浙江大学

本科实验报告

课程名称：	物联网安全
实验名称：	重安装键攻击
学　　院：	计算机学院
组员姓名：	刘哲　3150103520
组员姓名：	朱轶凡 3150104416
专　　业：	求计 1501
指导教师：	任奎

2018 年 7 月　26 日

一、 程序分工说明

本实验分为两部分，第一部分是 WPA2 加密的实现，第二部分是重安装键攻击。由朱轶凡和刘哲共同完成。

我们已经把项目的代码上传到了 github，其中 master 分支是第二部分，part1 分支是第一部分。这是 github 的地址：

https://github.com/770120041/WPA2KeyReinstallAttack

代码运行说明：

对于 ap，只需要在源代码目录下，输入命令 javac ap.java ccmp.java,然后运行 java ap 即可。对于 client，只需要在源代码目录下，输入命令 javac client.java ccmp.java,然后运行 java client 即可。对于 adversary，只需要在源代码目录下，输入命令 javac Adversary.java ccmp.java,然后运行 java Adversary 即可。

二、 WPA2 协议实现说明

根据 project 要求，第一部分是通过 Client 和 AP 在同一个端口使用 socket 连接实现的，我们使用了本地 IP 127.0.0.1 来实现连接。从下面的截图可以看到，WPA2 部分已经实现成功。

AP		Client	
收到 REQ 发出 ANonce 收到 CNonce 发送 Msg3 收到 Msg4 接受信息	当前客户端的IP: 127.0.0.1 Receiving : REQ sending : 75443 9528 Receiving : 76904 9528 sending : ACK 9529 Receiving : ACK 9529 AP 收到Msg4,正常接收消息 Receiving : 1000001000110100100100 nounce is :0 Normal receiving : 01010000010011 Trans receiving : POST 163 .com ! Receiving : 1111001000011110100101 nounce is :1 Normal receiving : 00100000011001 Trans receiving : end Receiving : 1001010100111110100103 nounce is :2 Normal receiving : 010001110100014 Trans receiving : GET Receiving : 1001101000101111100103 nounce is :3 Normal receiving : 010010000101014 Trans receiving : HTTP hello here Receiving : 1011101100001000111004 nounce is :4 Normal receiving : 011010010111003 Trans receiving : is nope Receiving : 1001101100110101100104 nounce is :5 Normal receiving : 010010010100113 Trans receiving : INPUT Receiving : 1001110100101110100103 nounce is :6 Normal receiving : 010011110101014 Trans receiving : OUTPUT Receiving : 1001101100110101100104	发送 REQ 收到 ANonce 发送 CNonce 收到 Msg3 发送 Msg4 发送信息	Connected ! Input ip, port, key and txt : 127.0.0.1 3196 z3dg35dg input.txt Sending :REQ rec : #75443 9528# ANounce : 75443 CNounce = 76904 Sending :76904 9528 rec msg3: #ACK 9529# Client发送Msg4. 开始发送消息 Sending :ACK 9529 发送消息,不知道AP是否收到Msg4 nounce is :0 CCMP: POST 163 .com !! 0 Code is !!!!!!!!!! 11010010011110111 Sending :1000001000110100100100101111 CCMP: end 1 Code is !!!!!!!!!! 11010010011110111 Sending :1111001000011110100101111110 发送消息,不知道AP是否收到Msg4 nounce is :2 CCMP: GET 2 Code is !!!!!!!!!! 11010010011110111 Sending :1001010100111110100101011010 发送消息,不知道AP是否收到Msg4 nounce is :3 CCMP: HTTP hello here 3 Code is !!!!!!!!!! 11010010011110111 Sending :1001101000101111100101011111 CCMP: is nope 4 Code is !!!!!!!!!! 11010010011110111 Sending :1011101100001000111000011100 发送消息,不知道AP是否收到Msg4 nounce is :5 CCMP: INPUT 5 Code is !!!!!!!!!! 11010010011110111 Sending :1001101100110101100100011111 发送消息,不知道AP是否收到Msg4 nounce is :6 CCMP: OUTPUT 6

如上图，展示了 WPA2 的连接过程和基本实现。其中不妨以第五个文档 is nope 为例：

发送的第一个八位为 10011011

密文的第一个八位为 11010010

所以明文的第一位为 01001001，ascii 码为 1+8+64=73，对应的字符为 65+8=i（此处 a 为 65）

说明加密成功。

三、 重安装键攻击实现说明

根据要求，我设计了 Client 与中间人通过 localhost 的 4416 端口通信，而中间人通过 localhost 的 4417 端口和 AP 通信。因为 WAP2 协议的问题是,client 不知道 AP 没有收到 Msg4 的情况下，就向 AP 发送消息，所以才能让重安装键攻击能截取到一部分 nonce 相同的密文，然后通过密文来字典攻击。

