第五次作业

学号：2017221302006 姓名：周玉川

1. 对TKIP和WEP做安全性比较

WEP（Wired Equivalent Privacy），即有线等效保密，目的是达到和有线网络相同的安全性。WEP安全服务包括身份认证，完整性和保密性。但是在WEP的提供保密服务的加密过程中，同一网络下的STA拥有相同的WEP Key，而且在网络中IV是通过明文传输的，所以会照成同一网络下的STA可以互相窃听。而且WEP存在RC4攻击，第三方在窃听网络中的流量后可以获取到RC4 Key。

对照WEP，TKIP改变的地方包括：

1. WEP Seed的生成。TKIP在加密数据时，采用密钥混合的方式来产生加 密密钥
2. Plaintext MPDU。TKIP的Plaintext MPDU会与使用称为Michael算法的KeyedHashfunction来生成的MIC拼接，然后根据需要分片生成新的Plaintext MPDU。
3. 帧封装。WEP在MACHeader后面紧随4-octet的IV字段，然后是加密 的MSDU||ICV；TKIP的MACHeader后面紧随8个octet的(IV||ExtendedIV)，然后是加密的MSDU||MIC||ICV。
4. 对CCMP和TKIP做安全性比较

TKIP作为补丁很快就出现了，它弥补了早期无线接入点（AP）和客户端被WEP削弱的安全性。TKIP不再使用相同的密钥来加密每一个数据包，它使用的 RC4对每一个数据包分配了不同的密钥。这些随数据包而变的密钥化解了黑客们对WEP加密方法的破解。另外，TKIP还使用了带密钥的消息完整性检查（MIC）技术来发现那些被重放和仿冒的数据包。虽然谁都可以从网络中截获经过TKIP加密的数据包，然后对这些数据包进行修改，最后再将它们发送到网络中去（注入），但这些数据包最终都会被丢弃，因为在对MIC和校验和进行检查时就会发现它们与数据包所携带的数据不匹配。当采用TKIP的无线接入点收到第一个不正确的MIC时，就会发送一个错误报告。如果在60秒内又收到了第二个不正确的数据包，则无线接入点就会停止监听1分钟，然后再为无线局域网更换密钥，即要求所有的客户端都开始使用新的“成对主密钥”去生成MIC密钥和用于每个数据包的各不相同的加密密钥。 这样就弥补了WEP留下的多个漏洞。任何经过WPA认证的产品都可以利用TKIP和它所使用的MIC抵御对802.11的各种窃听、仿冒和重放攻击（replay attack）。

802.11i定义了基于先进加密标准（AES）的密码块链信息认证码协议（CCMP）来代替TKIP和MIC。