Detecting Mobile Application-Based Smishing Attacks: Design and Implementation of The System

Moon-Ki Cho[1], Yang-Ha Chun[2]

[1]Professor, Computer Science, Soongsil University, 369 Sangdo-ro, Dongjak-gu, Seoul, Korea
[2]Professor, Department of AI, Yongin University, Cheoin-gu, Yongin-si, Gyeonggi-do, Korea

With the rapid development of smartphones in recent years, they have been utilized not only for basic phone functions, but also for web surfing, gaming, financial transactions, and more. As a result, smishing, a form of crime that allows access to unverified text messages in the form of a link to an Internet address, has emerged and is causing a lot of damage.
In this paper, we propose a system that can detect smishing attacks to prevent financial damage caused by smishing attacks. The system proposed in this paper collects and analyzes user messages based on mobile applications to block smishing attacks. Therefore, it is expected that the proposed system can block most of the smishing attacks.

Keywords: smishing, phishing, mobile application, personal information, detection systems.

1. Introduction

The global market for smartphones is expected to reach $514.6 billion in 2022 and $780.1 billion in 2030. The forecast period 2023-2030 is expected to represent a CAGR of 7.2%.

According to government data, the global smartphone market has experienced significant growth over the past decade and is expected to gain favorable market opportunities. Currently, the number of global smartphone users has exceeded 5.5 billion, and the penetration rate has exceeded 70%. The significant adoption of smartphones and the expanding market size are driven by a variety of factors, including falling prices, strengthening network infrastructure, and increasing access to digital services.

With a large number of smartphone users worldwide, the industry is expected to continue to expand and develop, especially with the Android OS holding a dominant market share of around 53%. By region, Asia-Pacific leads the way with more than 25% share [1]. With the proliferation of smartphones, we are increasingly exposed to a variety of crimes through mobile applications, and smishing is one of them.

In this paper, we propose a system that can detect smishing attacks to reduce the damage caused by smishing attacks. In this study, we focus on the design of a smishing attack detection system, and later refine the system and validate it by implementing it in practice. and then elaborate and implement the system to validate its effectiveness. validate its effectiveness.

2. MATERIALS AND METHODS

2.1. Smishing

Smishing is a social engineering attack that uses fake mobile text messages to trick people into downloading malware, sharing sensitive information, or sending money to cybercriminals. The term "smishing" is a portmanteau of "SMS" or "short message service," the technology behind text messaging, and "phishing."

Smishing is an increasingly popular form of cybercrime. According to Proofpoint's 2023 State of Phishing report, 76% of organizations experienced a smishing attack in 2022.

There are a number of factors contributing to the rise of smishing. For starters, the hackers who carry out these attacks, also known as "smishers," know that victims are more likely to click on text messages than other links. At the same time, advances in spam filters have made it harder for other forms of phishing, such as email and phone calls, to reach their targets.

With the rise of bring-your-own-device (BYOD) and remote work, more people are using mobile devices at work, making it easier for cybercriminals to access company networks through employees' phones.

2.2. How smishing attacks work

A smishing attack is similar to other types of phishing attacks, where scammers use fake messages and malicious links to trick people into compromising their phones, bank accounts, or personal data. The only major difference is the medium. In a smishing attack, scammers use SMS or messaging apps to carry out their cybercrime instead of email or phone calls.

Scammers choose smishing over other types of phishing attacks for a number of reasons. Perhaps most importantly, research shows that people are more likely to click on links in text messages. According to Klaviyo, SMS click-through rates range between 8.9% and 14.5% (ibm.com external link). In comparison, emails have an average click-through rate of only 1. 33% (ibm.com external link).

In addition, scammers are increasingly concealing the source of their smishing messages, using tactics such as spoofing phone numbers with burner phones or using software to send texts via email. It's also harder to spot dangerous links on a mobile phone. For example, on a computer, users can hover over a link to see where it leads, but on a smartphone, there's no such option. People are also used to banks and brands contacting them via SMS and receiving shortened URLs in text messages.

In 2020, the Federal Communications Commission (FCC) ordered telecommunications companies to adopt the STIR/SHAKEN protocol, which authenticates phone calls and is why some phones now display a "possible fraud" or "possible spam" message when they receive a call from a suspicious number. But while STIR/SHAKEN made it easier to spot fraudulent

calls, it didn't have the same effect on text messages, which led many scammers to focus on smishing attacks.

2.3. Examples of smishing scams

Like other forms of social engineering, most smishing attacks use fake stories as a pretext to manipulate the victim's emotions and trick them into doing the scammer's bidding.

2.3.1. Impersonating a financial institution

Scammers can pose as a victim's bank and alert them to a problem with their account, often through a fake notification. When the victim clicks on the link, they are taken to a fake website or app that steals sensitive financial information such as PINs, login credentials, passwords, bank account or credit card information. In 2018, a group of fraudsters stole US$100,000 from a Fifth Third Bank customer in this way.

