Volume 5, Issue 3
June 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Global Position System Location-Based Authentication (KERBEROS AS AN EXAMPLE)

Abdelmajid N T[i], Mahmoud K W[ii]

[1]Department of Computer Science, Zarqa;a University, Jordan

[2]Department of Internet technology, Zarqa;a University, Jordan

E-mail: nabihtj@yahoo.co.uk , kwkmmsy@yahoo.com

ABSTRACT

Authenticating user for granting permission of action a critical asset or service is a prerequisite for any secure information system. Security mechanism such as password, smart card or token, challenge response, and face recognition or finger print have commonly been used to identify and authenticate the users identity before get access to the service. However, the possibility to reveal the identity of the user in unauthorized way still remains open. Recently, works have been focused to use the user's physical location to increase the strength of user's identity protocol. This paper proposes anew phase for mutual authentication using Global Position System (GPS) to verify the user identity. This work implements the new idea using Kerberos authentication protocol as an example. The results of the discussion are compared with the existing techniques to demonstrate the merits and capabilities of using GPS signatures in-order to increase the authenticity of the user identity.

Keywords: Authentication, Kerberos, GPS signatures

1. INTRODUCTION

Ensuring information systems security has been a crucial challenge since medieval times and remains so to date. Users have been perturbed from this challenge. At all times, prevent interference from undesirable element in the personal information and other critical assets are source of major concern. Recently, the world turned to use online in all walks of life, especially after the Internet revolution. This rapid development in Internet as well as overall communications accelerated the work resulting in increased efficiency and productivity, but unfortunately it also increased opportunities for hackers to practice their undesirable act. This placed huge responsibility on researchers and industry community to develop methods and technologies to secure information system communication. Therefore, authenticate the user at an appropriate level is one of the important prerequisite for secure the overall system.

There are several authentication protocols from password based system to secure shell using strong encryption techniques such as Rivest, Shamir and Adelman (RSA), Data Encryption Standard (DES) or Message Digest version 5 (MD5). These protocols commonly rely on user performance. There is a direct relationship between the proficiently of the user and the strength of the security protocols. We need to choose the appropriate authentication technique based on the system specific context, i.e., complexity, usability.

This paper proposes an innovative phase for mutual authentication using Global Position System (GPS) to verify the user identity. Thus this work aims to improve security protocols based on the identified user location.

The rest of the paper is organized as follows. Section 2 presents an overview of GPS signal and how it can be used to authenticate the user's identity. Section 3 provides the proposed idea using Kerberos protocol as an example by three different faces. Finally discussion and limitations present in Section 4 and conclusion at the end.

2. GPS SIGNAL: C/A AND P- CODE

Each GPS satellite transmits two signals; a secure encrypted signal exclusively for military users called P(Y) code signal and a non-secure civilian signal called coarse acquisition or the civilian code (C/A)[1,2,3]. The length of P(Y) code is 6.1871×10^{12} bits long and repeats only once a week [4]. The military signal designed to resist electronic attack. P(Y) code encrypted by modulating with the W-code to generate the Y(Y) code in order to prevent any attacks by unauthorized users. The military signal is not easy to spoof or jam. It has a high level of accuracy. Moreover, P(Y) code has a good property, which is user can identify the location if s/he have a snapshot of received P(Y) code of his/her position, on the other hand, it is difficult to ascertain what P(Y) code should have done if s/he know where s/he are [5]. Again, using the facilities of P(Y) code increases the confidence of using it safely. In addition, GPS gives an accurate location output [5]. The increased security of the GPS has been discussed by many researchers in [2,3,6,7].

1.1 GPS FOR AUTHENTICATION

As stated previously, we proposed to use GPS signature to authenticate the user identity, in particular by using the

Volume 5, Issue 3
June 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

P(Y) code. A user needs to store his/her P(Y) code in the server to verify his/her physical address signature. Therefore, if the system could in advance know the possible user locations then the P(Y) signal could serve to publicize the location of the user profile as well as verify the user identity. GPS however used only outdoors in the sense that the receiver should have a direct "view" to at least four GPS satellites. In the next section, details of the proposed idea using Kerberos protocol as an example with the facility of the GPS.

