WAPI鉴别及密钥管理的两种实现方式

wlan安全 **陈铮** 2018-03-21 发表

基于证书的方式 （WAPI-CERT）

1）STA通过AP的信标帧或探询响应帧识别AP支持WAI鉴别及密钥管理套件；

2）STA和AP之间进行链路验证；

3）在关联过程中，STA在关联请求中包含WAPI信息元素确定选择的密码套件；

4）STA和AP进行证书鉴别过程，协商出BK；

5）STA和AP进行单播密钥协商过程、组播密钥通告过程；

6）把协商出来的密钥和密码套件通知WPI模块，进行数据传输保护。

基于共享密钥的方式（WAPI-PSK）

1）STA通过AP的信标帧或探询响应帧识别AP支持WAI鉴别及密钥管理套件；

2）STA和AP之间进行链路验证；

3）在关联过程中，STA在关联请求中包含WAPI信息元素确定选择的密码套件；

4）预共享密钥导出BK后，STA和AP进行单播密钥协商过程、组播密钥通告过程；

5）把协商出来的密钥和密码套件通知WPI模块，进行数据传输保护。