In computer security, **AAA** stands for authentication, authorization and accounting protocol.

Authentication

Authentication refers to the confirmation that a user who is requesting services is a valid user of the network services requested. Authentication is accomplished via the presentation of an identity and credentials. Examples of types of credentials are passwords, one-time tokens, digital certificates, and phone numbers (calling/called).

Authorization

Authorization refers to the granting of specific types of service (including "no service") to a user, based on their authentication, what services they are requesting, and the current system state. Authorization may be based on restrictions, for example time-of-day restrictions, or physical location restrictions, or restrictions against multiple logins by the same user. Authorization determines the nature of the service which is granted to a user. Examples of types of service include, but are not limited to: IP address filtering, address assignment, route assignment, QoS/differential services, bandwidth control/ traffic management, compulsory tunneling to a specific endpoint, and encryption.

Accounting

Accounting refers to the tracking of the consumption of network resources by users. This information may be used for management, planning, billing, or other purposes. Real-time accounting refers to accounting information that is delivered concurrently with the consumption of the resources. Batch accounting refers to accounting information that is saved until it is delivered at a later time. Typical information that is gathered in accounting is the identity of the user, the nature of the service delivered, when the service began, and when it ended.

source - AAA protocol. (2006, August 10). In *Wikipedia, The Free Encyclopedia*. Retrieved August 31, 2006, from http://en.wikipedia.org/wiki/AAA_protocol

Hautspot's captive portal technology from Sputnik presents WLAN users with an authentication page in their web browsers. This is the first step in the AAA process, allowing our central control server to determine if the potential user is known or unknown.

If known, the user is then authorized to access the WLAN. If not, and if desired by the hotspot venue, new users may click on a link on the captive portal page to create a new account for themselves.

Meanwhile, back at our network operations center, our central control server tracks network usage (accounting) for realtime feedback on network performance as well as later reporting purposes.

Besides authenticating against our internal database of users, Hautspot venues have the ability to authenticate against third party RADIUS servers.

Back