International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 10 Issue 10 ǁ October 2022 ǁ PP. 373-374

A Comprehensive Study of Authentication and Confidentiality for Tacacs Server

[1]P A.Koteswara Rao, [2]Shaik Taj Mahaboob, [3]K.Ravindra Reddy
1 M.Tech Student, 2Assistant Professor, 3Assistant Professor (Adhoc)
akoteswararao9@gmail.com
1Electronics and Communication Engineering,
JNTUA College of Engineering Pulivendula, Andhra Pradesh, India

ABSTRACT:
Through one or more centralised servers, TACACS+ offers access control for routers, network access servers, and other networked computer devices. Separate authentication, authorisation, and accounting services are offered by TACACS+. The TACACS+ protocol is described in this document.
Index Terms: *Authentication, Authorization, and Accounting, TACACS, Confidentiality*

Date of Submission: 02-10-2022 Date of acceptance: 15-10-2022

I. INTRODUCTION:

By separating the roles of authentication, authorization, and accounting and encrypting all data travelling between the NAS and the daemon, TACACS+ outperforms TACACS and XTACACS. Any authentication method may be used with TACACS+ clients since it supports authentication exchanges of variable duration and content. It leverages TCP to assure dependable delivery and is expandable to allow for site customisation and future development capabilities. The protocol enables the daemon to react to each part of the TACACS+ client's request for extremely fine-grained access control. A key aspect of TACACS+'s architecture is the separation of authentication, authorisation, and accounting. Since the differences between them are crucial, this document will discuss each one separately.

It is significant to note that TACACS+ supports all three, but that using all three does not necessitate an implementation or configuration. Each one has a particular function that, while useful on its own, when combined, may be rather potent. Separating authentication from authorization has several advantages, one of which is the possibility of dynamic authorisation (and per-user profiles). TACACS+ may be connected with other negotiations, such a PPP negotiation, allowing far greater flexibility than a one-time user profile. The accounting component might offer services for security audits or accounting/billing. TCP is used by TACACS+ for transport. The TACACS protocol's "LOGIN" port, port 49, is where the daemon should be listening.
Both UDP and TCP have reserved this port in the allocated numbers RFC. Utilizing port 49 are the current TACACS and extended TACACS implementations.

II. LITERATURE REVIEW:

Ravi.V: Contemporary routers include networking services including authentication, authorisation, and accounting capabilities are crucial in any network. Routers employ a variety of protocols to provide users with the degree of service they demand. Users may connect secretly and securely with the help of services like virtual private network service across networks. Commercial routers use the TACACS+ and RADIUS protocols to support the AAA services. In this article, we introduce a brand-new paradigm for examining authentication protocols like TACACS+, which aid in the establishment of a virtual private network in routers [1].
R Pradeep:It takes much work and expertise of the art of secret writing known as cryptography to create the ideal security protocol. Given its numerous flaws, the testing approach is inappropriate for obtaining high dependability of security procedures. To achieve high reliability of security protocols, it is essential to demonstrate their accuracy. The Formal Verification methodology presents a mathematical explanation for protocol accuracy, making it the best way to show and prove the accuracy of security protocol. TACACS [6] is one of the primary security protocols used by the majority of Cisco network communication devices to offer Authentication, Authorization, and Accountability (AAA) services to the host devices. To officially validate the TACACS+ security protocol, the proposed study use model checking approach. The secrecy and authentication security properties of the TACACS+ security protocol are successfully confirmed using the Scyther model checker [2].

T. Dahm: TACACS+ protocol is frequently used to operate routers, network access servers, and other networked computer equipment through one or more centralised servers.
Gabriel Lucian In terms of authentication, authorisation, and accounting, this article provides a solution for users desiring to access the Internet via a secured network. The RADIUS protocol is used to encapsulate the PAP, CHAP, MSCHAPv1, and MSCHAPv2 conventional authentication techniques, and the MD4, MD5, salted MD5, and SHA-1 hashing algorithms are then used to further protect the user credentials. The AAA-RADIUS system is implemented using the Alcatel-Lucent 8950 AAA software.
Toni Janevskil:AAA system presented in this article allows Public Land Mobile Networks (PLMN) and Wireless Local Area Networks (WLAN) to communicate with one another (WLAN). A variety of network nodes, such as a WLAN Access Controller, WLAN AAA gateway, and AAA server, as well as crucial network elements for dynamic IP address allocation and a web server for user access to the network, make up the planned system. WLAN Access Controller and AAA server provide WLAN users with access control. The WLAN AAA Gateway handles invoicing and payments for the WLAN service.The complete AAA system, which includes all network components, offers a cost-effective solution for PLMN-WLAN internetworking [5]
Zhang Jiange: Adopting 802.1x authentication for network access control has clear benefits. The AAA protocol, which is formulated on802.1x authentication, is built after this study evaluates the 802.1x, EAP, and RADIUS protocols. The messages of the whole authentication procedure have been recorded using software. It thoroughly analyses EAP and RADIUS communications in accordance with AAA mechanism. These messages' analysis offers significant value for study and application, and it greatly advances technology for specific research and future developments[10]

III. Conclusions

I have reviewed several articles related with authentication enables authorization, authentication, and accounting in addition to enabling efficient management for LAN users' network access. As a result, it is crucial for both research and application. However, the need for network connectivity has increased with the introduction of the Internet. Additionally, there are significant drawbacks to the AAA system that need to be addressed. Double authentication is one enhanced technique. For instance, identity authentication is implemented prior to network access authentication.
As a result, the network's security will improve.

REFERENCES

[1]. "Formal ways to validate authentication in TACACS+ protocol" by Ravi V, Dr. Sunitha N. R, and Pradeep R
[2]. Formal Verification of Authentication and Confidentiality for TACACS+ Security Protocol Using Scyther by Pradeep R, Sunitha N.R, and Ravi V IEEE - 45670
[3]. Ota, T. Dahm Medway, D.C. The Terminal Access Controller Access-Control System Plus (TACACS+) Protocol, Gash D. Carrel L. Grant, RFC 8907.
[4]. Victor CROITORU and Gabriel-Cătălin CRISTESCU "AAA-RADIUS Solution Implementation Based on Legacy Authentication Protocols" 978-1-5090-3748-3/16/$31.00 ©2016 IEEE
[5]. Aleksandar Tudzarov, Toni Janevski, Meri Janevska, PervojeStojanovski, DuskoTemkov, GoceStojanov, DuskoKantardziev, Mine Pavlovski, and Tome Bogdanov Serbia and Montenegro, Nis, September 28–30, 2005, "Integrated AAA System for PLMN-WLAN Interworking"
[6]. "Research of AAA messages Based on 802.1x Authentication" by Jiange Zhang, Yuanbo Guo, Yue Chen, and Jun Ma. 978-1-47--/1/$31.00 201IEEE
[7]. Feng Jian, "Design and Implementation of RADIUS Client Based on Finite State Machine," Pacific-Asia Conference on Circuits, Communications and System, July 2009, pp. 3-4.
[8]. International Conference on Computer Application and System Modeling (ICCASM 2010), pp. 1-2, October 2010. X. Chen and J. Hu, "Design and Implementation of VoIP Prepaid Service Based on RADIUS."
[9]. S. Zaghloul and AdmelaJukan, "Relating the AAA and the Radio Access Rates in 3G Cellular Networks," IEEE Commun.
[10]. "Research of AAA messages Based on 802.1x Authentication," Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), pp. 2-3, Dec. 2015; J. Zhang, Y. Guo, Y. Chen, and J. Ma