密码学课程第 3 次实验报告

实验名称：分析校园无线身份认证密码协议

学号： 2011428 姓名： 王天行 班级： 密码科学与技术

一、 实验目的

使用抓包软件捕获登录南开大学无线 WIFI——NKU_WLAN 的过程，根据抓包结果对所涉及的身份认证密码协议及其安全性进行分析。

抓包工具：Wireshark&Microsoft Network Monitor

实验环境：Windows

二、 实验内容说明

使用抓包软件捕获登录南开大学无线 WIFI——NKU_WLAN 的四次握手数据包，并进行分析

三、 实验原理

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。

1) 名词解释

Authenticator：认证者，指 AP，即无线接入点

Supplicant：请求者，指 Station，即任何企图接入 AP 服务集的设备

ANonce：由 AP 生成的随机数

SNonce：由 Station 生成的随机数

Mac(AA)：AP 的 Mac 地址

Mac(SA)：Station 的 Mac 地址

PRF：Pseudo-Random Function，表示伪随机函数

MSK：Master Session Key，主会话密钥

PMK：Pairwise Master Key，成对主密钥，由 MSK 生成，用于生成 PTK

GMK：Group Master Key，组主密钥，同样由 MSK 生成，用于生成 GTK

PTK：Pairwise Transit Key，成对临时密钥，用来加密 AP 和 Station 通讯的单播数据包，AP 与每个 Station 通讯用的 PTK 都是唯一的。PTK 的生成函数如下：

$$\mathrm{PTK} = \mathrm{PRF}(\mathrm{PMK} + \mathrm{ANonce} + \mathrm{SNonce} + \mathrm{Mac(AA)} + \mathrm{Mac(SA)})$$

GTK：Group Temporal Key，组临时密钥，用来加密 AP 和 Station 通讯的多播/广

播数据包，连接该 AP 的所有 Station 共享一个 GTK。GTK 的生成函数如下：

$$GTK = PRF(GMK + ANonce + Mac(AA))$$

MIC：Message Integrity Check，消息完整性校验码，针对一组需要保护的数据计算出的散列值，用来防止数据遭篡改

2) 协议描述

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。协议流程可以参考图 7。

（1）第一次握手：AP—>Station：ANonce

AP 产生随机数 Anonce，用 EAPOL-KEY 帧发送给 Station，Station 在收到消息后用它生成 PTK，前面已经提到 PTK 的生成函数：$PTK = PRF(PMK + ANonce + SNonce + Mac(AA) + Mac(SA))$。其中，PTK 的前 128 位是 KCK（EAPOL-Key Confirmation Key），用来校验 EAPOL-Key 帧的完整性。

（2）第二次握手：Station—>AP：SNonce，MIC

Station 创建了自己的 PTK 后，会立即响应一条包含 SNonce 和 MIC 的 EAPoL 消息给 AP，AP 将进行同样的计算得到 PTK， 然后用得到的前 128 位对 EAPoL

