Beyond Mobile Devices: A Cross-Device Solution for Smishing Detection and Prevention

Akira Kanaoka
KDDI Research Inc. / Toho University

Takamasa Isohara
KDDI Research Inc.

Abstract

Smishing, a phishing attack through SMS, has become a significant security concern. Attackers send fraudulent messages, including malicious URLs leading to personal information theft or malware infection. Current security mechanisms on mobile devices, such as anti-virus apps, are limited in detecting and preventing smishing attacks. This poster proposes a novel approach for detecting malicious URLs using images captured by a separate device. The proposed method enables cross-device smishing detection for various types of URLs, including those displayed on smartphones, laptop displays, televisions, or walls. We also implement a prototype system using AR glasses and conduct a user study to evaluate the effectiveness of our approach. Our experimental results demonstrate the potential of image analysis for smishing detection and prevention and the added benefit of AR glasses for a more immersive and efficient user experience.

1 Introduction

Smishing, a phishing attack in which an SMS message is sent to an actual organization and leads to a URL, has become a severe problem in recent years.

Several approaches have been considered for smishing countermeasures [1–3], but most are based on absolute access control within the terminal or operating system. While these approaches are effective, they are challenging to implement because they require support for applications and operating systems, and they are not a means by which users can protect themselves.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.
August 6–8, 2023, Anaheim, CA, USA

This study approaches the issue from a different perspective. This study approaches the issue from a different perspective. Instead of responding to the device that received the smishing message, another device inspects the message displayed to evaluate its malignancy. Another device can inspect the URLs to check whether they are listed in the database of malicious URLs or actually access the URLs in the sandbox and dynamically analyze their risk. These checks and analyses can be performed without risk to the user's device.

At first glance, this approach may seem impractical or inefficient, requiring devices other than smartphones. However, this concern may be dispelled in a few years. Currently, many glass-type AR devices (AR glass) are being developed. They are beginning to be used in various fields for entertainment, and enterprise applications in training, education, and work support. If AR glasses become commonplace, security solutions across multiple devices will become natural, and the mechanism proposed in this study will be welcomed with realism.

This poster presents an overview of the proposed system and outlines the prototype implementation and user experiments using it and the results.

2 Cross-Device Smishing Detection

2.1 System Structure

An overview of the proposed system is shown in Fig.1. The proposed system will have an independent device to evaluate the malignancy of the smishing message. The device has a camera and an interface to display the results. The camera first takes a picture of the device's screen to be evaluated for maliciousness, detects whether or not a URL is included in the image, and then evaluates the maliciousness of the URL. After the evaluation, the results are displayed on the screen.

In the case of AR glasses, the camera mounted on the AR glasses acquires the scenery that the user is looking at, the image is captured, and the URL is evaluated. If the URL is considered high-risk, an indication of the risk to the user is

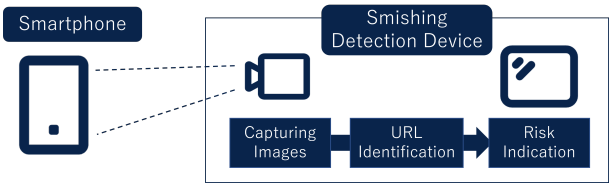

Figure 1: Overview of Cross-Device Smishing Detection

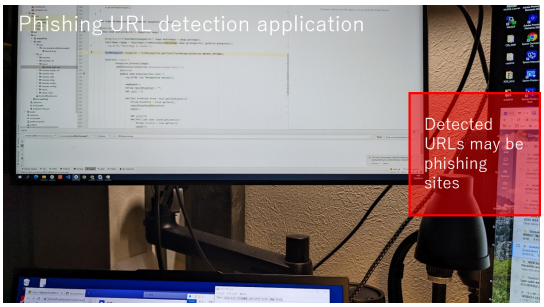

Figure 2: Example of maliciousness evaluation results displayed on AR glasses

displayed on the AR glasses, and the user is encouraged not to access high-risk URLs.

