Understanding Security and risks attributed with Video game privacy

Following American psychological association guidelines

In partial fulfillment of requirements of GPG220

Noaman Khalil

SAE Institute Dubai

Understanding Security and risks attributed with Video game privacy

Abstract

The goal of this paper is explore the analysis in regards to Security and risks as it relates to data and storage in video games with an additional factor of in game risk. The research also aims to take into account the privacy risks in regards to an existing project and focus on making sure that the personal data they enter in the premises of the game is safe and secure.

Introduction

In the modern world with the boom of technology and the constant change of it, the challenges associated to security and protection of the user's data is of the highest priority as this is a fundamental right of every user which is especially so in regards to video games with the increase in trends moving towards online gaming which require large amounts of customer data, this can be a wide variety of data which can entail personally identifying information or non- personally identifying information. Data such as this can be for example age and physical address alone could identify who an individual is without explicitly disclosing their name. The protection of such data is widely referred to as data privacy.

History

With the advent of the internet and online shopping there was an increasing need for security with regards to the data of users however this has become a more popular concern among users during the 21st century however this was the beginning in a larger spew on online services which required a large amount of the users data to be used such as online MMORPGS which saved the users billing address, Email IDs , passwords and even the players habits , likes & dislikes through the use of machine learning and in game data analysis which is a much recent trend which is used by many large game development studios

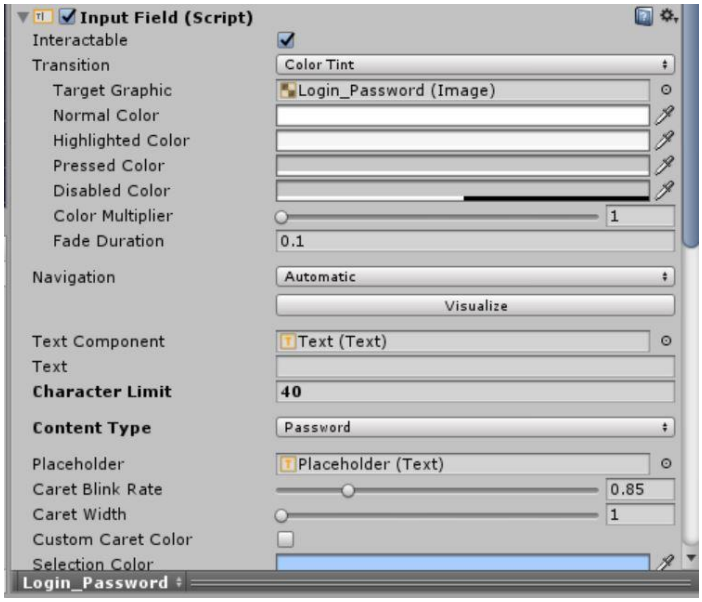
such as Game Loft according to the “INNOVATI ON PROCESS IN CREATIVE INDUSTRIES: INSIGHTS FROM THE MOBILE GAMES SECTOR”. This approach is commonly referred to as being “Data-Driven” approach according to techopedia . (Techopedia, n.d.)

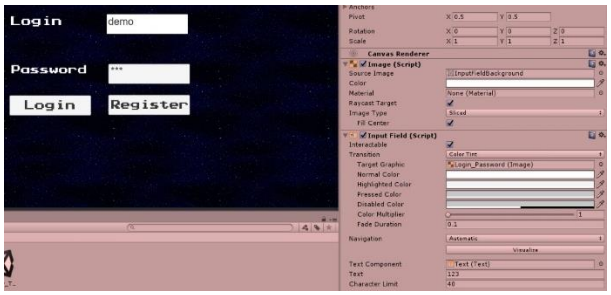
Again, the data Driven approach is used to analyses the players likes, dislikes based on their usage habits and other information which is later used to offer the user a much better user experience however this is seen as an invasion of privacy which is often agrees to upon signing up and not reading the terms and conditions which often sign such data or the right to collect this data to large companies which in turn waives our rights to privacy.