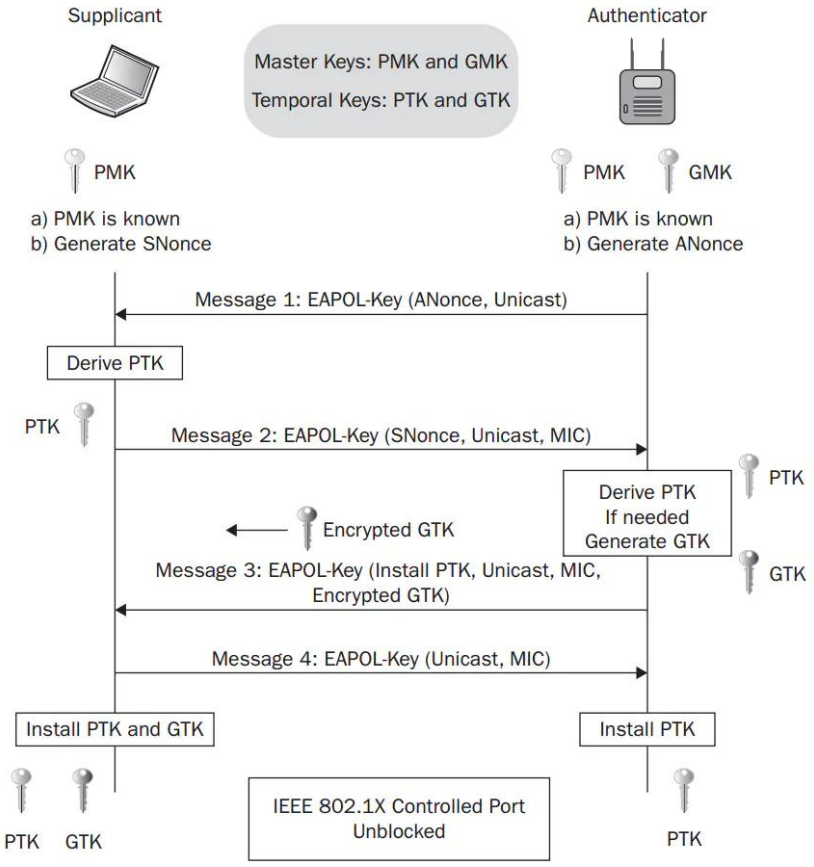


图 7 四次握手流程图

报文进行完整性校验：比较所得到的值是否和收到报文中的 WPA Key MIC 的值一致，如果一致，则验证成功，说明 Client 端（即 Station）拥有正确的 PMK，否则判定 Client 端拥有的 PMK 错误，整个握手就此停止。

（3）第三次握手：AP—>Station：MIC，Encryted GTK

验证成功后，AP 将 MIC 和用 PTK 加密后的 GTK 发送给 Station，并且告知 Station 安装 PTK 和 GTK。Station 收到消息后检查 MIC，同第二次握手的检查流程一样，如果不一致，将默默丢弃第三个报文，握手就此停止。验证成功后，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—>AP：MIC

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。安装的意思是指使用 PTK 和 GTK 来对数据进行加密。

