Multimodal Authentication - Biometric, Password, And Steganography

Alvin Prasad, Mohammed Farik

Abstract: Security is a major concern for everyone, be it individuals or organizations. As the nature of information systems is becoming distributed, securing them is becoming difficult as well. New applications are developed by researchers and developers to counter security issues but as soon as the application is released new attacks are formed to bypass the application. Kerberos is an authentication protocol which helps in to verify and validate a user to a server. As it is a widely used protocol minimizing or preventing the password attack is important. In this research we have analyzed the Kerberos protocol and suggested some ideas which can be considered while updating Kerberos to prevent the password attack. In the proposed solution we are suggesting to use password and biometric technique while registering on the network to enjoy the services and a combination of cryptography and steganography technique while communicating back to the user.

Index Terms: Authentication, Biometric, Cryptography, Kerberos, Password attack, Steganography

1 Introduction

INFORMATION, which is processed data are very important for any organization. Information plays a very vital role in any organization as it helps in to make important decisions in the area of production, sales, staffing and finance. Securing this information becomes the priority for the organizations. This information have sensitive data which you need to share with your colleague, like tender information, information on a new product, information on a new service, or any information which will put your organization on the competitive edge. If this information falls in the wrong hands it can be misused. Security is one of the major issues in information systems. The distributed nature of applications has made it more difficult to protect data. For example if two parties A and B are sharing data, anyone like C can come in the middle and capture the data before it reaches the destination. In this entire conversation C will access all the data form A and B and can modify it before forwarding. Together with the data C can have access to the entire network of the organization which can also be misused. C can use that data to defame or blackmail A and B. This man in the middle (C) can be an outsider or a person from the inside of the organization. According to an article [1], the greatest threat to the organization is not from the outsiders but it is from the people who are inside the firewall and have got access to most of the information. So, protection of data and information is very important. To send information in a secured manner encryption can be used. There are two ways of doing encryption. One is symmetric cryptography and the other is asymmetric cryptography. While sending the information sender can encrypt the plain information with a key and send it to the receiver and the receiver can decrypt the information with the same key. This technique used above is known as symmetric encryption where both the sender and receiver use the same key. It is one of the oldest and most used techniques.

- *Alvin Prasad is currently pursuing master's degree program in information technology in the School of Science and Technology at The University of Fiji. Email: alvinp@unifiji.ac.fj*
- *Mohammed Farik (Member IEEE) is a Lecturer in Information Technology in the School of Science and Technology at The University of Fiji. Email: mohammedf@unifiji.ac.fj*

This approach has a problem which is key distribution. As both the parties need the same key, sharing becomes the frail point as anyone can get access to the key during the sharing process. To solve the key distribution problem asymmetric cryptography was proposed. In this approach the sender and the receiver will have two keys. One key is public and the other is private. While sending the information the sender will encrypt the information with the public key of the recipient. After receiving the information the recipient decrypts the information with its private key. In this case there is no need to exchange any key. The information owners can use any symmetric encryption protocol to encrypt the information but if the key is not secured than encryption is useless. So, the strength of any encryption system depends on the method used to distribute key. Kerberos is a widely used key distribution and user authentication protocol which uses the symmetric key encryption technique to send the ticket granting ticket (TGT). Hence, have the same issue where the key can be decrypted and the password can be stolen. Therefore, in this research we have analyzed the Kerberos protocol and suggested some ideas which can be considered while updating Kerberos to prevent the password attack. In the proposed solution we are suggesting to use password and biometric technique while registering on the network to enjoy the services and a combination of cryptography and steganography technique while communicating back to the user.

2 Key Distribution and User Authentication

Key is the major attribute in encrypting and decrypting secret information. For a symmetric encryption only one key is used by both the sender and the receiver and it becomes difficult to secure the key. It is similar to having only one key for a property of yours (car, house, chest, etc) and losing it to a third party with malicious intention. It is advised to change the key frequently to limit the loss of data if the key is revealed [2]. According to [3], key can be distributed in a number of ways. In a situation where only two parties are involved the distribution can be like, first the key can be exchanged physically, where one party delivers the key manually to the other. Second method is where a third party generates a key and delivers it to both the parties; this is done physically as well. The two types of distribution above will not work in a wide-area distributed network. The third method is using an old or previously used key to send the new one and the fourth option is to have a third party involved similar to the second

option but here the communication will be encrypted. The third option cannot be used for first time users and if somebody is able to get one key than all the other keys will no longer be a secret. The fourth method is widely used today and is preferred in network communication with number of users. It uses two keys, session and permanent and requires a key distribution center (KDC) which determines the communication. Kerberos is one of the applications which use the fourth method.

