哈爾濱工業大學(深圳)
HARBIN INSTITUTE OF TECHNOLOGY, SHENZHEN

网络安全实验

苏　婷

关于实验课

要求：

1. 使用腾讯课堂上课，如遇到技术故障将改用腾讯会议；
2. 为方便考勤，请同学们将昵称改成“学号-真实姓名”；
3. 上课不定时发起签到，请同学们不要迟到早退。

CONTENTS
目录

本学期实验总体安排

- 网络安全实验做什么？
  - 1个PKI基础设施、 3个网络安全协议、1个防火墙

课次	序号	实验	实验类型	提交	分数	课时
1	1	PKI	配置验证实验	设计报告	6	4
2	2	TLS	编程和配置实验	代码和实验报告	8	4
3	3	IPSec	配置验证实验	设计报告	5	4
	4	VPN_Tunnel	编程和配置实验	代码和设计报告	5	
4	5	防火墙 iptables		代码和设计报告	6	4

本学期实验总体安排

欢迎有兴趣有余力的同学来挑战**附加题**，不会超过30分满分

序号	题目	提交	分数
1	TLS的任务3	代码及设计报告	1.5
2	VPN_Tunnel 任务7-9部分	代码及设计报告	1.5
3	防火墙的任务2编码部分	代码及设计报告	1.5
4	DNS系列实验	代码及设计报告	3

