CYBER SECURITY

Mubashar khan

W1814299

MODULE: (2021) 4COSC003W.2 Trends in Computer Science

Tuesday 9-11am

CYBER SECURITY

Cyber security according to Alan Calder(2020) is “related to how electronic information is kept safely and securely” cyber security is also a subset of information security. Generally we associate securing information through physical means such as locking or hiding sensitive information, however cyber security allows us to use our electronic devices safely and can maintain sensitive information such as card details passwords Further protecting our privacy. I will be exploring the impacts of cyber security when developing an application and the issues a developer may face.[1]

2.a. Overview of Computer Security. When developing an application, what are the typical security issues a developer should consider?

What is computer security [2]

What has computer security achieved [2]

Why is computer security important for businesses [2]

When developing applications there are many issues and things to consider during the planning and execution stage. One of the most important aspects of developing an application is security and privacy. There are many issues to consider but there are two that stand out. Malware and sql injection

MALWARE

Malware is malicious data that slows down, bypasses and exposes the security systems that we have in place to protect our data.[3]

Malware has many forms of viruses and variations of viruses such as worms that attack and affect computers. [3]

What is a virus?[3]

Why is malware an issue?[3]

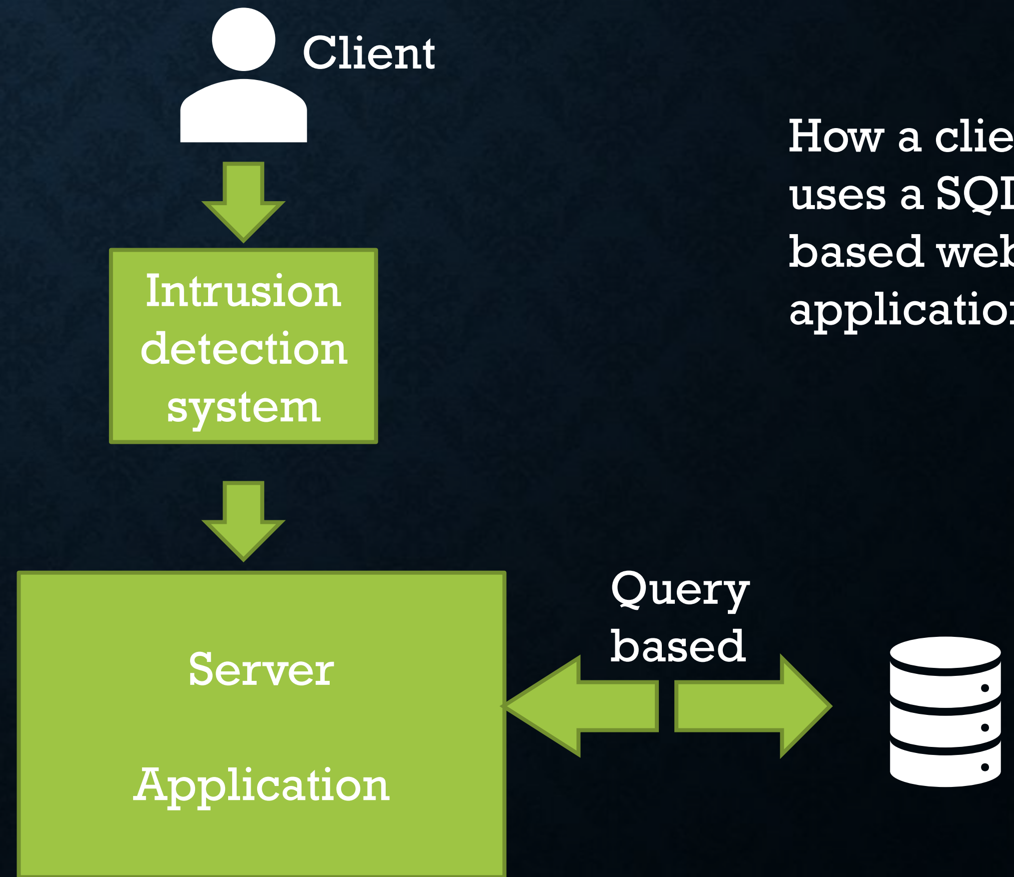
What is a possible solution?[5]

SQL INJECTION

Sql injection is when someone gains access to a database linked to a web application.[4]

What are the problems of this?[4]

How can this be avoided?[4]



How a client uses a SQL based web application

CONCLUSION

- It is very important for developers to consider these issues because data is given in full confidence to a company because the user trusts that it will not be hacked or used elsewhere. SQL injection and malware are common problems, and it is necessary for the developer to do research into it and provide ways to counter them such as intrusion detection system or possibly keep their antivirus software up to date if the developer or computer security system identifies a new form of virus or variation of it.