Data protection example

For the project I have been working on I have taken the level of security very highly by utilizing many security measures in code itself to make sure the users data is secure once it reaches the server , below are the precautions taken.

The first precaution taken would be salting the password of the user, in unity this is a simple drop down menu under the input field which allows the type to of string to be a password which would be slated in unity. Another option is adding a character limit which is shown in the inspector window below. Along with a comparison of string before and after salting, this makes sure that the password is not viewed by any 3rd parties screen-peeking into the user’s machine. Salting would be taking a string and converting it into a “*****” format from a string received “1234”.





Apart from salting there are some other techniques also applied to the project in the case of the code which works with the password used above, all the variables used in the code are private but serialized which allows them to have the benefit of dragging and dropping in the inspector window while the fields are still private by using the "[SerializedField]" before the private variable as can be seen in the snippet of code, there are only a limited amount of data protection methods which can be employed by the client side however the data which is stored and processed on the server are much different.

```
11  public class LoginSystemCs : MonoBehaviour
12  {
13      [SerializeField]
14      private string urlRegister , urlLogin;
15
16  /* [Header("UserInfo")]
17      public string UserName, UserPassword, UserEmail, InputName, InputPassword;*/
18      public bool UserLoggedIn,SamePass, loginValidated;
19      [Header("Login")]
20      [SerializeField]
21      private  Text LoginNameText, LoginPasswordText;
22      [Header("Register")]
23      [SerializeField]
24      private Text EmailText , UserText;
25      [Header("Register Password ")]
26      [SerializeField]
27      private GameObject PasswordTextPlaceHolder, PasswordVerifictationTextPlaceHolder;
28      [SerializeField]
29      private Text PasswordText, PasswordVerifictationText;
30
31      [SerializeField]
32      private GameObject ConnectingPanel;
33
34      [Header("OnScreen error")]
35      [SerializeField]
36      private Text[] updatetxt;
37      private bool isEmailValid;
```

For the server , the code is written in PHP as this is a language understood by the server and 00webhost is used for free hosting

```
75
76  //$encryptedPass = md5 ($password);
77  $hashed_password = password_hash($Password, PASSWORD_DEFAULT);
78  /*while ( $doesUserExist == true || $doesEmailExist = true)
```

Understanding Security and risks attributed with Video game privacy

however it has its limitations , thee limitations are enough in the confines of a student project . The Php side of things there is a system in place to encrypt the most important data of the user, the password. For all intents and purposes the best in class encryption was not used as the scale of the project is very limited thus the inbuilt encryption in Php had to suffice however this is very complex in its own right and an example code snippet is shown in the image below along with an example of how encrypted code looks like. Further reading on hashing can be found in the reference. (Php, n.d.)

The inbuilt hash is the simplest to use, thus it is used above as even the most advanced encryption methods can be broken using modern techniques which is evident according to yahoo hack in 2016. ("Important Security Information for Yahoo Users," 2016).

Above are two examples of passwords which are encrypted and not encrypted which is the best example to keep the users data private.

Conclusion

With technology pushing the boundaries of progress the question of security and risk attributed with the users safety will always remain a very controversial & sensitive matter in the eyes of the user but we as developers must do our very best in order to meet the expectations of the user with regards to data privacy .

References

Php. (n.d.). PHP: password_hash - Manual. Retrieved April 5, 2018, from http://php.net/manual/en/function.password-hash.php

Important Security Information for Yahoo Users. (2016, December 14). Retrieved from https://yahoo.tumblr.com/post/154479236569/important-security-information-for-yahoo-users

Techopedia. (n.d.). What is Data Driven? - Definition from Techopedia. Retrieved April 5, 2018, from https://www.techopedia.com/definition/18687/data-driven

Granados, C., Pareja, M., & Bernardo, M. INNOVATION PROCESS IN CREATIVE INDUSTRIES: INSIGHTS FROM THE MOBILE GAMES SECTOR.