****

**密码学实验**

实 验 报 告

|  |  |
| --- | --- |
| **学 院** | 网络空间安全学院 |
| **专 业** | 信息安全 |
| **班 级** | 17273612 |
| **学 号** | 17271229 |
| **学生姓名** | 杨尽能 |
| **教师姓名** | 吕秋云 |
| **完成日期** | 2019.3.30 |
| **成 绩** |  |
| 实验一 网络系统用户口令抓包分析 | | |
| 1. **实验目的**   本实验主要熟悉wireshark软件的使用，并利用wireshark软件抓取数据包，分析常用邮箱，常用网站和即使聊天工具对登录的用户口令的保护技术。 | | |
| 1. **实验原理和内容概述**   Wireshark是一个网络封包分析软件。网络封包分析软件的功能是撷取网络封包，并尽可能显示出最为详细的网络封包资料。本实验要求使用wireshark对4个网络系统登录时用户的账号密码进行抓包分析，熟练使用wireshark软件，对网络协议中的密码学理论的应用有初步的认识。 | | |
| 1. **实验环境**   Windows10，chrome浏览器（版本72.0.3626.121（32-bit）），wireshark（版本3.0.0） | | |
| 1. **实验主要步骤及实验结果记录（含截图，关键源码，文字解释等）**   1、4399小游戏网站用户口令抓包分析  开启wireshark后登录4399网站，    暂停wireshark捕获。通过表达式”http”进行过滤，如图所示。    通过观察，发现“POST /ptlogin/login.do?v=1 HTTP/1.1(application/x-www-form-urlencoded)”，请求方式为POST，请求URL与登录页面详细，于是双击该行，在HTML From URL Rncoded: application/x-www-form-urlencoded项中发现存在username和password数据，即为我刚才登录使用的用户名和密码。可以看到用户名和密码均为明文传输，可见该网站数据没有经过加密，不安全。    2、人人网用户口令抓包分析  打开人人网登录页面，输入用户名和密码登录。    暂停wireshark捕获，使用表达式“http.request.method=="POST"”，找到登录的数据包，即编号1247。    双击打开数据包，在HTML From URL Rncoded: application/x-www-form-urlencoded项中发现用户名和密码值。      可以看到用户名为key:email，是明文传输；密码key:password经过了加密。可见人人网的用户密码经过了加密，比起4399网站更加安全一点，但用户名还是明文传输。  3、数字杭电校园网用户名口令抓包分析  前面两个都是http网站，可看到它们的安全性都不是很好。因此下一个我抓取的是https协议的数字杭电登录系统。  首先打开数字杭电，来到登录界面输入账号密码登录。    暂停wireshark捕获，刚开始采用“http.request.method=="POST"”表达式进行过滤，发现什么都没抓到。    用http进行过滤也没用。    于是决定采用ip.dst的方式过滤。首先ping网址得到目标ip地址。    Ping不通，但是不要紧，只需要知道ip地址就行，ip地址为192.168.101.60。于是用“ip.dst==192.168.101.60”进行过滤。    发现其中有协议TLSv1，描述为Application Data，应该就是这个，双击打开它。    没有了HTML项，但是在Transport Layer Security项下，发现有Encrypted Application Data，后面的值应该就是被加密后的数据，包括用户名和密码。除此之外别的信息都没有用户名和密码的痕迹。  可见https对全部数据都进行了加密，且隐藏了应用层的信息，大大提高了保密性。  4、QQ用户口令抓包分析  QQ采用的是自己设计的协议，和普通的网站不同，依靠wireshark只能获取到数据包的原始数据，无法分析具体内容。所以最后一个我选择分析QQ。首先登陆QQ。    暂停wireshark捕获，用oicq进行过滤。    点开一个oicq数据包，可以看到在data部分是原始数据，无法分析。    然后利用追踪流来捕获所有与QQ进行通讯的数据。对数据包单击右键，选择追踪流->UDP流，可以追踪UDP的往来数据包。      发现所有UDP流都由02开头，02是QQ的报头，代表该包要执行某条指令。02是常用的报头，几乎包含用户要使用的所有功能，但也存在其他报头。38 0b代表QQ的版本，08 25代表要执行的命令，客户端首次与服务器接触便会发送此命令，29 e2为该包的序列号，63 44 18 ef为用户的QQ号，余下内容为秘钥和加密后的内容等信息，数据包由03代表结束。  由此分析发现，由产品自己设计的协议和加密算法对用户信息的保护更加有效。 | | |
| 1. **实验分析总结及心得**   （结合所学知识对实验过程中观察到的实验结果进行分析总结，以便加深对知识的理解，并总结通过实验学到的知识或技术）  特别推荐学生写出做实验遇到的问题，如何从原理分析得到解决方案，解决过程和结果结果   1. 遇到的问题和解决方法 2. **问题：**刚开始用http过滤后不知道用户名和密码在哪个协议下。     **解决方法：**登录时输入用户名和密码后点击登录其实就是发送一个请求，那么相应的信息就应该在POST方法下，于是双击POST项找到HTML项下的用户名和密码信息。     1. **问题：**在抓取校园网和其他https网站时，找不到请求方式为POST的数据包，用http过滤也什么都没有。     **解决方法：**https采用的是TLSv1协议，相比于http网站更加安全，也不用http协议。因此采用ip.dst对目标ip地址进行筛选，找到TLSv1协议的数据包，在其下找到被加密后的信息。       1. **问题：**Ping那些https网站时ping不通。     **解决方法：**校园网和其他https网站的服务器应该都设置了防火墙来阻挡，使得我们无法ping通他们的网页。不过这对于本实验没有什么影响，因为ip地址已经给出了，我们要的就是这个ip地址，ping不ping通没有什么。   1. **问题：**在登录一些网站后，抓取数据包时没有请求方式为POST的数据包，只有GET的。   **解决方法：**这个问题是我在随便抓取http网站时偶然发现的，当时没有找到POST数据包我就放弃了，后来才知道不只是POST才有账号密码信息，GET也会有。因此如果以后碰到只有GET没有POST的数据包时，就在GET项下面找。   1. **问题：**登录QQ时捕获的数据不知道在什么协议下面。   **解决方法：**QQ用的是oicp协议，所以要用oicp来进行过滤，双击任意一个oicp数据可以看到被加密的数据。       1. **问题：**登录https网站时双击TLSv1后没有发现HTML项，不知道用户名和密码被保存在了哪里。     **解决方法：**用tls进行过滤后，双击info为Application Data的数据包，里面的Transport Layer Security下就包含了被加密的数据（Encrypted Application Data）。     1. 总结 2. 刚开始我以为需要真正登录网站才能抓取到用户名和密码，但其实登录网站时不用真的登录进去，只需要伪登录即可，目的是发送POST请求，即可在抓取的POST数据包中得到刚刚发送的用户名和密码，然后分析有没有加密。 3. 用户名和密码等信息不只是会出现在POST请求中，在http网页中可能会出现在GET请求中，而在https网页中则会出现在TLSv1协议下。 4. 在QQ等采用自己协议的软件下，协议和加密算法都与其他网页不同，对用户信息的保护更加有效。 5. 以往的http网页大多都对用户名和密码采用明文传输，少数会对密码进行md5加密，安全性不高，容易泄露用户隐私。而新型的https网页采用TLSv1协议，对数据全程加密，无法分析具体传输内容，因此对用户信息的保护更加有效。对网站本身来说，https比http安全得多，所以现在大多数网站都改成了https。 6. **分析与思考** 7. 网络系统用户登录时的用户名和密码进行保护的技术都有哪些？ 8. 直接明文保存 9. 使用对称加密算法来保存，比如3DES、AES等算法 10. 使用MD5、SHA1等单向HASH算法保护密码 11. 特殊的单向HASH算法 12. PBKDF2算法 13. bcrypt、scrypt等算法 14. Wireshark的工作原理是什么？   （1）收集：从网卡上收集二进制信息（将网卡设置成混杂模式完成抓包）  （2）转换：将捕获的二进制信息转换成可读形式。  （3）分析：对捕获和转换后的数据进行分析。 | | |