本学期实验总体安排

- **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

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

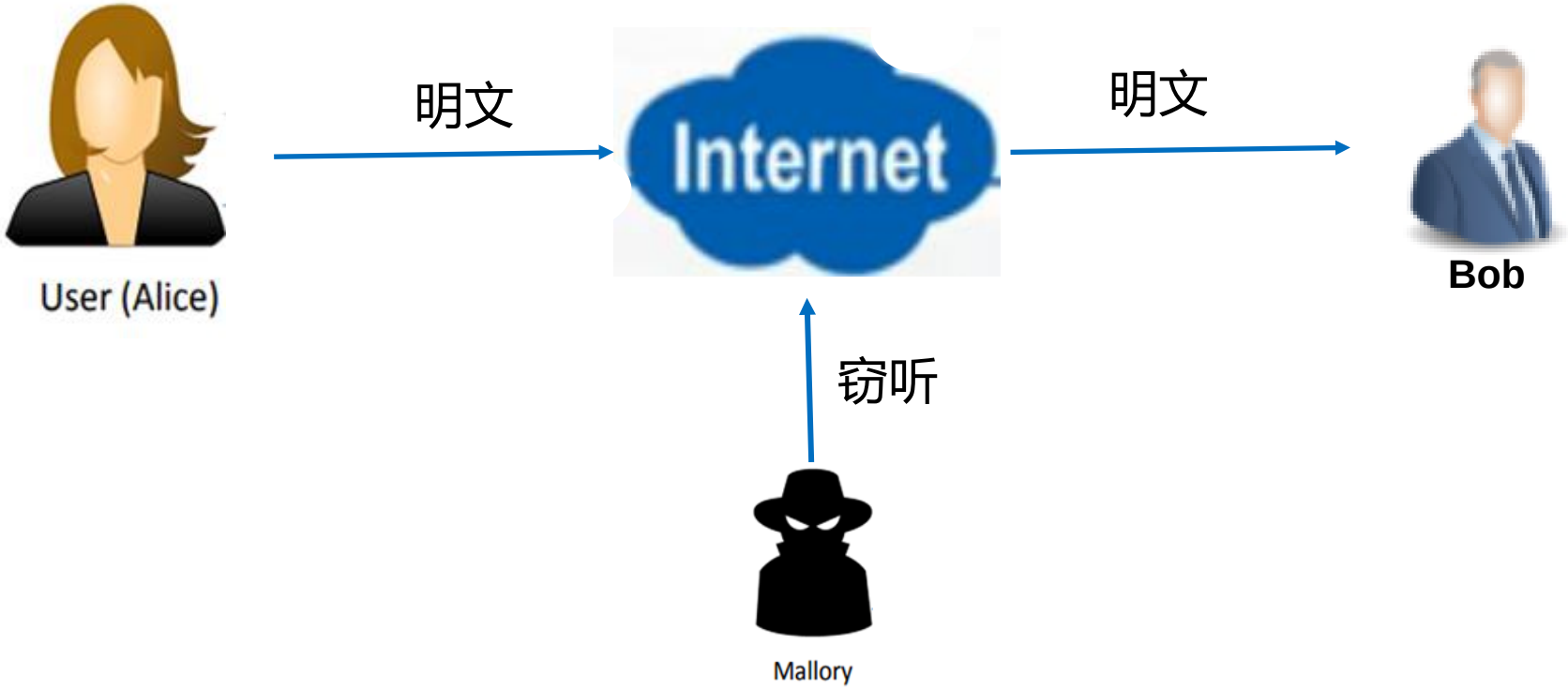
5、抵御中间人攻击

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

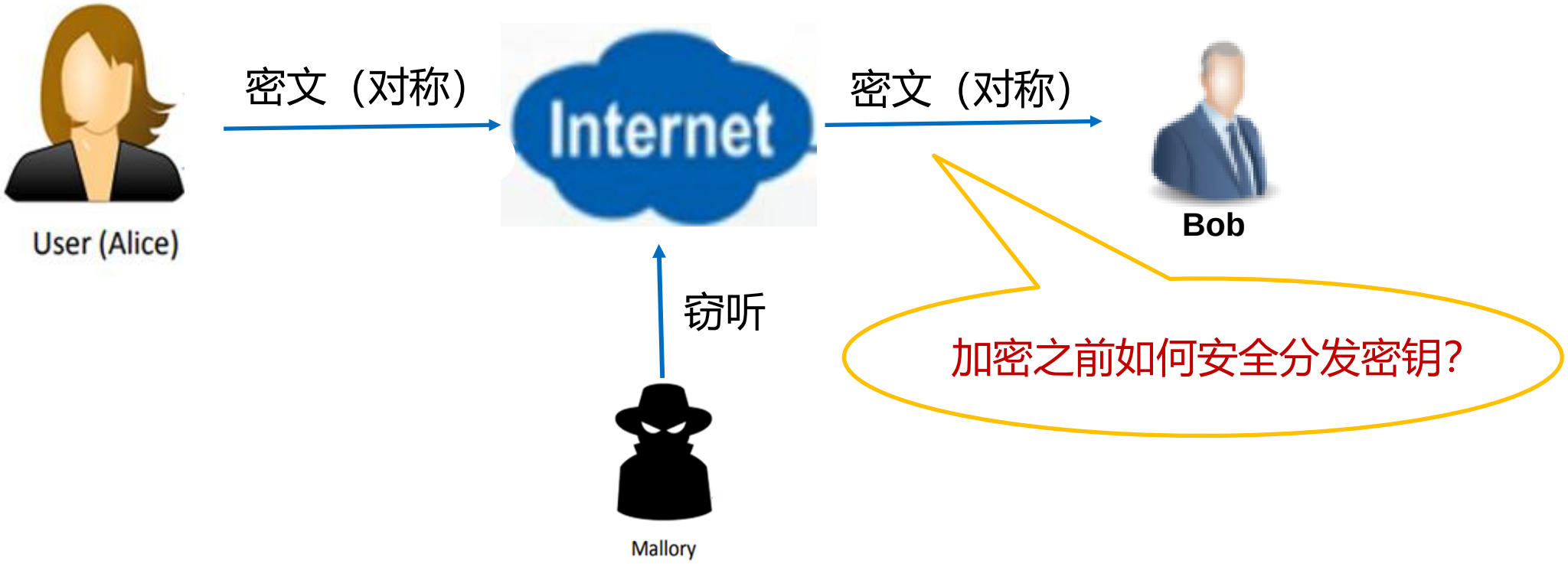
- 中间人攻击发生再两个设备之间的流量被截获的情况下。



实验原理

1 中间人攻击

