Running head: Kerberos

# CS3910: Assignment 5: Kerberos

# Mordred Cameron

# University of Colorado Colorado Springs

In partial fulfillment of the requirements for CS3910

Instructor: Rhett Saunders

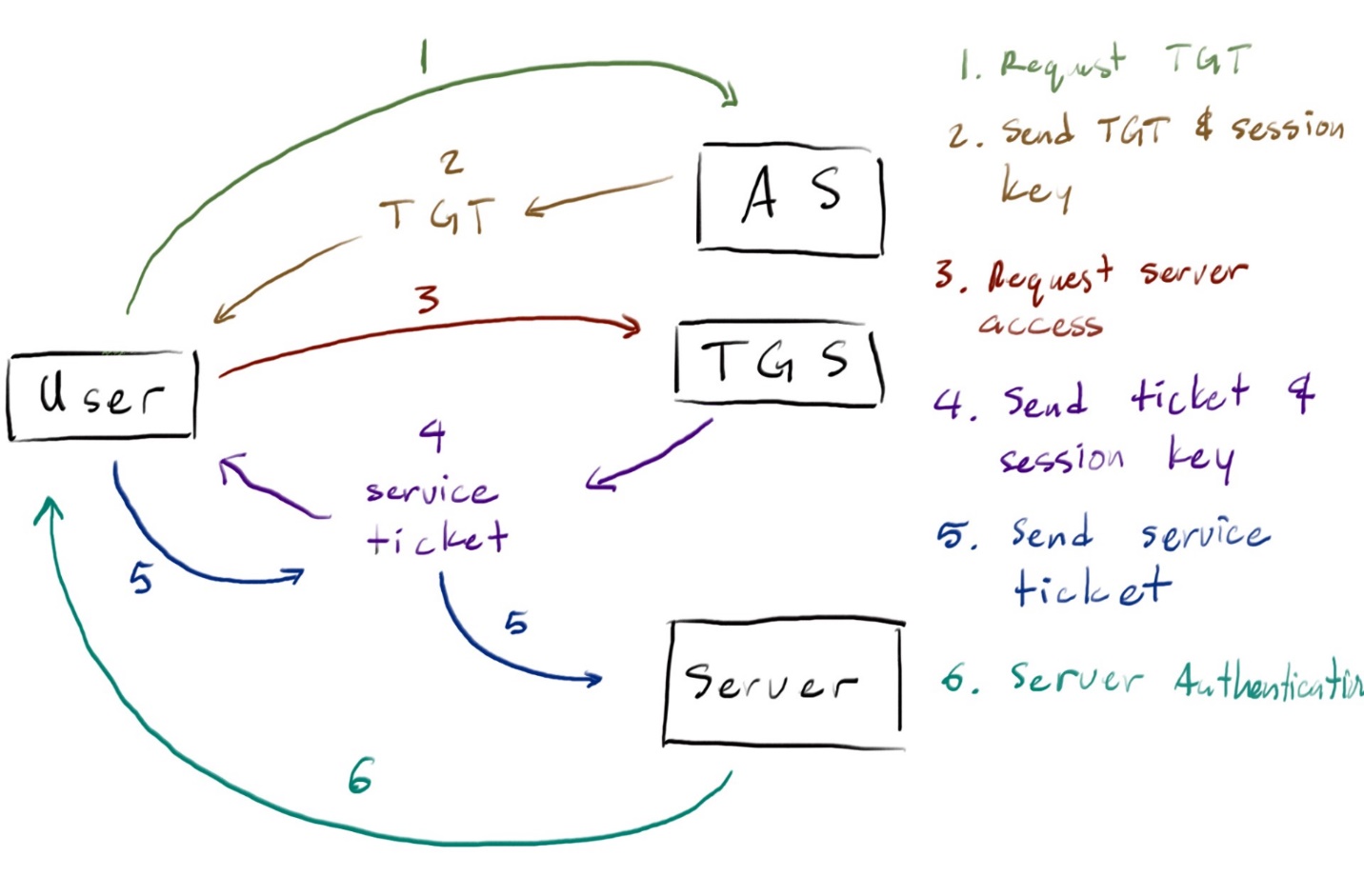
4/3/2024

# Introduction to Kerberos

In this assignment, the outcome provided insight into Kerberos, why it is implemented, how it is implemented, how it is used, and its importance.

