WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Password Management Against Versatile Attacks

Geetha D C, Dhanyatha R, Dr. Zafar Ali Khan

UG Student, Presidency University, India.

DOI: https://doi.org/10.55248/gengpi.2022.3.7.10

ABSTRACT

Passwords play a very critical role in authentication, information and security of web applications. Securing and managing passwords is a significant problem for most of the people in the modern world. As the number of accounts increases managing and securing of the passwords gets complicated. As a consequence, many users tend to adopt weak password management schemes which can significantly reduce the security of the systems. Prior to the research it confirms that security experts recommend Password managers to help users generate, store and enter strong unique passwords. In this research, after checking Password habits of users accounts, it allowed us to understand the password habits of users according to sensitive data of their account, and also revealed some critical issues associated with password choice. So we propose PasswordAgent(password hashing mechanism).It utilizes both salt repository(salt-sequence of randomly generated bytes) and a browser plug in to secure logins with strong passwords. Password hashing is a technique that allows user to remember simple low entropy passwords and have them hashed to create high-entropy secure passwords. PasswordAgent is less vulnerable to offline attacks, and it provides stronger protection against password theft.

Introduction

There are several users who logs on to several system or devices each and every day by using password. Passwords are used to secure our data or information, it is also used as security for web applications , services such as online services including banking, voting, mail, social networks, and other enterprise resources depend on passwords to maintain secure transactions. A user may have multiple accounts secured by passwords and these password protected accounts need to be managed. As the multiple accounts increases the management of password gets more complicated. Many users try to adapt to weak passwords to manage accounts but it would reduce the security of the accounts. There are ways to manage the password, We will come to know about why passwords are required to manage the security of our accounts , how are they stored what, are the effects of using weak passwords, what are the techniques we will use for password management.

What is Password Management?

Passwords are a set of strings or characters which is provided by users at the authentication of web accounts. It remains as one of the most secure methods of authentication available to date, they are subjected to a number o security threats when mishandled. Password management is a system that facilitates a simple, secure way to store passwords and access them quickly when required. It is a set o principles and best practices to be followed by users while storing and managing passwords in an efficient manner to secure passwords as much as they can to prevent unauthorized access. Passwords can be easily traced when the user is not able to create a unique password that can be managed and secured as well.

Why Password Management is important?

We all know that passwords are not the perfect security measures as most people's passwords are weak, easy to crack, and offer little protection, password-cracking software quickly cycles through common patterns and weak passwords can be easily identified so password management is important, password manager helps user by storing all the password. Any online service, paid or otherwise, requires users to login with a username and password combination .Passwords prevent unauthorized access and authenticate that the person logging in is the original user. Password management is different now than it was a few decades ago. Back then, there were very limited online activities to choose from, and online financial transactions were sporadic. Naturally, a person required only a few passwords to remember because there weren't many accounts in need of protection. Nowadays, the situation is entirely different, and people use around thirty different applications per month, most of them hidden behind a password. With that, the use of strong passwords became mandatory because weak and reused passwords may lead to stolen online accounts and online identity, or even financial losses.

Password Attacks and how to stop them.

Password attacks are one of the most common forms of corporate and personal data breach. A password attack is simply when a hacker trys to steal your password. In 2020, 81% of data breaches were due to compromised credentials. Because passwords can only contain so many letters and numbers, passwords are becoming less safe. Hackers know that many passwords are poorly designed, so password attacks will remain a method of

attack as long as passwords are being used. There are different type of password attacks namely

1.Phishing

It can be when a hacker posing as a trustworthy party or a person sends you a fraudulent email or a message might even call hoping you will reveal your personal information voluntarily . Sometimes they lead us to fake screen "reset your password" and sometimes it will install malicious code on the device.

To avoid these attacks there are following steps,

- **Check or verify who sent the mail:** match each and every line in every email to ensure that the person they are claiming to be matches the email address you're expecting .
- **Conirm or double the source:** if you get any doubt , contact the person who sent the mail from where the mail has been sent and ensure that they were the sender.

2.Man-in-the middle (MitM)

Man-in-the middle (MitM) attacks are when a hacker or compromised system sits in between two uncompromised people or systems and decodes the information they're passing to each other, including passwords. For example if we have two persons namely A and C and they both are exchanging the notes in class, but person B has to relay those notes, person B has the opportunity to be the man in the middle.