3. PROPOSED IDEA USING KERBEROS AS AN EXAMPLE

$$1: A \rightarrow S: A, B$$
$$2: S \rightarrow A: \{N_a, B, K_{ab}, \{N_s, K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$$
$$3: A \rightarrow B: \{N_s, A, K_{ab}\}_{K_{bs}}, \{N_a, A\}_{K_{ab}}$$
$$4: B \rightarrow A: \{N_b + 1\}_{K_{ab}}$$

Fig. 1. Kerberos authentication messages

In this section, we add user's physical position address by adding GPS parameter into the existing Kerberos message. Although that the civilian signal is not safe, we use it to prove that the quality of the idea due to the long process that should be taken with the military side to have the military signal. This Address can be determine by a GPS receiver. The physical address should be included in all communicating messages. The server maintains a database of a list of legitimate users' positions addresses. Having these, addresses will enable the server to test out the availability of a user's position address before allowing the users to utilize the services. Next is to demonstrate three different approaches of this new idea. Phase1 controlled by the server and phase 2 and 3 controlled by the user. Right parts of the phase's figures shows the messages exchange among users and server within the phases.

1.2 Phase 1- Check authenticity of the user location

$$1.A \rightarrow S: A, N_a, B$$
$$2.S \rightarrow A: \{N_s, GPS_b, B, K_{ab}, \{N_s, GPS_a, K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$$
$$3.A \rightarrow B: \{N_s, GPS_a, K_{ab}, A\}_{K_{bs}}, \{A, GPS_a, N_a\}_{K_{ab}}$$
$$4.B \rightarrow A: \{GPS_b, N_a + 1\}_{K_{ab}}$$

Phase 1: GPS with Kerberos protocol

In this phase, the task of confirming the authenticity of the location falls within the responsibility of the server. User *A* sends a request to obtain the key, used to communicate with the user *B*. The server then sends response to the user *A* with *a* special ticket ($\{N_s, GPS_a, K_{ab}, A\}_{K_{bs}}$) to be sent by *A* to *B* through message 3. New procedures were added for the use of the GPS; server uses the list of legitimate users' physical location addresses, so far server can add *A*'s physical address to the ticket ($\{N_s, GPS_a, K_{ab}, A\}_{K_{bs}}$) *and* the B's physical location address to the message (N_s, GPS_b, B, K_{ab}). Message 3 has both a ticket and authenticator. The ticket ($\{N_s, GPS_a, K_{ab}, A\}_{K_{bs}}$) is encrypted by K_{bs} and the session key K_{ab} encrypts the authenticator ($\{A, GPS_a, N_a\}_{K_{ab}}$). The Enhancement considering the existing protocol is:

- *A* adds his physical location address derived from the GPS receiver to a part of the authenticator.
- *B* will not believe the message unless the GPS_a located in part of the ticket, sent by server, matches the GPS_a located in part of the authenticator, sent by *A*.

In order for *A* to believe *B*, message 2 as ticket and message 4 as authenticator will be used to validate *B*'s physical location. The GPS_b locates in message4, derived from the GPS receiver of *B* must match the GPS_b located in the message 2, sent by the server. This method is preferred to compel the users to use their pre-defined physical location addresses, stored in the server, in order to acquire the private key used to communicate with each other. However, message 2 incurs security flaw as it does not contain A's physical address. Consequently, there is no evidence that the recipient of the message 2 is user *A*. Consequently, the hacker can compromise both the message 2 and 4 and performs the required comparison of the (GPS_b) in message 2 with the (GPS_b) in message 4 without having to confirm physical location. Therefore we include phase2 to address this issue.

1.3 PHASE2- PROVE AUTHENTICITY OF SPECIFIC *LOCATION BY USER*

$$1.A \rightarrow S: A, N_a, B$$
$$2.S \rightarrow A: \{N_s, GPS_a, B, K_{ab}, \{N_s, GPS_b, K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$$
$$3.A \rightarrow B: \{N_s, GPS_b, K_{ab}, A\}_{K_{bs}}, \{A, N_a\}_{K_{ab}}$$
$$4.B \rightarrow A: \{N_a + 1\}_{K_{ab}}$$

Phase2: GPS with Kerberos protocol

In this phase, user is responsible to prove authenticity of the location. Message 2 contains the physical address of user *A* (GPS_a) instead of the physical