Assignment Results

Based on these screenshots, this is what I learned.



Kerberos aims to solve the issue of implementing authentication of a system’s users to prevent attacks that previous approaches like passwords were vulnerable to. On systems accessed by multiple users, the identity of individual users must be verified. The identification mechanism on an open environment must be secure, reliable, and scalable (Steiner et al., 1988). Kerberos meets these requirements by being secure through the use of time-limited tickets. It is single-sign on (SSO), which allows its users to only need to sign on once to access all necessary resources in the session. Kerberos works through a centralized authentication server, and uses mutual authentication to prove the identity of both the user and the server. Through this, Kerberos aims to improve both the security and convenience on insecure networks (Garman, 2003).

In order to solve the authentication issue, Kerberos uses a series of elements. The Key Distribution Center (KDC) is responsible for granting tickets to users on a network (Boonkrong, 2021). This is made up of the Authentication Server (AS), which authenticates a user’s identity based on their username and password, it then provides the Ticket Granting Ticket (TGT) that are used to access tickets which are then used to access resources. The TGT, which is encrypted with a session key, is then sent to the Ticket Granting Service (TGS) which re-verifies the identity, before providing a ticket that allows access to whatever system or resource that they were trying to use, which is also once more verified before the client is given access (Steiner et al., 1988). Communication between these elements as well as the tickets are encrypted, providing yet another layer of security.

Time sensitivity is a valuable component of Kerberos, especially revolving around the distribution of tickets. To prevent malicious attackers from decrypting these tickets, the system must ensure that the duration of a valid ticket expires within a certain amount of time. When tickets are issued by the KDC, timestamps are assigned to indicate the valid time of the ticket. To ensure that these time limitations are functioning as they should by rejecting any replay attacks that have out of date timestamps, all systems, the client, servers, and KDC, must be synchronized on the same clock time (Davis et al., 1996).

Kerberos continues to be implemented today due to its efficiency and security. The SSO provides efficiency to its users, reducing the need to sign in repetitively. Kerberos is also widely compatible and therefore attractive to many environments. Centralization, security, and scalability are becoming more and more important as networks and organizations grow, using a system like Kerberos provides a reliable approach to system security. Kerberos continues to be actively used in environments and is essential to the world of cyber security.

Conclusion

In summary, Kerberos and how and why it is used are important elements to understand when considering organizations, companies, and institutions that will all most likely use systems that implement this protocol. Kerberos is an effective and relatively simple authentication protocol that allows for ease of use for users on an insecure network (MIT, n.d.). As technology progresses, this form of authentication is unlikely to disappear anytime soon, and working to understand and expand upon this is integral to cyber security. Through this assignment I better understood the functionality behind Kerberos and its importance in developing systems.

References

Boonkrong, S. (2021). *Authentication and access control: practical cryptography methods and*

*tools* (pp. 45-70). Berkeley, CA, USA: Apress.

Davis, D. T., Geer, D. E., & Ts'o, T. (1996). Kerberos with clocks adrift: History, protocols, and

implementation. *Computing systems*, *9*(1), 29-46.

*Designing an Authentication System: a Dialogue in Four Scenes*. mit. (n.d.). https://web.mit.edu/kerberos/dialogue.html

Garman, J. (2003). *Kerberos: The Definitive Guide: The Definitive Guide*. " O'Reilly Media,

Inc.".

*Kerberos: The Network Authentication Protocol*. mit. (n.d.-b). https://web.mit.edu/kerberos/

Steiner, J. G., Neuman, B. C., & Schiller, J. I. (1988, February). Kerberos: An Authentication

Service for Open Network Systems. In *Usenix Winter* (pp. 191-202).