Accufier: The Accurate Verifier for Keeping Flight Booking Applications More Secure Using WSN

V.M. Karthik Sai

UG Student, B. Tech, Computer Science and Engineering, VIT Chennai, Vandalur-Kelambakkam Road, Rajan Nagar, Chennai, Tamil Nadu, India

Abstract - *The most common mistake that is noticeable nowadays is that many people use same passwords for different accounts in different applications. The flight booking websites and applications currently provide the users with passwords(temporary) which aren't very secure at all and this needs to be protected as fast as possible or else the level of cyber-crime activities will start raging automatically as it will become easy for the hackers to tap into other people's accounts in flight booking applications. My opinion is to introduce or add a two-step verification called "Accufier" which uses a WSN (i.e. Wireless Sensor Network) that acts as an extra layer of security to his/her account apart from the PNR and passport number of a person while making their account and also have that verification process always whenever the person is booking a flight.*

Key Words: Accufier, two-step verification, Wireless Sensor Network, security.

1.Introduction

The cybercrimes have increased a lot due to the lack of proper network security across many flight booking applications and because of that there has been an increase in fake tickets, fake passports and fake names. Accufier solves many of these problems from happening to the real/innocent users by keeping their flight booking app accounts more secure by having two factor authentications protected by a powerful WSN (wireless sensor network). The name has been given "Accufier" mainly because it's an accurate verifier and keeps every person's data and booking process more secure. Accufier has two levels of authentication which is secured by a unique WSN called Accufier-WSN which protects user's data (especially face data) and information to a much greater extent. One of the two steps in the authentication process of Accufier includes a new type of face scan called as FaceBolt Scan which scans the user's face multiple times before it can be assured that it is verified accurately and then only lets the user proceed to the next step. FaceBolt scan is also secured by the Accufier-WSN and involves three tests in verification for the first time when the user creates an account.

Talking in terms of merits of the Accufier, it has a regulated system throughout the authentication process. The two-step authentication process with face code generation makes it even more secure. The face scanner of the Accufier makes sure that every inch of the details of the face is scanned perfectly and even if someone else tries to get their dirty hands into another person's account by scanning a photo of another user, the face scanner will easily make out that it's fake and hence the scan test fails immediately and that person gets logged out of the app. Accufier can be a time-consuming process at times which means that if the user makes a mistake in the second step of the authentication process, the user will have to scan his/her face again three times for the three face scan tests in the previous step but this is only for the good of the users as it will keep their accounts and data more protected and safer.

2. Working Process of the Accufier

Accufier is a two-factor authentication secured by Accufier-WSN which asks the user first for generating a unique face code by scanning every part/details of the face (FaceBolt Scan) accurately under all dim and bright surroundings with the webcam or camera (mobile phone) turned on. The unique face code generated is a 3-digit code which gets saved in that particular username for that moment when logged in the flight booking app. After the face code is generated for that time, in the next step it asks the user to fill in the 6 blanks which pops up in which the first three blanks should contain last three characters of that person's username followed by the 3-digit face code which should be entered in the remaining three blanks making the authentication process more secure and protected. After these two steps get verified perfectly, the user can then proceed to book and confirm his/her flight ticket before transaction or payment for the flight ticket. When the user makes an account in the flight booking app or website for the first time, it will ask them to add their face data for Accufier security authentication process. When the user lets his/her face to be scanned by the FaceBolt Scan through the camera or webcam, Accufier makes sure that every detail of the face is completely and accurately scanned by asking the user to show each side of their face (i.e. left, right and front part of the face) till the scan gets completed. When the scan is completed, the face data will be saved in that person's account secured by the Accufier-WSN in that respective flight booking app where no one can access it including the users themselves. If the user wants to update their face data, it can only be done with the help of scanning their current face (with their current face data) to see whether the person who is wanting to update is the same person and not anyone else. In this way, it can be ensured that no one else other than that of the user can get access to their account and flight booking process. So, whenever a user wants to book a flight in a flight booking app in future after giving his face data to Accufier after account creation, the first step of authentication where a face code gets generated for the user takes place in three tests of the face scan.

The first test asks for the user's face to be scanned on their right side followed by the second test which asks for the user's face to be scanned on their left side and finally the third test asks for the user's face to be scanned on their front. Only after these three tests of the first step authentication gets approved and a face code gets generated, it takes the user for the next and final step of authentication.

If any one of these three tests fail during the face scan, then the user gets logged out of the app and he/she has to wait for 10 minutes until their next login. After passing the first step of authentication, if the user makes a mistake or doesn't get approved in the second step of authentication after filling the 6 blanks, then he/she will automatically get back to their previous step of authentication where the user has to scan his/her face again for approval.

In this way of two-step authentication secured by the Accufier-WSN, there can be an environment in the app where the cyber-crimes can be reduced and even prevented in a great manner.

3. Role of the Accufier-WSN

The Accufier-WSN is a unique WSN which protects the authentication process in a manner in which hackers can't easily break into other people's flight booking application accounts. Accufier-WSN has sensor nodes which are dispersed in a ranged manner in a sensing field and those systemized sensor nodes gather the required data and hand it over to the base station (also known as the sink node) in order to promote the communication or transference through different routing protocols. The FaceBolt Scan takes place with the help of the Accufier-WSN where the position of the sensor nodes gets changed to easily define the area of sensing. This type of WSN organizes and heals by itself and the mechanism of security it provides to the Accufier's authentication process is synchronized with time due to its kinetic nature. This wireless sensor network is specially and carefully modelled to identify bugs by figuring out the position of the sensor nodes and removing the bugs immediately.

4. Accufier-WSN Problems

The only problems that can happen could be on the assertion or authentication, integrity, privacy and accessibility. There can be an attack during the starting phase when the systemized sensors start to capture the location of the adjacent sensor nodes and this type of attack could be adverse at times. Sometimes, there can be packet spoofing where the attackers (hackers) make their own IP packets based on the location of the target/victim but makes the hacker's IP field is altered in order to hide the hacker's IP address location. The hackers can also get access to the victim's information and sprawl virus through their account first in the flight booking applications followed by infecting their computer slowly. But the Accufier makes sure that most of these problems are avoided and also prevented to large extent due its highly secured authentication process.

5. Solutions and Analysis

The level of security in the flight booking applications can be maintained at a decently high level by implementing key management which keeps hackers away from attacking targets. In this method, keys are generated among the systemized nodes in a responsible and protected manner. The network will have to be supported with addition of nodes and since those nodes in the Accufier-WSN will be having power constraints and computational constraints, the protocols used in key management will be notably light in weight. We can also prevent jamming attacks on targets/users by applying variations like hopping of frequency and spreading of the code in spread-spectrum communication.

6. Conclusion

The process of the Accufier's two-step authentication and the role of the WSN discussed above will be really helpful to not only the flight-booking applications but also to any other application in many ways by keeping accounts and their computers safer. So, I strongly believe that the implementation of my idea used in the Accufier along with Accufier-WSN in flight booking applications will provide organizations with much higher network security than ever before without making it difficult for the user in any way possible.

7. References

[1] Computer Networking: A Top-Down Approach Featuring the Internet, J.F. Kurose and K.W. Ross, 6th Ed., Pearson Education, 2012.M. Young, The Technical Writer's Handbook. Mill Valley, CA: University Science, 1989.

[2] www.valencynetworks.com

[3] www.researchgate.net