3 KERBEROS

Kerberos is an authentication protocol which works with the use of tickets; it allows communication between two parties over a non-secure network. Kerberos is used by most of the well known operating systems like Microsoft Windows where it is the default authentication method. It is also used by Linux, Apple and FreeBSD. It is also used by the broadband service providers to authenticate their modems and receivers [4]. Kerberos was designed and developed to solve the issue of peer identification [5]. The protocol allows the users to trust each other and share the information in a secured manner. It is a client server model which uses a symmetric key for encryption and decryption [3]. It requires a trusted third party which is a Key distribution center (KDC). KDC has two servers, one is an authentication server (AS) and the other one is a ticket granting server (TGS). KDC stores all the secret keys which are used in message exchange like the users and their corresponding passwords in a database linked with the authentication server. The tickets for all the services which are provided by the system are stored in the ticket granting server. In Kerberos, as shown in fig 1. [3] [6], if two parties want to communicate in a secure manner, they will have to first communicate with the KDC for a session key. Session key allows communication between two parties with a randomly generated key which will be used for a particular session (meeting). To generate the session key or to get access to the services, the user sends a request to the KDC where the authentication server sends a message back to the user to check if the key which is stored in the database is the same or not. The user than uses it's key to validate its identity and sends the message back to the KDC. In the KDC, the authentication server will verify and request the ticket granting server (TGS) to send a ticket which will allow the user to communicate over the network.

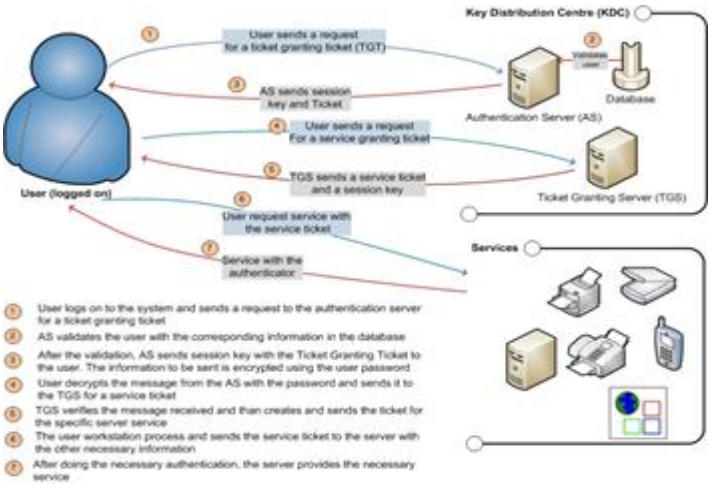

Fig 1. *Overview of the Kerberos authentication process*

3.1 Differences in the versions

Version 4 of Kerberos uses Data Encryption Standard (DES) for the authentication service. It is still in use by most organization and applications [5]. Some applications and working environment require things which is not available in version 4 so, after collecting feedbacks from the stakeholders version 5 was developed to support the activities which was lacking in version 4. The problems with version 4 was that it was the first release to the general public and hence did not consider the detailed application areas. The issues which were addressed in the new version were environmental and technical issues [3]. Some environmental issues like restriction on the export of DES, uncertainties on DES's potential, inflexibility with the address type, confusing byte ordering, limitation in the ticket lifetime, collaboration/ communication issues with other hosts and interoperability issues. Some of the technical issues as discussed in [7], are that version 4 was doing a wasteful use of system resources encrypting the ticket twice, using of an nonstandard mode of DES and replay attack on session key. Both the version has a major issue which needs attention and that is the password attack [3] [5].

3.2 Kerberos password attack

Kerberos is one of the most used application which was released to be used as a general application with its version 4 release. Version 4 had a number of vulnerabilities which was rectified in its version 5 release. But one of the issues which was present in version 4 and was not resolved in version 5 is the password attack as stated earlier. In this type of attack the attacker captures the communication between the user and the KDC specifically the authentication server (AS). When the user sends a request for a ticket to access the network services, the AS sends a message to the user that contains the ticket which is encrypted with the users key [7] [8]. The encryption technique used to secretly send the ticket is known to others as it is available or known to all, which can be decrypted (reversed) and the attacker will have access to the user password which is the key. Many authors have proposed their ideas in regards to solving the issue, in a research [9], authors proposed the idea of using triple password to solve the problem of replay and password attack. In this scenario a new user will have to provide three passwords when logging-in for the first time. This means that the user will have to remember the three difficult passwords to use a service. In another research [10], the author gave the idea of sending the TGT from the AS to the user as well as to the TGS and the TGS sends the TGT to the user as well as the application server. This way the tickets will be stored at different databases and will allow easy reference in case of an attack. Another research [11], proposes the use of Diffie-Hellman algorithm and a dynamic factor in the key exchange between the client and the AS. Jesudoss and Subramaniam [12], proposed the idea of including the session key in the initial message which is sent from the user to the authentication server. Moreover, in a research [13] the author raised the idea of using the biometric system. It is proposed that when the user first logs into the authentication server biometrics can be used, like the users finger prints, iris, and face can be captured and stored in the authentication server. Biometric authentication is also used in another research during the authentication process to solve the problem of password guessing [14]. There can be several issues which can arise, like scar on a face, moisture on the fingers, cut on the fingers

or duplication of this biometrics using 3D technology. Generating random numbers is another way to prevent the attackers to use the application services but it does not help in preventing the password attack [15]. Whereas, in another research [16] the use of random number which will be like a onetime password used in the initial authentication where the communication is between the user and the authentication server.

