Name: Pramod kumar

pjk5502@psu.edu

Task 1: Create CA root certificate:

```
[09/28/19]seed@VM:~/lab2$ mkdir crl certs newcerts private
[09/28/19]seed@VM:~/lab2$
[09/28/19]seed@VM:~/lab2$
[09/28/19]seed@VM:~/lab2$
[09/28/19]seed@VM:~/lab2$ openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf
Generating a 2048 bit RSA private key
.....................+++
.................................+++
writing new private key to 'ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:PENN
Locality Name (eg, city) []:STATE
Organization Name (eg, company) [Internet Widgits Pty Ltd]:seedpkilab2018.com
Organizational Unit Name (eg, section) []:seed
Common Name (e.g. server FQDN or YOUR name) []:seedpkilab2018.com
Email Address []:seedpkilab2018@com
[09/28/19]seed@VM:~/lab2$
[09/28/19]seed@VM:~/lab2$
[09/28/19]seed@VM:~/lab2$
```

Task 2: create certificate of customer Seedlabs2018.com

Subtask 1: generating server key

```
9/27/19]seed@VM:~/lab2$
9/27/19]seed@VM:~/lab2$ openssl genrsa -aes128 -out server.key 1024
nerating RSA private key, 1024 bit long modulus
.............................++++++
...............................................++++++
is 65537 (0x10001)
ter pass phrase for server.key:
rifying - Enter pass phrase for server.key:
9/27/19]seed@VM:~/lab2$ openssl rsa -in server.key -text
ter pass phrase for server.key:
ivate-Key: (1024 bit)
dulus:
  00:d8:a1:3c:29:d9:ad:d0:61:be:a6:31:d6:45:5d:
  a9:f8:ca:e6:de:f7:5d:d7:6b:69:98:7a:f4:55:94:
  72:de:d2:55:f4:4d:45:f6:78:ff:7d:53:5e:0f:60:
  43:ed:d6:98:7f:38:ad:7c:c8:82:07:da:35:4e:8b:
  a1:92:ee:b0:cd:08:2c:2a:30:75:c5:84:bf:5a:25:
  45:ca:a8:7b:42:40:c3:13:7d:ca:44:9a:28:74:26:
  ae:cb:d7:a6:33:83:1b:0d:3a:a1:85:60:8a:f1:57:
  30:10:f0:b8:7e:b5:96:f0:aa:34:66:b6:0c:a0:85:
  52:55:64:8c:db:72:6c:05:e5
blicExponent: 65537 (0x10001)
ivateExponent:
  00:c5:d1:86:a5:18:d8:76:3f:ab:df:0c:07:84:d4:
  61:50:85:c8:89:b7:0e:04:97:5b:98:18:3f:62:9e:
  ea:be:bb:08:2e:cd:19:a4:57:1d:c7:8e:07:88:b6:
  f9:91:08:b3:bd:09:3e:b3:82:4d:eb:69:c1:df:f5:
  f6:17:bc:cb:c8:e1:21:4a:5b:f5:60:64:76:e4:a5:
  67:ee:dc:06:bb:28:1e:39:70:b1:be:34:3a:d3:eb:
  be:73:18:42:77:03:4d:cd:21:9d:a5:a0:b9:a3:52:
  f4:a6:b8:64:83:4a:2c:fa:9b:e3:f6:e3:ef:45:a5:
  0f:f7:a2:00:c3:6a:da:63:81
ime1:
  00:ec:ef:87:56:b4:fe:5b:47:d9:41:08:e6:89:70:
  0f:62:d1:4d:5f:93:73:2f:68:30:81:e8:e3:2d:4a:
  fb:23:ee:5a:35:da:a4:40:0c:d1:2e:da:26:3c:c9:
  f8:07:8e:54:06:3e:12:28:cb:13:63:64:c0:fd:30:
  ea:3d:18:60:15
ime2:
  00:ea:0f:70:d2:8c:f5:02:ae:1f:d0:39:7c:26:23:
  49:0c:15:f4:c4:1f:31:6a:81:cf:59:5f:ab:65:e1:
  b4:35:ea:e1:ae:84:e3:1a:02:ca:d5:45:bb:48:f3:
```

Subtask 2: give the above key for CSR to CA.

```
[09/27/19]seed@VM:~/lab2$
[09/27/19]seed@VM:~/lab2$
[09/27/19]seed@VM:~/lab2$ openssl req -new -key server.key -out server.csr -config openssl.cnf
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:PENNSLVANIA
Locality Name (eg, city) []:STATE COLLEGE
Organization Name (eg, company) [Internet Widgits Pty Ltd]:SEEDPKILab2018.com
Organizational Unit Name (eg, section) []:seenlabs
Common Name (e.g. server FQDN or YOUR name) []:seedlabs
Email Address []:seedslab@123

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:pramod
An optional company name []:seed
[09/27/19]seed@VM:~/lab2$
[09/27/19]seed@VM:~/lab2$
[09/27/19]seed@VM:~/lab2$
```

