

密码学课程第3次实验报告

实验名称：校园无线身份认证密码协议分析

学号：2113683 姓名：柳致远 班级：密码科学与技术

一、实验目的

校园网用户的数量不断增长，校园网提供的业务形式也有很大程度上的增多，用户的接入方式也多样化，面临着复杂的信息安全问题。在这个实验中，我们将分析校园无线身份认证密码协议，了解当前校园网的认证方式，对认证过程及其安全性进行简单的分析说明

二、实验内容说明

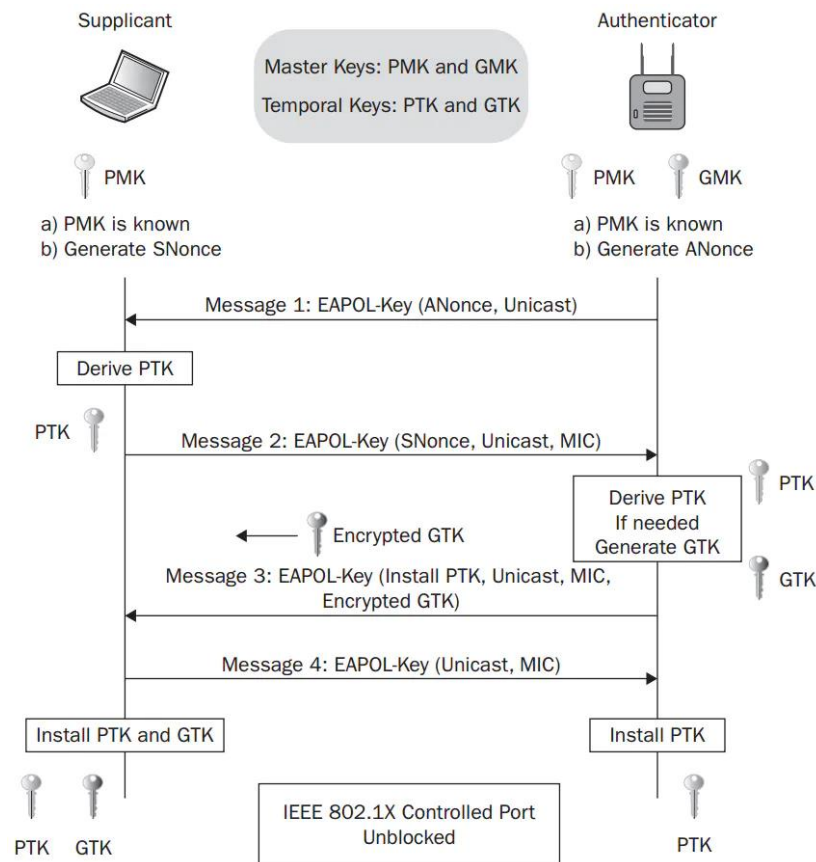
（概述本次实验要做什么）

利用抓包工具抓取 wifi 身份认证过程中四次握手的过程。并根据协议内容，针对每一条报文进行具体分析。

三、实验原理

（画出所分析的协议流程图并简要说明）

本节以捕获到密钥信息报文 EAPoL-Key 为例，即分析 WiFi 身份认证中四次握手的过程。



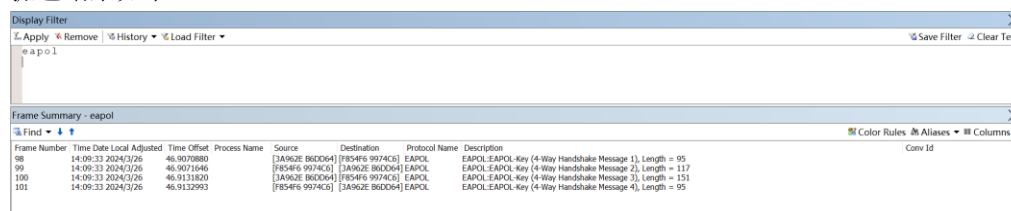
四次握手是 AP（Authenticator）和 Station（Supplicant）为了生成一个用于加密无线数据的密钥而进行四次消息交换的过程。