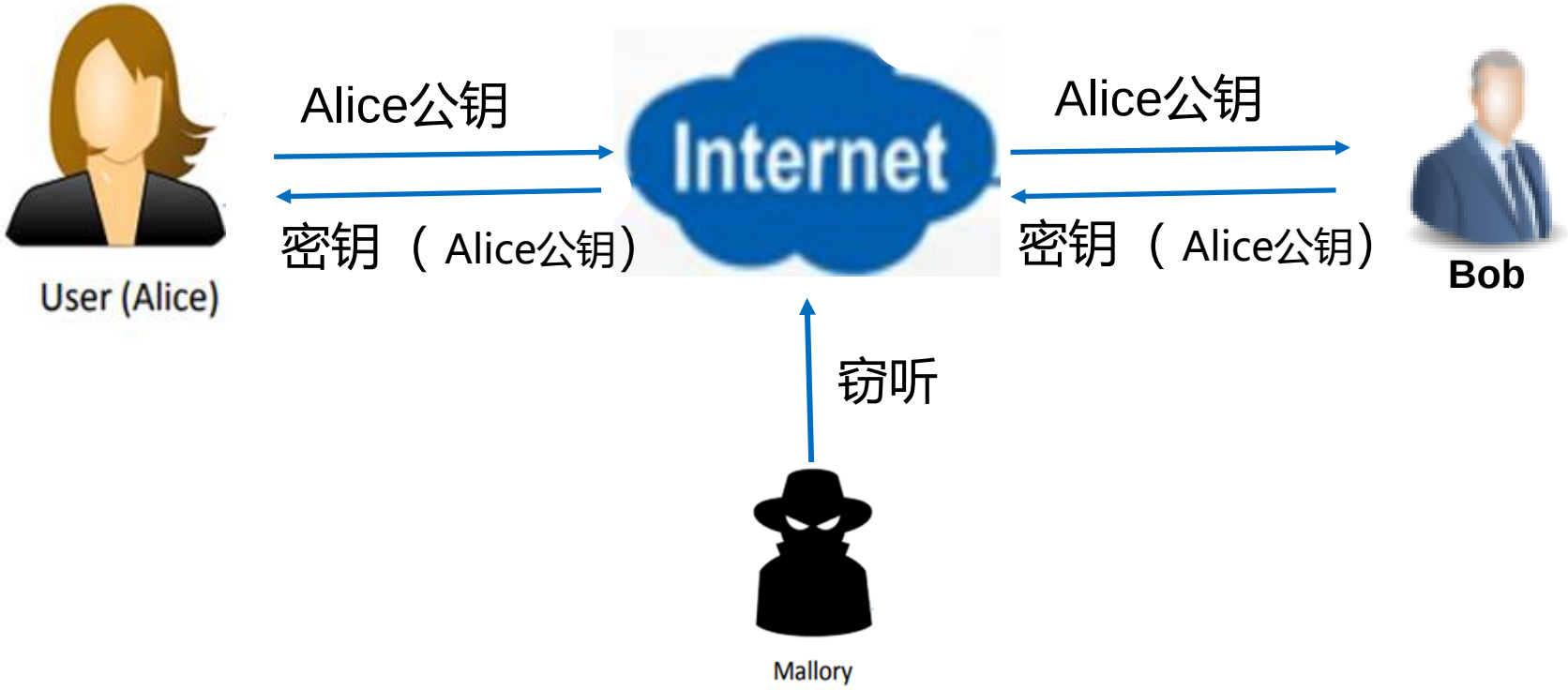
- 中间人攻击发生再两个设备之间的流量被截获的情况下。



实验原理

1 中间人攻击

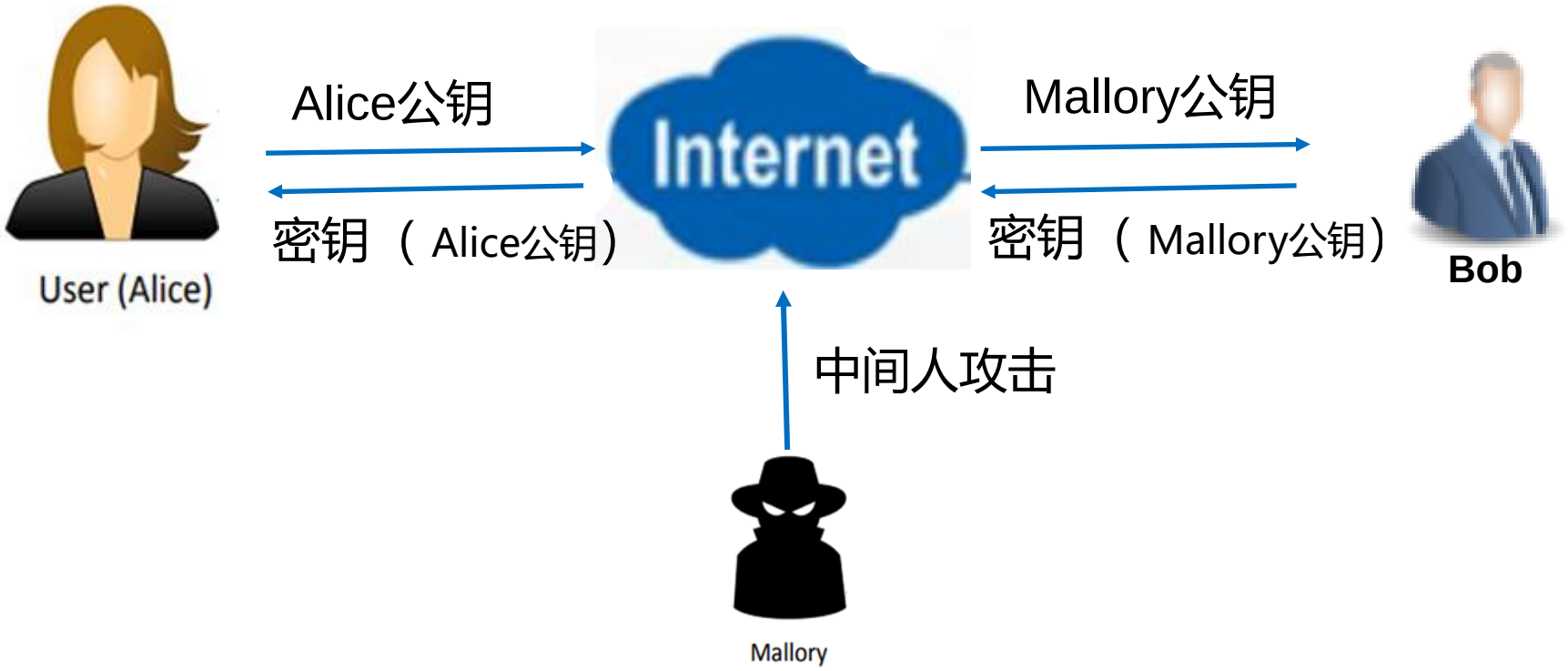
- 中间人攻击发生再两个设备之间的流量被截获的情况下。



实验原理

1 中间人攻击

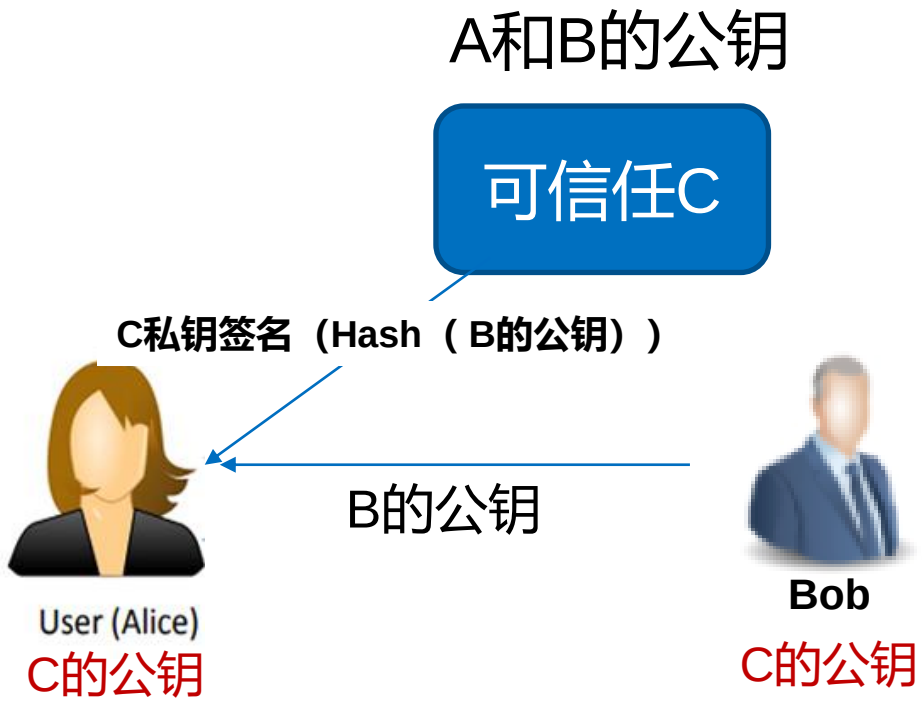
- 中间人攻击发生再两个设备之间的流量被截获的情况下。



实验原理

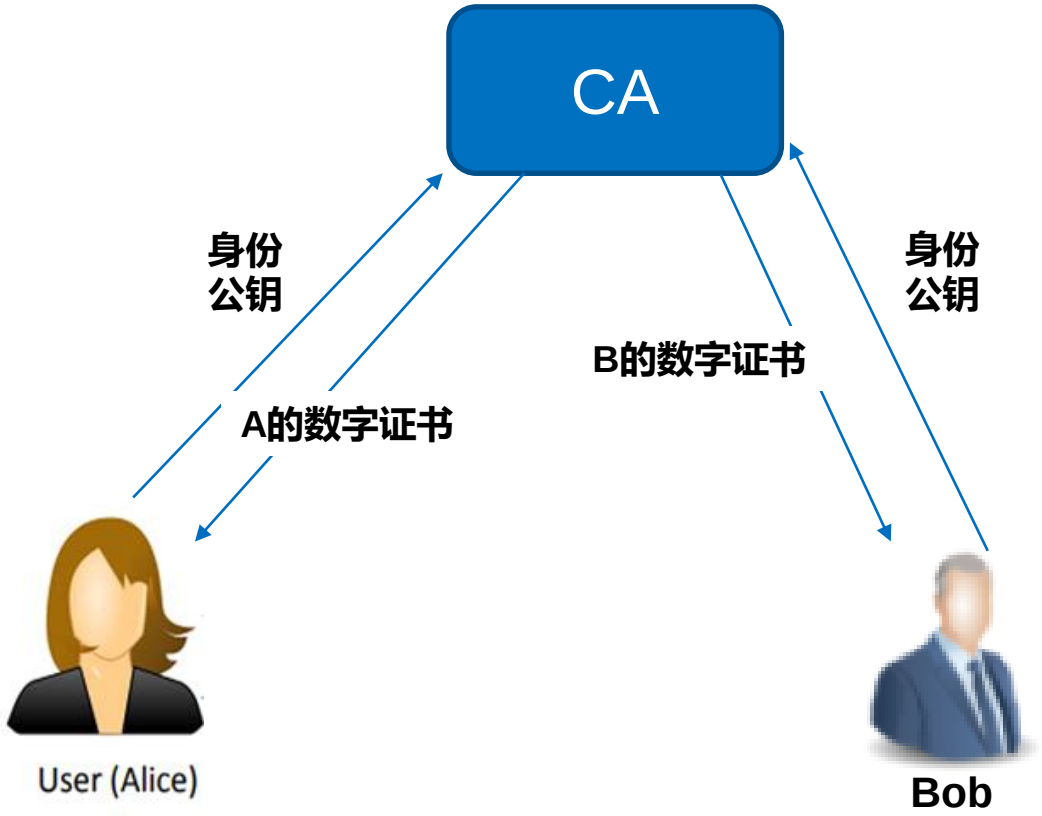
2 数字证书

- 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

