**ADDITIONAL SECUIRTY FOR USER AUTHENTICATION**

**ABSTRACT:**

The outcome for this project would be as described below.

When a user logins to any application, an extra layer of security will be provided in the form of security code for the user authentication.

Chances of unauthorized access to the secured application with the legacy user authentication (Username & Password). The solution is to introduce second factor authentication in the form of one-time passcode (OTP) sent to their mobile or other devices.

We can avoid cybercrimes in user authentication by introducing an additional layer of security in the form of dynamic one-time passcode sent to their authorized mobile or other devices.

**INTRODUCTION:**

In regard to the current situation, the usage of online applications has augmented in all the sectors because of the lockdown. This increased usage has given rise to more cybercrimes. The necessity to increase the security on user authentication could reduce cybercrimes. So, the aim of this project is to implement the security component as a plugin that can easily couple with any existing application. By integrating this security component, it will add an additional security layer for the user actions.

Research Question: How can we implement an additional security component to overcome the cybercrimes for user authentication?

**BACKGROUND:**

The scope of data analysis is minimal in this application. But will make sure to follow GDPR guidelines.

As it requires to initiate the security in the form of security code that needs to be sent to the user, will get the consent from the user.

The application’s aim will be fulfilled if the user connects to the internet and an extra security protection would be provided in the form on security code for the user authentication. So this procedure would be followed to test the application and to determine the requirements fulfillment for the project.

The main challenge would be understanding encryption and decryption algorithms. As this project is irrespective of any specific application, so it should be able to integrate with any kind of application which are implemented in different technologies and on different platforms.

The project plan is described as follows:

1. Requirements Analysis
2. Technical Architecture
3. Low level design
4. Development
5. Junit testing

The comparison is made between the application with additional security component developed (Username, Password & OTP) against legacy application (Username & Password).

|  |  |
| --- | --- |
| **Advanced security authentication** | **Legacy authentication** |
| More secure because of two levels of authentication | Less secure because of single layer authentication |
| Less chances of hacking due to dynamic one-time passwords at the second level of authentication | More chances of hacking due to static passwords |

**METHODS:**

Agile methodology is used to develop the application. Agile methodology is widely used because the requirements can be changed whenever required and the deliverables for a project can be done in frequent intervals which are possible not possible when using traditional methodologies like Waterfall model.

The application development is divided into sprints. The length of each sprint will be 2 weeks. The different stages in agile methodology are;

1. Requirements: Analyze the project and based on the analysis, define the requirements for the project.
2. Development: Design and develop the application based on the requirements defined in the above step.
3. Testing: System testing to check the aim of this project is fulfilled

**REFERENCES:**

|  |
| --- |
| 1. T. Dressel, E. List and E. Florian, "SecuriCast: zero-touch two-factor authentication using WebBluetooth," pp. 1-6, 2019. |
| 1. H. Dianqi, C. Yimin, L. Tao, Z. Rui, Z. Yaochao and H. Terri, "Proximity-Proof: Secure and Usable Mobile Two-Factor Authentication," pp. 401-415, 2018. |
| 1. P. Shrestha and N. Saxena, "Listening Watch: Wearable Two-Factor Authentication using Speech Signals Resilient to Near-Far Attacks," pp. 99-110, 2018. |
| 1. P. Mayer, C. Schwartz and M. Volkamer, "On The Systematic Development and Evaluation Of Password Security Awareness-Raising Materials," pp. 733-748, 2018. |
| 1. E. Esiner and A. Datta, "Layered security for storage at the edge: on decentralized multi-factor access control," pp. 1-10, 2016. |
| 1. D. Preuveneers and W. Joosen, "SmartAuth: dynamic context fingerprinting for continuous user authentication," pp. 2185-2191, 2015. |
| 1. B. Chapuis, O. Omolola, M. Cherubini, M. Humbert and K. Huguenin, "An Empirical Study of the Use of Integrity Verification Mechanisms for Web Subresources," pp. 34-45, 2020. |
| 1. R. K. Konoth, "How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication," pp. 405-421, 2017. |
| 1. B. Adida, "Beamauth: two-factor web authentication with a bookmark," pp. 48-57, 2007. |
| 1. J. Olli, *Intelligent two-factor authentication – Deciding authentication requirements using historical context data,* p. 116, 2014. |
| 1. D. Dasgupta, A. Roy and A. Nag, "Multi-Factor Authentication," pp. 185-233, 2017. |
| 1. S. Jarecki, H. Krawczyk, M. Shirvanian and N. Saxena, "Two-Factor Authentication with End-to-End Password Security," pp. 431-461, 2018. |
| 1. N. Paudel and R. . C. Neupane, "A General Architecture for a Real-Time Monitoring System Based on the Internet of Things," pp. 1-12, 2019. |
| 1. R. Peeters, J. Hermans, P. Maene, K. Grenman, K. Halunen and J. Häikiö, "n-Auth: Mobile Authentication Done Right," pp. 1-15, 2017. |
| 1. S. Kiljan, K. Simoens, D. D. Cock, M. V. Eekelen and H. Vranken, "A Survey of Authentication and Communications Security in Online Banking," 2016. |