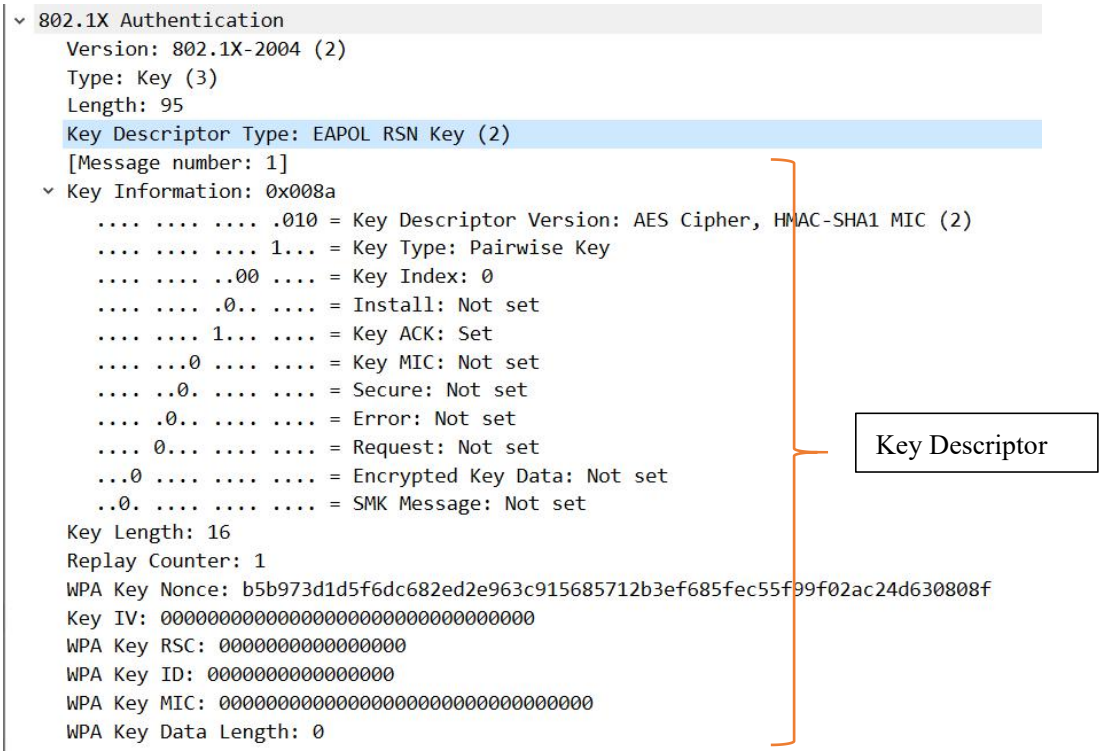
四、 实验步骤

12	15:11:45 2023/3/14	3.3372044	[DEAA27 3B388D]	[F057A6 FBA2D4]	EAPOL	EAPOL:EAPOL-Key (4-Way Handshake Message 1), Length = 95
13	15:11:45 2023/3/14	3.3372329	[F057A6 FBA2D4]	[DEAA27 3B388D]	EAPOL	EAPOL:EAPOL-Key (4-Way Handshake Message 2), Length = 123
14	15:11:45 2023/3/14	3.3522511	[DEAA27 3B388D]	[F057A6 FBA2D4]	EAPOL	EAPOL:EAPOL-Key (4-Way Handshake Message 3), Length = 183
15	15:11:45 2023/3/14	3.3522943	[F057A6 FBA2D4]	[DEAA27 3B388D]	EAPOL	EAPOL:EAPOL-Key (4-Way Handshake Message 4), Length = 95

用 MNM 抓取到连接手机热点 WIFI 的四次握手数据包如上图。在 wireshark 中打开：

12	3.166938400	de:aa:27:3b:38:8d	f0:57:a6:fb:a2:d4	EAPOL	165 Key (Message 1 of 4)
13	3.166966900	f0:57:a6:fb:a2:d4	de:aa:27:3b:38:8d	EAPOL	191 Key (Message 2 of 4)
14	3.181985100	de:aa:27:3b:38:8d	f0:57:a6:fb:a2:d4	EAPOL	253 Key (Message 3 of 4)
15	3.182028300	f0:57:a6:fb:a2:d4	de:aa:27:3b:38:8d	EAPOL	163 Key (Message 4 of 4)

1）第一次握手 AP—>Station:ANonce



Key Descriptor 部分用来描述 EAPOL-Key 帧的 Key 信息

Key Info：Secure 位为 0 表示该帧没有加密的数据；Key ACK 为 1 表示 AP 要求 STA 回复此帧；Install 为 0 表示现在还无法安装 PTK。Key Type 为 1 表示当前时 Pairwise 密钥派生；Key Mic 为 0，表示该帧不包含 MIC 数据。

Replay Counter：STA 需要保存这个值（这里为 1）以检测重放攻击

WPA Key Nonce 存储的就是 Nonce，这里由 AP 生成的 Nonce 叫做 ANonce。

2）第二次握手 Station—>AP:SNonce，MIC

```
802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 123
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 2]
  Key Information: 0x010a
      .... .... .... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
      .... .... .... 1... = Key Type: Pairwise Key
      .... .... ..00 .... = Key Index: 0
      .... .... .0.. .... = Install: Not set
      .... .... 0... .... = Key ACK: Not set
      .... ...1 .... .... = Key MIC: Set
      .... ..0. .... .... = Secure: Not set
      .... .0.. .... .... = Error: Not set
      .... 0... .... .... = Request: Not set
      ...0 .... .... .... = Encrypted Key Data: Not set
      ..0. .... .... .... = SMK Message: Not set
    Key Length: 0
    Replay Counter: 1
    WPA Key Nonce: 04b28b81b3212a8faf473e1743473d2e7e853505a7d717982e89ac8bd42a6685
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 01653c6135163e18bb54c1a4533bb706
    WPA Key Data Length: 28
  > WPA Key Data: 301a0100000fac040100000fac040100000fac02bc000000000fac06
```

Key Info：Key Mic 为 1，表示该帧包含 MIC 数据。

Replay Counter：等于第一个帧中的 Replay Counter。

WPA Key Mic 是对整个 EAPOL-Key 帧进行计算而来，计算方法由 Key Descriptor Version 指定

WPA Key Nonce 存储 Station 生成的 SNonce。

WPA Key Data

```
WPA Key Data: 301a0100000fac040100000fac040100000fac02bc000000000fac06
  Tag: RSN Information
      Tag Number: RSN Information (48)
      Tag length: 26
      RSN Version: 1
    Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
        Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
        Group Cipher Suite type: AES (CCM) (4)
      Pairwise Cipher Suite Count: 1
    Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
      Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
          Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
          Pairwise Cipher Suite type: AES (CCM) (4)
      Auth Key Management (AKM) Suite Count: 1
    Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
      Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
          Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
          Auth Key Management (AKM) type: PSK (2)
    RSN Capabilities: 0x00bc
        .... .... .... ...0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
        .... .... .... ..0. = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
        .... .... .... 11.. = RSN PTKSA Replay Counter capabilities: 16 replay counters per PTKSA/GTKSA/STAKeySA (0x3)
        .... .... ..11 .... = RSN GTKSA Replay Counter capabilities: 16 replay counters per PTKSA/GTKSA/STAKeySA (0x3)
        .... .... .0.. .... = Management Frame Protection Required: False
        .... .... 1... .... = Management Frame Protection Capable: True
        .... ...0 .... .... = Joint Multi-band RSNA: False
        .... ..0. .... .... = PeerKey Enabled: False
        ..0. .... .... .... = Extended Key ID for Individually Addressed Frames: Not supported
      PMKID Count: 0
      PMKID List
    Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
        Group Management Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
        Group Management Cipher Suite type: BIP (128) (6)
```