**实验二 网络应用系统安全技术分析**

* 1. **实验目的**

本次实验主要利用wireshark抓包软件抓取系统登录、支付过程、聊天功能的数据包，通过抓取的数据包，分析以上系统功能的安全保护技术。

* 1. **实验原理和内容概述**

本实验继续使用wireshark抓包软件来抓取网站信息，实验要求使用三类系统应用功能，了解其登录过程、支付过程和聊天等功能的安全保护技术，通过抓包数据流程，分析是否进行加密处理，使用哪种协议，以及存在的安全问题。

* 1. **实验环境**

Windows10，chrome浏览器（版本72.0.3626.121（32-bit）），wireshark（版本3.0.0）

* 1. **实验主要步骤及实验结果记录（含截图，关键源码，文字解释等）**

1. 系统登录安全分析
2. 某网站登录系统分析

在我们使用计算机的过程中，由于不同的需求，经常会浏览各种各样的网站，还会注册成为该网站的用户，更加方便我们使用网站的功能。但是由于网站的后台维护人员水平参差不齐，所以用户隐私数据存在泄漏的风险。接下来我以网站“泛雅培训平台”为例，分析它的登录安全性。

下图是其注册和登录界面：





1. 网站登录系统的抓包数据分析

利用charles抓包软件，对该网站的注册和登录功能进行抓包，抓取的注册数据包为：



登录数据包为：



可以看到，在网站注册时的邮箱、用户名、密码、验证码等，还有登录时的用户名、密码、验证码等都是明文，没有经过任何的加密处理。

1. 网络功能的安全性分析

我们经常访问并注册各种各样的网站，这些网站中不乏欺骗用户、窃取用户个人信息的钓鱼网站，但大部分是应用服务类网站。由于网站安全保护技术水平的不同，我们在不知不觉中，一些隐私的信息就已经泄露，甚至可能被不法分子利用。

1. 分析与思考

什么样的网站安全保护级别较高？什么样的网站安全保护级别较低？

由实验一抓包分析可知用https协议和自己设计的协议的网站安全级别较高，因为它们都有复杂的加密机制，不易被人获取数据；而传统的http网站安全级别较低，因为它们通常只用明文储存数据或用md5加密密码，容易被人抓取数据。

