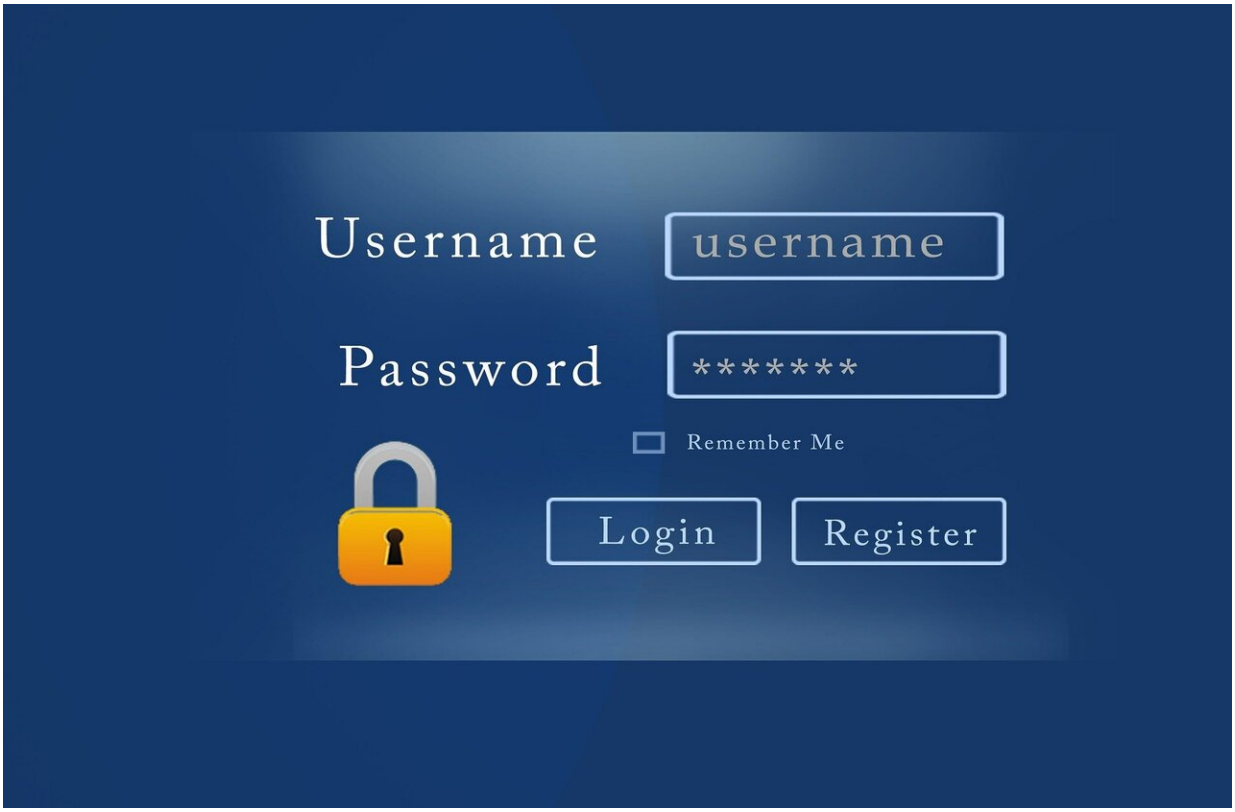
Researchers expose vulnerabilities of password managers

March 16 2020



Credit: CC0 Public Domain

Some commercial password managers may be vulnerable to cyber-attack by fake apps, new research suggests.

Security experts recommend using a complex, random and unique

password for every online account, but remembering them all would be a challenging task. That's where password managers come in handy.

Encrypted vaults accessed by a single master password or PIN, they store and autofill credentials for the user and come highly recommended by the UK's National Cyber Security Centre.

However, researchers at the University of York have shown that some commercial password managers may not be a watertight way to ensure cyber security.

After creating a malicious app to impersonate a legitimate Google app, they were able to fool two out of five of the password managers they tested into giving away a password.

The research team found that some of the password managers used weak criteria for identifying an app and which username and password to suggest for autofill. This weakness allowed the researchers to impersonate a legitimate app simply by creating a rogue app with an identical name.

Senior author of the study, Dr. Siamak Shahandashti from the Department of Computer Science at the University of York, said: "Vulnerabilities in password managers provide opportunities for hackers to extract credentials, compromising commercial information or violating employee information. Because they are gatekeepers to a lot of sensitive information, rigorous security analysis of password managers is crucial.

"Our study shows that a phishing attack from a malicious app is highly feasible—if a victim is tricked into installing a malicious app it will be able to present itself as a legitimate option on the autofill prompt and have a high chance of success."

"In light of the vulnerabilities in some commercial password managers our study has exposed, we suggest they need to apply stricter matching criteria that is not merely based on an app's purported package name."

The researchers also discovered some password managers did not have a limit on the number of times a master PIN or password could be entered. This means that if hackers had access to an individual's device they could launch a "brute force" attack, guessing a four digit PIN in around 2.5 hours.

As well as these new vulnerabilities, the researchers also drew up a list of previously disclosed vulnerabilities identified in a previous study and tested whether they had been resolved. They found that while the most serious of these issues had been fixed, many had not been addressed.

The researchers disclosed these vulnerabilities to the password managers.

Lead author of the study, Michael Carr, who carried out the research while studying for his MSc in Cyber Security at the Department of Computer Science, University of York, said: "New vulnerabilities were found through extensive testing and responsibly disclosed to the vendors. Some were fixed immediately while others were deemed low priority.

"More research is needed to develop rigorous security models for password managers, but we would still advise individuals and companies to use them as they remain a more secure and useable option. While it's not impossible, hackers would have to launch a fairly sophisticated attack to access the information they store."

Revisiting Security Vulnerabilities in Commercial Password Managers will be presented at the 35th International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2020) in September, 2020.

Provided by University of York