**Peer Response 1**

Hi Miguel,  
  
Thank you for providing your thoughts on what broken access control is and how to prevent it. I found it to be rather informative.  
  
I liked how you used the Equifax breach in 2017 as a case study as it showed the aftereffects of an attack from the perspective of a company and its customers. Thinking about the knock-on effects of an attack and showing different perspectives shows a good level of knowledge about broken access controls.  
  
You have clearly done a lot of research into broken access controls showing how different techniques can be combined to fix any access control issues.  
  
Your use of swimlanes in your UML diagram made it clear what aspect of the system manages each part of the process. I liked how you used separate diagrams to demonstrate what broken access controls are and how to prevent broken access controls.  
  
Regarding your flowchart an oval should be used to represent the start and end process (Oblikwu. et al., 2019), you have used the state diagram start and stop notation. Additionally, could you have used separate headers or annotations to distinguish the flow charts to make it clearer which diagram is which.  
  
Have you thought about how access control policies can be used in the cloud to enforce role-based access control? For example, AWS uses IAM Roles to manage access based on roles. (Amazon, N.D)  
  
Have you considered how following the Principle of Least Privilege to limit the access of users can reduce the impact a hacker can have after exploiting broken access controls? (Maric, 2023)  
  
Regarding you references I noticed you aren't showing the access date that is shown in the UoEO Harvard referencing guide. I would suggest to have a look at the Harvard referencing guide which can be found in the Plagiarism and Referencing section on the Study Skills Hub. I have attached the University of Essex Harvard Referencing Guide that shows examples of how to reference sources.  
  
Best regards,  
  
Sam

**References**

Amazon. (N.D.) AWS Identity and Access Management. Available from: https://aws.amazon.com/iam/ [Accessed 24 March 2024]  
  
Maric, N. (2023) Broken Access Control: Attack Examples and 4 Defensive Measures. December 29, 2023. Available from https://brightsec.com/blog/broken-access-control-attack-examples-and-4-defensive-measures/#:~:text=Implementing%20the%20Principle%20of%20Least%20Privilege,-The%20Principle%20of&text=The%20principle%20is%20used%20to,system%20or%20accessing%20confidential%20information [Accessed 24 March 2024]  
  
Oblikwu, P., Dekera, K. & Udo, Edward. (2019). THE PRACTICALITY OF ENGINEERING PRINCIPLES IN SOFTWARE ENGINEERING. International Journal of Advanced Research. 7. 923-934. 10.21474/IJAR01/10234.

**Peer Response 2**

Hi Gareth,

I found your post to be rather interesting as I had limited knowledge on cryptography, so I learnt a lot from your post.

I liked how you contextualised the importance of cryptography. Focusing on how cryptographic failures on an ecommerce website for online transactions can lead to the exposure of sensitive data. I was wondering if you had done any research into the relevant legislation such as The Payment Services Regulations (The Payment Services Regulations, 2017).

I thought it was a good idea to give examples of cryptographic failures in a bullet point list as it is very clear and, it can be used to spot common cryptographic failures.

Giving examples of deprecated hashing algorithms shows that you are very knowledgeable about the different hashing algorithms available. Perhaps you could have added more context into why MD5 or SHA1 shouldn’t be used. For example, with MD5 it is susceptible to collision attacks and preimage attacks (TechClaw, 2023).

Have you considered how bleeding edge technologies implement cryptography differently to your average device? For example, how a salt is used in cryptography on a blockchain to defend against rainbow table attacks (Fudhah, 2022).

Regarding your UML diagram I noticed you were missing the start and stop processes and I noticed your flowchart is on a grid did you consider exporting it to a PNG or hiding the grid.

An improvement you could have made to your post was to have a separate flowchart for all of the examples of cryptographic failures instead of having just one general flowchart.

Additionally I noticed you haven’t referenced any academic articles in your initial post such as journal articles as this is something Dr Peoples recommended I would advise you on the summary post to make sure to include a reference to an academic article.

Best Regards,

Sam

**References**

Fudhah A., A. (2022). 'Blockchain and Bigdata to Secure Data Using Hash and Salt Techniques', Journal of Information Technology Management, 14(2), pp. 15-25. doi: 10.22059/jitm.2022.86924

TechClaw. (2023). Exploring the Power and Vulnerabilities of the MD5 Algorithm. September 13 2023. Available from: <https://medium.com/@techclaw/exploring-the-power-and-vulnerabilities-of-the-md5-algorithm-feb249ef9dfb> [Accessed 24 March 2024]

The Payment Services Regulations 2017. United Kingdom. Available from: <https://www.legislation.gov.uk/uksi/2017/752/part/7/made> [Accessed 24 March 2024]