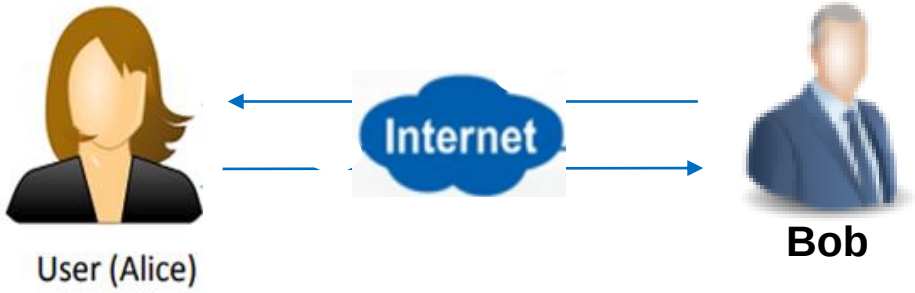


实验原理

2 ➢ 数字证书

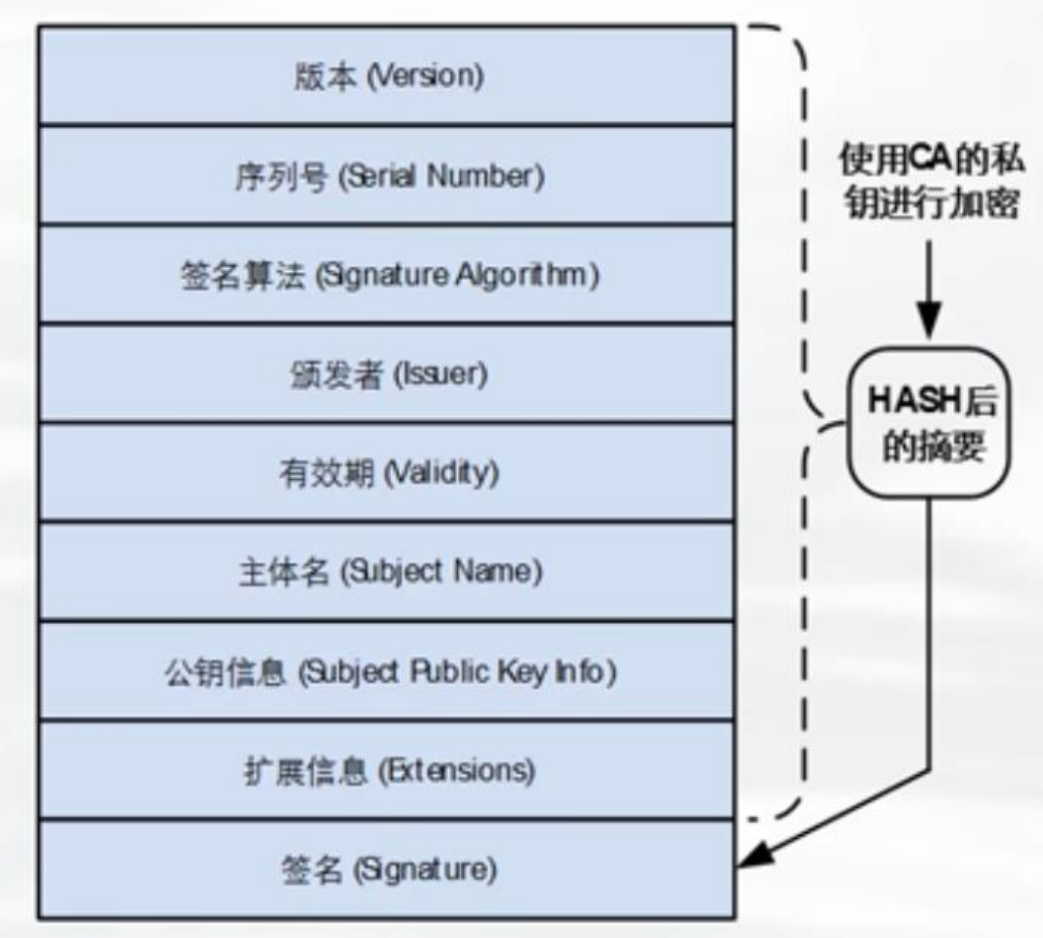


证书实现了公钥安全的交换过程



实验原理

2 数字证书

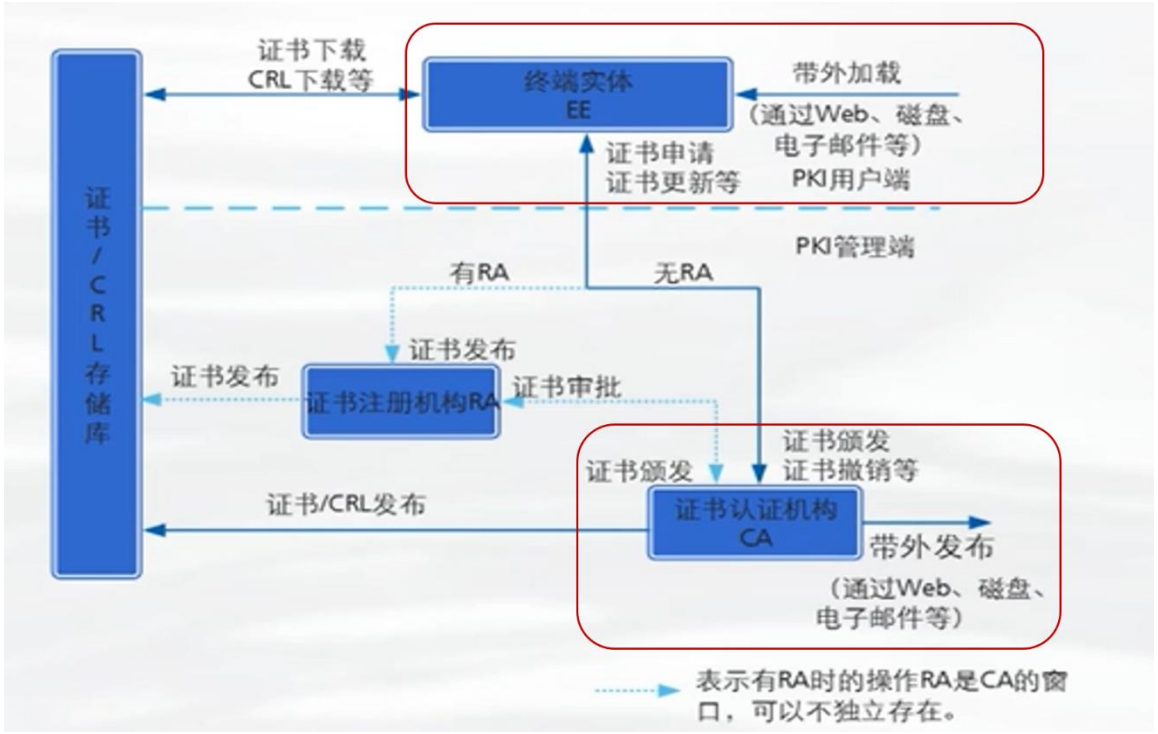



```
Certificate:
Data:                                          每个证书都有一个独特的序列号
    Serial Number:
        2c:d1:95:10:54:37:d0:de:4a:39:20:05:6a:f6:c2:7f
    Signature Algorithm: sha256WithRSAEncryption   签名算法：SHA256+RSA
    Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com,
        CN=DigiCert SHA2 Extended Validation Server CA   → 证书签发机构
    Validity
        Not Before: Aug 14 00:00:00 2018 GMT       证书的有效时间
        Not After : Aug 18 12:00:00 2020 GMT
    Subject: businessCategory=Private/Organization/
        jurisdictionC=US/
        jurisdictionST=Delaware/                   证书的拥有者信息
        serialNumber=3014267, C=US, ST=California, L=San Jose,
        O=PayPal, Inc., OU=CDN Support, CN=www.paypal.com
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:                               这个域包含的实际公钥，包括模数和指数信息
                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)
Signature Algorithm: sha256WithRSAEncryption       签名信息
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
```

实验原理

3 PKI

- 公共基础设施PKI（Public Key Infrastructure）是由硬件、软件、策略和程序构成的一整套体系，用来创建、管理、分发和撤销建立在非对称密码算法之上的数字证书。