4 PROPOSED SOLUTION

Many solutions have been proposed by different authors but it has been noted that the proposed solutions have some sort of drawbacks. According to the literature as discussed earlier, some of the drawbacks in the proposed solutions were that it makes the Kerberos application complex, some increases the cost, and some are inefficient. After the analysis in this research we would like to suggest a solution to the password attack problem in Kerberos. We are proposing to use password, biometric and combination of cryptography and steganography technique which might provide relieve to the using organization.

4.1 Password

Passwords are combination of numbers or characters which are kept secret as it is used to verify the users of the system. As time progresses password alone cannot be used to protect data or verify data and individuals. Attacks can easily retrieve the password in this advanced technological world using different password cracking techniques [17]. So, we suggest using the combination of password together with steganography and biometric technique.

4.2 Steganography

Steganography is a technique where communication is done secretly. It is covering or hiding secret messages within something. Anybody receiving such messages will not suspect about the secret message in it [18] [19]. The usage of steganography is mostly done using digital media like audio, images and video which is transferred over the network in the current era as it is easy. Many different types of stenographic technique exist and the comparison is done in different literature which explains that different techniques have its own advantage and disadvantage in different context [18] [20] [21] [22]. We are proposing to use spread spectrum image steganography technique (SSIS) because in the paper by [18], it states that it is very difficult to visualize, that the secret message is embedded within, meaning suspicious level will be low. Also, if anybody in the middle is suspicious and captures the image and manipulates it, the chances that the secret is not edited are high. Furthermore, according to research [23] [24] [25], it is also highlighted that the combination of cryptography and steganography will provide more security rather than using it alone.

4.3 Biometric authentication

Biometric authentication is a process where the physicality or the biometric data of an individual is used to verify if the individual is the same individual as claimed. It has some advantages and disadvantages discussed in the literature [26]. Some advantages are like it provides enhanced protection as it will be very difficult to steal. Also the possibility of forgetting is null. It also cannot be easily shared and changed. Moreover, the disadvantages are the accuracy, not everyone can use all biometric devices, it can also violate user's privacy and some systems are not for lifetime which can increase cost. The combination of the three techniques stated above can be incorporated in the following manner:

Step 1: When a user joins the network to enjoy the services in a Kerberos environment the user needs to register in the system. We suggest that when the user is registering the administration should take in the user's password and thumbprint. This information will be stored in the AS database.

Step 2: After the user registers to use the services he/she needs to log in to the system and request the TGT from the authentication server. We propose to use the thumbprint for the login.

Step 3: When the user is logged in, the AS will validate the user by comparing the parameters stored in the database. If the user is valid than AS sends a TGT with the session key which is hidden inside the thumbprint data using the combination of cryptographic algorithm and steganography technique, which is again protected with the password stored in the database during registration as the key. On the other end the AS sends the user password and the thumbprint information to the TGS which is encrypted with a key which is a secret between the AS and TGS.

Step 4: User gets the session key with the password which was known to him/her. Here the user creates the authenticator which consists of network address and timestamp and this document is encrypted using session key. The authenticator and the TGT received earlier will be sent to the TGS.

Step 5: The TGS after receiving the message from the user decrypts it with the key known to AS and TGS only. After verifying the information like the network address, timestamp and user id, the TGS sends service granting ticket to the user to access the specific server services.

Step 6: After the user receives the service granting ticket, the user can use the ticket to access the services from the network.

We believe that the use of the three way authentication might help the organization from the intruders. As we proposed the use of password, thumbprint information and stenography we believe that it will be very difficult for them to get access to information easily.

5 CONCLUSION AND FUTURE WORK

Security is a very important aspect of the current era. Organizations lose millions of dollars to intruders due to security breaches. Kerberos is one of the most used applications by the major operating systems and organizations to protect their information resource. Unfortunately it has a gap where hackers can do a password attack and gain access to the information and services provided by the organization. We have proposed a solution to use password, biometrics and combination of cryptography and steganography technique together to make it difficult for the attackers to access the password. In future research we would like to analyze and test the suggested method in this paper and compare the results with the other methods.

