实验相关链接

- **课程主页及指导书**地址：https://hitsz-cslab.gitee.io/net-work-security/
- **SEED实验室的链接：**https://seedsecuritylabs.org/
- **实验提交地址（校内网/VPN）：** http://grader.tery.top:8000/#/login

网络与系统安全实验

实验4　PKI

实验目的

Lab1 公共基础设施（PKI）

- 了解PKI的工作原理；
- 掌握如何使用PKI保护网络；
- 掌握PKI如何击败中间人攻击。

实验任务

本次实验来自于SEED实验室，共需要完成如下6个分解的任务。通过这6个任务我们完成一个银行服务器bank32.com的部署、认证、攻击过程。

1、 成为认证颁发机构（CA）

2、为web server生成签名请求

3、为web server生成签名证书

4、在网络服务器中部署公钥证书

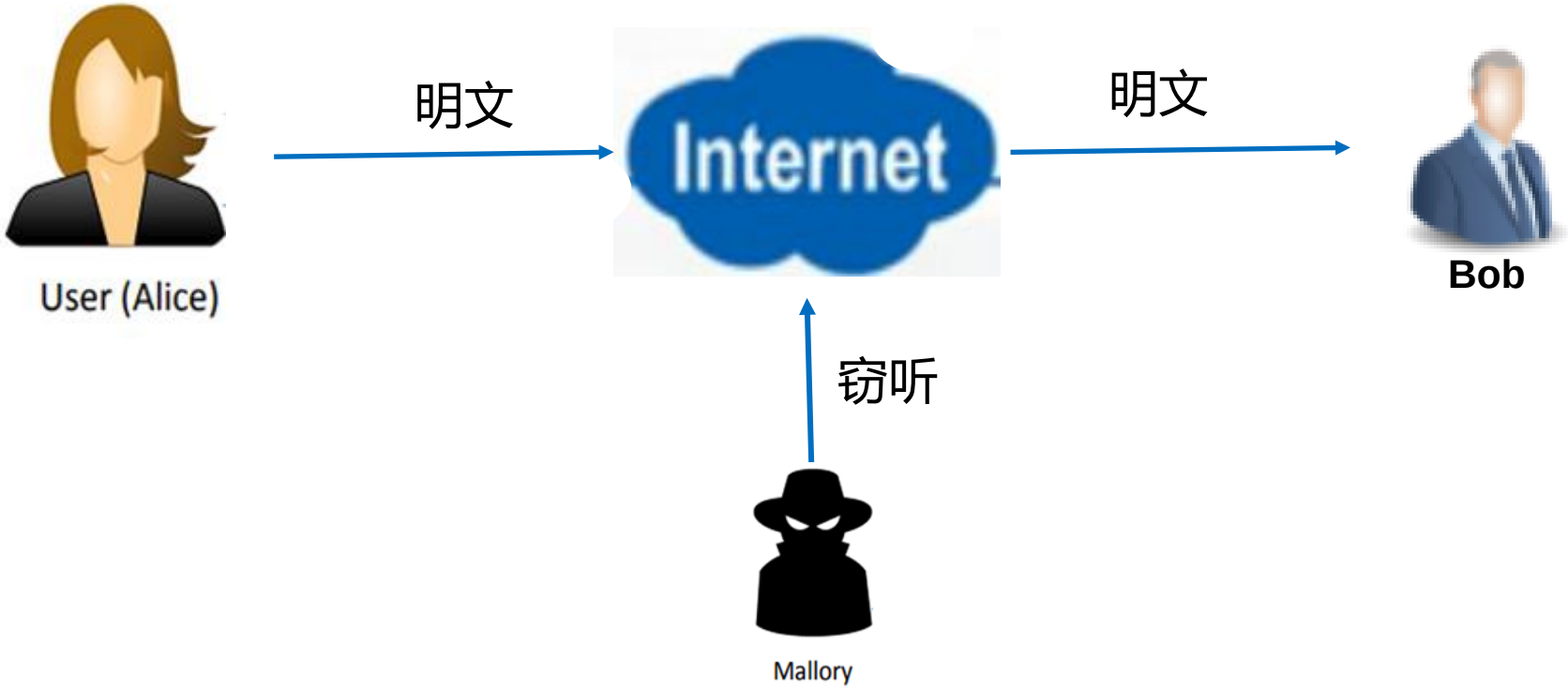
5、抵御中间人攻击

6、用一个已经劫持到的CA发动一次中间人攻击

实验原理

