分組名單（不足 5 個人空著就好）:

姓名	學號
施柏江	110550108
王振倫	110550068

1. **Name of the paper:**

   Password Managers: Attacks and Defenses

2. **Summary:**

   The paper thoroughly explores the security issues related to password managers. It looks at different ways attackers can exploit these systems, like phishing or snooping on the clipboard, pointing out where password managers fall short. The paper provides ways to better protect against these attacks, such as tightening browser extension security and using stronger encryption. The paper also talks about the balance between security and ease of use in password managers, stressing the importance of continued research and cooperation to stay ahead of new threats. To sum up, it gives insights into making password managers safer in today's interconnected digital environment.

3. **Strengths of the paper:**

   The paper thoroughly looks at different ways attackers can target password managers and how to defend against them, which is important for cybersecurity. The authors back up their points with real-world examples and experiments, making their research trustworthy. They present their findings in an understandable way, suitable for anyone interested in the topic. To be short, the paper gives useful information about password manager security and is helpful for both researchers and people working in cybersecurity.

4. Weaknesses of the paper:

(1) The article assumes users are unaware of the potential risks associated with connecting to unsecured networks, such as rogue WiFi routers in public places.

(2) The study only focuses on attacks facilitated by active man-in-the-middle network attackers, neglecting other potential threats such as phishing attacks or malware targeting password managers.

(3) It assumes users will only log in to websites during the initial phase and won't perform any other actions that might expose their passwords, which might not reflect real-world user behavior.

(4) It does not address how multi-factor authentication might mitigate the impact of such attacks by adding an extra layer of security beyond passwords.

(5) The article doesn't provide recommendations or solutions to mitigate the risks posed by the described attacks, leaving users vulnerable to potential exploitation.

5. What did you learn from this paper?

From this paper, we learned a lot about cryptography-related knowledge.

Firstly, we learned about various attacks that could pose a threat to the security of password managers, such as phishing attacks, injected iFrames, and malicious browser extensions.

Then, the paper also indicated weaknesses in the implementation of password managers, such as insecure communication channels between the password manager and browser extensions.

Thirdly, the paper discussed potential defense methods against these attacks, such as improving the security of browser extensions, adopting stronger encryption methods, and implementing stronger password authentication systems.

Fourthly, we knew that enhancing security measures may sometimes bring inconvenience to users, so it discussed the trade-offs between security and usability in password managers.

Lastly, we understood the importance of ongoing research in the field of password manager security, as it is closely related to everyday browsers like Chrome or Safari. Learning how to identify and address emerging threats and vulnerabilities is crucial.

How would you improve or extend the work if you were the author?

If I were the author, I would hope to provide a more comprehensive process for individuals and web engineers to avoid these attacks. For example, the paper mentioned sweep attacks, and if everyday users could understand these attacks, it would bring more benefits. For individuals, they can avoid using insecure public WiFi, be cautious with unfamiliar links, and even know how to respond if they find themselves under attack. For web engineers, it's crucial to ensure that web pages are not affected by iFrames and to ensure that website links are encrypted. Providing this information helps readers understand the risks and stay away from them.

Also, I would conduct a study to track the evolution of password manager vulnerabilities and attacks over time. This would provide insights into emerging trends, allowing for more proactive security measures. Additionally, I would conduct user-centered research to explore user behaviors regarding password managers. Understanding user needs and challenges can inform the design of more user-friendly and secure solutions. Furthermore, by accumulating more real-world testing of password manager security features and defenses across different platforms and environments would provide more realistic insights into

their effectiveness and potential weaknesses. With these approaches, the research on password manager security can be extended to provide more nuanced insights, practical recommendations, and effective solutions for addressing the evolving threats in cybersecurity.

What are the unsolved questions that you want to investigate?

(1) How can password managers securely collaborate with third-party services, such as cloud storage providers or authentication services, without compromising user credentials or privacy?

(2) How can password managers effectively utilize biometric authentication methods, such as fingerprint or facial recognition, while reducing potential privacy concerns and risks associated with storing such data?

(3) In the paper, the concept of the 'password booth' is introduced to allow users to securely input passwords, but it requires significant changes which may be difficult for users to accept, considering human factors such as cognitive biases and user trust. As an engineer, how should one consider these human factors and ensure user to accept this new technology?

What are the broader impacts of this proposed technology?

Firstly, it contributes to improvements in cybersecurity by reducing the risk of credential theft, unauthorized access, and data breaches. This helps protect sensitive information and reduces the financial and reputational damages associated with cyberattacks.

Secondly, it boosts the users' confidence in managing online credentials securely. This might encourage more people and companies to use password managers and practice better password habits. Thirdly, stronger password

manager security measures preserve user privacy by safeguarding personal information and preventing unauthorized access to sensitive data. This is particularly important because of rising concerns about data privacy and regulatory compliance requirements. Additionally, stronger security in password managers builds more trust in online services and platforms, as users depend on these tools to safely log in to their accounts on different websites and apps. This trust is essential for the continued growth and innovation of the digital economy. Overall, it contributes to creating a safer and more secure digital environment for individuals and organizations alike.