SECP 1013

TECHNOLOGY AND INFORMATION SYSTEM

DESIGN THINKING:

COMPUTER SECURITY (GROUP 5)

LECTURER:

DR. ARYATI BINTI BAKRI

SUBMITTED BY:

DAYANG FARAH FARZANA BINTI ABANG IDHAM (A23CS0071)

FARRA NURZAHIN BINTI ZAHARIL ANUAR (A23CS0079)

HARINI A/P SANGARAN (A23CS0081)

SYARIFAH DANIA BINTI SYED ABU BAKAR (A23CS0183)

SEMESTER I (2023/2024)

TABLE OF CONTENT

INTRODUCTION

Design thinking is a process of iteration in which we aim to learn about the user, challenge theories and redefine problems in order to discover ideas that may not be immediately obvious based on our basic level of intelligence (Dam & Siang, 2021). Additionally, design thinking offers a solution-oriented strategy to problem solving. Design thinking has five processes which are empathise, define, ideate, prototype and text. All of these methods provide problem solutions towards the problem encountered by users.

The number of computer security attacks on personal devices and in the business has increased. Ransomware is a type of cyberattack involving an encryption of a victim's data and preventing them from accessing it until they pay a ransom. Therefore, an understanding of the fundamental threats to data as well as ongoing training are essential for effective computer security.

PROBLEM BACKGROUND

We have identified the problem based on the interview we conducted with Mr Haslan which has led us to conclude that ransomware is the biggest problem among computer security threats and attacks. Therefore, we came up with an application to resolve this issue.

EMPATHY

To gain more knowledge and further understanding on computer security, we conducted an interview session with Mr Noor Haslan Bin Sallehudin who is one of the security technicians in UTM Digital Care. We have asked questions that are all related to computer security in order to obtain some insights upon the topic. From the interview session, we can deduce that people are lacking in the knowledge of computer security. This has led to the increasing number of ransomware which is considered as one of the biggest problems among all cyber security attacks. So as to reduce and prevent occurrence of more attacks, we were suggested to develop comprehensive technologies such as XDR and WAF that have a broader capability to provide more information of the threats while employing automation to help detect current and future attacks. Other than that, Mr Haslan also emphasised on installing the latest version of anti-virus and doing frequent updates of the anti-virus and OS

patches to mitigate the attacks. Installing updates is essential in order to fix performance bugs and to provide enhanced security features.

DEFINE

With growing technology, the usage of electronic devices has been a necessity to sustain our everyday lives. As we all know, data is wealth. Data could possibly change someone's life. Therefore, storing these data safely is very important. For example, we can store our data online by using cloud computing. We can upload our data in the cloud to have a backup. However, hackers get an opportunity to threaten us when we fail to store our data safely. For example, hackers who breach our computer operating system can steal our information and ask for ransomware. Ransomware is a type of malware that prevents users from accessing their system or personal files unless a ransom is paid. Ransomware has been a popular trend these days as everyone values their personal data and would do anything to retrieve them. However, hackers are not honest and kind hearted to delete those copies of files when the ransom is paid. Even though they return those data to the victims, they still have a copy of those files so that they could ask for ransom again if needed. Hence, we can conclude that computer security attacks like ransomware are one of the biggest threats to our population as we are moving towards Industrial Revolution 4.0.

IDEATE

A brainstorming session was arranged to find solutions to our main problems. Lastly, we decided to develop an application. Our team interviewed Mr. Noor Haslan Bin Sallehudin and used Google Forms with student feedback as sources along the way to create our application. We have determined on the main features that we want to include in it. We all drew and finished the design of our applications on our laptops. Concentration on the application's ability to detect cyber threats and respond quickly in order to prevent unauthorised parties from obtaining our data are the main points of our applications. While conducting our own research, we discovered certain features that fulfil our standards to include in our application.