1 中间人攻击

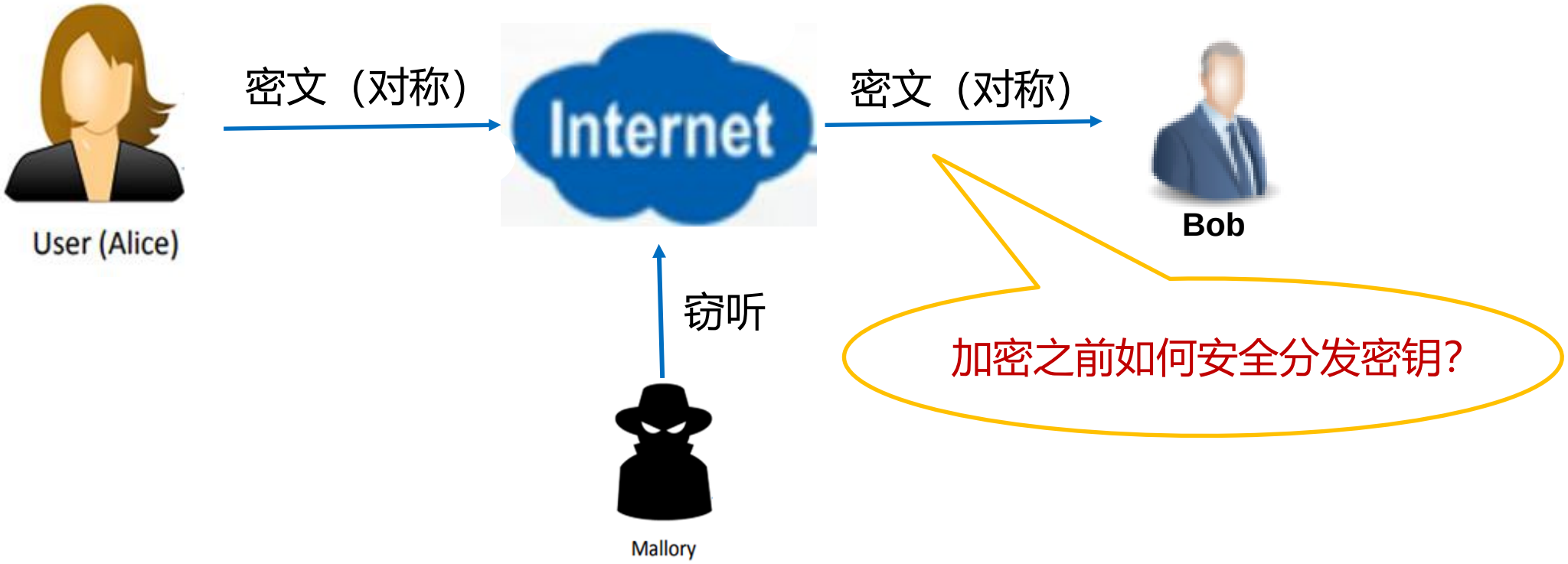
- 中间人攻击发生再两个设备之间的流量被截获的情况下。



实验原理

1 中间人攻击

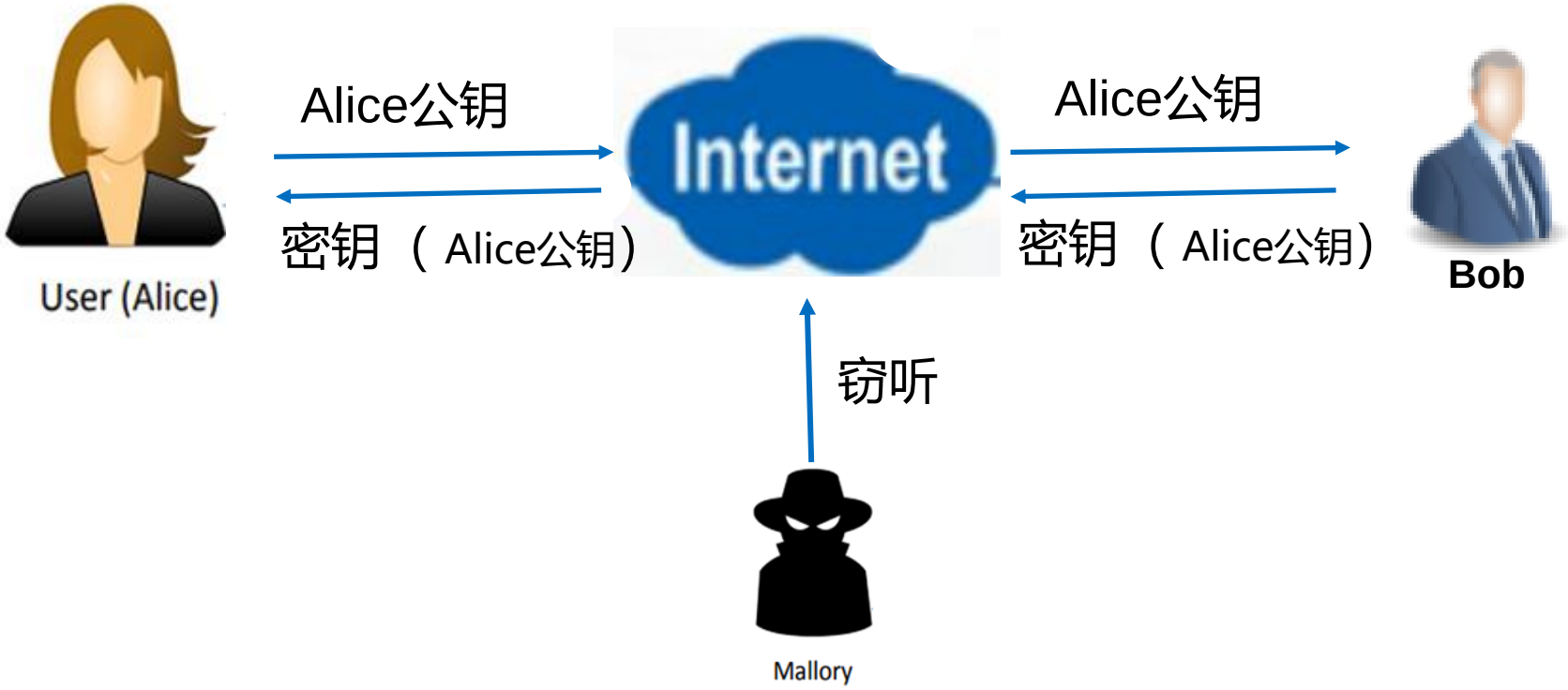
- 中间人攻击发生再两个设备之间的流量被截获的情况下。



实验原理

1 中间人攻击

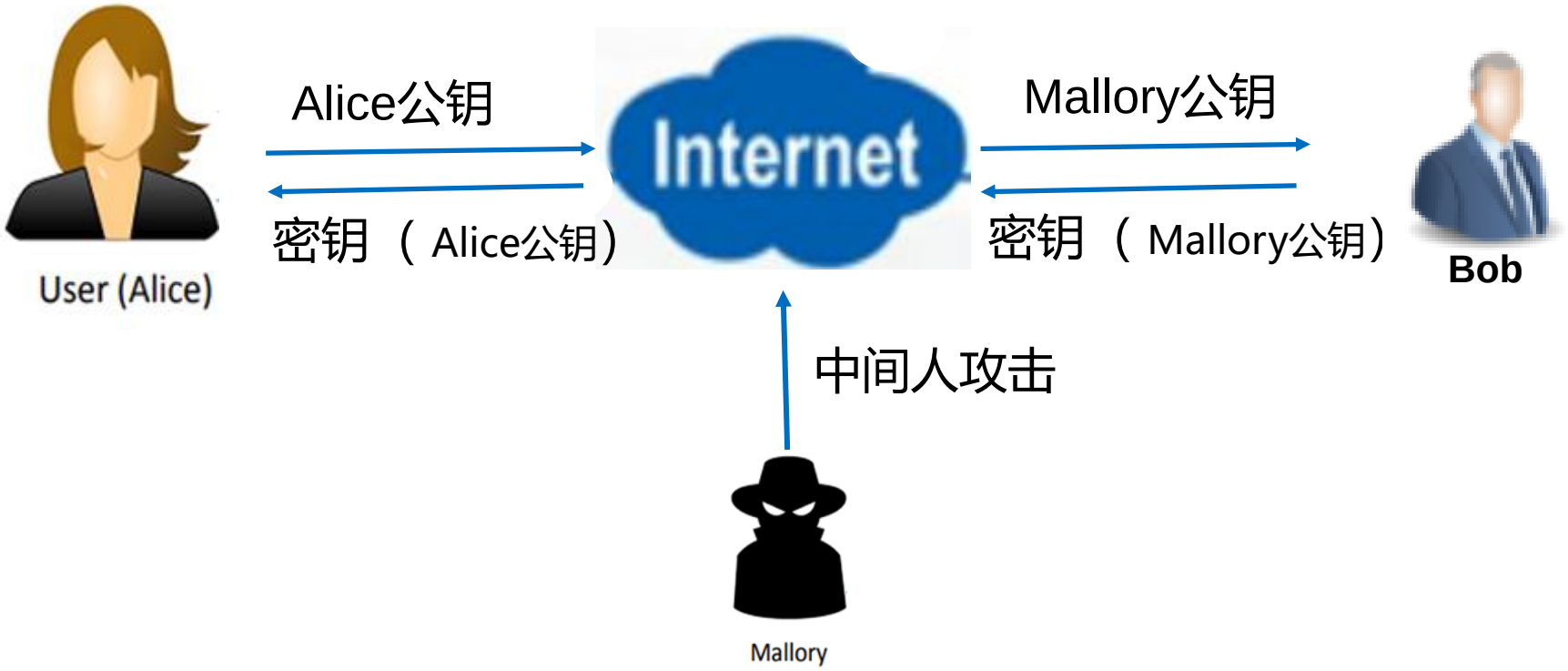
- 中间人攻击发生再两个设备之间的流量被截获的情况下。



实验原理