包含一个 RSN Information Element。该 RSN IE 来自 STA 之前和 AP 在关联操作时获

得的 RSN IE。

3）第三次握手 AP—>Station:MIC，Encryted GTK

```
802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 183
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 3]
  Key Information: 0x13ca
      .... .... .... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
      .... .... .... 1... = Key Type: Pairwise Key
      .... .... ..00 .... = Key Index: 0
      .... .... .1.. .... = Install: Set
      .... .... 1... .... = Key ACK: Set
      .... ...1 .... .... = Key MIC: Set
      .... ..1. .... .... = Secure: Set
      .... .0.. .... .... = Error: Not set
      .... 0... .... .... = Request: Not set
      ...1 .... .... .... = Encrypted Key Data: Set
      ..0. .... .... .... = SMK Message: Not set
    Key Length: 16
    Replay Counter: 2
    WPA Key Nonce: b5b973d1d5f6dc682ed2e963c915685712b3ef685fec55f99f02ac24d630808f
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 96a8360d2aec061e55a881aafad6e6fe
    WPA Key Data Length: 88
    WPA Key Data: 6b6c9066ca5326bbe19d45bf02922255360666252 2bf49f691f97c63057b6a5af2bf394a…
```

Key Info：Install 为 1 表示 STA 收到该帧后可以安装 PTK 了；Secure 位为 1 表示 AP 已经派生了 PTK；Encrypted Key Data 设为 1，表示 Key Data 被加密了。

Replay Counter 为 2，比前面的值增加 1。

Key Nonce 的值和第一帧一样。

MIC 对 EAPOL-Key 整个进行计算得来。

Key Data 由 PTK 加密后而来，其解密后的内容包括 GTK 信息

4）第四次握手 Station—>AP:MIC

```
802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 95
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 4]
  Key Information: 0x030a
      .... .... .... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
      .... .... .... 1... = Key Type: Pairwise Key
      .... .... ..00 .... = Key Index: 0
      .... .... .0.. .... = Install: Not set
      .... .... 0... .... = Key ACK: Not set
      .... ...1 .... .... = Key MIC: Set
      .... ..1. .... .... = Secure: Set
      .... .0.. .... .... = Error: Not set
      .... 0... .... .... = Request: Not set
      ...0 .... .... .... = Encrypted Key Data: Not set
      ..0. .... .... .... = SMK Message: Not set
    Key Length: 0
    Replay Counter: 2
    WPA Key Nonce: 0000000000000000000000000000000000000000000000000000000000000000
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 314b403d63fc5fe38e2abea3e940b864
    WPA Key Data Length: 0
```

五、实验结果分析

对于手机热点 WIFI 的安全性分析

1）数据安全性

协议使用的成对临时密钥 PTK 包含 3 个部分，KCK（Key Confirmation Key），KEK（Key Encryption Key），TK（Temporal Key）。其中，KEK 和 KCK 在四次握手中用于数据加密和完整性验证。协议还使用 MIC 来防止数据遭篡改，保证数据完整性。