String extraction from images and URL detection are areas that have already been well-researched and can be extracted with high accuracy. The accuracy of URL maliciousness evaluation can be expected because the evaluation API is publicly available, and academic research has already been conducted. The risk display method in the AR glasses display has not yet been fully discussed, and the discussion on the risk display in the AR glasses display, or more broadly, "usable security for alert UI in HMDs," has not yet started. Alerts must be discussed from a different perspective for HMDs, which offer a much more immersive experience than PC displays or smartphones.

2.2 Prototype System and User Study

We implemented a prototype using AR glass EPSON Moverio BT-30ES (Fig.3). The application was implemented as an Android application, the string extraction was performed using Google's ML Kit API, and the URL evaluation was self-made. The risk evaluation was a simple list match, and the list of malicious URLs was locally stored in the AR Glass device.

A user study was conducted using the prototype. In the study, we conducted a task in which users were asked to evaluate whether each message was real or smudged in a situation where they received 36 messages and did not know whether the message was real or smudged. The first 18 messages were evaluated without AR glasses, and the second 18 were evaluated with AR glasses using that information as material

Figure 3: Prototype system using AR glasses

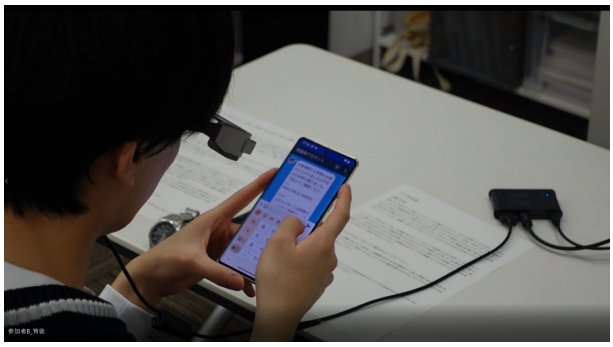

Figure 4: User study with prototype implementations

(Fig.4). There were nine participants in the user study. After the task was conducted, a survey of the SUS of the prototype and a semi-structured interview were conducted. The results showed that using AR glasses facilitated appropriate evaluation, with the percentage of correct decisions being 85.19% when using the prototype compared to 46.3% when not using the prototype. These results support the findings of existing studies [4, 5]. The SUS score was 74.4, indicating high usability. In the NVivo coding analysis of the semi-structured interview results, the codes "myself" and "decision" were extracted, indicating users' difficulty making decisions by themselves, the significance of the support by the prototype, and the difficulty of smishing evaluation. On the other hand, some users did not trust SMS messages from the beginning. There were also opinions that wearing AR glasses is fine until they get used to the decision-making process, but once they get used to it, it may become a hindrance.

The results also indicate that users tend to trust the prototype app more than other devices due to the immersive nature of AR glasses and that there are other problems with using HMDs, such as inaccuracies caused by the camera position of AR glasses.

The results of this study are very encouraging, as they are the gateway to the advancement of this research.

References

[1] Mishra, Sandhya, and Devpriya Soni. "Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysis." Future Generation Computer Systems 108 (2020): 803-815.

[2] Joo, J.W., Moon, S.Y., Singh, S. et al. "S-Detector: an enhanced security model for detecting Smishing attack for mobile computing." Telecommun Syst 66, 29–38 (2017). https://doi.org/10.1007/s11235-016-0269-9

[3] Ankit Kumar Jain, B.B. Gupta, "Rule-Based Framework for Detection of Smishing Messages in Mobile Environment." Procedia Computer Science, Volume 125, 2018, Pages 617-623, ISSN 1877-0509, https://doi.org/10.1016/j.procs.2017.12.079.

[4] Yeboah-Boateng, Ezer Osei, and Priscilla Mateko Amanor. "Phishing, SMiShing & Vishing: an assessment of threats against mobile devices." Journal of Emerging Trends in Computing and Information Sciences 5.4 (2014): 297-307.

[5] Sara Albakry, Kami Vaniea, and Maria K. Wolters. 2020. What is this URL's Destination? Empirical Evaluation of Users' URL Reading. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20). Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376168