THE PASSWORD RESET MITM ATTACK

MONICA BERNARD

EBIN SCARIA

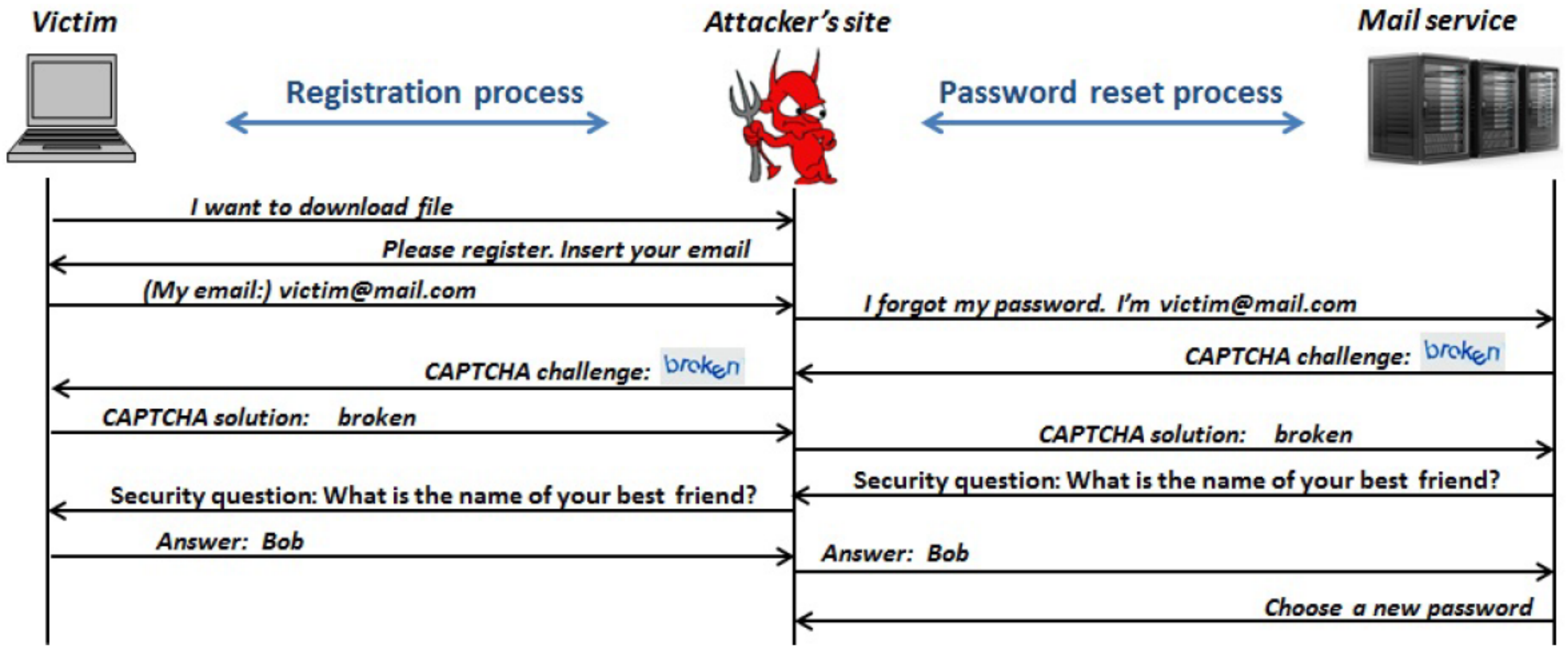
IEEE PAPER DETAILS

- We have selected the paper **The Password Reset MitM Attack** written by Nethanel Gelernter Senia Kalma, Bar Magnezi and Hen Porcilan.
- This paper was published in 2017.

Introduction

- All sites that carry a user authentication system has a password reset mechanism.
- This helps users to retrieve or reset their password.
- The identity of the user is verified during a password reset.
- This is usually done by sending a code via email, SMS or over the phone. There are many other ways as well.
- User information is collected when user signs up to an attacker's site.
- In a MitM attack, the user account's password is reset without the knowledge of the user but with the help of the user himself.

Methodology



I want to download file

Please register. Insert your email

(My email:) victim@mail.com

I forgot my password. I'm victim@mail.com

CAPTCHA challenge: broken

CAPTCHA challenge: broken

CAPTCHA solution: broken

CAPTCHA solution: broken

Security question: What is the name of your best friend?

Security question: What is the name of your best friend?

Answer: Bob

Answer: Bob

Choose a new password

What we intend to do.

- Our goal is to provide a demonstration of an attack similar to the attack mentioned in the paper.
- We create a dummy website which represents the attacker’s site.
- To show our demonstration, we will create a dummy account on one of the vulnerable websites mentioned in the paper
- And we will try to take control of the dummy account via a password reset using the information provided to the attacker’s site.

Implementation Plan

- We plan to complete this project in the next 5 weeks.
- We have already built the attacker’s site required for the demo.
- The plan has been outlined below.
- Week 1: Fixing minor bugs that the dummy attacker’s site implementation has.
- Week 2:Building the back end logic required for the attack demo.
- Week 3:Testing and adding improvements.
- Week 4:Writing the report.
- Week 5 Writing the report.

References

https://www.ieee-security.org/TC/SP2017/papers/207.pdf

https://blog.acolyer.org/2017/06/21/the-password-reset-mitm-attack/

https://www.schneier.com/blog/archives/2017/07/a_man-in-the-mi.html

https://inspiredelearning.com/blog/wary-password-reset-man-middle-mitm-atta