2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)

Emerging Threats Abusing Phone Numbers Exploiting Cross-Platform Features

Srishti Gupta
Supervised by Dr. Ponnurangam Kumaraguru
Indraprastha Institute of Information Technology (IIIT-Delhi), India
srishtig@iiitd.ac.in

***Abstract*—Phone number, a unique identifier has emerged as an important Personally Identifiable Information (PII) in the last few years. Other PII like e-mail and online identity have been exploited in the past to launch phishing and spam attacks against them. The reach and security of a phone number provide a genuine advantage over e-mail or online identity, making it the most vulnerable attack vector. In this work, we explore the emerging threats that abuse phone numbers by exploiting cross-platform features. Given that phone number space hasn't been extensively studied in the past, there is a dire need to understand the threat landscape and develop solutions to prevent its abuse.**

I. Motivation and Problem

Personally Identifiable Information (PII) is the information that can be used on its own or with other information to identify or locate a person. [1] Phone (mobile) number is a PII with which an individual can be associated uniquely, in most cases [7]. Phone numbers are like fingerprints, and are linked to a wealth of information about the owner like name, the place where he lives. They are a verified source of user identity; one needs to obtain a physical SIM card and complete the verification process by service provider to obtain a phone connection. As a result, attacks abusing phone numbers are likely to have higher success rate because (i) telephony systems have higher trust than traditional e-mails due to verification process with phone numbers; (ii) a greater percentage of people can be reached via phone than e-mail; and (iii) timing of message delivery can be leveraged to increase odds of success.

Abusing phone numbers for phishing, started on the voice or telephony channel, which is called as vishing (voice phishing). Spammers usually pretend to be a legitimate business, and lure the victims into thinking he will profit. Landline numbers have been abused in the past by carrying out vishing attacks on traditional telephony medium. Due to the advent of Voice over IP (VoIP) technology, phone numbers in addition to landline numbers are under vishers' attack. Phishing attacks have also exploited traditional text messaging services, i.e., SMS (SMiShing) to obtain sensitive, personal, or private information. Past literature has shown techniques to filter phishing attacks on voice [5] and SMS [3]. However, with the proliferation of new forms of messaging communication and other related smartphone applications, there are emerging threats related to phone numbers, which need to be studied.

In our work, we explore how phone numbers are abused with emerging new technologies, and how cross-application features can be exploited in carrying out these attacks.

A. Phone Number Abuse Exploiting Smartphone Applications

Due to the reach, security, and trust associated with phone numbers, several instant messaging applications are using only phone numbers for user authentication while registration. One of the prominent and new form of mobile communication, due to the convergence of telephony with the Internet, are Over-The-Top (OTT) messaging applications (like WhatsApp, Viber, and WeChat). Millions of people have started using them to interact with friends; the volume of messages have overtaken SMS. [2] Because of the growing popularity of OTT messaging applications, particularly WhatsApp, malicious actors are now abusing it for unsolicited activities like delivering spam and phishing messages. Messages like investment advertisements, adult conversation ads were seen to propagate on the channel in 2015. [3] To understand the phone numbers abuse exploiting cross-application features on OTT messaging applications, we test following hypotheses:

H1: *Large-scale targeted attacks are feasible on OTT messaging applications.*

We develop a novel, automated system to study the feasibility and scalability of launching targeted attacks on OTT messaging applications.

H2: *Cross-application features can be leveraged to gather more information about the victim.*

We assume that multiple applications will return comprehensive set of attributes for a victim, which will help in crafting more personalized and sophisticated attack. We used Truecaller and Facebook to test this hypothesis.

While researchers have looked into the privacy aspect of divulging personal information from OTT messaging applications [1], [6], feasibility of large scale threats that abuse phone numbers have not been studied.

B. Phone Number Abuse Exploiting Online Social Networks

The explosive growth of Online Social Networks (OSN) has been the perfect opportunity for criminals and sophisticated

[1] http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

[2] http://mobilemarketingmagazine.com/over-the-top-messaging-apps-overtake-sms-messaging/

[3] http://www.adaptivemobile.com/blog/headsup-for-whatsapp

IEEE/ACM ASONAM 2016, August 18-21, 2016, San Francisco, CA, USA
978-1-5090-2846-7/16/$31.00

hackers. The mass of detailed information stored on social networking sites make them a tempting target for phishing attacks, as they can be used for identity theft on a large scale. Literature has shown how spam and phishing attacks were carried out on OSNs, where spammers used URLs to monetize their actions. Victims were lured into giving money by crafting phishing and malware attacks against them [2], [4]. As an ongoing work, we found that spammers are also using phone numbers in large spam campaigns, where victims are lured into calling a phone number. In addition, the campaigns are not restricted to a particular social network, but are propagated to multiple OSNs. Since the identifier used to carry out the attack (phone number) is different from what has been previously studied (URLs), the purpose and monetization model behind these attacks needs to be looked into. Specifically, we plan to test following hypotheses:

H1: *How phone number spam campaigns are different from other spam campaigns studied in the past?*

As we observed, spam campaigns do not necessarily contain URLs. The monetization model needs to be studied.