Volume 5, Issue 3
June 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

address of user *B* (GPS_b). *A* has to prove that s/he is using the legitimate position. This can be achieved by comparing the physical address in the message, sent by the server ($N_s, GPS_{a,} B, K_{ab}$), with that acquired from the GPS receiver, which is installed in *A*'s location. Thus, *A* will not be able to obtain the key K_{ab} in the absence of matching addresses. The ticket of messages3 ($\{N_s, GPS_b, K_{ab}, A\}_{K_{bs}}$), sent from the server, contains the physical address of user B (GPS_b) instead of the physical address of user *A* (GPS_a). *B* has to prove that s/he is using her/his legitimate position. This can be achieved by comparing the physical address in the ticket, sent by server ($\{N_s, GPS_b, K_{ab}, A\}_{K_{bs}}$), with what would receive it from his GPS receiver which is installed in his location. Again, *B* will not be able to get the key K_{ab} in the absence of matching addresses. There is no need to add GPS_a in both the authenticator and message parts of message 3, and no need to include GPS_b in message four, as in this phase; there is no longer a need to compare the GPS_a's in message three, and the GPS_b's in messages 2 and 4. Subsequently, the key can used from any other place. Clearly, this causes a limitation, however this modification provides more protection against replay attacks. Unfortunately, another problem found in this phase; there is nothing compelling the user to make a comparison between the two physical addresses. In other words, there is nothing preventing a hacker stop the comparison process, or to make it appear as if the comparison result is positive. As a result, Phase 3 introduced to require users to make the comparison.

1.4 PHASE 3 - CAPTURE P(Y) CODE FOR VERIFICATION

$$1.A \rightarrow S: A, N_a, B$$
$$2.S \rightarrow A: \left\{N_s, \{K_{ab}\}_{sig_a}, B, \left\{N_s, \{K_{ab}\}_{Sig_b}, A\right\}_{K_{bs}}\right\}_{K_{as}}$$
$$3.A \rightarrow B: \left\{N_s, \{K_{ab}\}_{Sig_b}, A\right\}_{K_{bs}}, \{A, N_a\}_{K_{ab}}$$
$$4.B \rightarrow A: \{N_a + 1\}_{K_{ab}}$$

Phase3: GPS with Kerberos protocol

Users can capture their physical location signature and store it into the server. Fig. 3 show phase 3 of the proposed idea. The user's location signature has been used to encrypt the key K_{ab}. This will enforce the user to decrypt the signature using his/her physical location signature. User B has to do the same procedure to read the key from the ticket when received through message 3. The details procedures to implement phase3 of the proposed idea are as follows:

- The server needs to encrypt the Key (K_{ab}) using the value of the A's GPS code.
- User *A* needs to decrypt the message by the key K_{as}, and decrypt the key k_{ab} using his/her GPS code.
- The ticket, sent through message 3, has *B*'s signature. *B* needs to decrypt the ticket using K_{bs}, and then to uses the value his/her GPS code to decrypt the K_{ab}.

Users are required to use their physical location addresses signature (GPS signature) in order to read the key. The attacker will be constrained to use a maximum amount of time trying to decrypt the signature, which will cause problem with time synchronization. Therefore, we believe that the proposed idea will eliminate the possibility of the replay attacks.

Evaluation of security protocol is necessary to understand the security features of the protocol. Next section is to evaluate the proposed idea.

4. DISCUSSION

We evaluate the proposed idea using the two different scenarios. Fig. 2 depicts the detailed of the evaluation. The scenarios are further refined into two different cases. This allows generalizing the discussion considering both Kerberos and using GPS signature in addition to Kerberos. The goal of this discussion are to understand the usefulness of using physical location addresses signature (GPS signature) for the authentication purpose and check the applicability of using GPS by two different location.

4.1 GPS SIGNATURE USEFULLNESS

The aim of this discuss is showing the benefit of using GPS signature to authenticate the user identity. This test checks whether the GPS signature can be used to protect the user identify despite of the poor performance by the user; in particular choosing a weak password or not specifying in advance the use of a specific time in the message. The steps to explain this test are as follows:

Step 1 (Experimental setup): We set up the experiment before performing the real test. Following actions are performed for the experiment setup:

- Prepare a *GPS* receiver and install it at the site of user *A*.
- Capture the GPS signature of user *A*.
- Prepare a tool to steal and decrypt the packet.