1 中间人攻击

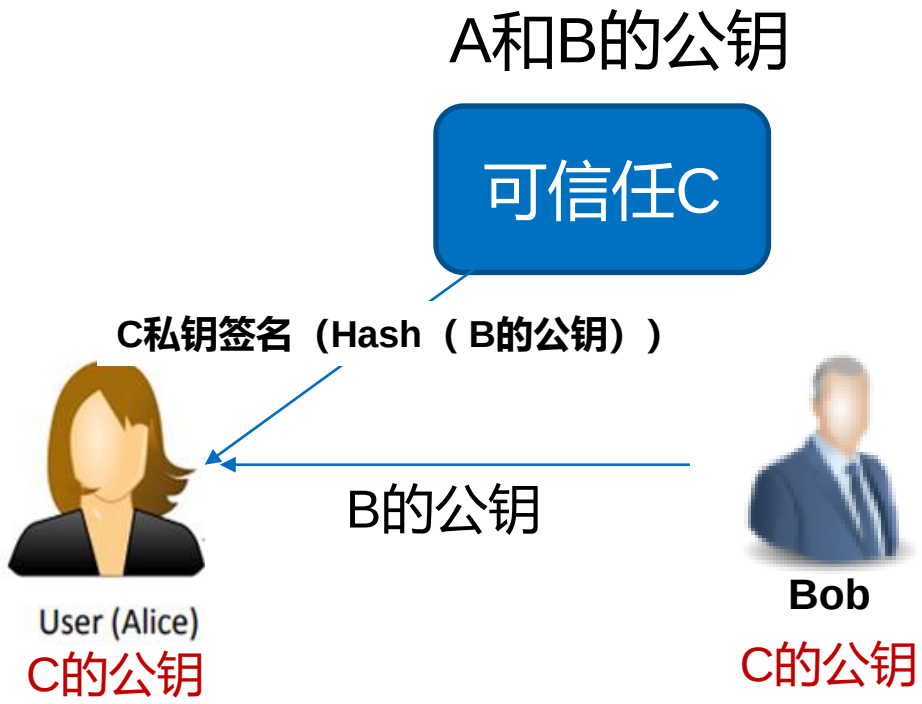
- 中间人攻击发生再两个设备之间的流量被截获的情况下。



实验原理

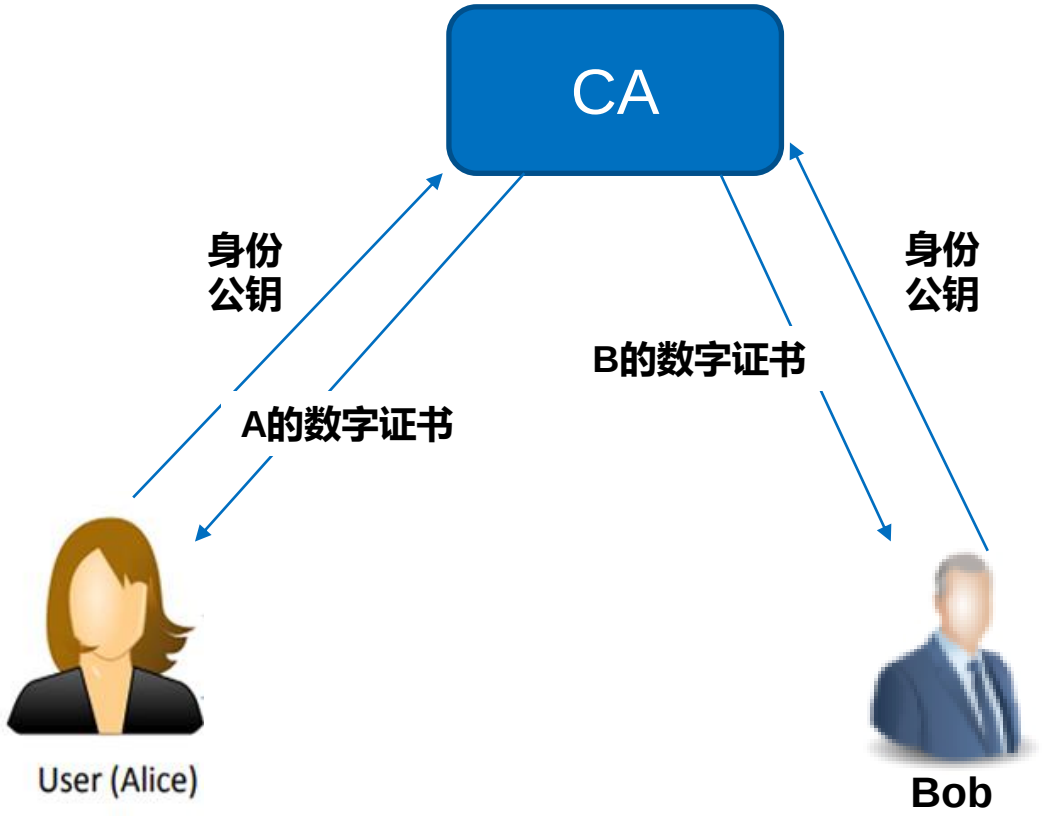
2 数字证书

- 可信任C把Bob的公钥做Hash
- 然后用C的私钥对Hash进行签名后发送给Alice
- Alice就用C的公钥解密得到B公钥的Hash值
- Alice再跟对方Bob发过来的公钥Hash后的值做比较，就能确认对方是不是Bob

