**Part 2: Product Implementation**

**(Script for Power point presentation)**

**Slide 1 and 2: INTRODUCTION**

**Maribeth:** Good evening everyone, I’m Maribeth and tonight together with my other team members, we will be presenting our project which is about “Password Generator”. Before we begin, please allow us to give a bit of a background about ourselves. Let me start with me. So, again, I am Maribeth Estimos. I work in a Community based Kindergarten as a Teacher here in Auckland and to be honest, I do not have any IT background at all prior to joining this course. Hence, it was a mix feeling during the time that we started as I am not sure how I will go during this learning journey but nonetheless, I am happy to be part of this team, especially being in my group as I am the only rose among the thorns (there’s only 3 of us! they’ve been very patient with me to all my queries) so without further ado, let me call my other team member to also give a bit of a background about themselves, Richard and Steven.

**Richard:**

**Steven:**

**Maribeth:** Thank you, Richard and Steven. Let me now, proceed to our presentation.

**Slide 3: AGENDA**

**Maribeth:** For tonight’s Agenda, we will discuss with you;

1. What is a Password Generator?
2. Then, me and Richard will share “Why we chose it as our project”
3. While, Steven will share the risks of password leaking and he will also introduce the Technologies and Methodology that we have used in this project. He will also share snippets of information how we split each part of the project among the group.

**Slide 4: WHAT IS A PASSWORD GENERATOR?**

**Maribeth:** Password Generator is a software tool that creates random or customized passwords for users. It helps users create a stronger password that provide greater security for a given type of access. Some password generators are simply random password generators. These programs produce complex/strong passwords with combinations of numbers, uppercase and lowercase letters, and special characters such as braces, asterisks, and slashes.

It is no secret how much effort we exerted to keep our passwords safe from hackers, who would like to have access to all electronic devices. Of course, no one would like their personal information stolen. I will give myself as an example, In my previous work place, we needed to change our password every 3 months for security reason and there were like 3 programs that required constant change of passwords and way back then, I have little to zero idea about password generator. I only had my tiny book with me where I kept and jotted down all the passwords I used. Thanks to technological developments that we have now to protect our personal information.

**Slide 5-8: WHY WE CHOSE THIS PROJECT?**

**Maribeth:** The main objective why we chose Password Generator to be our project is to help users who have to constantly come up with new passwords to ensure authorized access for programs and to manage a large number of passwords for identity and access management.

I have Richard on the line to give us more insights on why we chose this project.

**Richard:** Hello everyone, It’s me Richard. In addition to what Maribeth shared a while ago, Why we chose Password Generator as our project is also because we as team agreed that this comes in handy to all potential users as it can save you from memorizing hundreds of passwords every now and then.

Another objective of using a password generator is to create a strong and unpredictable password for all of your accounts.

I guess everyone here is aware that most websites have different requirements for passwords. Let me show you some example.

***Google Account*** asks for a password including characters, numbers and symbols. Microsoft needs to enter a password including two of the uppercase characters, lower characters, numbers and symbols.

Meanwhile, for ***Air New Zealand***, it asks for a password of at least 12 characters, but it cannot contain username, or email address.

Here are some of the most common used passwords that users are using;

‣123456

‣1234567890

‣ qwert

‣ qweryuiop

‣ 123456qwerty

‣ 1qaz2wsx

Do they look familiar to you? According to Wikipedia, they are all weak passwords and they are in the top 20 weakest passwords.

I have here another set of “Top 25 most common passwords by year” according to Splashdata.

Let me now call Steven to further explain the Risks of Password Leaking. He will also share what technologies and methodology we used in this project.

**Slide 9: RISKS OF PASSWORD LEAKING**

**Steven:** Thank you Richard, Hi again everyone!

Think about what will happen if your password has been leaked. Of course, no privacy anymore. Of course, all of your relevant information will be exposed. If the account related with purchasing, that usually means money loss. Sometimes, your account will be used in ID frauds. Even more, we are likely to use the same password in all the website because it is hard to remember all kinds of passwords when they are totally different. That is to say if one of the websites didn’t protect well your password, your personal data/information is at risk.

**Slide 10-11: TECHNOLOGIES and METHODOLOGY**

**Steven:** Now, let’s move on to the Technologies that we’ve used. As my team mates, mentioned earlier. We are more likely to use the password generator in all electronic devices and all of the operation systems. Therefore, we decided to develop it as a web base software. Then, we can use it wherever and whenever we have access to internet. The coding language would be java script and html – which we have learned in this course.

The methodology we choose to use is waterfall. We have four reasons for using waterfall. Firstly, for this project, the requirements are explicit. They are;

|  |  |
| --- | --- |
| 1.    Allow input of various input parameters on password such as Password Length, Include Symbols, Numbers, Lower/Upper case Characters, etc |  |
| 2.    Save the above parameter :( save all the settings above for later use) |  |
| 3.    Generate a random password for based on the above parameters |  |
| 1. Copy function to copy the generated password to the buffer (like Control + C) |  |

Secondly, it is a relatively simple system. It only has four requirements.

Thirdly, it can only be used in certain circumstance, such as, registering an account or reset a password.

Lastly, it is a course project; it is unlikely to be changed in the future

**Slide 12-13: TEAM WORK**

**Steven:** How does our team work?

We divided the system into three parts.

The frontend part responsible for interacting with client users. It collects the parameters and initiates a request to the server - nodejs. When server finished processing, it will display either some error information or the password that server part has just created. Another function of this part is to copy the password to the clipboard.

The server part has been divided to two items. One is for dealing with the client request, responsible for parsing parameters and calling the third part, the module part, to create an appropriate password. Of course, before that, it will need to check all the parameters to make sure these parameters are valid. When a password is created by the module part, it will pack all the data and transmit them to the frontend. If all the parameters are correct, an additional job need to do in this part is to save them in a cookie so that the user can use them in the next time.

Maybe the module part is the purest, but it is not the simplest. It is in charge of creating a password. This is the main part of the project.

In this project, Richard finishes the part 1, Steven, me, the part 2 and Maribeth did Part3.

Let us proceed to our reflections, Maribeth will shares hers follow by Richard then me.

**Slide 14: REFLECTIONS**

**Maribeth:**

**Richard:**

**Steven:**

**Slide 15: REFERENCES**

**Maribeth:** These are the references that we used for the entire project from Part1: System Proposal up to the Part2: Product Implementation

**Slide16: Q&A**

**Maribeth:** And from here we end our presentation. We appreciate your time and Thank you for being with us as we shared our presentation.

Now, it is time for Questions & Answers.