PROTOTYPE

With the problem identified, we start to map out all the possible solutions to overcome the problem. Then, we turned our rational thinking into a prototype which was designing an

application called PAWTEX. This prototype contains features that can prevent ransomware. The features are Recognition and Response Extension (RRE) which is to connect data from various security solutions so they may cooperate to enhance threat visibility and shorten the time needed to recognize, Breaches Blocking System (BBS) to keep an eye for harmful activity and block it and the last features is Trafficker which is basically just to monitor network traffics and send an early alert to RRE and BBS if harmful activity incoming.
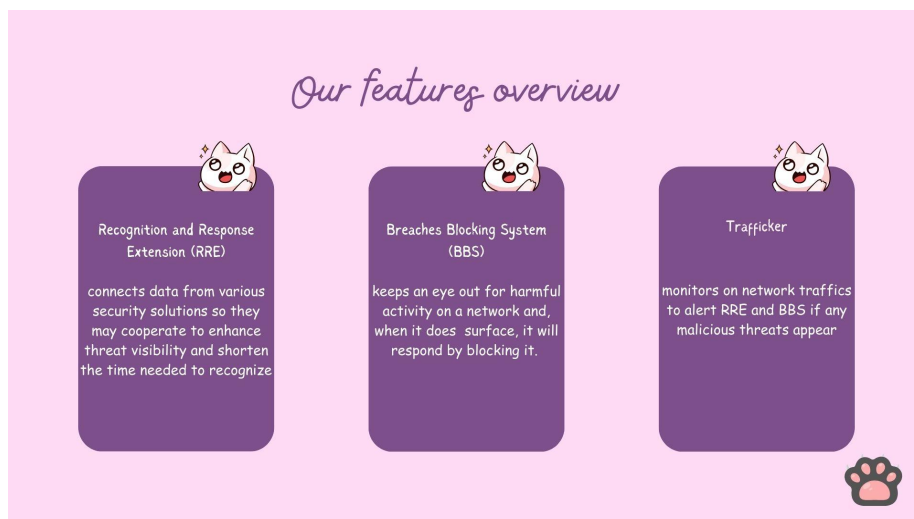

Diagram 1
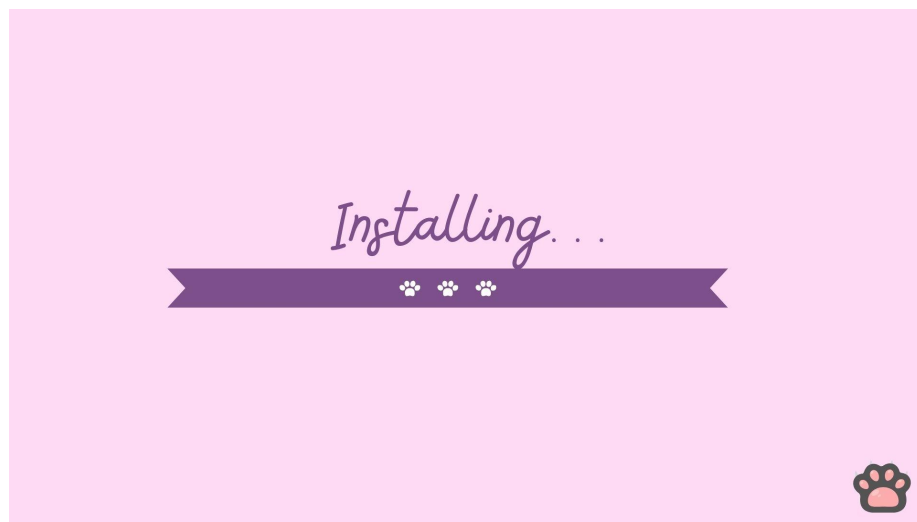

Diagram 2

Diagram 3

Diagram 4

Diagram 5

TEST

      In this stage, we have described our application to the users in order to get their feedback and comments on their perspectives of it. This makes it possible for us to recognise the issues that we had not previously considered. In order to conduct this, we carried out a survey via Google Form. Through this approach, we can gather user's suggestions and develop a more thorough and effective solution to resolve the issue.

PAWTEX

Assalamualaikum and greetings all.

We are students from Group 5 taking Computer Science in Data Engineering. For Technology and Information System subject, we have built a prototype named PAWTEX.

