Timing attack (Karthik, 2020) is one the form of side channel attack in which attackers gets access to the sensitive information by just observing the systems response time to the various input commands. The difference of time is used to deduce the sensitive information such as financial information and cryptographic keys. The attackers measure the amount of time taken by the system to execute a particular command such as in password based timing attack the observe how time does the system takes to process all the possible passwords as longer processing time would indicate the correct password. They can target many systems such as authentication based systems, web applications and cryptographic implementations. Specially those websites in which server side authentication or authorization is required. They can reveal sensitive data such as number of bits in a secret value, patterns which can help to predict the original values and time difference which can assist in revealing length of secret values and numbers.. There was no documented real case in the real world instance but in 1996 such type of attack was performed to crack the RSA encryption algorithm as many web application as well as authentication systems are highly valuenrable to such attacks as they fail to tackle the difference of timings during the password validation and authentication process. It can be applied to any algorithm that has a data dependent timing variation as removing it is quite difficult job in few algorithms and it frequently shows the varied execution time. As the majority of cryptographic algorithms (ARCSERVE, 2023) can be implemented which can remove the data dependent timing information also known as constant timing algorithm as this type of algorithms is less likely to leak information about the data. To encounter timing attacks developers and systems administration have to be proactive and vigilant to safeguard the data from the attacks .Developers should use advance coding practices and timely updates

# References

ARCSERVE, 2023. *ARCSERVE.* [Online]   
Available at: https://www.arcserve.com/blog/5-common-encryption-algorithms-and-unbreakables-future  
[Accessed 05 10 2023].

Karthik, S., 2020. *Meduim.com.* [Online]   
Available at: https://medium.com/spidernitt/introduction-to-timing-attacks-4e1e8c84b32b  
[Accessed 06 10 2023].

Mitchel, R., 2023. *Electropages.* [Online]   
Available at: https://www.electropages.com/blog/2023/05/new-side-channel-attack-discovered-intel-processors#:~:text=Another%20real%2Dlife%20example%20of,data%20corruption%20or%20privilege%20escalation.  
[Accessed 03 10 2023].