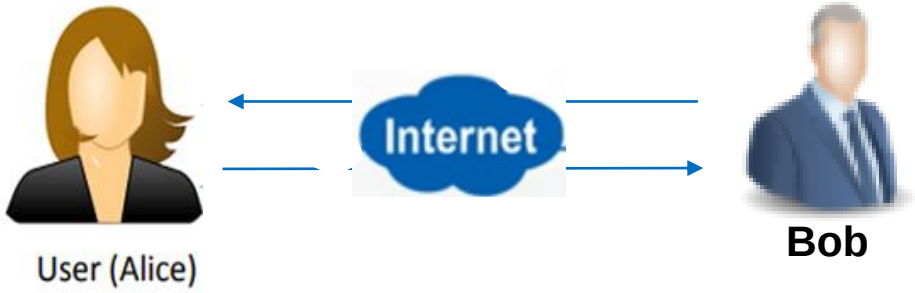


实验原理

2 ➢ 数字证书



证书实现了公钥安全的交换过程



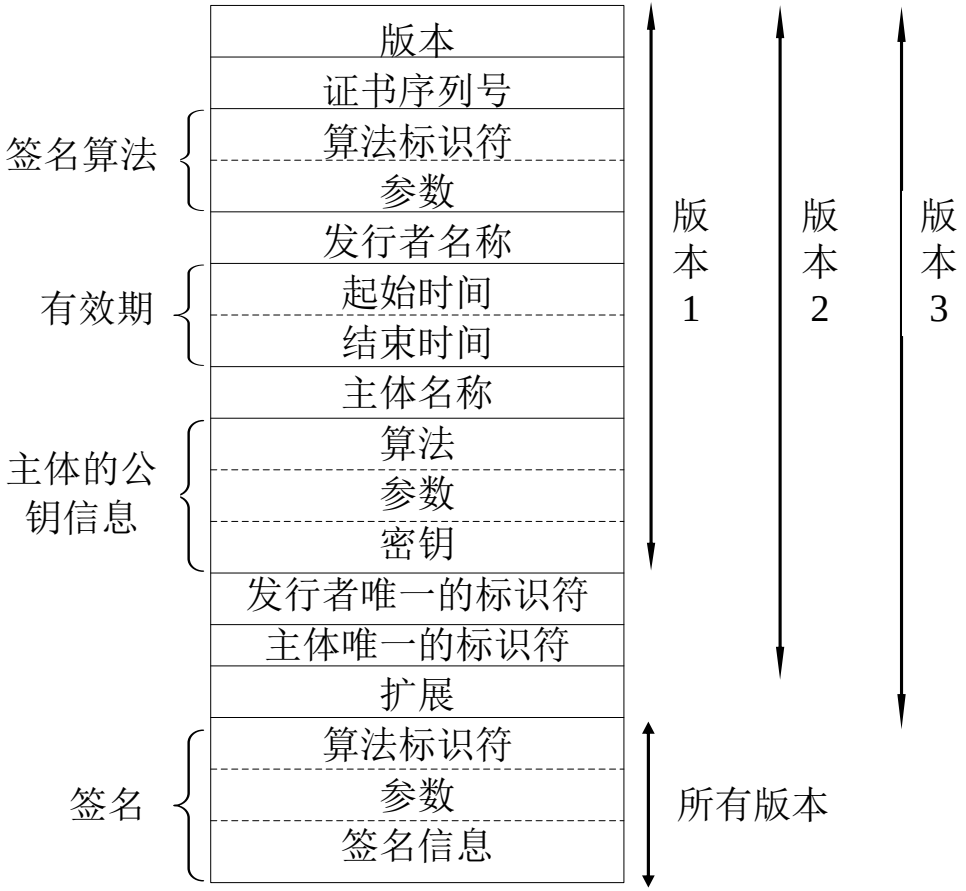
实验原理

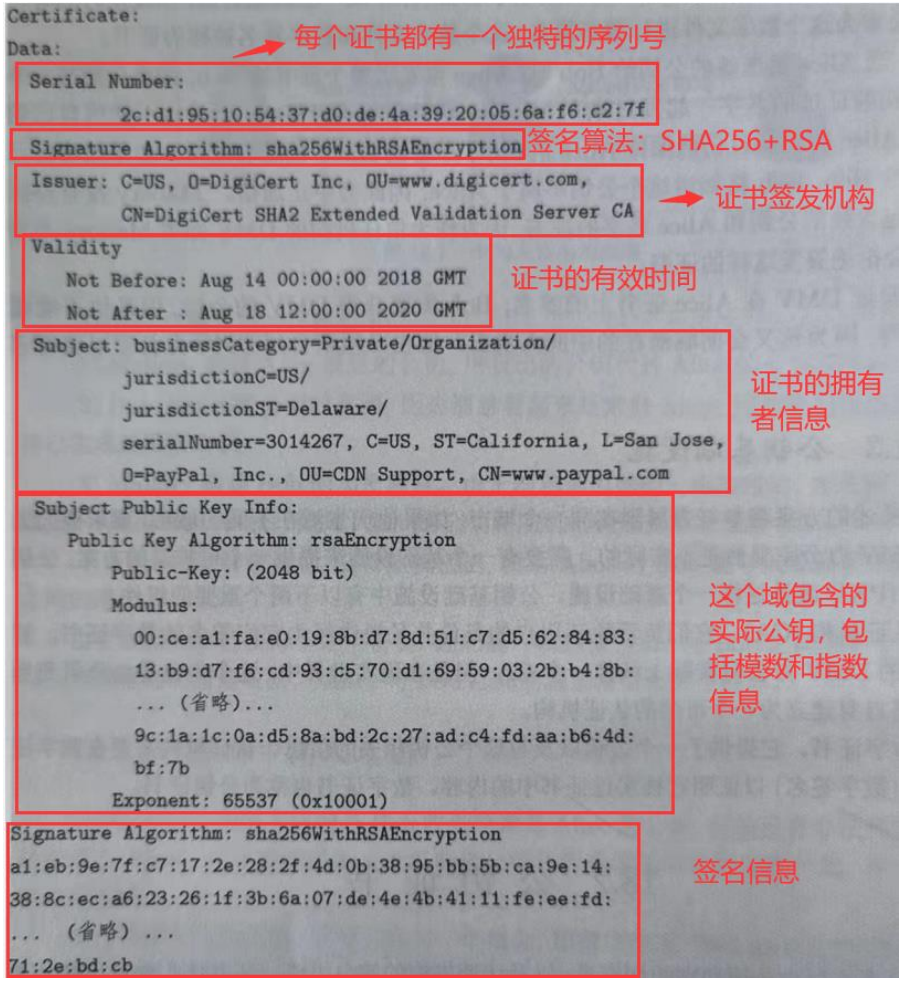
2 数字证书

公钥证书主要用于确保公钥及其与用户绑定关系的安全，一般包含持证主体身份信息、主体的公钥信息、CA信息以及附加信息，再加上用CA私钥对上述信息的数字签名。目前应用最广泛的证书格式是国际电信联盟（International Telecommunication Union, ITU）制定的X.509标准中定义的格式。X.509最初是在1988年的7月3日发布的，版本是X.509 v1，当时是作为ITU X.500目录服务标准的一部分。在此之后，ITU分别于1993年和1995年进行过两个修改，分别形成了X.509 版本2 (X.509 v2)和版本3 (X.509 v3)，其中v2证书并未得到广泛使用。

实验原理

2 数字证书


版本
证书序列号
签名算法
算法标识符
参数
发行者名称
有效期
起始时间
结束时间
主体名称
主体的公钥信息
算法
参数
密钥
发行者唯一的标识符
主体唯一的标识符
扩展
签名
算法标识符
参数
签名信息
版本1
版本2
版本3
所有版本