PAWTEX is an application that contains features that can protect computer from ransomware. There are three features provided;
1. Recognition and Response Extension (RRE) - connects data from various security solutions so they may cooperate to enhance threat visibility and shorten the time needed to recognize

2. Breaches Blocking System (BBS) - keeps an eye out for harmful activity on a network and, when it does   surface, it will respond by blocking it.

3. Trafficker - monitors on network traffics to alert RRE and BBS if any malicious threats appear

Users can choose to activate any desired features. Users can also activate all the features and all of it will cooperate to protect your computer from ransomware.
Please answer all these questions.

Diagram 6

1. Do you think PAWTEX can protect your computer from ransomware?

◯ Yes

◯ No

◯ Maybe

2. Are you satisfied with PAWTEX?

◯ Yes

◯ No

3. Please feel free to give us some feedbacks.

Your answer

Submit   Clear form

Diagram 7

REFLECTION

DAYANG FARAH FARZANA BINTI ABANG IDHAM (A23CS0071)

My dream is to accomplish excellence as a data engineer equipped with good technical skills, can handle multiple programming languages and be familiar with things related to data. This design thinking assignment has taught me how to solve problems in an effective way by using all the elements in it. By using design thinking, I can solve problems in my daily life in an efficient way. To improve my potential in the industry, I suppose soft skills are what I aspire to possess including communication skills, problem solving skills and have high leadership skills.

FARRA NURZAHIN BINTI ZAHARIL ANUAR (A23CS0079)

I am inspired to join the technology industry as a data scientist or data analyst. My goal is to use data analyst skills to help organisations and technology advancement by coming up with intelligent solutions. Design thinking provides five unique methods that help designers to solve issues. I can also detect customer difficulties more effectively thanks to design thinking. I hope to improve my potential by using the knowledge I've gained during my profession, especially by using the Design Thinking methods.

HARINI A/P SANGARAN (A23CS0081)

I aspire to be a successful data engineer in the future as I believe that the job scope of data engineers can possibly change the dynamic of industries. Design thinking has multiple phases that allows us to identify the problem and then find a solution accordingly. By using design thinking, resolving a problem could be much more efficient and faster. Thus, when design thinking is applied in working life, we could save much more time and work efficiently. To improve my potential in the industry, I have been working on my soft skills, mainly on my communication skills as I would be required to work with people on tasks every day.

SYARIFAH DANIA BINTI SYED ABU BAKAR (A23CS0183)

My goal with regards to this program is to be well educated in Information and Technology. The design thinking assignment has taught me to be more empathetic in understanding problems in order to come up with a well constructed solution. As a way to improve my potential in the industry, I need to be consistent in improving my way of viewing things and problems, preferably by following the Design Thinking phases because it is able to help me make a thorough and comprehensive plan to successfully solve a problem. Consequently, I will be able to produce a well planned solution for my problem.

TASK ASSIGNMENT

All members are assigned to specified tasks in completing the report. Farra was given the task to do the introduction and Ideate phase. Dayang was incharge of the Google form and Test phase. While Harini was assigned to do the Define phase. Lastly, Dania was

incharge of doing the Empathy phase. The rest of the report was done together by everyone. The prototype was also completed together by all of us.

Video link: https://youtu.be/Z6f8uyXInJ4?si=Mmpvk1Qlo9jVPmkG

REFERENCES

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & security*, *111*, 102490. Retrieved from https://www.sciencedirect.com/science/article/pii/S016740482100314X

Cisco (2023). What is XDR? Retrieved from https://www.cisco.com/c/en/us/products/security/what-is-xdr.html

Interaction Design Foundation, Dam, R. F., & Siang, T. Y. (2021). What is design thinking and why is it so popular? Retrieved from https://athena.ecs.csus.edu/~buckley/CSc170_F2018_files/What%20is%20Design%20Thinking%20and%20Why%20Is%20It%20So%20Popular.pdf

Gazet, A. (2010). Comparative analysis of various ransomware virii. Journal in computer virology, 6, 77-90. Retrieved from https://link.springer.com/article/10.1007/s11416-008-0092-2

Sangfor (2022). What are EDR Tools. Retrieved from https://www.sangfor.com/blog/cybersecurity/what-are-edr-tools-5-best-open-source-edr-tools