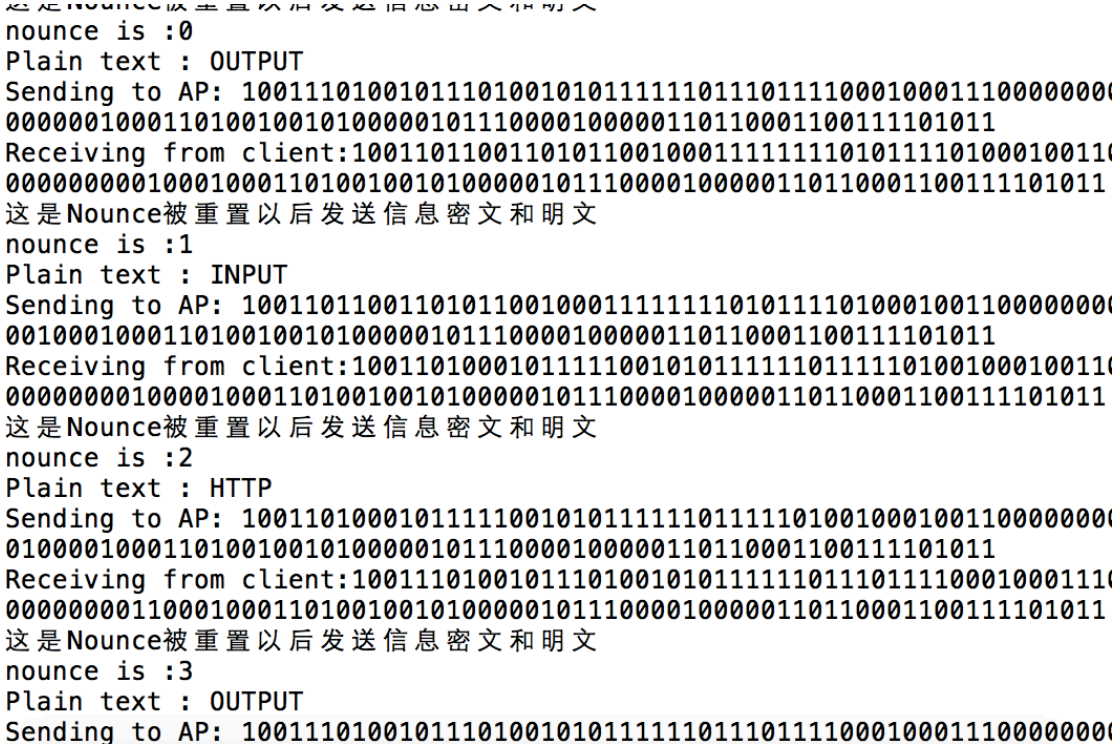
具体实现是，中间人首先建立了一个 serversocket，接受 client 的消息，然后再建立一个 socket 和 ap 通信，首先实现了转发功能。下面是运行的一个截图。

```
lz-2:middle apple$ java Adversary
***中间人，等待客户端的连接***
客户端： 0 socket= 59567
当前客户端的 IP: 127.0.0.1
中间人和AP连接创建！
Receiving from client:REQ
中间人发现认证开始
Sending to AP: REQ
Receiving from AP:98916 9527
中间人从AP获得ANounce:98916,和Random:9527
Sending to Client : 98916 9527
Receiving from client:58678 9527
中间人从Client获得CNounce:58678
Sending to AP: 58678 9527
Receiving from AP:ACK 9528
中间人从AP获取到Msg3
Sending to Client : ACK 9528
Receiving from client:ACK 9528
中间人从Client获取到MSg4,截取不发送给AP
Receiving from client:1000001000110100100100101111111111110100100010011000000000
0000000000000110000010011001000000111001010011011010110001100111101011
获取到Msg4丢失的消息内容
Sending to AP: 1000001000110100100100101111111111110100100010011000000000000000000
0000001100000100110010000001110010100110110101100011001111010 11
```

可以看到中间人能够正常转发和接受 ap 和 client 的消息，并且转发出去。实现了实验要求的第一部分。

对于实验要求的第二部分，中间人 Adversary 设置了一个 counter,来记录 ap 发出新的 Msg3 之前的所有消息，这样就获得了丢失的消息内容。可以看到我输出的内容里有“这是丢失 Msg4 的消息内容”，这就是丢失 Msg4 时候，client 发给 ap 的消息。而下面的是重新发送 Msg4 以后，client 重置 nonce 的内容。通过截图可以看到，第二部分已经实现了。

由于一共有 5 种输入，所以至少需要从 client 获取 4 条信息，然后通过字典攻击，获取明文，通过截图可以看到明文已经获取，这就完成了第三部分。



四、 讨论、心得

这次实验，丰富了我们对计算机网络知识的运用，让我们对网络安全与整个协议的设计，有了一个更加深入的了解。此外，这次实验也让我们对整个网络协议的细节实现，有了更加深入的了解，给了我们很大收获。