584- Wireless Technical Paper - 2

The Password Reset MitM Attack

Rahul Godugupally

CWID -10470581

1.Summary of fundamental ideas presented in the paper

The paper presents Password Reset Man in the Middle(PRMitM) attack to show how it can be used to gain access to user accounts on various platforms. The attack exploits “a set of vulnerabilities in password research procedures of popular websites and mobile applications.” [1] Websites like Google, Facebook and many popular websites were vulnerable to this attack. The authors then evaluated this attack and pointed out the vulnerabilities which the attack exploited.

In this attack, the attacker starts a password reset process with an application or a website and forwards every challenge sent by the application to the victim who wants to use the service of a particular web application or website. There can be variations to the attack including exploitation of the password reset process that sends the reset message to the victim's mobile phone.

The authors then evaluate that most of the popular websites are vulnerable to PRMitM (Password Reset Man in the Middle). They then conclude that straightforward solutions are not as effective when dealing with PRMitM.

Hence, they then designed and evaluated a secure password reset process which significantly improved the effectiveness of the reset process compared to traditional ones used by popular companies today. In addition to this, they propose techniques and guidelines which would improve the security of the websites. They intend for these guidelines to be used during the audit process and in the secure password reset process.

2.Issues paper addresses and how they have been addressed in the past

The main issue this paper addresses is passwords or rather how easy it is to exploit the password reset process. The author mentions that the need for passwords started to arrive with the rise of shared environments. At the beginning, the passwords were saved in plain text, but due to passwords being stolen they started storing passwords in the form of hashes and also saw the use for encryption and salting the hashes.

Despite this, the password databases are vulnerable to being decrypted. With the improved computational power of modern-day computer parts any form of stored password, encrypted or hashed can be recovered if time is not a concern with attacks such as brute force and dictionary attacks.

Also, they argue that due to human tendencies of choosing weak, easy to remember passwords even the most secure password storage will not be of any aid to the user. To prevent this many websites, force their users to use strong passwords with a mixture of uppercase and lowercase letters along with numbers and special characters. In addition to this “web-services such as banks, which allow sensitive operations, often force their clients to change their passwords frequently.” [1] These enforcements were shown to be effective in maintaining account security.

However, the fact that many users tend to forget their passwords due to the enforcement of maintaining strong passwords and frequently changing passwords. This raised the need for password reset mechanisms. This is a challenging process as websites need to authenticate users without their passwords. Most websites send a password reset link to the email they registered with. But in the case of email websites like Gmail, Yahoo mail etc. this is not possible unless the user has a backup email registered with the website. Due to this, they have to offer alternative methods to reset the password. These methods include answering security questions or using mobile phones to authenticate users before they can receive an option to reset their password.

3.Discussion of core ideas of the paper

The core ideas of the paper include the Password reset man in the middle attack (PRMitM)

In this attack, the attacker makes the user access a resource from the malicious website. The attacker requires the user to log in to the website. During the registration process or with cross-site attacks like cross site scripting, cross-site request forgery, clickjacking the attacker obtains the email id of the victim. However, this can only be achieved when the user is logged in to the website. And the malicious webpage must lure the victims to provide their info. This can be done by social engineering methods. “For example, the attacker can create a website that offers (or claims to offer) free services, e.g., streaming or files download.” [1]

Then, on the server side the attacker accesses the email service provider and initiates a password reset process for this the attacker needs basic information such as username, email or the phone number “The attacker forwards every challenge that he gets from the email service provider to the victim in the registration process.” [1] then he turns into Mitm and “In the other direction, every solution that is typed by the victim in the registration process is forwarded to the email service provider. That way, the cross-site attacker is a man in the middle of a password reset process.” [1]

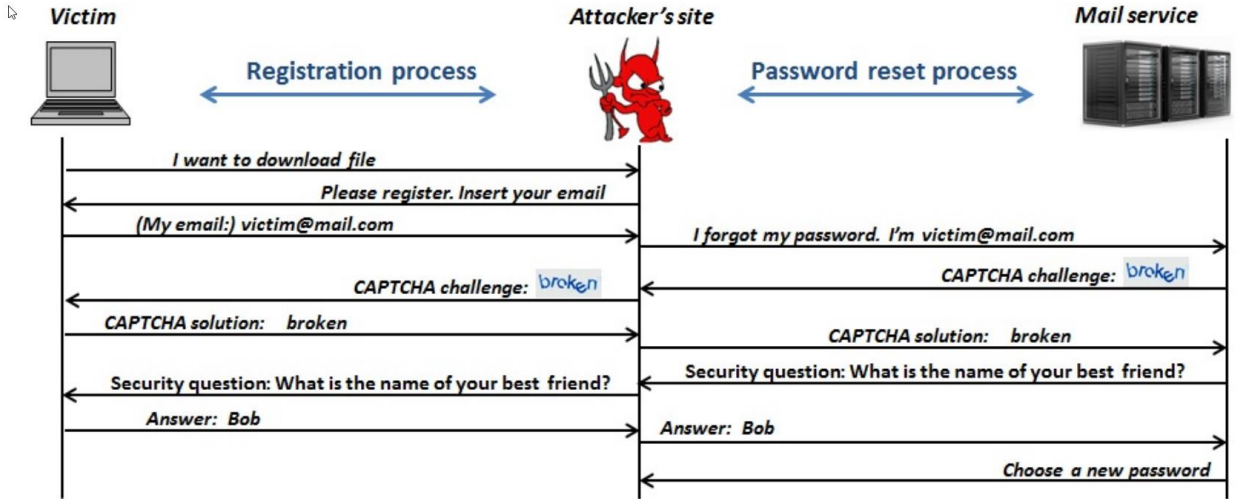

Figure 1[1]: Basic PRMitM attack illustration, in this the email service provider challenges the attacker with a CATPCHA and a security question.