2.3.2. Impersonating the government

Scammers may pretend to be police officers, IRS representatives, or other government officials. These smishing texts often claim that the victim owes a fine or needs to take some action to receive a government grant. For example, during the height of the COVID-19 pandemic, the Federal Trade Commission (FTC) warned about smishing attacks offering tax relief, free COVID-19 testing, and similar services. When victims followed the links in this text, scammers stole social security numbers and other information that could be used for identity theft.

2.3.3. Impersonating customer support and shipping carriers

The attackers pose as customer support agents from trusted brands and retailers, such as Amazon, Microsoft, or the victim's wireless provider. They usually say there's a problem with the victim's account or an unclaimed reward or refund. Typically, these texts send the victim to a fake website that steals their credit card number or banking information.

Shipping impersonation smishing messages claim to be from a shipping company, such as FedEx, UPS, or the U.S. Postal Service. They tell the victim that there was a problem delivering the package and ask them to pay a "shipping fee" or log into their account to fix the problem. Of course, the scammer runs off with the money or account information. These scams are common around the holidays, when many people are waiting for packages.

2.3.4. Act like you're texting the wrong number

The scammer sends a text that appears to be intended for someone other than the victim. When the victim corrects the scammer's "mistake," the scammer starts talking to the victim. These wrong number scams tend to be long-term, where the scammer tries to win the victim's friendship and trust through repeated contact over months or years. The scammer may even pretend to develop romantic feelings for the victim. The goal is to eventually steal the victim's money through fake investment opportunities, loan requests, or similar stories.

Also called a multi-factor authentication scam (MFA), a hacker who already knows the victim's username and password attempts to steal the verification code or one-time password needed to access the victim's account by pretending the account is locked. The hacker may pose as one of the victim's friends and claim that their Instagram or Facebook account is locked

and ask the victim to get the code. The victim actually receives the MFA code for their account and gives it to the hacker.

Not only that, but by acting like they're offering free apps, some smishing scams trick victims into downloading apps that look legitimate, such as file managers, digital payment apps, and even antivirus apps, but are actually malware or ransomware.

2.4. Related research

Many studies and smartphone applications exist to prevent smishing attacks and reduce the damage caused by such attacks. Phishing, Vishing, and Smishing studied institutional measures to respond to new crimes related to smartphones, including smishing, and Types of New Smartphone Crimes and Police Response Measures. In addition, there are existing applications that block smishing texts, but most of them use the method of detecting smishing texts through monitoring on the smartphone itself [3-18].

The smishing attack detection system proposed in this paper is modeled by complementing existing works. In the case of the proposal proposed in the study on the types of new smartphone crimes and police response measures, each site is authenticated through an authorized organization, and users have to go through a cumbersome process of checking the authentication through the organization every time they access the site. Instead of this cumbersome process, the system proposed in this paper simplifies it by accumulating a list of sites that distribute malware and simply comparing them. In addition, the use of smartphone resources is minimized by having the user's smartphone simply send and receive messages, and the detection of smishing attacks is designed to be centralized by having a separate server in charge of detection. This has the advantage of blocking the impact of malware on the user's smartphone and enabling quick response to new and evolving attack techniques.

3. SMISHING ATTACK DETECTION SYSTEM

3.1. How the smishing attack detection system works

The smishing attack detection system proposed in this work proposed in this study consists of a server-client structure as shown in Figure 1. When a user receives a suspected smishing text, the user requests the server to determine whether the URL in the text is a legitimate URL using a smartphone corresponding to the client.

The server performs primary detection by comparing the URL requested for verification with the list of smishing URLs in the DB. If the URL is in the smishing URL list, the server immediately sends the result to the user, otherwise, it performs a secondary detection. Secondary detection is when the server tries to access the URL directly the URL directly from the server and checks if the malware is being distributed. malware is being distributed. After secondary detection, the result is sent to the user and if the URL is found to be a malicious URL the DB is updated with a list of smishing URLs to prepare for future requests. to prepare for future requests.