- 1、第一次握手：AP 向 Station 发送一个 eapol-key 帧，内部含有 AP 自己产生的一个随机数 ANonce，Station 在接收到该帧后，利用 PTK 生成函数 $PTK = PRF(PMK + ANonce + SNonce + Mac(AA) + Mac(SA))$ 生成 PTK，PTK 的前 128 位是 KCK，用来校验 EAPOL-Key 帧的完整性。
- 2、第二次握手：Station 在创建了自己的 PTK 之后，会相应回复 AP 一条 eapol-key 帧，该帧中包含 Station 中产生的随机数 SNonce 以及 Station 计算得到的 MIC。AP 收到后同样利用 SNonce 计算出 PTK。同样利用前 128 位与收到的 MIC 值是否一致，若一致则验证成功，若不一致说明消息被篡改，握手停止。
- 3、第三次握手：AP 将 MIC 和用 PTK 加密后的 GTK 发送给 Station，Station 收到消息后检查 MIC。若不一致一样丢弃报文，若一致，Station 可以使用掌握的 PTK 进行解密，恢复 GTK 的值，并安装 PTK 和 GTK。
- 4、第四次握手：Station 向 AP 发送 EAPOL-Key 消息，确认密钥已经安装，AP 收到该消息后再次检查 MIC，验证成功后也安装 PTK。PTK 是单播加密临时密钥，GTK 是多播加密临时密钥。

四、实验步骤

（抓包并根据协议流程具体分析报文内容）

抓包结果如下：



Frame Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protocol Name	Description
98	14:09:33.2024/3/26	46.9070880		[JANUZE B6C064]	[7854F6 9974C8]	EAPOL	EAPOL-EAPOL-Key (4-Way Handshake Message 1), Length = 95
99	14:09:33.2024/3/26	46.9071646		[7854F6 9974C8]	[JANUZE B6C064]	EAPOL	EAPOL-EAPOL-Key (4-Way Handshake Message 2), Length = 117
100	14:09:33.2024/3/26	46.9111820		[JANUZE B6C064]	[7854F6 9974C8]	EAPOL	EAPOL-EAPOL-Key (4-Way Handshake Message 3), Length = 151
101	14:09:33.2024/3/26	46.9112993		[7854F6 9974C8]	[JANUZE B6C064]	EAPOL	EAPOL-EAPOL-Key (4-Way Handshake Message 4), Length = 95

共四条 eapol-key 报文

下面对每一条报文逐个分析：

第 1 次握手机文内容如下：

```
▼ 802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: Key (3)
  Length: 95
  Key Descriptor Type: EAPOL RSN Key (2)
  [Message number: 1]
  ► Key Information: 0x008a
    Key Length: 16
    Replay Counter: 1
    WPA Key Nonce: cbc1a8761202a4f8640634dd0a23307dcd6d4a0406ce2994f50033575927690
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 00000000000000000000000000000000
    WPA Key ID: 00000000000000000000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Data Length: 0
```

Version: Eapol-key 是在 802.1X 认证协议下使用，版本号为 2

Typel: 报文类型为 3

Lengh: 报文长度为 95

Key Descriptor Type: 传输密钥的类型为 EAPOL RSN Key

Message number:报文序号为 1

Key Information: 密钥信息 0x008a 对应十进制的 138

Key Length:密钥长度

Replay Counter:重播计数器, 用于抵抗重放攻击的机制

WPA Key Nonce: 一次性随机数

Key IV:密钥初始化向量 00000000000000000000000000000000

WPA Key RSC:密钥重播计数器 0000000000000000

WPA Key ID: 标识密钥版本的参数 0000000000000000

WPA Key MIC:用于验证数据完整性 00000000000000000000000000000000

WPA Key Data Length:传输密钥数据的长度 0

第 2 次握手报文内容如下:

```
~ 802.1X Authentication
  Version: 802.1X-2001 (1)
  Type: Key (3)
  Length: 117
  Key Descriptor Type: EAPOL RSN Key (2)
  [Message number: 2]
  > Key Information: 0x010a
    Key Length: 0
    Replay Counter: 1
    WPA Key Nonce: 8bc822e59905f65d330c9477c313544633820fdbca784a6c6b
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 7963013f33f140d9b7c7a444df34f375
    WPA Key Data Length: 22
  > WPA Key Data: 30140100000fac040100000fac040100000fac020000
```