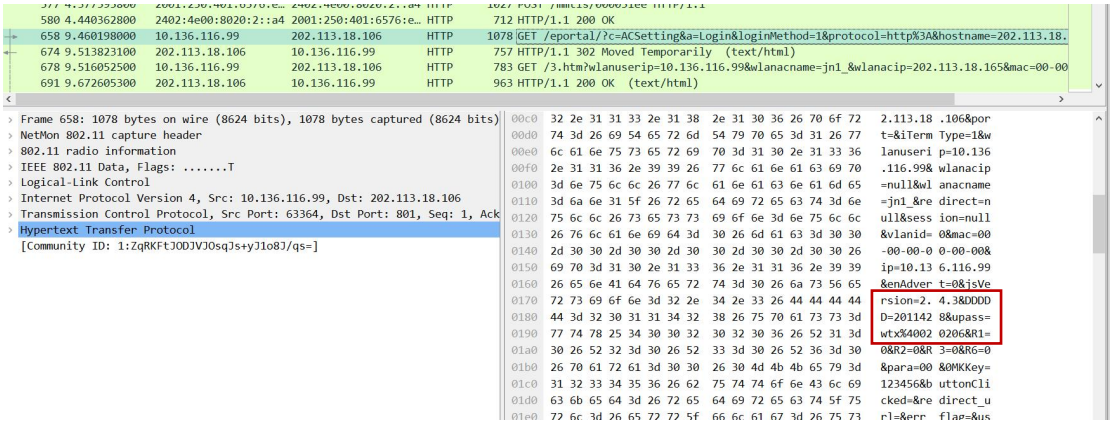
2）拒绝服务攻击（DoS）

消息 1 并没有使用任何加密或完整性校验措施，而且如果 AP 在规定时间内没有收到客户端发回的应答消息 2，就会启动超时装置，重传刚才发送的消息 1。因此，客户端会对收到的每一个消息 1 计算 SNonce 和 PTK。攻击者可以根据这一点伪造消息 1，使客户端重新计算 PTK，由于前后的 Nonce 值不一样，因此很容易造成 PTK 生成的混乱。若攻击者重复这样的攻击过程，那么客户端永远无法与 AP 完成四次握手过程，更不可能通过 AP 访问其他合法资源，从而实施 DoS 攻击。

对于连接校园网的安全性分析

连接校园网捕获的数据包中，并没有 EAPOL 数据包和 802.11 协议相关数据包。

通过注销页（网页）进行登录，在捕获的数据包中可以获得学号与密码。



在电脑中查询网络相关信息，发现校园网的安全类型为无身份验证（开放式）

六、 总结感想

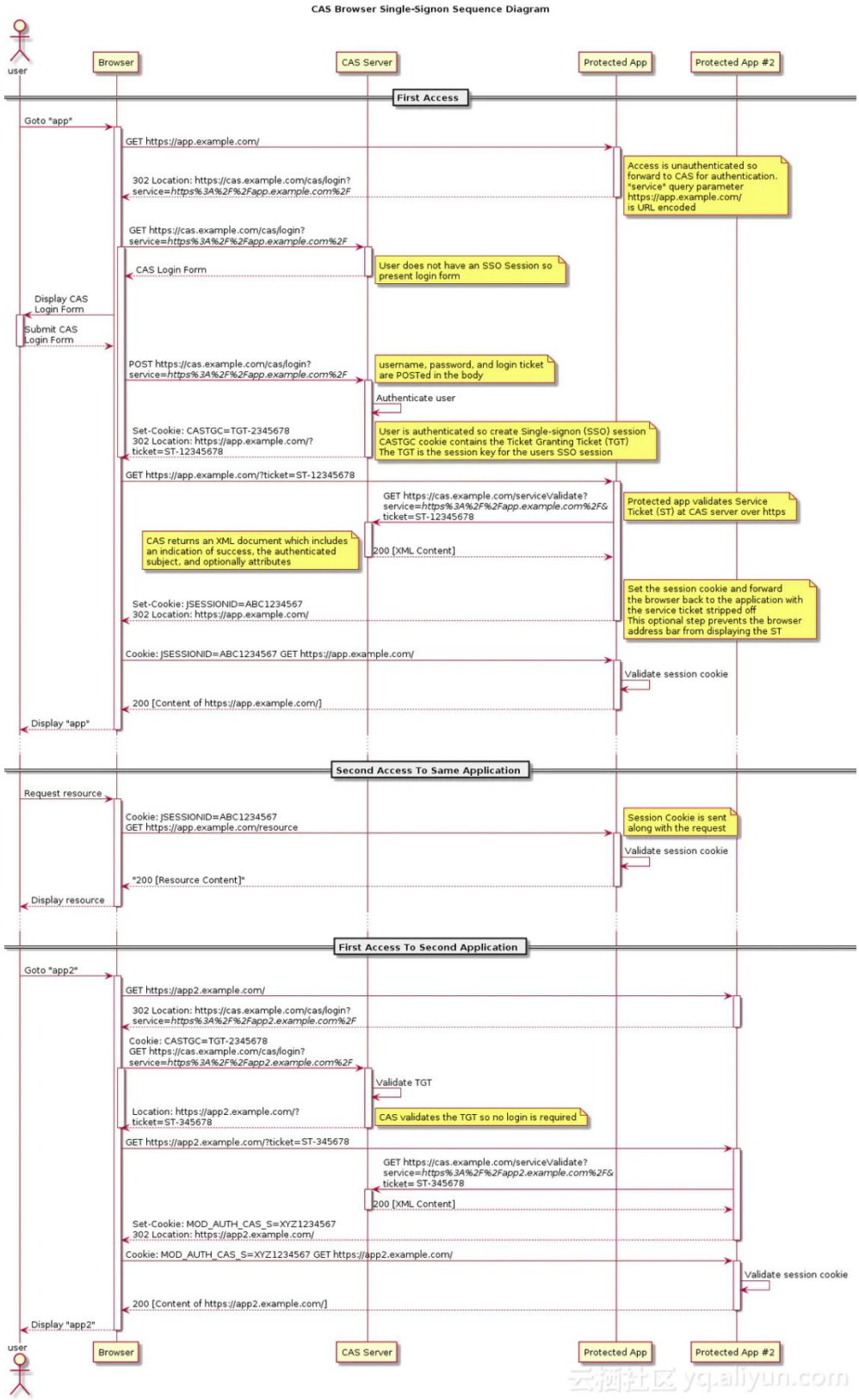
Q.通过抓包对南开大学 SSO（Single Sign On 单点登录）协议进行分析。

