A mobile phone identification method using packet arrival time in web access for user authentication

Mio Sagara, Kensuke Kodama, and Masami Kihara

Department of Computer Engineering, College of Science and Technology, Nihon University, 7–24–1 Narashinodai, Funabashi 274–8501, Japan

a) kihara.masami@nihon-u.ac.jp

Abstract: A new method of identifying a user’s mobile phone for user authentication is proposed. When the authentication server receives packets from the mobile phone, it is identified by the packet arrival time. The authentication in the server is based on the change in packet arrival time when the mobile phone receives a call to the user’s telephone number registered with the server. This paper describes how the transmission delay characteristics yield the identification data; the viability of the proposed method is verified for a wide variety of mobile phone wireless environments in which mobile phones are used.

Keywords: authentication, packet arrival time, mobile phone, telephone number

Classification: Internet

References

[1] IT Security Center (ISEC), “10 Major Security Threats 2015~ What should you do to avoid damage from cyber attacks?~,” Information-technology Promotion Agency, Japan, Mar. 2015.
[2] https://www.google.com/landing/2step/features.html.
[3] https://support.microsoft.com/en-us/help/12408/microsoft-account-about-two-step-verification.
[4] 3rd Generation Partnership Project “Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function,” Technical Specification, Reference: 33.220 (Release10), Mar. 2011.
[5] M. Sagara, K. Kodama, and M. Kihara, “A cellphone identification system using packet arrival time in web access,” Proc. of the 2016 IEICE Society Conference, B-6-83, Sep. 2016.

1 Introduction

A lot of unauthorized password use and malicious attacks on authentication systems are being reported [1]. Major network services such as Google [2] and Microsoft [3] currently adopt some kind of two-step verification to protect their
users’ data against illegal access. Two-step verification generally uses two different passwords. The first one, most often a secret string, relies on the user’s memory. The second password, provided by the user’s authentication server, is generally sent to the user’s mobile phone via e-mail or SMS (Short Message Service). The user manually inputs the second password to the user authentication server, and is then authorized by the two correct passwords.

The reliability of existing two-step verification depends on the security with which the second password is returned to the authentication server via the user’s computer. The second password is, however, vulnerable to virus contamination as the MITB (Man-in-the-Browser) [1] attack is capable of intercepting and tampering with data passed between the browser transaction and the secure transmission protocol such as TLS (Transport Layer Security). Two-step verification is thus ineffective as the two passwords pass through the same infected browser in the same computer and thus are exposed to the same risk.

Another authentication method, Generic Bootstrapping Architecture (GBA), has been standardized by 3GPP (3rd Generation Partnership Project) [4]. While GBA authentication accuracy is very high as it is based on an intrinsic function of the mobile phone, connection to a mobile phone carrier is necessary. Our proposed method, however, allows network service providers to independently achieve the authentication function by themselves without considering the carriers authorized by the Subscriber Identity Module (SIM) cards in the user’s mobile phones.

The proposed user authentication method uses the packet arrival time characteristics, gathered by the authentication server from communication with the mobile phone identified with the user [5]. The key components in our method are the user’s telephone number registered in the authentication server and spike characteristics of packet arrival time induced by calling the user’s telephone number. In this paper, we describe our authentication mechanism, the packet arrival time characteristics as measured by the authentication server, and the impact of mobile transmission environment on identification feasibility.

2 Proposed system configuration

The proposed authentication system consists of the user’s computer, assumed to be accessing a network service, the user’s identified mobile phone, and an authentication server functioning with the network service as shown in Fig. 1(a). The user’s computer is connected to the authentication server via wired and/or wireless networks. The user mobile phone is connected via a mobile phone wireless network. The mobile phone wireless connection, which excludes wireless LAN network access, is an indispensable precondition for the realization of our proposed method.

Service requests and authentication are executed by two processes using the same password shown in Fig. 1(b). The first process, a general service request, uses the user’s account and password. The second process implements user mobile phone identification and request confirmation. While the proposed system is classified as two-step authentication, there is neither a second password nor secret data transferred from the user mobile phone to the user’s computer. There is no link between the user’s computer and the user’s mobile phone.
2.1 Service provision step
The user first logs in from the computer and requests a network service from the server (Step 1 in Fig. 1(b)). The user then logs in from the user mobile phone using the same password (Step 2). It is required that the user mobile phone is connected via a mobile phone wireless network to the authentication server. After these logins are completed, the authentication server starts the user mobile phone identification step, which confirms whether the mobile phone accessing the authentication server is the registered mobile phone of the user or not (Step 3 is described in 2.2).

User’s eligibility is certified when the user’s mobile phone is identified as being the registered one. The general two-step verification process terminates at this stage and the user request is executed. The proposed method, however, adds Step 4, which reconfirms that the request received by the server is actually what the user wanted. Since the MITB attack is emphasized in this paper, it is important to consider that the data transferred from the user’s computer to the authentication server may have been corrupted. For a content download service, examples include purchase of over-priced content and indicating a different destination for purchased content.