协议内容与第一条报文基本类似

Message number 报文序号为 2

WPA Key Data : 密钥数据更新

WPA Key Nonce:一次性随机数更新

WPA Key MIC: 完整性验证码更新

密钥长度及报文长度更新

第 3 次握手报文内容如下:

```
~ 802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: Key (3)
  Length: 151
  Key Descriptor Type: EAPOL RSN Key (2)
  [Message number: 3]
  > Key Information: 0x13ca
    Key Length: 16
    Replay Counter: 2
    WPA Key Nonce: cb1c1a8761202a4f8640634dd0a23307dcd6d4a0406ce2994f
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: a48a238b7571a26047abfe7d2d31b54c
    WPA Key Data Length: 56
    WPA Key Data: e8da4b6fe475657f476f6e77ec420e478def624b3a2cc0337c2
```

Message number 报文序号为 3

Replay Counter:重放计数器更新，由于密钥的更新需对重放计数器进行更新
密钥长度及报文长度更新

[illegible]

更新完整性验证码

(对抓包获得的协议进行安全性分析, 例如节 2.2.2)

协议采用 MIC 数据完整性验证码来验证数据是否被他人篡改

协议采用重播计数器 **Replay Counter**，该数值递增，若重播计数器出现数据回卷或重复则认定该消息为重放的消息。

采用一次性随机数在身份认证过程中加入挑战—响应机制。有效防止攻击者冒充身份进行通信。

加入消息序号字段，防止攻击者恶意截停或延迟发送某条消息导致通信双方无法发现。

(说说本次实验的总结感想)

通过本次实验，我掌握了 AP 和 Station 的四次握手过程，并通过 Microsoft Network Monitor 软件对该握手过程进行抓包验证。通过抓包对 eapol 协议进行详细的分析，对 eapol 的安全性有了一定的了解。遗憾的是，由于始终无法抓到校园网的 eapol 协议数据包，并没有找到有效的解决方法，在本次实验中我采用的是抓取手机热点的该数据包。

七、 拓展部分

问题：在安全协议设计中，常使用时间戳和随机数，分析这两种机制的作用和优缺点。

答：

时间戳

作用：

1. **唯一性标识**: 时间戳可以用于标识事件或消息的唯一性，因为它们随着时间的推移而不断增加。

2. **防止重放攻击**: 时间戳可以用于防止重放攻击，接收方可以检查时间戳以确保消息的时效性。

优点：

1. **简单易实现**: 时间戳是易于实现的，因为它们只是表示当前时间的数字。

2. **时效性检查**: 时间戳可以用于检查消息的时效性，从而防止重放攻击。

缺点：

1. **依赖时钟同步**: 时间戳的有效性依赖于系统的时钟同步，如果发送方和接收方的时钟不同步，可能会导致验证失败或安全性问题。

2. **时钟回滚攻击**: 攻击者可以尝试回滚自己的系统时钟，以生成过期的时间戳，从而绕过时效性检查。

随机数

作用：

1. **增加熵**: 随机数引入了随机性和不确定性，增加了协议的安全性，使攻击者更难以猜测下一个值。

2. **防止重放攻击**: 随机数可以用于生成唯一的令牌或标识符，从而防止重放攻击。

优点：

1. **高度随机性**: 随机数是高度随机的，提供了更强的安全性。

2. **不依赖外部因素**: 随机数的生成不依赖于外部因素，如时钟同步，因此更加灵活。

缺点：

1. **难以验证**: 随机数的随机性可能导致接收方难以验证其真实性，特别是如果没有足够的信息来验证其生成方式。

2. **性能开销**: 生成高质量的随机数可能需要较大的计算开销，特别是在低资源环境下可能会成为性能瓶颈。