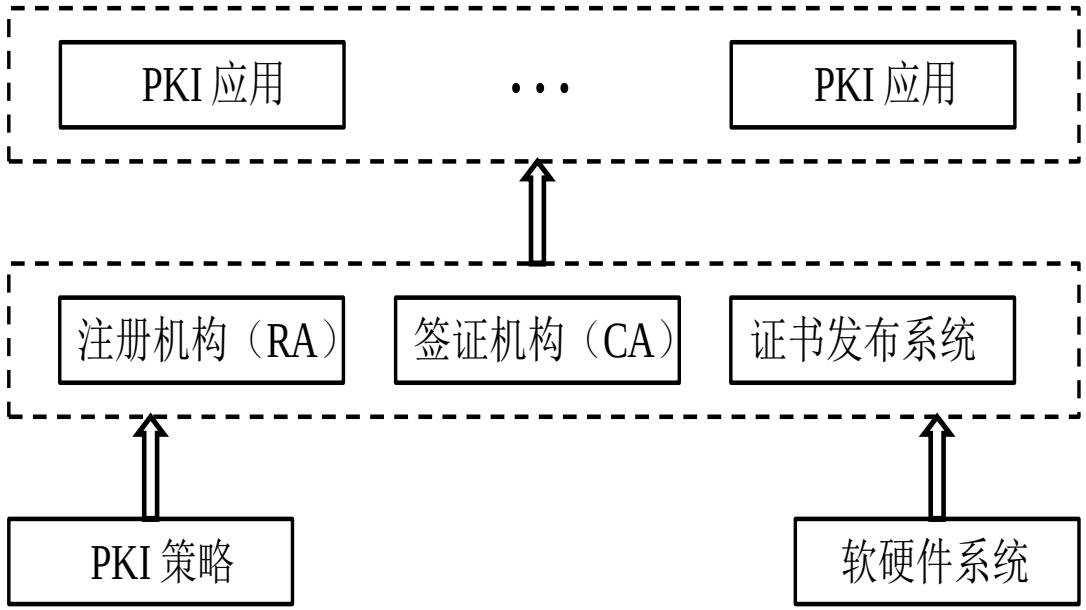

Certificate:
Data:
每个证书都有一个独特的序列号
Serial Number:
2c:d1:95:10:54:37:d0:de:4a:39:20:05:6a:f6:c2:7f
Signature Algorithm: sha256WithRSAEncryption
签名算法：SHA256+RSA
Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com,
CN=DigiCert SHA2 Extended Validation Server CA
证书签发机构
Validity
Not Before: Aug 14 00:00:00 2018 GMT
Not After : Aug 18 12:00:00 2020 GMT
证书的有效时间
Subject: businessCategory=Private/Organization/
jurisdictionC=US/
jurisdictionST=Delaware/
serialNumber=3014267, C=US, ST=California, L=San Jose,
O=PayPal, Inc., OU=CDN Support, CN=www.paypal.com
证书的拥有者信息
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:ce:a1:fa:e0:19:8b:d7:8d:51:c7:d5:62:84:83:
13:b9:d7:f6:cd:93:c5:70:d1:69:59:03:2b:b4:8b:
... (省略)...
9c:1a:1c:0a:d5:8a:bd:2c:27:ad:c4:fd:aa:b6:4d:
bf:7b
Exponent: 65537 (0x10001)
这个域包含的实际公钥，包括模数和指数信息
Signature Algorithm: sha256WithRSAEncryption
a1:eb:9e:7f:c7:17:2e:28:2f:4d:0b:38:95:bb:5b:ca:9e:14:
38:8c:ec:a6:23:26:1f:3b:6a:07:de:4e:4b:41:11:fe:ee:fd:
... (省略) ...
71:2e:bd:cb
签名信息


只有敲代码才能
感受到温暖

实验原理

3 PKI

- 有了证书以后，将涉及证书的申请、发布、查询、撤销等一系列管理任务，因此需要一套完整的软硬件系统、协议、管理机制来完成这些任务，由此产生了公钥基础设施（PKI）。