H2: *Why spammers are moving to different social networks to spread the spam campaigns?*

One needs to study why spammers are moving to multiple networks to spread spam; getting better visibility or prevent themselves from getting down by one network, could be some potential reasons.

H3: *Can cross-platform intelligence be used in preventing onset of spam campaigns on other social networks?*

If a spam campaign start on a particular network before others, this intelligence can be leveraged in to prevent onset of spam on other networks.

II. Methodology and Results

A. Phone Number Abuse Exploiting Cross-Application Features

To understand the feasibility of targeted attacks abusing phone numbers, we created a system to automate the process of launching a variety of phishing attacks (see Figure 1). Specifically, the system has four main steps. a) Based on a numbering plan, phone numbers are randomly generated and inserted into an address book of a smartphone. This address book is on a device that is under the control of the attacker; b) the system fetches data from Truecaller and Facebook applications to determine any additional information about the owners of those phone numbers. The 'search' endpoint of Truecaller application provides details of an individual like name, address, phone number, country, Twitter ID, e-mail, Facebook ID, Twitter photo URL, and *photo URL*. We use Facebook to obtain friends' information which can make the attack more personalized and targeted; c) after the information is aggregated, the system determines the attack channel (OTT messaging applications, voice, e-mail, or SMS), and; d) crafts an attack vector and targets the victim with the best possible attack (based on the information collected).

We define *scalability* of our proposed attacks as the fraction of people who can be reached over an attack channel.

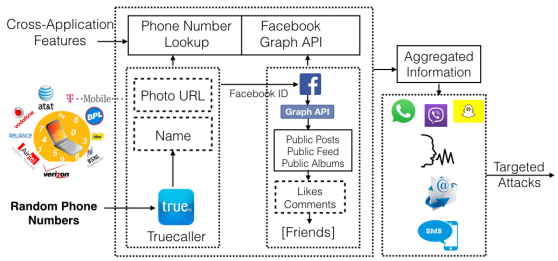

Fig. 1. System for Cross-Application Information Gathering and Attacks.

To demonstrate scalability, we enumerated through a list of 1,162,696 random Indian phone numbers. Detailed information for 722,696 (62%) users was collected using Truecaller; name was obtained for all the users. To check the presence of these numbers on an attack channel, they were synced with WhatsApp application (WA) using address book syncing feature. About 51,409 users were present on WA. Social phishing attacks can be launched against these users whereas spear phishing attacks can be launched against other 180,000 users whose social circle was not obtained.

B. Phone Number Abuse Exploiting Cross-Platform Online Social Networks

To understand the phone numbers abuse in OSNs, we developed a module which collects data from multiple OSNs, viz. Facebook, GooglePlus, YouTube, and Flickr. The input seed (phone number) to the system comes from Twitter; one of the collaborators has been collecting data about phone numbers from Twitter from May 2015. We started our data collection on April 25, 2016 and the system has collected more than 12 million posts across different networks for apprx. 200K unique phone numbers. We found that some of the popular scams, like tech support and fake follower scam are still active; we plan to dig deeper in current phase of the research work.

Acknowlegment

I am grateful to my advisor, Dr. Ponnurangam Kumaraguru for his continuous guidance. I would also like to thank my collaborators, Dr. Payas Gupta (NYU, Abu Dhabi) and Prof. Mustaque Ahamad (GaTech, Atlanta) for their inputs.

References

[1] Y. Cheng, L. Ying, S. Jiao, P. Su, and D. Feng, "Bind Your Phone Number with Caution: Automated User Profiling Through Address Book Matching on Smartphone," in *ACM SIGSAC*. ACM, 2013.

[2] Z. Chu, I. Widjaja, and H. Wang, "Detecting social spam campaigns on twitter," in *Applied Cryptography and Network Security*. Springer, 2012, pp. 455–472.

[3] B. Coskun and P. Giura, "Mitigating sms spam by online detection of repetitive near-duplicate messages." IEEE, 2012, pp. 999–1004.

[4] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao, "Detecting and characterizing social spam campaigns," in *Proceedings of the 10th ACM SIGCOMM conference on Internet measurement*. ACM, 2010, pp. 35–47.

[5] P. Gupta, B. Srinivasan, V. Balasubramaniyan, and M. Ahamad, "Phoneypot: Data-driven Understanding of Telephony Threats," in *NDSS*, 2015.

[6] S. Schrittwieser, P. Frühwirt, P. Kieseberg, M. Leithner, M. Mulazzani, M. Huber, and E. R. Weippl, "Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Applications," in *NDSS*, 2012.
[7] E. Zheleva and L. Getoor, "Privacy in social networks: A survey," in *Social network data analytics*. Springer, 2011, pp. 277–306.