If the user confirms that the request received by the authentication server is what was intended, the approved content is downloaded to the user’s computer (Step 5).

Since the second password is not returned to the authentication server via the user’s computer in the second process, authentication is not compromised by virus
contamination of the user’s computer. The isolation of the second process is one of the most important characteristics in realizing authentication security.

2.2 User mobile phone identification (Step 3 in Fig. 1(b))

After the user logs in from the user mobile phone using a browser via a mobile phone wireless network (Step 2 in Fig. 1(b)), the browser receives an html (Hyper Text Markup Language) file used in the identification step. The html file includes 300 to 800 small images. The browser tries to retrieve these images by sending GET method in HTTP (HyperText Transfer Protocol) to the authentication server. The authentication server receives these request packets, and stores their timestamps indicating the arrival time of the packets, \(TS(t_n)\) where \(n\) is the \(n\)th packet. The identification step calculates the arrival time difference between the timestamps,

\[
\Delta TS(t_n) = TS(t_n) - TS(t_{n-1}),
\]

and the maximum arrival time difference, \(\Delta TS(t_n)_{\text{max}}\).

In the final identification process, the authentication server calls the registered user telephone number as per the account used for user login. This call causes a spike in the arrival time difference that is if the order of several seconds (actual arrival time difference data are shown in 3.1). The detection of the spike gives an accurate estimation of whether the mobile phone currently logged into the authentication server has the registered telephone number. This estimation functions even when the user ID and password are stolen. The user is finally certified as legitimate assuming that the identified mobile phone is not stolen or abused.

3 Experiments and results

3.1 Packet arrival time difference characteristics

Fig. 2(a) shows typical values of arrival time difference, \(\Delta TS(t_n)\), measured in the authentication server when the browser in the user mobile phone accesses the html file in the authentication server. The typical arrival time difference (without a call) lies in the range from several milliseconds to several hundreds of milliseconds. The maximum arrival time difference in Fig. 2(a), \(\Delta TS(t_n)_{\text{max}}\), is 22 [ms] \((n = 1140)\).

In the next process, the authentication server calls the user’s mobile phone while the browser in the mobile phone is accessing the authentication server. This call induces a spike in arrival time difference (with a call) of the order of several seconds, \(\Delta TS(t_n)\). The spike of 6.5 s \((n = 171)\) is measured as shown in Fig. 2(b). It must be possible to differentiate the spike from the maximum arrival time difference without a call, and that the spike is detected within calling delay when the authentication server calls the user.

4G LTE (Long Term Evolution) mobile phones are used in this experiment. The spike in the 4G LTE receiving process of the phone call is caused by CSFB (Circuit Switched FallBack) which switches to the 3G voice function upon receipt of a phone call. The switching drastically increases the arrival time difference, \(\Delta TS(t_n)\).

Since this phenomenon occurs only in the user’s registered mobile phone, this process can function even if the registered password is illegally used provided the registered mobile phone is not accessed illegally. This identification mechanism,
however, requires randomization of the time at which the registered user is called, since an illegal user can transmit packets intentionally delayed from the usual timing.

3.2 Influence of mobile system conditions

We evaluate the proposed method’s characteristics in this section, focusing on explicitly differentiating the maximum arrival time difference without a call and the magnitude of a spike with a call. In particular, the influence of mobile phone wireless network conditions on arrival time difference is measured. Three locations are assessed; suburban area in the day time, urban area around a train station, and within a station during the evening commute which is estimated to represent the peak traffic time for mobile phone wireless networks.

Fig. 3 shows the maximum arrival time difference without a call and the magnitude of spikes with a call. The horizontal axis in Fig. 3 is average time to send an image from the authentication server to a user based on the total sending time of the html file and image size. The average time is, as expected, affected by mobile phone wireless network conditions.

![Maximum arrival time difference and magnitude of a spike](image)

**Fig. 2. Arrival time difference**

**Fig. 3. Characteristics of the maximum arrival time difference and the magnitude of a spike**
It is observed that the maximum arrival time difference without a call is within 1 s and the magnitude of spikes with a call lies in the range of 5 s to 9 s. Since the relative time difference between them is always over 4 s, the spike upon the receipt of the call from the authentication server is clearly detected.

In addition, 5 image sizes, 1 kB to 100 kB, in the html file, are used in these experiments. While the total time to send the html file varies, there is no change in the distributions for both the maximum arrival time difference without a call and the magnitude of spikes with a call.

4 Conclusion

We proposed an authentication method based on identifying the user’s mobile phone through packet arrival time differences, and clarified the method’s feasibility in various mobile phone wireless network environments.

Since more mobile phones are being used to place packet-based voice calls in 4G LTE, and access high transmission speed services in 5G, a mobile application for detecting a packet-based voice call instead of CSFB is needed.

While service provision based on content download is described in this paper, the proposed system can be applied to Internet banking services that process only requests, such as fund transfers, without content downloads. Internet banking is one of the most promising applications.