DESIGN AND DEVELOPMENT OF GEOGRAPHIC LOCATION BASED SECURED AUTHENTICATION SYSTEM

Borse Yogeshwari Suklal,[1] Dr. Anil Kumar[2]

[1] *Research Scholar, Computer Science & Engineering, SSSUTMS, Sehore, M.P. India*
[2] *Professor, Computer Science & Engineering, SSSUTMS, Sehore, M.P. India*

ABSTRACT

Authentication is the only method which protects information or data of an individual or organization from a second party to access. Based upon the confidentiality of particular data or information, the level of authentication depends. Now-a-days, all this data and information what the discussion is about is getting digitized all around the world. For this digitized data or information to be secure, a proper authentication procedure must be set. This arise the need for an authentication secret which belongs to the category "Something people know" to come into picture. These secrets authenticate each secret holder as the authorized legitimate user to access their particular account. Technology is getting more advanced every day, existence and usage of online applications increase. This requires each user to remember more such authentication secrets or to reuse the same secret to access multiple accounts.

Keyword : *Data , authorized, User , digitized data*

The location verification mechanism takes into account the following parameters:
1. Two sets of location coordinates from two different location sources;
2. IP address of the client (smartphone);
3. MAC (Media Access Control) address of a nearby access point with the strongest signal.

1) Registration

During the registration process the location information of the user is collected by the LBC running in the smartphone, sent to the server and stored in the database. This information includes the latitude (LAT), longitude (LNG) and accuracy (in a certain unit of measurement e.g. meters) as obtained from the location API of the smartphone. As shown in Figure4.4, it represents the exact location and a range that the user wants to signify as an authorized location, from which access can be granted.

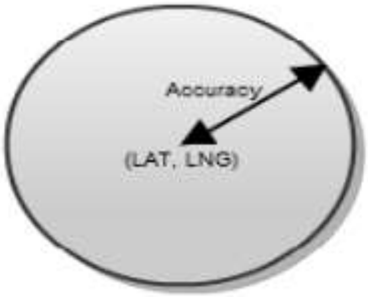

Figure 4.4 Location information

In addition, the MAC address of the strongest nearby WiFi access point is detected and stored in the database as an additional parameter. This value is obtained by comparing the RSSI (Received signal strength indicator) of all detected Wi-Fi signals and choosing the one with the highest signal strength. All of these values are then stored in the database as part of the user registration information.

2) Authentication and authorization

During the authentication and authorization stage, the location of the user is detected and verified by the LBID server using the following mechanism:

Step 1:

In most of the major smartphone platforms there is usually more than one source (APIs) for obtaining location.

For example, on Android there is the normal Android Location API, Skyhook, etc. This is the same for iOS, Blackberry and others. Based on this, our location verification utilizes two sets of location coordinates (LAT, LNG and accuracy) that are obtained from two different location APIs. In this way, the reliability and accuracy of the location is ensured since the result does not depend only on one source.

These two location coordinates are then compared to see if the location areas they represent overlap. In normal circumstances these two areas should always overlap, as shown in the left part of the following Figure 4.5. If there is no overlap at all between these two location areas, as shown in the right part of the following Figure 4.5, it is a good indication that one or both of the sources of location are not correct and may have been compromised through one of the methods described previously.

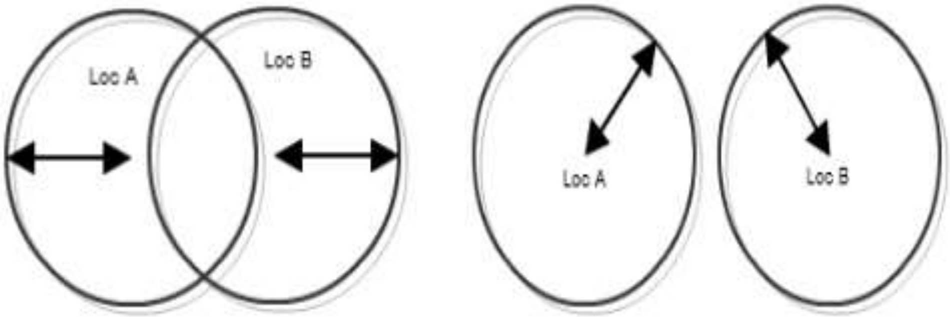

Figure 4.5. Step 1 of location verification

If there is no overlap location, the verification fails and the process stops. If the two results overlap, the process continues to step 2.

