might be the people that the phone owner wants to communicate with.

Schrittwieser et al. (2012) reported a similar security flaw named *enumeration* attack in several smartphone messaging applications (e.g., WhatsApp, Viber and Tango). In this paper, we extend their work by presenting new *enumeration* attacks targeted the KakaoTalk service which already have several countermeasures unlike the other applications such as WhatsApp.

In this paper, we show that users' names and phone numbers can be obtained by automatically generating a specific sequence of user activities and examining the heap memory that is used for the KakaoTalk process. We reported the discovered attacks to the KakaoTalk developers, so the related software vulnerabilities have been confirmed and patched. We also suggest three countermeasures to prevent such *enumeration* attacks including a misuse detection system. Our prototype implementation of the detection system shows the feasibility of a server-side defense solution — abnormal behaviors from attackers (i.e., malicious programs) can effectively be detected by monitoring the attacker's activities in KakaoTalk. Our key contributions can be summarized as follows:

- First, we introduce new *enumeration* attacks that targeted KakaoTalk and examine their feasibility and efficiency in practice. We collected more than 50,000 users' personal data and analyzed the data. The best attack method takes 0.26 s on average to obtain the information about a user's name and phone number.
- Second, we show the impacts of these attacks by analyzing the collected user profile information. Our experimental results show that 36,817 out of 50,567 samples (72.8%) have used real name or real-like name in their profiles.
- Third, we suggest three countermeasures to mitigate such *enumeration* attacks. Here, we particularly implement a misuse detection technique to detect such automatic attacks based on their signatures. Our defense model would incur a high cost to attackers while achieving a high accuracy at the same time.

The rest of this paper is organized as follows. In Section 2, we explain how the automated friend registration process in KakaoTalk works to provide a better understanding of *enumeration* attacks. Then we present the three *enumeration* attacks that targeted KakaoTalk to collect KakaoTalk user's personal data in Section 3. In Section 4, we introduce the implementations for *enumeration* attacks and evaluate their feasibility and efficiency by conducting experiments in the real-world environment. We present a discussion on countermeasures to mitigate *enumeration* attacks in Section 5. Next, we discuss ethical issues in Section 6. Related work is discussed in Section 7. Finally, we conclude in Section 8.

2. Automated friends registration in KakaoTalk

KakaoTalk is the most widely used free IM in Korea — it currently has over 145 million registered users worldwide, including 93% of smartphone users in South Korea (Khan, 2014). The KakaoTalk service was originally developed as a mobile application (similar to WhatsApp) for smartphones such as Android and iOS devices, but the PC and Mac versions of KakaoTalk applications were also recently released.

To encourage a user to find and add other users as his/her KakaoTalk friends, there are three ways: (1) searching for a user by KakaoTalk ID, (2) using a quick response (QR) code and (3) automatic syncing address book contacts with the corresponding KakaoTalk accounts. When a user wants to add a specific KakaoTalk user as a KakaoTalk friend, the user's KakaoTalk ID or the related QR code can be used. However, the most popular way is to use the automated friends registration option. In fact, this feature is turned on by default and can be disabled for only those who do not want to use this.

Once the automatic sync feature is enabled, the contacts in the phone owner's address book are added to the list of her KakaoTalk friends without manual intervention if the phone number of them are associated with KakaoTalk accounts. This process is shown in Fig. 1. The newly added phone numbers (step 1) from the address book are uploaded to the KakaoTalk server (step 2); the KakaoTalk server tries to find the KakaoTalk accounts with the phone numbers matched to the received phone numbers from the phone owner's KakaoTalk application and returns those to the KakaoTalk applications running on the requested user's devices such as smartphone (step 3) to update the list of her KakaoTalk friends with new friends (step 4). This automatic process is based on the intuition that address book contacts in a mobile phone might be the people that the phone owner wants to communicate with.

Interestingly, the KakaoTalk service does not provide the newly added friends' original display names, which are registered to the KakaoTalk server, via the automated friends registration process. Therefore, their names are displayed on the KakaoTalk application as the contact names in the address book rather than their original display names which are kept confidential. We surmise that this naming policy has been established to protect users' personal data from *enumeration* attacks which attempt to collect the KakaoTalk users' names and phone numbers with enumerated the (possibly) entire phone number range. Since the display names are not synced, the owner of a phone number cannot be identified even when there exits a KakaoTalk account associated with the phone number.

Therefore, in designing a new *enumeration* attack against KakaoTalk, the main hurdle we had to overcome was to obtain the information about KakaoTalk accounts' original display names without any knowledge about the account holders. We

Please cite this article in press as: Kim E, et al., Design and analysis of enumeration attacks on finding friends with phone numbers: A case study with KakaoTalk, Computers & Security (2015), http://dx.doi.org/10.1016/j.cose.2015.04.008