1. 网络支付过程安全技术分析
2. 支付宝支付分析

支付宝的登录方式主要有三种，第一种是普通的用户名登录，第二种是利用淘宝会员登录，第三种是扫码登录。支付宝登录界面如下：



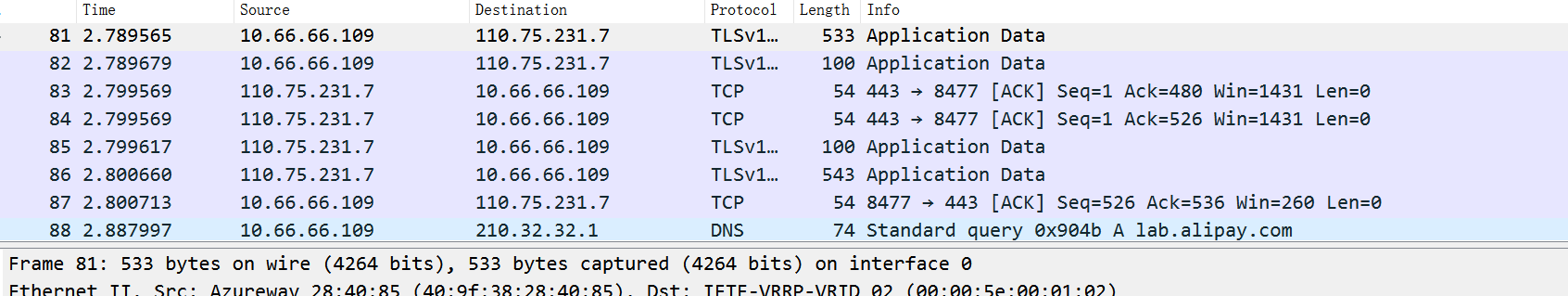


登录后支付宝的界面如图所示：

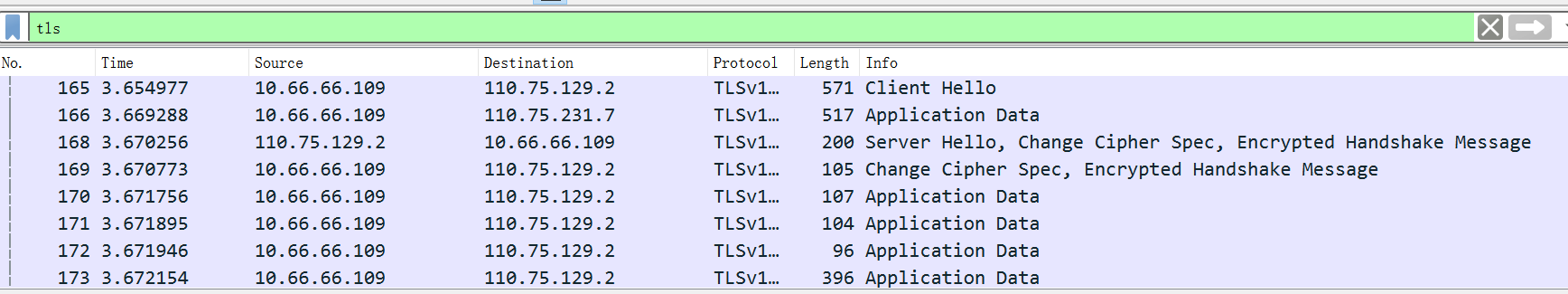


1. 支付宝支付过程的抓包数据分析

用支付宝进行转账，利用wireshark抓取支付过程中的数据包，并进行分析。转账后，暂停wireshark捕获，抓包的截图如图所示：

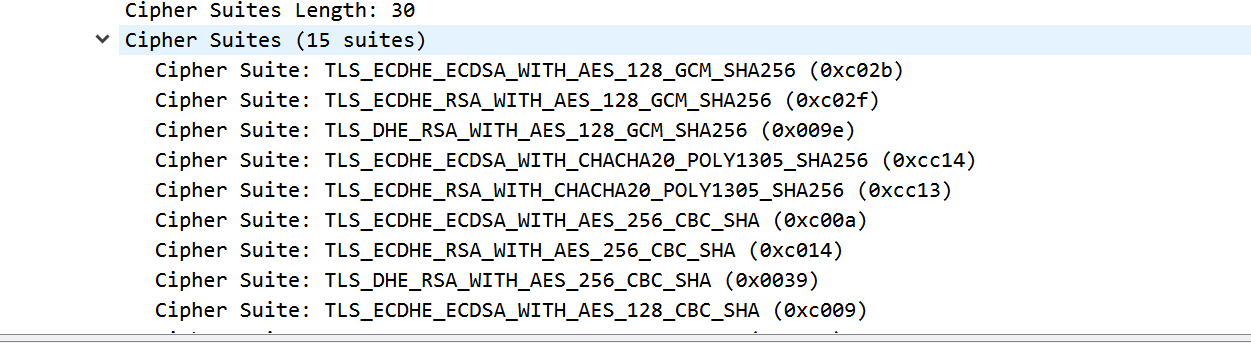


用tls进行过滤，得到数据如下：

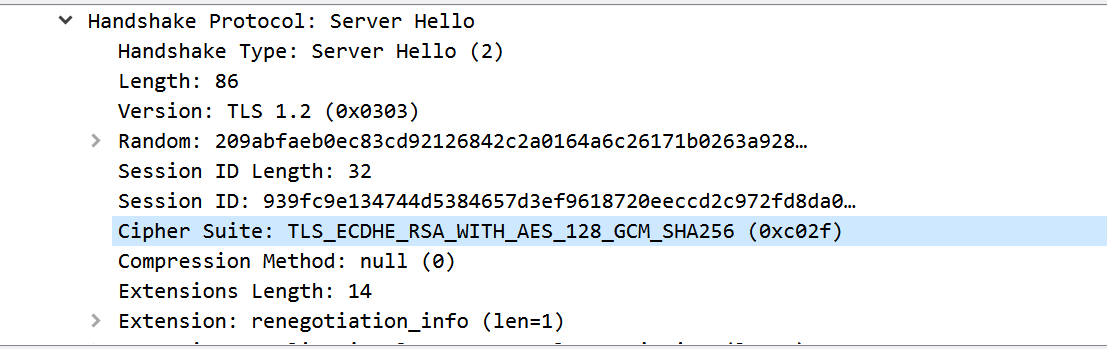


根据抓包的结果分析，可以看到，在info一列中，在支付之前，要经过Client Hello（客户连接）、Server Hello（服务器回应）、Certificate（颁发证书）、Client Key Exchange（客户密钥交换）、Change Cipher Spec（改变密码规范）、Encrypted Handshake Message（加密握手消息）等工程，才能传输Application Data（应用程序数据），并且可以发现，以上步骤全部使用TLSv1.2协议进行加密，保障转账用户的用户名、转账金额等数据的安全性。