To prevent from these attacks we have :

- **Enable encryption on your router:** If your modem and router can be accessed by anyone o the street, they can use "snifer" technology to see the information that is passed through it.
- **Use strong credentials and teo-actor authentication:** Many router credentials are never changed from the default username and password. If a hacker gets access to your router administration, they can redirect all your traffic to their hacked servers.

3.Brute force attack

If a password is equivalent to using a key to open a door, a brute force attack is using a battering ram. A hacker can try 2.18 trillion password/username combinations in 22 seconds, and I your password is simple, your account could e in the crosshairs.

To prevent from brute force attacks:

- Use a complex password: The difference between an all-lowercase, all-alphabetic , six-digit password and a mixed case ,mix-character, ten digit password is enormous. As your password complexity increases , the chances of a successful brute force attack decreases.
- Enable and configure remote access:Ask your IT department if your company uses access management. An access management tool like One Login will mitigate the risk of a brut-force attack.

By checking the Password habits of users like how the users will generate passwords to the accounts they create , nowadays users tend to create multiple accounts they try to give the same password or similar password to each account they use because they feel its very hard to remember these password. Most of the users use their birth date, name or something related to their personal life which may be available somewhere like social media so now it becomes easy for the hacker to hack by using this sensitive data . So it also revealed some critical issues associated with password choice.

PasswordAgent

PasswordAgent consists o two major components; the salt repository and the agent. The repository stores salt lists enabling passwordAgent to function transparently across either enterprise networks or the Internet. The Agent is used to retrieve the salts from the repository, provide visual security indicators, and generate site specific passwords. In our design, each enterprise network maintains a salt repository providing salt storage services for its users. To achieve high reliability and scalability, it is possible that multiple servers unction as the salt repositpry within one enterprise network. Usually, each user has a primary salt repository, but it is possible that one user has salt lists stored in multiple repositories PasswordAgent consist o two major components: the Salt Repository and the Agent. The Repository stores salt lists enabling PasswordAgent to function transparently across either enterprise networks or the Internet. The Agent is used to retrieve the salts from the Repository, provide visual security indicators, and generate site specific passwords. In our design, each enterprise network maintains a Salt Repository providing salt storage services for its users. To achieve high reliability and scalability, it is possible that multiple servers function as the Salt Repository within one enterprise network. Usually, each user has a primary Salt Repository, but it is possible that one user has salt lists stored in multiple repositories.

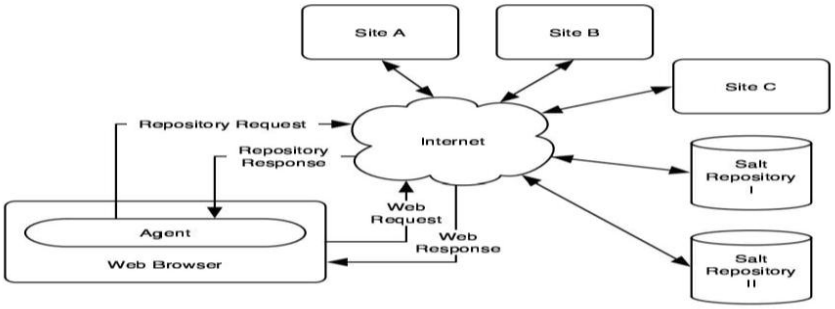

Figure 1: The architecture of PasswordAgent.

Conclusion

In this paper we have described about password, password management, what are the password attacks and how to stop or avoid those attacks and a new method called PasswordAgent is also discussed by using the below mentioned refrences we came to know about all the issues faced due to weak passwords we have also stated how to make a habit of using strong password and where these passwords can be stored for safety purpose.

Refrences:

1. https://ir.kiu.ac.ug/bitstream/20.500.12306/2332/1/STRATEGIES%20FOR%20OPTIMIZING%20PASSWORD%20MANAGEMENT%20AGAINST%20VERSATILE%20ATTACKS.pdf
2. https://www.onelogin.com/learn/6-types-password-attacks
3. https://www.usenix.org/legacy/event/lisa09/tech/full_papers/strahs.pdf