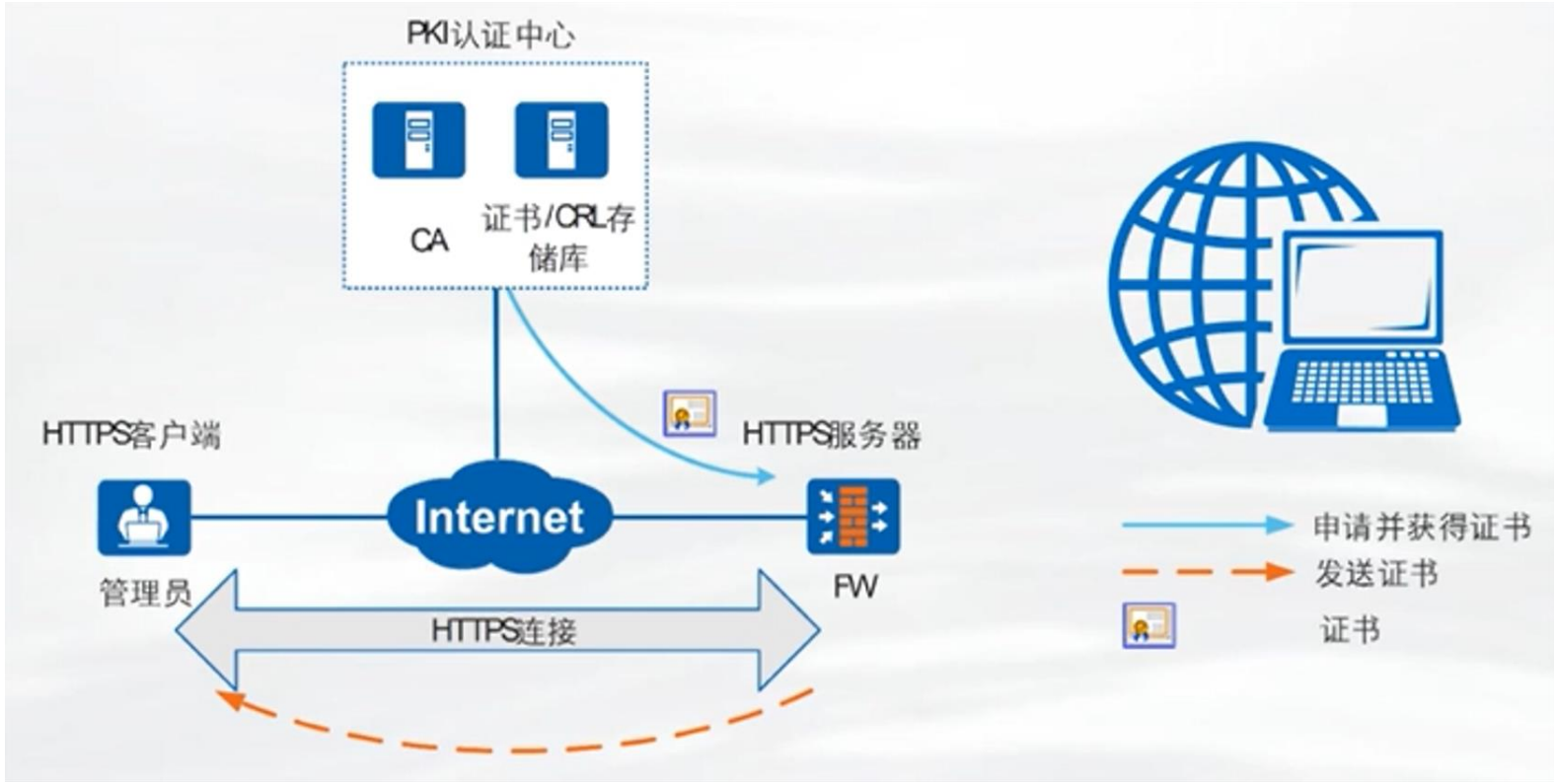


B站上讲解PKI的来龙去脉
https://www.bilibili.com/video/BV13b4y1a7ku?spm_id_from=333.337.search-card.all.click

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！

对网络安全有兴趣深入研究的，可以参考如下链接：

D:\2022春季课程\
机网络安全\网络安