Volume 5, Issue 3
June 2016

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

- Assume a weakness in the setting of prior verification of using the model, such as chose a weak password to encrypt the packet and the allowed period time for sending the message is unlimited. Therefore, the message does not have a specific expiry time.

Step 2 (Test): Testing was performed and described using the following two cases:

Case1: Using Kerberos protocol

Fig. 2a shows the flow chart of Kerberos protocol. In this case, the following steps were undertaken:

- An encrypted packet sent using KDC's PC to A's PC using a weak password and unlimited time for using this message.

- We intentionally monitor the traffic from the network and copy the message during the communication.

- Decrypt the message to retrieve the plain text

Since there is an open time to decrypt the key and the password is weak, several attempt made with all possibilities until realizing the key. Therefore, following the testing, the code were compromised and read the session key.

Case2: Using Kerberos protocol in addition to GPS signature

Figure 2b shows same scenario from case 1 in addition to use GPS signature. It is essential for hackers to penetrate different levels of protection. The first level is to break through the encryption mechanism as described in case1 and case2, where the second level is to penetrate the GPS signature protection. This case has the following steps:

- Repeat all steps performed in case 1. Despite this, it was not able to read the session key. To do so, the second level of protection, (GPS signature), must be breached.

- We intentionally attempt to monitor and copy the message for the decryption, but we were not able to decrypt the message. The scenario is trying to penetrate the system from unofficial site. Note that by the term unofficial site is the site not defined in advance in the server.

As a conclusion of this test, due to the anti-spoof (AS) used in P(Y) code. The P(Y) code used to make the replay attack more difficult, even in the case of bad verification of the protocol. Moreover, we did not get to the system because the captured GPS signature from the unofficial site does not exist in the server.

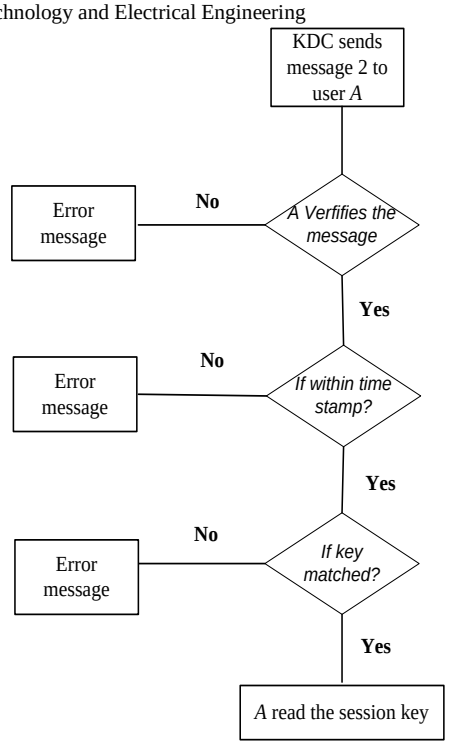

Fig. 2. a) Flow chart of case 1, Kerberos protocol,

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

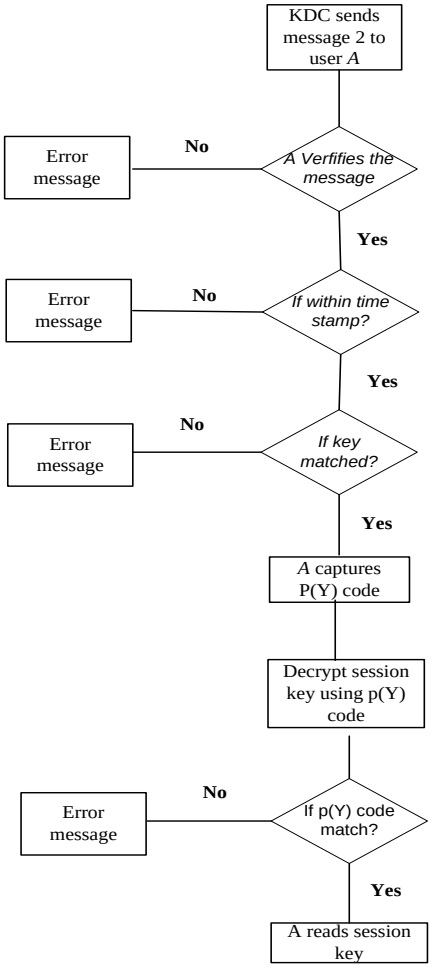

Fig. 2.b) Flow chart of case 2, N-Kerberos protocol

4.2 WHERE CAN IT BE APPLY

Based on the experiment, we have several observations based on the location used for the GPS. The GPS has more possibility to use in the non-variable workplace. List of such areas presented below:

- **Embassy buildings**: or similar security sensitive buildings. The embassies do not allow staff to transfer files to work outside the perimeter of the embassy. In such system, it is suggested creating a security network based on the GPS signal in order to authenticate the user identity. This will increase the level of data transfer protection.

