RADIUS中的Authenticator是什么

AAA 朱恺 2017-12-29 发表

Authenticator:16个字节，用于验证服务器端的应答，另外还用于用户口令的加密。RADIUS服务器和NAS的共享密钥(Shared Secret)与请求认证码(Request Authenticator)和应答认证码(Response Authenticator)，共同支持发、收报文的完整性和认证。另外，用户密码不能在NAS和RADIUS服务器之间用明文传输，而一般使用共享密钥(Shared Secret)和认证码(Authenticator)通过MD5加密算法进行加密隐藏。Authenticator：鉴别码，分为请求鉴别码，回应鉴别码。

在“Access-Request”数据包中，Authenticator是一个16字节的随机数，称为“Request Authenticator”。在机密的整个生存周期中（如RADIUAS服务器和客户端共享的机密），这个值应该是不可预测的，并且是唯一的，因为具有相同密码的重复请求值，使黑客有机会用已截取的响应回复用户。因为同一机密可以被用在不同地理区域中的服务器的验证中，所以请求认证域应该具有全球和临时唯一性。

为防止数据包中数据被截获被篡改，回应鉴别码采用如下方式生成：

RespOnseAuth= MD5(Code+ID+Length+RequestAuth+ Attributes+Secret)；

回应鉴别码是对整个数据包进行MD5演算产生的16字节索引，防止伪造服务器的回应。

比如802.1X认证中，设备每次发送报文的Authenticator都不一样，校验时设备只校验最后一次发送的Access-Request报文与最后收到的Access-Accept报文中的Authenticator字段，同时得到其他加密符号的MD5运算关系。