# 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：

(一) 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

(二) 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。

(三) 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。

## 2. 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。