These challenges include CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), Security questions, code (OTP- One Time Password) that is sent to phone and reset link that is sent to the email address. In the last case where the link is sent to the email, the PRMitM cannot be used as it would involve gaining access to the data in the email account of the victim. However, the authors argue that this method cannot be used for email services themselves and popular email services like Yandex, mail.com ask security questions or mobile phones if the user has not set up a backup email account. Sometimes the websites that send the code are more vulnerable to attack. "This is because the attacker can launch the PRMitM attack on them even in scenarios that are simpler than registration to a website." [1]

The PRMitM is exceedingly difficult to detect for users as it exploits the server-side design of the password reset process and depending on the severity of the bug there is no way even client-side defenses can detect the attack.

The authors then analyzed various reset SMS and calls sent by the websites to the users. And surveyed the password reset mechanism used by popular websites and did a vulnerability analysis on them. The results showed that most of them are vulnerable to PRMitM and a few are even more vulnerable like google (using phone call). Along with this, they mention that lack of language compatibility during the password reset process is a problem as it is vulnerable to PRMitM as they only check for the code rather than reading through the message. Also, they discovered additional vulnerabilities in mobile messaging platforms like WhatsApp and Snapchat.

The authors suggest countermeasures for improving the security of websites including password reset notification in case the password reset was initiated by a malicious user. Among the websites they tested only google provided a SMS notification after the password reset process. This is even better if the website provides an application notification as they are immune to PRMitM. They also suggest using their friend's email for them to verify by dividing them into bits. Suppose 3 parts are required for verification the 3 parts are sent to friend A, B, C and all of them are required for verification. For this the user must give their friends email in advance and it is not a feasible solution.

Further, they include defenses against the PRMitM attacks. These countermeasures are easy to deploy and improve on the standard followed by the current websites. They include utilizing good security questions which combine other parameters such as the IP address and originating browser. Implementing Link-via-SMS(LVS) instead of sending the code in clear text could prevent MitM access. Using phone calls for secure password reset is another defense against the attack. Lastly, they mention using their own mobile applications to send the reset links through as they are less vulnerable than traditional SMS.

4.Identification of any wireless-related issues brought up in the paper

The wireless issues bought up in the paper include the classic man in the middle attack where the attacker intercepts the communication between the sender and the receiver and can not only obtain the messages being sent by them but also could manipulate the messages and destroy the integrity of the message. The classic man in the middle attack compromises all 3 factors of the CIA triad I.e., Confidentiality, Integrity and Authentication.

In this paper the authors mention various man in the middle attacks which they use for the password reset process of websites and mobile phones. The man in the Browser attack (MitB) in which the “malware takes over the browser and acts as a proxy between the user and the web”. [1] This malware can obtain information typed by the user and can even manipulate the operations performed by the user. They mention an example where the attacker changes the recipient of the financial transaction from the intended.

Further, they mention evil twin attacks where the attacker lures the victim to use a malicious router with an innocuous name controlled by the attacker. In some cases, the attacker can pass de-authentication packets to disconnect the victim from the router and then force them to connect to a rogue access point with the same SSID by spoofing the SSID. This way all the communication from the victim goes through the rouge ap controlled by the attacker.

5. Potential applications of the technology presented

The paper presents new guidelines to be implemented by websites for password reset process this could help strengthen the websites and by implementing these new techniques in the audit process they could easily figure out the appropriate solutions for the problems faced.

The PRMitM could be included in active penetration testing procedures done in the real world to find the vulnerabilities in other processes such as secure communications within the company's infrastructure and test the confidentiality of the remote connections to the company.

For crucial applications such as bank websites, the new ways to authenticate can prevent frauds or huge financial implications. Similarly, for companies whose websites host confidential data this could benefit from unauthorized users gaining access to them and could prevent huge financial losses and reputation loss.

On the other hand, the technology presented in this paper could further be applied for malicious processes with sophisticated phishing attacks and could render multi factor authentication useless. As sophisticated phishing attacks do an excellent job of impersonating the target website the user plans to visit and pair that with dns spoofing so that and normal user would not be able to figure out that he landed on a phishing website.

6. Future opportunities created by the technology

The technology presented in the paper could help to bring new ways for authentication, in case a password reset is needed. Multi-factor authentication can be used for password reset process rather than just using a single factor like something you know or something you have to authenticate users during the password reset process.

The PRMitM could further be improved for developing secure communications between different nodes. With a compromised node in a communication network the technology could be very dangerous as it could destroy the integrity of the information sent over the network. With the technology presented in the paper we could develop procedures for finding vulnerabilities in communication networks which are meant to kept secure.

The vulnerabilities disclosed in this paper can be used as guidelines for authentication or sending critical information such as one-time passwords (OTP) for critical applications such as banking. Here due to MitM attacker can read or intercept the information sent from the bank to the victim's mobile. Hence, audits can be done based on the guidelines mentioned by the authors in the paper. Application of the guidelines will secure message communication between the users and the servers.

Citations

[1] N. Gelernter, S. Kalma, B. Magnezi and H. Porcilan, "The Password Reset MitM Attack," 2017 IEEE Symposium on Security and Privacy (SP), 2017, pp. 251-267, doi: 10.1109/SP.2017.9.