Abstract

Authentication, authorization, and accounting (AAA) is a framework which intelligently controls access to resources by enforcing policies, administering usage, and calculating the information to bill for services utilized. The combination of these three processes is very important for network security and management.

Description, implementation and experiences with three A’s of security

# Three A’s of security

Authentication is a way of identifying a user, generally the user enters a user name and password to enter the system and if the credentials are accurate, access is granted. If the credentials are a mismatch, authentication fails, and network access is denied.

After authentication, a user must gain authorization for performing tasks. For example, a user might want to issue some commands after gaining access to the system. The authorization process determines whether the user has the authority to issue such commands. Authorization determines if the user is eligible to perform certain activities or utilize certain resources, or services provided by the system. Authorization mostly occurs after authentication. Authorization might not happen without authentication.

Accounting measures the metrics of the user’s activity during the process. This includes the amount of system time or the amount of data a user has sent and/or received during a session. Accounting is carried out by logging of session statistics. The data collected is used for billing, trend analysis, and for machine learning.

## Technologies used

Latest technologies to authenticate a user to login into a system include using a strong password, smart card, biometrics, multifactor-authentication, session management, cryptography etc. These can be used individually or in combination to give an added security layer to the user. Authorizing a user to access the system typically happens after authenticating him, and the technologies are used in combination with authentication technologies such as OAUTH, XACML and SPML.The tools used in accounting purpose usually gather network data and analysis is done on the data to study the user behavior. Few technologies include WinPcap, PRTG Network Monitor, NetScout etc.

## Experiences with AAA technologies

Even though accounting technologies are less common with developers, WinPcap is a very common tool which is used by them to assess the performance of certain programs over the network. It is a very powerful tool among network engineers and gives statistical data based on time, user or any other specific parameter. Authentication and authorization technologies go hand in hand and it is difficult for the user to identify if authorization follows authentication while logging into a system. Biometric authentication looks promising and fool-proof since it matches either, fingerprint, iris, or a combination. For emails, and software applications password authentication with OTP generation works well followed by OAUTH for authentication.

References

Saxena, Preeti & Sikarwar, Arun Pratap Singh (2017). "An Analytical and Experimental Study of AAA Model with Special Reference to RADIUS and TACACS+". *International Journal of Computer Applications*, Pages 6 - 7.

Metz, C (1999). "AAA protocols: authentication, authorization, and accounting for the Internet," in *IEEE Internet Computing*,