REFERENCES

- Calder, A 2020, Cyber Security: Essential Principles to Secure Your Organisation, IT Governance Ltd, Ely[1] Book

- Conklin, W. A. et al. (2018) *Principles of Computer Security : CompTIA Security+ and Beyond, Fifth Edition*. Fifth edition. New York: McGraw-Hill Education [2] Book

- Gillespie, A.A. (2019). Cybercrime: Key Issues and Debates (2nd ed.). Routledge. https://doi-org.uow.idm.oclc.org/10.4324/9781351010283 [3] Book

- Zhuo, Z. et al. (2021) Long short-term memory on abstract syntax tree for SQL injection detection. IET software. 4] Journal

- Min, B. et al. (2014) Antivirus security: naked during updates. Software, practice & experience. [5] Article

CYBER SECURITY

Module: 4COSC003W

Trends in Computer Science

Title: Cyber Security

Author: (Mubashar khan w1814299)

Contents

Introduction

The topic of our group is cyber security. This report will cover my research that I carried out to understand what cyber security is and how it affects us in different aspects. I chose question 2a which was overview of computer security and the issues a developer may face when making an application. The report will provide information about SQL injection alongside malware which are the main two problems I have concentrated on, furthermore it will also provide ways to counter these problems.

Computer security

My question was the overview of computer security and what issues a developer might face when making an application. It was important to explore computer security for this question because I had to understand what a general topic was. computer security is when an electronic device does what it has been told to do so without any influence by a 3rd party user. It essentially relates to the authorisation given or set by a person which restricts who can access the electronic device. Furthermore, during the research process computer security has a huge role in businesses and how companies use them to further to do business and attract customers. Although computer security is important in many aspects it does bring its challenges. [1] [4]

It is important for a developer to plan as these problems because common problems can keep occurring and be very irritating for both users and developers to handle. It is crucial to find possible solutions to the possible problems in the planning and execution stage. I will be discussing two common problems that are interesting as well as dangerous for developers to deal with if they do not counter them as I said before in the planning and execution stage because it may lead to delays in the schedule of developing the application alongside having enough time to anticipate issues and dealing with them.[4]

Malware

Malware is the first issue I discussed, and it simply relates to how data can be manipulated to bypass security systems that we have on our computers. Malware has many forms or ways of attacking computers and one way is through viruses. A virus is a self-replicating program that will attach itself to files and keep spreading by moving in and out of these files. This will slow down your computer and presents security issues as accessing the files that you need can cause further problems. One way for the developer to counter this is to implement an antivirus. This will keep the files safe from a virus attack. It is important to keep the anti-virus up-to date as new viruses are released and to be on top of them the anti-virus needs to have knowledge of how to counter it before it damages any files. It blocks attempts to further damage the computer. [2] [5] [7]

SQL Injection

The second problem I have discussed is SQL injection. SQL injection is when someone gains access to a database linked to a web application. Data that has been stored in the database is attacked using malicious SQL statements which can be used to bypass security systems that are in place and get authorisation to files that they are not allowed to view. This information is sensitive as it could be password, bank and personal details that are unique to an individual. Any access to this is a clear violation of privacy. The way a developer can counter this issue is the use of an intrusion detection system. This helps secure the servers which hold data and eliminate any vulnerabilities they may have by acting as a strong layer of security that the malicious SQL statements need to get past to be able to view any sensitive information. This is an issue and has a solution that developers can use to be at ease if mind as they will have a layer of security that is hard to bypass. This can also be used to notify the developer if suspicious activity is taking place which grants the developer time to find a solution to this problem. [3] [6]

Conclusion

To conclude I would say it is very important for the developer to consider issues in the planning and executing stage of an application which is being developed. This is important in delivering a successful product which is the main aim of the developer. Issues this big are important to solve or have a plan for so that they do not affect the application when it is being released. The target audience must be satisfied and since safety is an issue that everyone is interested in. The stronger the safety system the more it will appeal to audiences. I have mentioned the main two problems which are malware and SQL injection. Sensitive data is given to companies, and it is given based on the how well the security system works. Malware can be countered as I have mentioned before with antivirus which blocks any attempts at affecting files that a user has on their computers. SQL injection can be countered by an intrusion detection system Which monitors the system for any suspicious activities that are happening. These are important as the developer can further develop on these to provide and identify the best security system in future projects they are working on

References

Thomas, JP, & Essaaidi, M (eds) 2006, Information Assurance and Computer Security, IOS Press, Incorporated, [1]

Razak, M. F. A. et al. (2016) The rise of ‘malware’: Bibliometric analysis of malware study. *Journal of network and computer applications*. [2]

Clarke, J 2012, SQL Injection Attacks and Defense, Elsevier Science & Technology Books, Saint Louis. [3]

Conklin, W. A. et al. (2018) *Principles of Computer Security : CompTIA Security+ and Beyond, Fifth Edition*. Fifth edition. New York: McGraw-Hill Education [4]

Gillespie, A.A. (2019). Cybercrime: Key Issues and Debates (2nd ed.). Routledge. https://doi-org.uow.idm.oclc.org/10.4324/9781351010283 [5]

Zhuo, Z. et al. (2021) Long short-term memory on abstract syntax tree for SQL injection detection. IET software. [6] Journal

Min, B. et al. (2014) Antivirus security: naked during updates. Software, practice & experience [7]