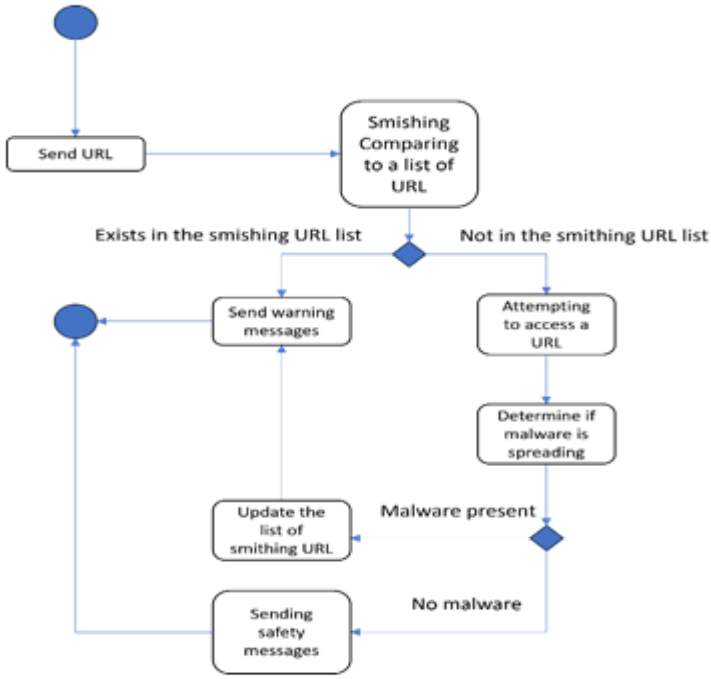

Figure 1. Smishing Attack Detection System Activity Diagram

3.2. Configure a smishing attack detection system

The smishing attack detection system consists of a client, a server, a DB, and a smishing attack server, all connected to each other via the Internet, as shown in Figure 2. The client is the user's smartphone, which needs to install a message sending application to send the URL to the server when a suspected smishing text message is received. The server is responsible for detecting smishing attacks and is connected to a database where a list of smishing URLs is stored. The server is responsible for detecting smishing attacks and is connected to a database where a list of smishing URLs is stored.

The server can be virtualized and configured to detect smishing attacks on various platforms at a low cost. Servers are exposed to the risk of malware infection because they have direct access to the smishing attack server to detect smishing attacks. Servers in virtualized environments can handle this risk. servers in a virtualized environment can cope with this risk. By virtualizing your server When you virtualize your server, creating and deleting new VMs is easy and simple. Because of these benefits, virtualized servers In a virtualized server, if a malware infection causes the server to malfunction malware infection, you can delete and recreate VMs, giving you the flexibility to respond by deleting and recreating VMs.

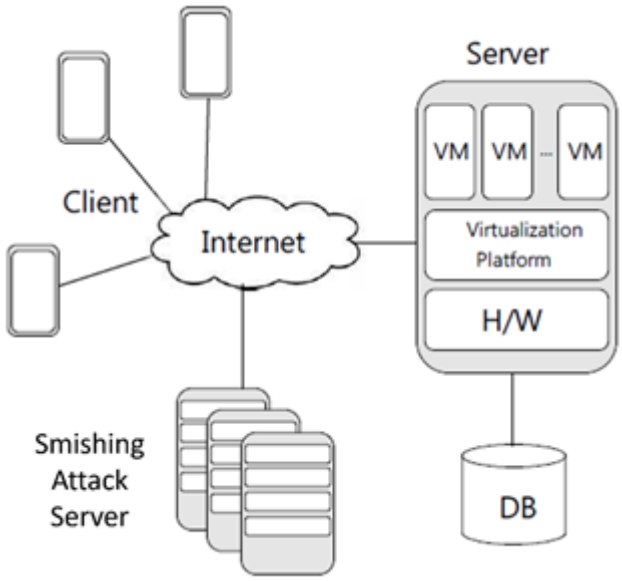

Figure 2. Configure a smishing detection system

3.3. Smishing attack server detection algorithm

When a user makes a smishing detection request to the server, the server first compares the URL with the smishing URL list in the DB. If the URL does not exist in the smishing URL list, the server tries to access the URL directly. To determine whether the URL distributes malware, we focus on files with the .apk extension, which are application installation files for Android smartphones.

First, check if the apk file crashes when accessing the URL using a web browser on a regular PC. If it does, it is considered a server that distributes malware and the detection process stops. If it does not, try accessing the URL again using an Android virtual machine instead of a PC. If the APK file is still not downloaded when accessed from the Android virtual machine, consider it a safe site and send a message to the client. This sequence is shown in Figure 3 as a pseudocode.

The reason why the PC environment first accesses the URL and checks whether the file with the .apk extension is downloaded or not is due to the difference in performance speed. The Android virtual machine is very slow compared to the actual smartphone, and since this system is a real-time processing method rather than a batch processing method, the response time is one of the important factors to measure the performance of the system. Therefore, we configured the algorithm to access the URL from the PC first to minimize the processing time and reduce the response time.

