

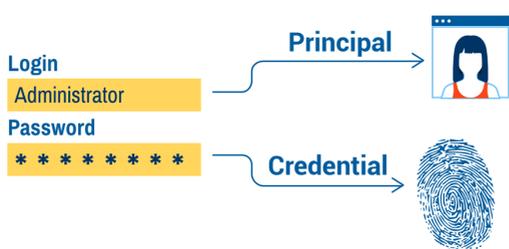
AAA

AUTHENTICATION AUTHORIZATION ACCOUNTING



THE THREE CHAIN LINKS of RADIUS Security

Most people are familiar with the concepts of typing in their user name and password before they can access the internet.



In network security terms, these two pieces of information are also known as the **principal** (user name or other identity) and the **credential** (password, one-time use access code, biometric marker).

A third parameter, called the **context**, provides a frame of reference for each attempted login (time of day, network load, user's IP address).

The principal, the credential, and the context are used together by a network security system to identify the user (**authentication**), to allow or deny access to network privileges (**authorization**), and to track usage parameters (**accounting**).

Authentication, Authorization, and Accounting (AAA) are the foundations of network security.



► **RADIUS** is one of the major AAA networking protocols and acts as the security gatekeeper, allowing or denying access to a network.

AUTHENTICATION



Authentication is the process that determines whether a client really is who they say they are.



If authentication is not properly set up, unauthorized clients can access your network and authorized clients can be rejected.

Good → ✓

The RADIUS server makes an authentication decision (**accept** or **reject**) based on the principal and the credential of the client.

Bad → ✗

If everything checks out, the server grants the client access to the network. If anything is amiss, the server denies access.

AUTHORIZATION



Authorization is the process that determines what an authenticated client can and cannot do on a network. Authorization works hand-in-hand with authentication.

The Network Privileges for each user are stored in a database and enforced by the RADIUS system. These rules can limit:



What parts of the network the user has access to



What servers or applications can be used



The length of time a user is allowed on the network



What type of network access is allowed



If authorization is not set up properly, sensitive information (such as credit card numbers) could be exposed to unauthorized clients, or clients could end up without access to a service for which they have paid.

ACCOUNTING

Accounting is the process of monitoring and recording a client's use of the network.

RADIUS accounting must be set up properly to ensure that the system does not overload and that clients are billed appropriately.

RADIUS accounting can also provide vital information, such as:



Peak usage times,



Who was logged on at the time of a data breach,



How much to charge a user.

IMPLEMENTING AAA

Correctly implementing the three chain links of RADIUS security requires know-how, planning, testing, and documentation.



The best way to implement RADIUS security is to bring in an expert who knows what's needed to put together a solid and reliable security system.

A RADIUS expert is an invaluable ally in your quest for strong network security.



Sources:
 Network RADIUS – AUTHENTICATION: Is It Really You?
 Network RADIUS – AUTHORIZATION: Authorized Personnel Only
 Network RADIUS – ACCOUNTING: Keeping Track Of It All