- **Universities:** The Student in the university uses password to get access to the university's services such as access to their account; printer, library, financial account academic record where applicable and many other services. Most students do not take adequate precaution regarding the level of password strength because they are distant from the security area. Therefore, using the location signature will be appropriate for those people. In order to overcome the limitation problem, the administrator can add an option to the student's profile; they can enable or disable the using of the location signature based on the importance or the confidentiality of the requested service; in case of using student's account accessing the computer system off campus.

- **Multiple Sites:** There are many companies that have several sites spread over different locations in various parts world. The positions of these sites are fixed. Therefore, the position signature would use to protect the transmitted documents among these sites. For example, Banks branches needs to send and receive important documents and figures through online transactions.

4.3 LIMITATION

Despites of the applicability of using GPS, we also observe several limitations. They are:

- ***Fixed locations.*** User must use his official and authorized location in order to have the key. This considered a limitation. For instance, where an employee travels out of his authorized nominated location would be denied access.

- ***Poor Signals.*** In the likely event of adverse weather conditions, the user may not capture good quality signal. One practical example is the recent explosion of volcanic ashes in Iceland that affected most of west and northern Europe. Moreover, it has been noted that GPS receiver needs to be viewed by 3 or 4 GPS satellites in order to calculate the location or capture the GPS signature. Therefore, the GPS receiver may not work in a basement or in an underground location, and also where the signals are obstructed.

5. CONCLUSIONS

This paper has presented a new idea of user authentication based on location access control. The proposed idea used the user's physical address; obtained by the GPS signal, as a new authentication factor to verify the identity of the user. GPS signal P(Y) code used to achieve the robust protection scheme for user identity. It demonstrates that using P(Y) code provides additional level of protection. GPS signal has been chooses as an alternative robust password in order to avoid poor user performance in choosing password.

Finally, the proposed idea discussed for two different cases. The result demonstrated that using GPS

signature can be applicable to specific location within the organizational context, and can be to, effectively, secure communication within the group of users. However, several limitations observed in terms, location and poor signal. Inserting the P(Y) code signature into the user device is proposing in the future work. In addition, more test cases will considered for further evaluation of the proposed idea to generalize the findings.

REFERENCES

[1]. D. Gustafson, J. Dowdle, and K. Flueckiger. "A High Anti-Jam GPS Based Navigator", Proceedings of the ION-NTM 2000, Anaheim, CA, January 2000.

[2]. M. Lehtinen, A. Happonen, and J. Ikonen. "Accuracy and time to first fix using consumer-grade GPS receivers," in *Software, Telecommunications and Computer Networks*. 2008.

[3]. A. Schmid, "Positioning Accuracy Improvement With Differential Correlation," *Selected Topics in Signal Processing*," IEEE Journal of, 2009. 3(4), pp. 587-598.

[4]. Kythe, Prem K. *Sinusoids: Theory and Technological Applications*. CRC Press, 2014.

[5]. D.D.L. Sherman Lo, Dennis Akos, Paul Bradley, "Signal Authentication A Secure Civil GNSS for Today," *Inside GNSS*, 2009, pp. 30-39.

[6]. Denning, D.E. and P.F. MacDoran, "Location-based authentication: Grounding cyberspace for better security," *Computer Fraud & Security*, 1996. 1996(2), pp. 12-16.

[7]. \M. Matosevic, Z. Salcic, and S. Berber, "A Comparison of Accuracy Using a GPS and a Low-Cost DGPS," *Instrumentation and Measurement*, IEEE Transactions on, 2006. 55(5), pp. 1677-1683.

Acknowledgment

This research is funded by the deanship of scientific research in Zarqa university/Jordan

[i] Zarqa'a University
[ii] Zarqa'a University