Even though it is slow, we secondarily check whether the APK file is loaded on the Android virtual machine because it is more accurate to detect smishing attacks by conducting experiments in an environment similar to a real smartphone.

```
boolean detectingSmishing(URL){
  boolean isValide = true;
  //PC에서 URL 접근
  if(findApkFileOnPC(URL)){
    isValide = false;
    return isValide;
  }else{
    //안드로이드 VM에서 URL 접근
    if(findApkFileOnAVD(URL){
      isValide = false;
      return isValide;
    }else{
      return isValide;
    }
  }
  return isValide;
}
```

Figure 3. Smishing attack server detection algorithm

4. CONCLUSION

In this study, we proposed a smishing detection system by devising an algorithm to detect smishing attacks to reduce the damage caused by smishing, a new criminal behavior related to smartphones.

This study focused on the design of a smishing attack detection system, and this system focuses on the presence of apk files by collecting URL information in messages, and based on this, smishing attacks are detected. In future research, we will further elaborate the algorithm to detect smishing attack servers and consider how to improve the accuracy of detection by applying AI, and we will verify the validity of the system proposed in this study by implementing the actual system.

References

1. Global Smartphone Market - 2023-2030, DataM Intelligence (2023) https://www.giikorea.co.kr/report/dmin1285072-global-smartphone-market.html
2. What is smishing (SMS phishing)?,IBM ,"Smishing (SMS phishing)", (2021) https://www.ibm.com/kr-ko/topics/mishing
3. What is Smishing and How to Defend Against it, Kaspersky (2021), https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it
4. Shweta, Kelly Main, What Is Smishing? Definition, Examples & Protection,forbes (2023) https://www.forbes.com/advisor/business/what-is-smishing/

5. Choi, Byung-Hwan, "Defense Techniques of Smishing Attacks Using Electronic signature on Network Environment", Korea Information Processing Society (2014), Pages.399-402 https://doi.org/10.3745/PKIPS.y2014m11a.399
6. Baek, Seong-Bin, Automatic knowledgebase extraction based smishing SMS detection, Annual Conference on Human and Language Technology, 2021. 10a, p564-567 (2021) Automatic knowledgebase extraction based smishing SMS detection -Annual Conference on Human and Language Technology | Korea Science
7. K. Kolluru, V. Adlakha, S. Aggarwal, Mausam, and S. Chakrabarti, "OpenIE6: Iterative Grid Labeling and Coordination Analysis for Open Information Extraction," Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing (EMNLP), pp. 3748–3761, Nov. 2020. Available: https://aclanthology.org/2020.emnlp-main.306
8. S. Aggarwal, and M. Mausam, "CaRB: A crowdsourced benchmark for open IE," Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing and the 9th International Joint Conference on Natural Language Processing (EMNLP-IJCNLP), pp. 6262–6267, Nov. 2019. Available: https://aclanthology.org/D19-1651
9. T. A. Almeida, J. M. G. Hidalgo, and A. Yamakami, "Contributions to the study of sms spam filtering: new collection and results," DocEng '11, 2011.
10. Hyo-Min Park, Cloud Messaging Service for Preventing Smishing Attack, The Society of Digital Policy and Management, (2017), p.285-293 https://doi.org/10.14400/JDC.2017.15.4.285
11. Smishing(2008), http://www.police.go.kr/portal/main/ contents.do?menuNo=200287 (accessed Jun., 24, 2016)
12. Desktop as a Service(2016), https://en.wikipedia.org/ wiki/Desktop_virtualization
13. Hongbo Zhou, Lionel Ni and Matt Mutka, "Prophet Address Allocation for Large Scale MANETs," In Proceedings of the IEEE conference on Computer Communications(INFOCOM), San Francisco, 2003. https://www.sciencedirect.com/science/article/pii/S1570870503000428
14. Casbeer, David W., et al. "Forest fire monitoring with multiple small UAVs."American Control Conference, 2005. Proceedings of the 2005. IEEE, 2005. https://ieeexplore.ieee.org/abstract/document/1470520
15. Kim, Jang Il , A Study on Damage and Countermeasures of SMS Phishing, Journal of Service Research and Studies, Volume 5 Issue 1, p71-78,(2015) https://doi.org/10.18807/jsrs.2015.5.1.071
16. Maltare, N. N., Sharma, D., Patel, S. (2023). An Exploration and Prediction of Rainfall and Groundwater Level for the District of Banaskantha, Gujrat, India. International Journal of Environmental Sciences, 9 (1), 1-17 https://www.theaspd.com/resources/v9-1-1-Nilesh%20N.%20Maltare.pdf
17. Min, P.K., Mito, K. and Kim, T.H. (2024). The Evolving Landscape of Artificial Intelligence Applications in Animal Health. Indian Journal of Animal Research. https://doi.org/10.18805/IJAR.BF-1742
18. Kim, T. H. and AlZubi, A.A. (2024). AI Enhanced Precision Irrigation in Legume Farming: Optimizing Water Use Efficiency. Legume Research. https://doi.org/10.18805/LRF-791