REFERENCES

[1]. R. N. Rose, "The Future Of Insider Threats," 30 August 2016. [Online]. Available: https://www.forbes.com/sites/realspin/2016/08/30/the-future-of-insider-threats/#7f6c4fb17dcb.

[2]. E. Barker and A. Roginsky, "Recommendation for Cryptographic Key Generation," National Institute of Standards and Technology, 2012.

[3]. W. Stallings, Network Security Essentials: Application and Standards, USA: Prentice Hall, 2011.

[4]. Techtarget network, "Kerberos," 31 August 2016. [Online]. Available: http://searchsecurity.techtarget.com/definition/Kerberos. [Accessed 29 March 2017].

[5]. J. T. Kohl, B. C. Neuman and T. Y. Ts'o, "The Evolution of the Kerberos Authentication Service," in European Conference on Open Systems, Norway, 1991.

[6]. Massachusetts Institute of Technology, "Kerberos: The Network Authentication Protocol," 3 March 2017. [Online]. Available: https://web.mit.edu/kerberos/. [Accessed 23 April 2017].

[7]. S. M. Bellovin and M. Merritt, "Limitations of the Kerberos Authentication system," Computer Communications Review, pp. 119-132, 1990.

[8]. T. Wu, "A Real-World Analysis of Kerberos Password Security," 1999.

[9]. G. Dua, N. Gautam, D. Sharma and A. Arora, "Replay attack prevention in Kerberos authentication protocol using triple password," International Journal of Computer Networks & Communications, pp. 59-70, 2013.

[10]. J. Yang, "An Improved Scheme of Single Sign-on Protocol," in Fifth International Conference on Information Assurance and Security, 2009.

[11]. Y.-y. Du, H.-y. Ning, P. Yang and Y.-x. Cui, "Improvement of Kerberos protocol based on dynamic password and "One-time public key"," in 10th International Conference on Natural Computation (ICNC), 2014.

[12]. A. Jesudoss and N. Subramaniam, "Enhanced Kerberos authentication for distributed environment," Journal of Theoretical and Applied Information Technology, pp. 368-374, 2014.

[13]. R. Hegde, "Biometric authentication technique with Kerberos for email login," International Journal of Advances in Engineering & Technology, pp. 1735-1744, 2015.

[14]. Q. Le, H. P. Truong, H. T. Van and T. H. Le, "A new pre-authentication protocol in Kerberos 5: biometric authentication," in 2015 IEEE RIVF International Conference on Computing & Communication Technologies - Research, Innovation, and Vision for the Future (RIVF), 2015.

[15]. T. Thakur, S. Dogra and Y. Sood, "Replay Attack Prevention by Using a Key with Random Number in Kerberos Authentication protocol," International Journal of Innovative Research in Science, Engineering and Technology, pp. 5616-5622, 2015.

[16]. W. Lei, H. Cao, X. Liang and H. Zhang, "An Improved Kerberos Scheme Based on dynamic password," I.J. Information Technology and Computer Science, pp. 33-39, 2010.

[17]. D. Winder, "Top ten password cracking techniques," 2 December 2011. [Online]. Available: http://www.alphr.com/features/371158/top-ten-password-cracking-techniques. [Accessed 24 May 2017].

[18]. F. M. Shelke, A. A. Dongre and P. D. Soni, "Comparison of different techniques for Steganography in images," International Journal of Application or Innovation in Engineering & Management (IJAIEM), pp. 171-176, 2014.

[19]. Learn Cryptography, "What is Steganography?," 2017. [Online]. Available: https://learncryptography.com/steganography/what-is-steganography. [Accessed 23 4 2017].

[20]. M. Hussain and M. Hussain, "A Survey of Image Steganography Techniques," International Journal of Advanced Science and Technology, pp. 113-123, 2013.

[21]. N. F. Johnson and S. C. Katzenbeisser, "A Survey of Steganographic Techniques," in Information Hiding, Darmstadt, Springer International Publishing, 2009, pp. 43-78.

[22]. P. Rai, S. Gurung and M. K. Ghose, "Analysis of Image Steganography Techniques: A Survey," International Journal of Computer Applications, pp. 11-17, 2015.

[23]. H. V. Desai, "Steganography, Cryptography, Watermarking: A Comparative Study," Journal of Global Research in Computer Science, pp. 33-35, 2012.

[24]. A. J. Raphael and V. Sundaram, "Cryptography and Steganography – A Survey," Int. J. Comp. Tech. Appl, pp. 626-630, 2011.

[25]. D. Bloisi and L. Iocchi, "Image based steganography and cryptography," International conf. on computer vision theory and applications, 2007.

[26]. V. Matyas and Z. Riha, "Biometric authentication - security and usability," in 6th Joint working conference on communications and multimedia security, Deventer , 2002.