Analysis of the KAIST Dooray Mailing System: Enhancing Security Against Phishing and Identity Attacks

Ilman Mohammad Al Momin - 20246512
Youri Merzouk - 20246513
IS543 - Web Service Security and Privacy

Abstract

Email systems are the backbone of modern communication. Widely used in organizations for exchanging sensitive information, they have become prime targets for cyberattacks, with over 90% of breaches originating from phishing emails [1]. Securing these systems is more critical than ever. This project analyzes the Dooray mailing system at KAIST to understand its defenses against phishing and identity spoofing. Our primary goal is to comprehend how the Dooray system operates to secure sensitive communications.

1 Introduction

The Dooray mailing system, widely used at KAIST for academic and administrative communications, plays a crucial role in managing sensitive information. However, it is vulnerable to threats such as phishing attacks and identity spoofing. This project aims to analyze the Dooray mailing system to understand its defenses against these threats, focusing on exploring its security mechanisms, including user authentication, encryption, and protocols like SMTP, DKIM, and DMARC.

2 Background

2.1 Mailing Systems and Security Threats

Mailing systems like Dooray handle large volumes of sensitive communications, making them frequent targets for phishing, spoofing, and other identity-based attacks. Phishing attacks aim to steal sensitive information through deceptive emails, while identity spoofing can lead to impersonation of legitimate users, facilitating more advanced attacks. These threats can undermine the trustworthiness of email communications and put both users and institutions at risk.

2.2 Security Protocols and Tools

Dooray relies on standard mailing protocols such as Simple Mail Transfer Protocol (SMTP), Domain Keys Identified Mail (DKIM) [2], and Domain-based Message Authentication, Reporting & Conformance (DMARC) to verify sender identity and ensure email integrity. However, attackers often exploit vulnerabilities in these systems, necessitating a deeper analysis of how effectively Dooray implements these protocols to prevent attacks.

3 Proposal

This project aims to investigate the Dooray mailing system's security measures, focusing on its ability to handle identity verification and prevent phishing attempts. We will assess the system's user authentication processes and defenses against common email-based attacks. By understanding the system's architecture and its implementation of protocols like SMTP, DKIM, and DMARC, we hope to uncover potential vulnerabilities and propose solutions to improve the robustness of its security.

Specifically, we will analyze Dooray's implementation of email security standards and evaluate its resistance to phishing attacks, and investigate user authentication mechanisms to prevent spoofing.

4 Expected outcomes

As students, we expect to gain a comprehensive understanding of the Dooray mailing system, including its architecture and the protocols employed to secure communications. By analyzing how Dooray implements user authentication and the effectiveness of protocols like SMTP, DKIM, and DMARC, we aim to learn how the system prevents phishing attacks and identity spoofing. This project will enhance our knowledge of email security practices and equip us with the skills to identify vulnerabilities, ultimately preparing us to propose informed solutions to improve Dooray's defenses against cyber threats.

5 References

[1] Verizon. (2023). 2023 Data Breach Investigations Report.
[2] Kitterman, S. (2014). DomainKeys Identified Mail (DKIM) Signatures. Internet Engineering Task Force (IETF). RFC 6376.