Step 2:

The public IP address of the client as observed by the server is recorded and used to estimate the location coordinates (LAT, LNG and accuracy) of the user using IP2Location service [16]. The result of this is then compared with both sets of coordinates from Step 1 to see if location areas are contained within the area represented by the coordinates from Step 2.

Both location areas, described in Step 1 should be contained within the location area that is calculated based on the IP address, as shown in Figure 4.6. The location area obtained from IP address is usually of lesser granularity which covers a bigger area and should contain both locations described in Step 1, which are more precise with smaller areas. If both locations coordinates are not contained within the larger range of area from the IP address then it is good indication that one or both of the location coordinates from Step 1 are inaccurate and may have been spoofed.

Therefore, the location verification process fails and stops if both locations from Step 1 are not contained in location from Step 2. If this check is successful the process continues to the final Step 3.

Step 3:

The MAC address of the access point, with the strongest detected Wi-Fi signal is captured and compared to the one saved during the registration process. If the two values do not match the verification process fails and stops. On the other hand if the values match, the verification process succeeds and becomes completed.

These three steps provide a series of checks to ensure that user’s location as detected and reported by the LBC is correct and has not been spoofed or tampered with. After all the steps have been completed successfully, there is a high confidence in the validity of the location reported by the user.

The most accurate location result from Step 1 – the one with the highest accuracy (small range) represents the location of the user and thus is used to make further location based authorization decisions depending on the authorized location registered by the user.

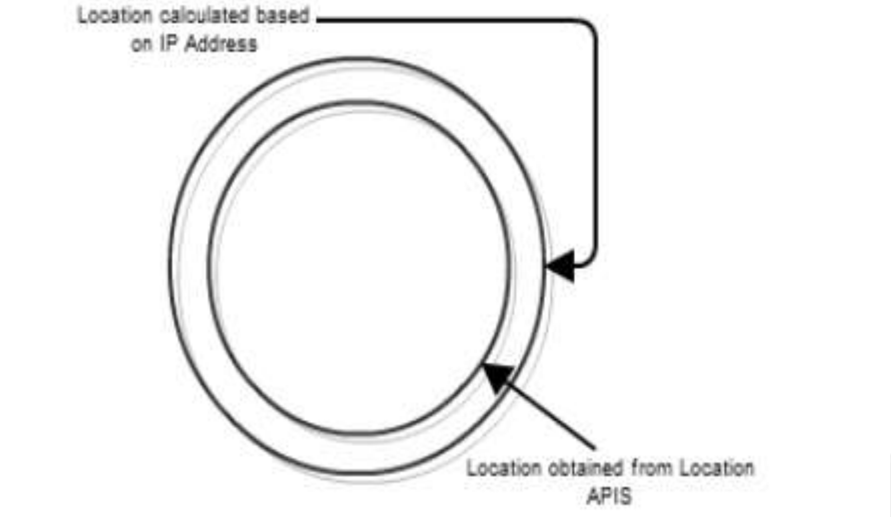
Location calculated based on IP Address
Location obtained from Location APIS

Figure 4.6. Step 2 of location verification

CONCLUSION

The proposed solution provides comprehensive protections for transmission, procession and verification of location information. For location verification, we propose a hybrid approach, which combines various technologies. This approach improves the confidence of verification results, compared with other solutions where only one factor is used for location verification. As a result, our location-based authentication and authorization mechanism becomes more secure and valid. The use of location however is just the first step in using contextual information for improving security mechanism.

