2023 Spring CNS Reading Critique #4

The Password Reset MitM Attack VS Is Real-time Phishing Eliminated with FIDO?

R11921A16 何秉學

I. Summary of 1st Topic

The Password Reset MitM Attack" paper aims to address a security vulnerability in the password reset process that allows attackers to intercept a victim's password reset link and gain access to their account. This problem matters because attackers can compromise personal information and sensitive data. The paper presents the Password Reset Man-in-the-Middle (PRMitM) attack and proposes several defenses to mitigate the risk, including challenge-response protocols and additional authentication factors. The authors conclude that PRMitM attacks are a significant threat to online account security, and suggest implementing additional security measures and informing users of the risks to strengthen the security of their accounts.

II. Summary of 2nd Topic

The paper addresses the problem of social engineering downgrade attacks against FIDO authentication protocols, which can bypass its strong authentication measures and lead to phishing attacks. Phishing attacks are a significant cybersecurity threat, and FIDO was developed to provide stronger authentication methods. The researchers analyzed the FIDO protocols and conducted experiments to demonstrate the effectiveness of social engineering downgrade attacks against FIDO. The study concludes that social engineering downgrade attacks can bypass FIDO's authentication measures and launch phishing attacks.

III. Comparison

"Is Real-time Phishing Eliminated with FIDO?" paper identifies and analyzes a previously unknown vulnerability in the FIDO authentication protocol: social engineering downgrade attacks. In addition, the others identify a vulnerability in the password reset process, where an attacker can intercept and modify the reset process to gain access to an account. And I think the paper's (The Password Reset MitM Attack) threat model is quite easier to achieve for attackers due to its trivial process and low cost of deploying a website that seduces some users to provide their sensitive information for free resources. They have very similar threat models and attack methods in different domains. They both discussed men-in-the-middle attacks with different platforms, such as websites or authentication vendors

IV. Reflection

If I were the author of either paper, I would explore solutions to improve security, such as incorporating user education and awareness or implementing secure communication channels for a password reset. Unsolved questions that I want to investigate include how to balance security and usability in the authentication and password reset processes. The broader impacts of these proposed technologies are significant, as compromised authentication or passwords can lead to data breaches and financial losses. Overall, these papers highlight the need to address not only technical vulnerabilities but also human factors in cybersecurity, and to continually strive for more secure practices.