作业四

(密码学与网络安全课程报告)

姓　　名：肖文韬

学　　号：2020214245

专 业 方 向：电子信息（计算机技术）

邮　　箱：xwt20@mails.tsinghua.edu.cn

二〇二一年三月二十六日

第 1 章　作业内容

1. 请简要写出抵御重放攻击的几种方案。

   解：

   重放攻击（Replay Attacks）又称重播攻击、回放攻击或新鲜性攻击（Freshness Attacks），是指攻击者发送一个目的主机已接收过的包，来达到欺骗系统的目的，主要用于身份认证过程，破坏认证的正确性。

   防御重放攻击的一般策略是通过使用会话 ID 和组件编号标记每个加密的组件，可以防止重放攻击。之所以可行，是因为为程序的每次运行创建了唯一的随机会话 ID，因此先前的结果更加难以复制。由于每个会话的 ID 不同，攻击者无法执行重放。

   具体的防御方案有：

   (a) **会话标识符**。会话标识符是一种可用来帮助避免重放攻击的机制。Bob 将一次性令牌发送给 Alice，Alice 使用该令牌来转换密码并将结果发送给 Bob。例如，她将使用令牌来计算会话令牌的哈希，并将其附加到要使用的密码上。Bob 使用会话令牌执行相同的计算。当且仅当 Alice 和 Bob 的值都匹配时，登录成功。会话令牌应通过随机函数选择（通常使用伪随机函数）。

   (b) **一次性密码**。一次性密码与会话令牌类似，因为一次性密码在使用后（或在很短的时间内）就会过期。除会话外，它们还可用于验证单个交易，也可以在身份验证过程中使用，以帮助在彼此通信的两方之间创建信任。

   (c) **随机数和 MAC**。Bob 还可以发送随机数，但消息认证码（MAC）应随其后发送，Alice 应检查该消息。

   (d) **时间戳**。添加时间戳是防止重放攻击的另一种方法。同步应使用安全协议来实现。例如，Bob 定期广播他的时间和 MAC。当 Alice 要向 Bob 发送消息时，她会在消息中包含最佳的估计时间，这也是经过身份验证的。Bob 仅接受时间戳在合理范围内的消息。这种方案的优点是 Bob 不需要生成（伪）随机数，而 Alice 不需要向 Bob 询问随机数。在单向或接近单向的网络中，这可能是一个优势。但是，如果重放攻击执行得足够快（即在该“合理”范围内），则可以成功。

2. 列举四种密钥分配的方式，描述其优缺点。

解：

(a) **基于对称密码体制的密钥分配: 无中心的密钥分配**。需要进行保密通信的两个用户事先应该具有主密钥。对 n 个用户的网络这种方法无实用价值。

(b) **基于对称密码体制的密钥分配: 有中心的密钥分配**。每个用户与 KDC 都有共享密钥，用户必须完全信任 KDC。在 N 个用户时，KDC 只需要分发 N 个密钥，成本比较高。

(c) **基于非对称加密：公钥的公开发布**。用户将自己的公钥发送给每一个其他的用户。方法简单，容易伪造这种发布。

(d) **基于非对称加密：通过公钥管理机构发布公钥**。公钥管理机构为用户建立维护动态的公钥目录。每个用户知道管理机构的公开钥，只有管理机构知道自己的秘密钥。目录表的建立和维护，公布由可信的实体和组织承担。

3. 简述三种数字签名方案。

数字签名是一种功能类似写在纸上的普通签名、但是使用了公钥加密领域的技术，以用于鉴别数字信息的方法。一套数字签名通常会定义两种互补的运算，分别用于签名和验证。

解：

(a) **RSA 签名体制**。任意选取两个大素数 p 和 q，计算 n=p*q，然后随机选取一个与 φ(n) 互素的数 e 作为公钥，用扩展 Euclid 算法计算出私钥 $d \equiv e^{-1} \bmod \varphi(n)$。基于大整数的质因数分解是 NP 问题作为密码安全性的理论基础。