REFERENCES

1) YounSun Gho, L. Bao, M.T. Goodrich, "LAAC: A Location-Aware Access Control Protocol", Mobiquitous, Third Annual International Conference on Mobile and Ubiquitous Systems, Networking, and Services, pp.1-7, 2006
2) Denning, D. and Macdoran, P., “Location-based Authentication: Grounding Cyberspace for better Security”, Computer Fraud & Security, 1996(2), pp.12-16.
3) Jansen, W. & Korolev, V., “A Location-Based Mechanism for Mobile Device Security”, in WRI World Congress on Computer Science and Information Engineering, Los Angeles, California USA, pp. 99-104, 2009
4) Anon, “40 Percent of U.S. Mobile Users Own Smartphones; 40 Percent are Android | Nielsen Wire”. Available at: http://blog.nielsen.com/nielsenwire/online_mobile/40-percent-of-u-smobile-users-own-smartphones-40-percent-are-android/[Accessed September 19,2019].
5) Anon, “Gartner Says Sales of Mobile Devices in Second Quarter of 2011 Grew 16.5 Percent Year-on-Year; Smartphone Sales Grew 74.
6) Percent”. Available at: http://www.gartner.com/it/page.jsp?id=1764714 [Accessed September 19, 2019].
7) Anon, “IMS Research - Electronics market research & consultancy”. Available at: http://imsresearch.com/pressrelease/Global_Smartphones_Sales_Will_Top_420_Million_Devices_in_2011_Taking_28_Percent_of_all_Handsets_According_to_IMS_Research [Accessed September19, 2019].
8) S. von Watzdorf and F. Michahelles, “Accuracy of positioning data on smartphones,” 2010, pp. 1–4.

9) Bao, L., “Location Authentication Methods for Wireless Network Access Control”, in IEEE International Performance Computing and Communications Conference (IPCCC), Austin, TX, USA, pp. 160167, 2008.
10) Takamizawa, H. & Kaijiri, K., “A Web Authentication System using Location Information from Mobile Telephones”, Proceedings of the IASTED International Conference Web-based Education (WBE 2009)
11) Ardagna, C.A., Cremonini, M., Capitani di Vimercati, S., Samarati, P., 2009. Access Control in Location-Based Services, in: Bettini, C.,
12) Jajodia, S., Samarati, P., Wang, X.S. (Eds.), Privacy in Location Based Applications. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 106–126.
13) He, W., Liu, X., and Ren, M. Location Cheating: A Security Challenge to Location-based Social Network Services. In Proceedings of CoRR. 2011.
14) Anon, Location Spoofing Attacks on the iPhone and iPod. Available at: http://www.syssec.ch/press/location-spoofing-attacks-on-theiphone-and-ipod [Accessed November 15, 2019].
15) J. Chiang, J. Haas, and Y. Hu, “Secure and precise location verification using distance bounding and simultaneous multilateration,” in Proceedings of the second ACM conference on Wireless network security. ACM, 2009, pp. 181–192.
16) M. Balakrishnan, I. Mohomed, and V. Ramasubramanian, “Where’s that phone?: geolocating IP addresses on 3G networks,” in Proceedings of the 9th ACM SIGCOMM conference on Internet measurement conference. ACM, 2009, pp. 294–300.
17) KATZ-BASSET, E., JOHN,J., KRISHNAMURTHY,A., WETHERALL, D., ANDERSON, T., AND CHAWATHE, Y. Towards IP geolocation using delay and topology mesurements. In Proceedings of the ACM SIGCOMM Internet Measurement Conference (October 2006).
18) Anon, IP Address Geolocation to Identify Website Visitor’s Geographical Location. Available at: http://www.ip2location.com/ [Accessed October 31, 2019].
19) Von Watzdorf, S., Michahelles, F., 2010. Accuracy of positioning data on smartphones. ACM Press, pp. 1–4.