

**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

# 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。

# 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 | 发送REQ  收到ANonce  发送CNonce  收到Msg3  发送Msg4  发送信息 |

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

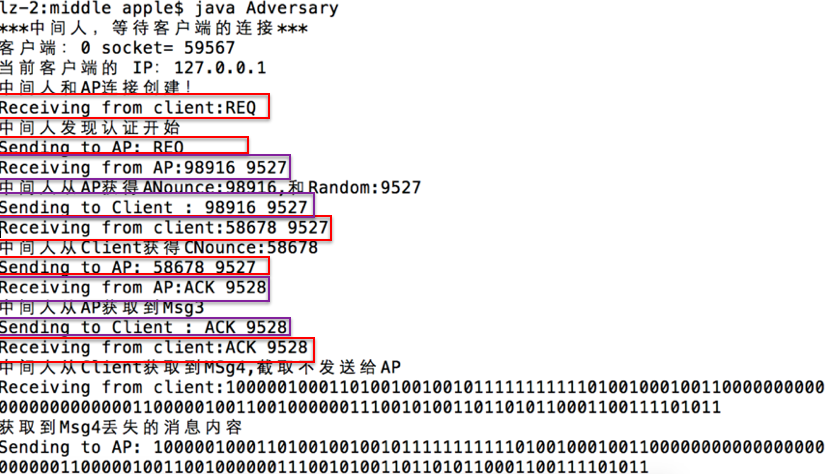
（此处a为65）

说明加密成功。

# 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。

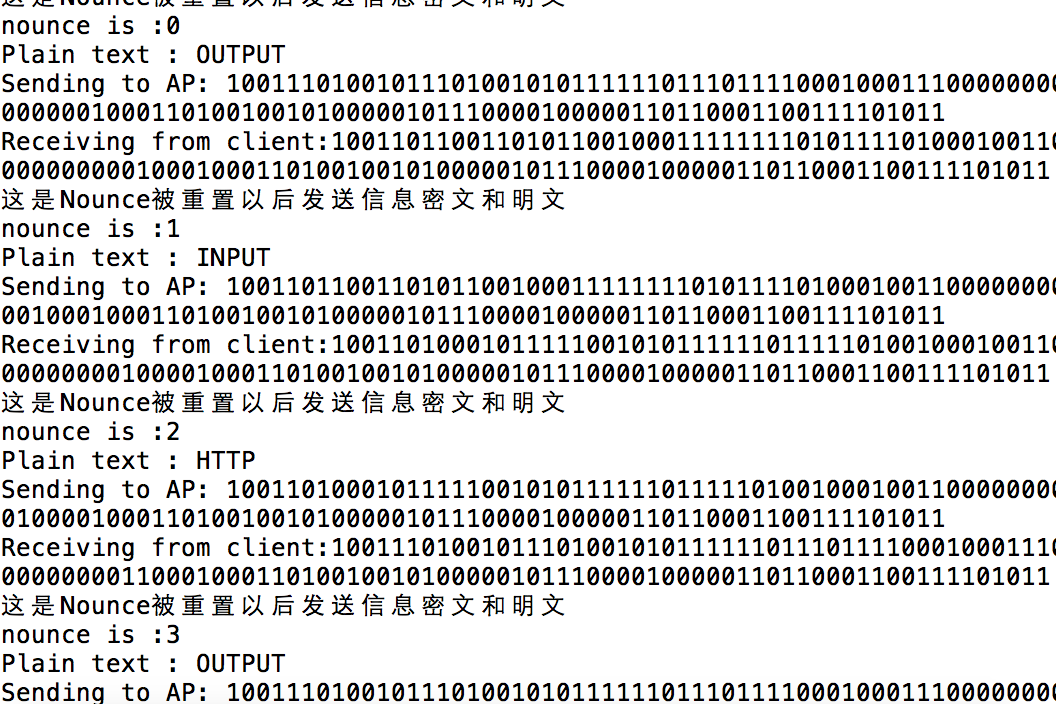


可以看到中间人能够正常转发和接受ap和client的消息，并且转发出去。实现了实验要求的第一部分。

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。



# 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。**