(b) **Rabin 数字签名方案**。签名算法对应 Rabin 密码体制中的解密过程。待签名的消息为 m，判断消息 m 是否同时是模 p 和模 q 的平方剩余。若是，那么对 m 签字就是计算模 m 的平方根；若否，则对 m 作一个变换，将其映射为满足需要的 m’。求解合数模的平方根是困难的，除非能够对模数进行素因子分解。即知道模数 n 的两个素因子 p 和 q，然后将问题转化成以此同余方程组，再利用中国剩余定理求解。

(c) **DSA 数字签名算法**。Digital Signature Algorithm (DSA) 是 Schnorr 和 El-Gamal 签名算法的变种，被美国 NIST 作为 DSS 标准。DSA 是基于整数有限域离散对数难题的，其安全性与 RSA 相比差不多。DSA 的一个重要特点是两个素数公开，这样，当使用别人的 p 和 q 时，即使不知道私钥，你也能确认它们是否是随机产生的，还是作了手脚。RSA 算法却做

不到。

4. 如何利用伪造的 X.509 证书实现 SSL 会话劫持?

解：

当 SSL 客户端与 SSL 服务端建立连接时，在正常的连接握手阶段，客户端必定会要求服务端出示其 X.509 公钥证书，并根据以下 3 个要素验证服务器证书的有效性：

(a) 该公钥证书的 subject name(主题名) 和所访问的服务器站点的名称是否一致；

(b) 该公钥证书的是否过期；

(c) 该公钥证书及其签发者证书链中的证书的数字签名是否有效（层层验证，一直验证到根 CA 证书为止）。

当 SSL 客户端访问一个基于 HTTPS 的加密 Web 站点时，只要上述三个要素有一个验证没有通过，SSL 协议就会发出告警，大多数浏览器会弹出一个提示框，提示服务器证书存在的问题，但不会直接断开 SSL 连接，而是让用户决定是否继续。因为用户往往由于缺乏安全意识或者图方便而选择接受不安全的证书。这就使得伪造一个和合法证书极为相似的“伪证书”骗取 SSL 客户端用户信任的手段成为可能。

主机 M 通过数据流重定向技术，使得主机 C 与主机 S 之间的通信流量都流向主机 M，主机 C 本欲与主机 S 建立 SSL 连接，但发送的连接建立请求被重定向到了主机 M；主机 C 首先与主机 M 建立 TCP 连接，然后向主机 M 发起 SSL 连接请求；主机 M 收到来自主机 C 的连接请求后，首先与主机 S 建立 TCP 连接，然后向主机 S 发起 SSL 连接请求；主机 S 响应主机 M 的请求，由此主机 M 与主机 S 之间成功建立 SSL 连接，主机 M 同时获得主机 S 的 X.509 公钥证书 Certificate_S；主机 M 根据 Certificate_S 中的关键信息（主要是 subject name、有效期限等）伪造一个极相似的自签名证书 Certificate_S’，并以此证书响应第 □ 步中，来自主机 C 的 SSL 连接请求；主机 C 的浏览器验证 Certificate_S’的有效性，发现 subject name 与请求的站点名称一致，证书还在有效期内，但是并非由信任的机构颁发。于是弹出提示框，让用户选择是否继续。由于 Certificate_S’与 Certificate_S 从外表上几乎看不出来差别，大部分用户会选择继续（这是 SSL 会话劫持可以成功的关键），由此主机 C 与主机 M 成功建立 SSL 连接。这样以后，主机 C 发往 SSL 服务端的数据，主机 M 可以捕获并解密查看；主机 S 返回给 SSL 客户端的数据，主机 M 也可以捕获并解密查看。至此，主机 M 实现了完整的 SSL 中间人监测。

5. 下列对 SSL/TLS 协议描述正确的是:
   (a) 工作于 TCP/IP 协议栈的网络层
   (b) 不能够提供身份认证功能
   (c) 仅能够实现加解密功能
   (d) 可以被用于实现安全电子邮件的传送

   解：

   D.

6. 基于 RSA 密钥交换的 TLS 握手流程中，通信双方需要交换几个随机数?
   (a) 1
   (b) 2
   (c) 3
   (d) 4

   C.

7. 以下哪种语言没有内建的 TLS 库?
   (a) Java
   (b) Golang
   (c) C++
   (d) Python

   C.