Cilent Hello部分内容截图：



Server Hello部分内容截图：



通过对比可以发现，在Client Hello中，共给出了22个Cipher Suites,可使用RSA、ECDSA、ECDHE与AES加密算法进行数据保护，而在Sever Hello中，通过协商选取了22组中的一组。

1. 支付宝支付功能的安全性分析

支付宝使用HTTPS协议传输数据，在HTTP协议层下加入SSL协议来实现对传输数据的加密。通过分析抓取的数据包可以发现，在支付宝支付过程中，利用了ECDSA、RSA、Diffie-Hellman密钥交换算法，AES加密算法和SHA报文认证信息码（MAC）算法等，共同保障传输数据的安全性。

1. 分析与思考

分析支付宝付款码支付和声波支付的工作原理，分析它们可能存在的安全隐患，并说明原因。

答：支付宝付款码支付时，用户的付款码中包含的是识别该用户的专属ID，商家通过收银系统向支付宝提交订单时，把扫码枪识别出来的信息传递给支付宝，他们根据这个专属ID找到对应的用户，通过代扣直接就扣款了。

声波支付时，手机客户端发出声波，终端设备获取声波并转化为一个交易号。售货机将商品信息+交易号通过网络发送到支付宝后端生成账单。随后推送到客户端里；交易号实际就是用来识别这个订单是谁。