A.通过 https://sso.nankai.edu.cn/sso/login 看到 SSO 的定义：

“Single Sign On”，简称 SSO。主要是解决学校师生访问学校的应用系统时，都需要去输入一遍账号密码进行登录，不方便而且不容易记住（应用系统特别多，密码账号还不一样）。单点登录，只需记住一个登录账号，登录一次后，可进入其他系统，不需要再次登录。

下图是 CAS 官网上的标准流程，具体流程如下：

1. 用户访问 app 系统，app 系统是需要登录的，但用户现在没有登录。
2. 跳转到 CAS server，即 SSO 登录系统，以后图中的 CAS Server 我们统一叫做 SSO 系统。SSO 系统也没有登录，弹出用户登录页。
3. 用户填写用户名、密码，SSO 系统进行认证后，将登录状态写入 SSO 的 session，浏览器（Browser）中写入 SSO 域下的 Cookie。
4. SSO 系统登录完成后会生成一个 ST（Service Ticket），然后跳转到 app 系统，同时将 ST 作为参数传递给 app 系统。
5. app 系统拿到 ST 后，从后台向 SSO 发送请求，验证 ST 是否有效。
6. 验证通过后，app 系统将登录状态写入 session 并设置 app 域下的 Cookie。



Q.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。

A.时间戳（Timestamp）

优点：

1. 时间戳服务器与权威的国家授时中心对接，通过与数字签名的有效结合，可为互联网活动任何电子文件或网上交易所产生的电子数据提供保密性、完整性、防抵赖等功能，通过数字签名保证内容和签发人的不可抵赖性，通过时间戳提供准确的、权威的、不可篡改的时间证明和内容完整性证明。时间戳已成为网络数据安全不可或缺的一部分。
2. 防 dos 攻击（第三方使用正确的参数，不停请求服务器，使之无法正常提供服务）
3. 操作简单、迅速，存储容量小，验证简单

缺点：

1. 双方可以进行串通篡改或伪造时间戳
2. 需要双方调整时间一致，对于时钟的准确性要求高

随机数（Nonce）

优点：

1. Nonce 是由服务器生成的一个随机数，在客户端第一次请求页面时将其发回客户端；客户端拿到这个 Nonce，将其与用户密码串联在一起并进行非可逆加密（MD5、SHA1 等等），然后将这个加密后的字符串和用户名、Nonce、加密算法名称一起发回服务器；服务器使用接收到的用户名到数据库搜索密码，然后跟客户端使用同样的算法对其进行加密，接着将其与客户端提交上来的加密字符串进行比较，如果两个字符串一致就表示用户身份有效。这样就解决了用户密码明文被窃取的问题，攻击者就算知道了算法名和 nonce 也无法解密出密码。每个 nonce 只能供一个用户使用一次，这样就可以防止攻击者使用重放攻击，因为该 Http 报文已经无效。可选的实现方式是把每一次请求的 Nonce 保存到数据库，客户端再一次提交请求时将请求头中得 Nonce 与数据库中得数据作比较，如果已存在该 Nonce，则证明该请求有可能是恶意的。

缺点：

1. 有可能在两次正常的资源请求中，产生的随机数是一样的，这样就造成正常的请求也被当成了攻击，随着数据库中保存的随机数不断增多，这个问题就会变得很明显
2. 所有使用的随机数需要进行存储，存储量大