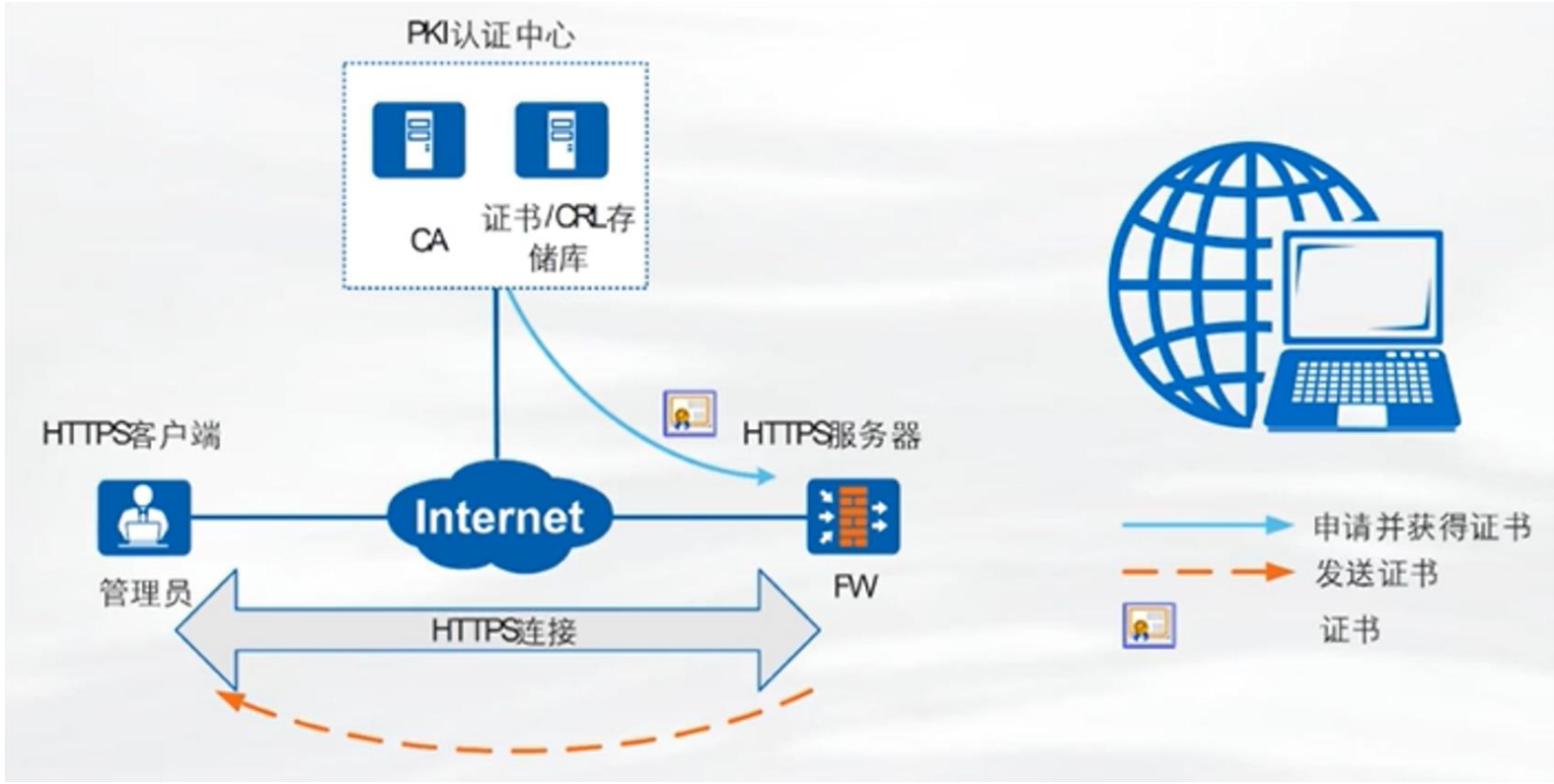


B站上讲解PKI的来龙去脉
https://www.bilibili.com/video/BV13b4y1a7ku?spm_id_from=333.337.search-card.all.click

实验原理

4 HTTPS访问

- www.bank32.com服务器到CA申请证书
- 那么用户在访问这个网站时，浏览器就可以根据证书来确定这个域名确实是www.bank32.com的网站而不是其他伪造的。



实验原理

5 Apache

- /var/www/ 路径下存放网页的显示信息
- Apache的配置文件最终是链接在/etc/apache2/sites-available路径下
- 修改配置后请重新使能SSL和重启apache

实验步骤

1、 让**主机**服务器成为认证颁发机构（CA）

2、为www.bank32.com服务器生成签名请求

3、为www.bank32.com服务器生成签名证书

4、在容器中部署www.bank32.com服务器并部署其公钥证书

5、尝试使用www.bank32.com的证书访问其他的服务器，PKI是否能够抵御中间人攻击?

6、模拟用一个已经劫持到的CA发动一次中间人攻击

指导书中所有说道主机的都是相对容器来说的，是指虚拟机

作业提交

提交内容：实验报告（有模板）

截止时间：

下周一提交至HITsz Grader 作业提交平台，具体截止日期参考平台发布。

- 登录网址：： http://grader.tery.top:8000/#/login
- 推荐浏览器： Chrome
- 初始用户名、密码均为学号，登录后请修改

注意

上传后可自行下载以确认是否正确提交

同学们
请开始实验吧！