ISEC 400 Homework 5 Name: Megan Leonard

Answer the following questions based on your reading of the textbooks, any supplemental material, and the instructor’s presentation this week. If you use an external source (i.e. a web page, the required textbook, or an additional book) to help you answer the questions then be sure to cite that source. Hint: you should probably always be citing a source.

## Questions

1. **[8 points]** Read the ArsTechnica article “[Anatomy of a hack: how crackers ransack passwords like ‘qeadzcwrsfxv1331](http://arstechnica.com/security/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/).’” What mitigation strategies presented in this week’s material would have caused the attacks to either fail or take significantly longer? How do they accomplish this?

Some mitigation strategies that would have helped against the attack are the use of multiple rounds of hashing as the attack took place with the MD5 cryptographic hash function, so by hashing the hashes, we can have more layers that make it harder to decrypt without knowing the specific hash patterns and when each was used. There is also salt and pepper that helps by adding in its own injections, so it helps prevent acquiring the real password.

1. **[7 points]** Read “[The definitive guide to form base website authentication](http://stackoverflow.com/questions/549/the-definitive-guide-to-form-based-website-authentication)” on StackOverflow. What additional or modified strategies are suggested, and how would they be helpful in increasing the password and authentication security?

The first strategy they mention that I find helpful is the use of CAPTCHAS as sometimes humans have trouble solving them so it would help against brute force attacks using bots. There is also account locking that can help prevent brute attacks and attempt delaying as it mentions so each failed attempt means the delay to login increases making it hard for brute force attacks and helps dissuade people from continuing their attack as the failed attempt delay could be increased to go hours or days at a time if they try too many times.

1. **[5 points]** What are some advantages and disadvantages to securing a web application with an [OAuth](https://en.wikipedia.org/wiki/OAuth)-based single sign-on (SSO) provider such as Google, Facebook, Twitter, Github, etc?

Some advantages are that it uses password tokens so that the sensitive data and the passwords are stored remotely and harder to access. It also does not interact with the user credentials themselves and it keeps the data safe using cryptography. Some disadvantages are that there is an increase in risk of identity spoofing and phishing and if it fails, then the access to those related systems is lost with it.

1. **[5 points]** Once a user successfully authenticates against a web application, they are typically provided with an authentication token (i.e. a session ID). Anyone holding that ID can impersonate the authenticated user. What steps should an application author take to protect that ID as it is stored in either the client or server or as it is transmitted between them?

Some steps that should be taken are to first put a time limit on the tokens, use HTTPS authentication to make sure the token is on a secure website, and make sure there is verification to make sure the ticket matches the one generated using the server.

1. **[5 points]** In approximately 300 to 400 of prose (i.e. sentences, not bullet lists) using APA style citations if needed, summarize and interact with the content that was covered this week in class. In your summary, you should highlight the major topics, theories, practices, and knowledge that were covered. Your summary should also interact with the material through personal observations, reflections, and applications to the field of study. In particular, highlight what surprised, enlightened, or otherwise engaged you. Make sure to include at least one thing that you’re still confused about. In other words, you should think and write critically not just about what was presented but also what you have learned through the session. Ask at least one question that your instructor can answer in the returned assignment or class discussion.

This week we went over authentication and different attacks that we may see. There are many different means of authentication such as input like passwords or pins, physical like fingerprint scanners or facial recognition, and even confirmation like SMS and security tokens. An authentication that can be quite helpful is the HTTP and HTTPS authentication as it is the base authentication, we see most of the time with the need for usernames and passwords to access protected resources. Today, we see most sites using the multi-factor authentication whether it is using an authentication app or through texting/emailing someone a code. My question is do you have an authentication type that you like the most?

Citation:

Auth0. (n.d.). *Token based authentication made easy*. Auth0. Retrieved February 26, 2023, from <https://auth0.com/learn/token-based-authentication-made-easy>

Chakray\_Admin. (2022, November 2). *What is single sign on (SSO)? characteristics and advantages*. Chakray. Retrieved February 26, 2023, from <https://www.chakray.com/what-is-single-sign-on-sso-definition-characteristics-and-advantages/>

Dan Goodin - May 28, 2013 1:00 am U. T. C. (2013, May 28). *Anatomy of a hack: How crackers ransack passwords like "Qeadzcwrsfxv1331"*. Ars Technica. Retrieved February 26, 2023, from <https://arstechnica.com/information-technology/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/>

*The definitive guide to form-based website authentication*. Stack Overflow. (1955, June 1). Retrieved February 26, 2023, from <https://stackoverflow.com/questions/549/the-definitive-guide-to-form-based-website-authentication>

Gorman, B. (n.d.). *Why your organization should be using OAUTH 2.0*. Clowder. Retrieved February 26, 2023, from <https://www.clowder.com/post/why-your-organization-should-be-using-oauth-2.0#:~:text=OAuth%202.0%20is%20a%20secure,the%20user's%20identity%20or%20credentials>.

Whittaker, T., &amp; Whitney, T. (2022). Week05 Power Point. Retrieved February 26, 2023, from <https://franklin.instructure.com/courses/11070/files/1516719?module_item_id=623552>