公钥基础设施

C4.1. 以下是 X.509 证书。

```
Certificate:
 Data:
   Version: 3 (0x2)
   Serial Number:
     3d:0e:98:b2:bf:af:fa:9e:99:91:05:64:69:6e:11:2a
 Signature Algorithm: sha256WithRSAEncryption
   Issuer: C=US, O=Symantec Corporation,
           OU=Symantec Trust Network,
           CN=Symantec Class 3 EV SSL CA - G3
   Validity
      Not Before: Aug 14 00:00:00 2017 GMT
      Not After : Sep 13 23:59:59 2018 GMT
   Subject: ... C=US/postalCode=22230, ST=Virginia,
         L=Arlington/street=4201 Wilson Blvd,
         O=National Science Foundation, OU=DIS,
         CN=www.nsf.gov
   Subject Public Key Info:
     Public Key Algorithm: rsaEncryption
       Public-Key: (2048 bit)
         Modulus:
            00:ca:fb:26:78:06:25:b1:9e:67:1d:69:0b:10:06:
            cf:25:b6:7d:de:8e:56:80:e1:1c:38:52:62:43:fd:
            ...
      Exponent: 65537 (0x10001)
 Signature Algorithm: sha256WithRSAEncryption
     4b:0d:62:11:b4:dc:78:09:12:c1:1b:24:ff:98:43:58:1c:54:
     0a:34:be:8f:3f:12:8f:17:4a:fe:5b:26:13:1a:5f:a7:87:ad:
     ...
     ba:2c:10:c7:bc:8b:2c:15:6e:0c:d2:d0:8b:74:52:c8:ed:05:
     0b:9b:62:41
```

(a) 证书由谁颁发？

(b) 证书的所有者是谁？

(c) 该证书上的签名由谁生成？应如何验证？

(d) 证书包含一个 RSA 公钥。使用 RSA 加密消息 M 时计算 M^e `mod n`。这个公钥中的 `e` 和 `n` 分别是什么？若数值太长，只需写出前四个字节。

(e) CA 颁发证书前，需要围绕证书的 Subject 字段进行验证。请说明验证什么，以及为什么必须进行这项验证。

C4.2. 浏览网站时出现以下消息。“证书不是由受信任的 CA 颁发”是什么意思？什么样的 CA 才会被视为可信？

```
There is a problem with this website's security certificate.
The security certificate presented by this website was not
issued by a trusted certificate authority.
```

C4.3. 某银行最近将其网站名称从 `www.bank32.com` 更改为 `www.bank48.com`，因此用户必须使用这个新名称来访问银行的网上服务。为了降低成本，银行希望使用相同的证书，而不是获取新证书。这可能吗？为什么？

C4.4. 攻击者创建了自签名 CA 证书，并设法让受害者把它加入浏览器的受信任证书列表。这可能造成什么危害？

C4.5. 不在浏览器地址栏输入 `https://www.example.com`，而是先查到 Web 服务器的 IP 地址 `93.184.216.34`，再直接访问 `https://93.184.216.34`。能否正常建立 HTTPS 连接？请解释。

C4.6. 如果 CA 的私钥被攻击者窃取，攻击者可能造成什么损害？

C4.7. 请解释什么是证书固定（certificate pinning），以及它能实现什么保护。

C4.8. HTTPS 可以抵御中间人攻击，但组织也可以部署 HTTPS 代理来监控和修改 HTTPS 流量，而代理本身正位于通信双方之间。这是否说明 HTTPS 仍会受到中间人攻击？请解释。

C4.9. 课堂作业要求实现一个简单的 VPN，客户端与服务器通过 SSL 加密通信。连接时，多数学生要求用户在命令行输入 VPN 服务器的 IP 地址，并另行输入期望的证书通用名（即服务器主机名），以便验证证书。虽然可用性不佳，但安全逻辑没有问题。

一名学生为了不再要求用户输入主机名，改为对用户提供的 IP 地址做反向 DNS 查询，将查到的主机名与证书通用名比较；若匹配就信任服务器。

请回答以下问题。以 `syr.edu` 为例，假设其 VPN 服务器为 `vpn.syr.edu`，IP 地址是 `128.230.53.1`，命令为 `"vpnclient -s 128.230.53.1"`。假设没有 CA 遭到入侵，因此攻击者无法获得其他域名的有效证书。

(a) 请描述一种攻击，使 VPN 客户端接受通用名为 `attacker32.com` 的攻击者证书。客户端一旦连到攻击者，用户的账户凭据就可能泄露。

(b) 若改用 `"vpnclient -s vpn.syr.edu"`，由客户端通过正向 DNS 查询 IP，是否仍存在与上一问相同的漏洞？请解释。

C4.10. 验证 VPN 服务器时需要检查证书名称。开发人员不用 `strcmp()` 做精确比较，而改用 `strstr()`，代码如下：

```
if (strstr(commonName,"vpnserver.com")==NULL)
{
     printf("names do no match\n"); exit(-1);
}
```

这样会放宽匹配条件，不仅 `vpnserver.com`，连 `abc.vpnserver.com` 也能匹配。开发人员认为这样一个站点只需一张证书，无需为每个主机名分别申请证书。`strstr()` 的解释如下：

```
char * strstr(char * str1, char * str2):
   Return a pointer to the first occurrence in str1
   of the entire sequence of characters specified in str2,
   or a null pointer if the sequence is not present in str1.
```

这种放松是否安全？请解释一下。