Subtask3 : CA will create certificate for seedpkilab2018.com using CSR given by customer

```
[09/27/19]seed@VM:~/lab2$ openssl req -new -key server.key -out server.csr -config openssl.cnf
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:PENN
Locality Name (eg, city) []:STATE COLLEGE
Organization Name (eg, company) [Internet Widgits Pty Ltd]:SEEDPKILab2018.com
Organizational Unit Name (eg, section) []:seed
Common Name (e.g. server FQDN or YOUR name) []:seed lab
Email Address []:seed@com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:seed
An optional company name []:seed
[09/27/19]seed@VM:~/lab2$
[09/27/19]seed@VM:~/lab2$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Sep 27 19:33:26 2019 GMT
            Not After : Sep 26 19:33:26 2020 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = PENN
            organizationName          = SEEDPKILab2018.com
            organizationalUnitName    = seed
            commonName                = seed lab
            emailAddress              = seed@com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
```

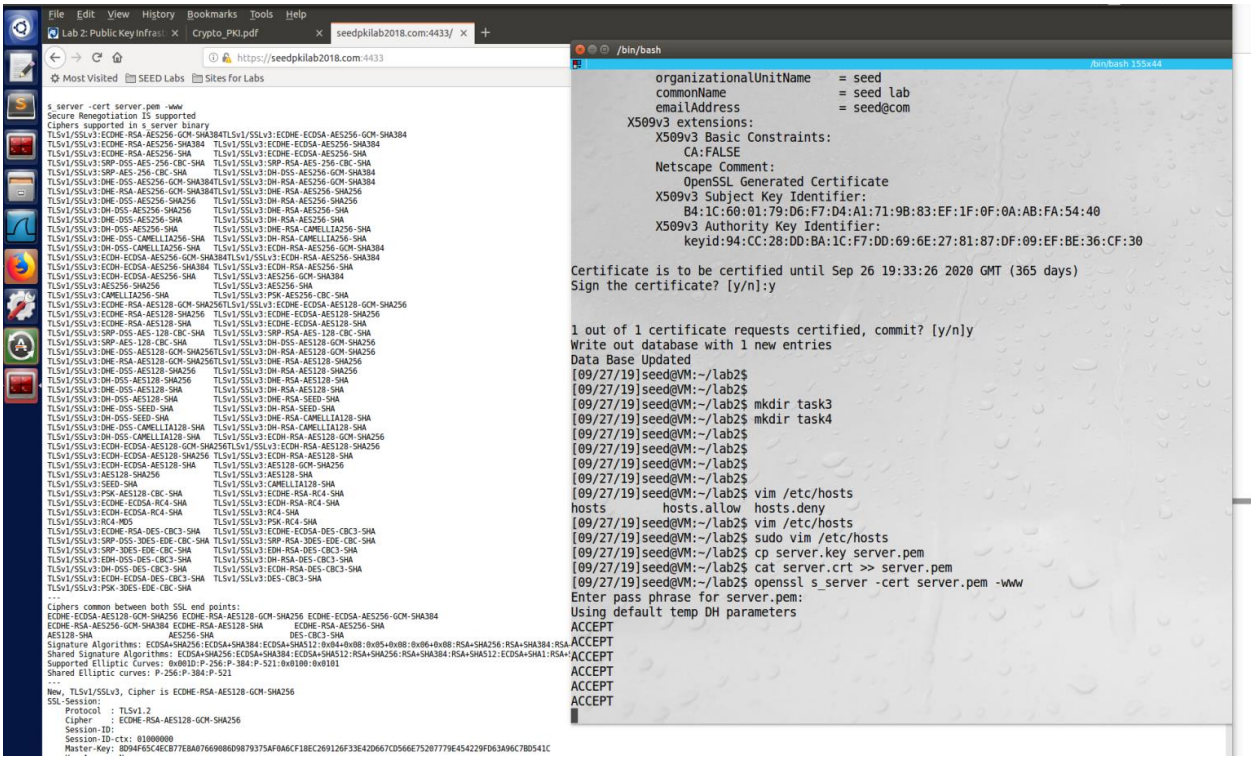
```
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                B4:1C:60:01:79:D6:F7:D4:A1:71:9B:83:EF:1F:0F:0A:AB:FA:54:40
            X509v3 Authority Key Identifier:
                keyid:94:CC:28:DD:BA:1C:F7:DD:69:6E:27:81:87:DF:09:EF:BE:36:CF:30

Certificate is to be certified until Sep 26 19:33:26 2020 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
[09/27/19]seed@VM:~/lab2$
[09/27/19]seed@VM:~/lab2$
[09/27/19]seed@VM:~/lab2$
```

Task 3:

Created server.pem using server key and crtificate signed by ca crt and ca key.

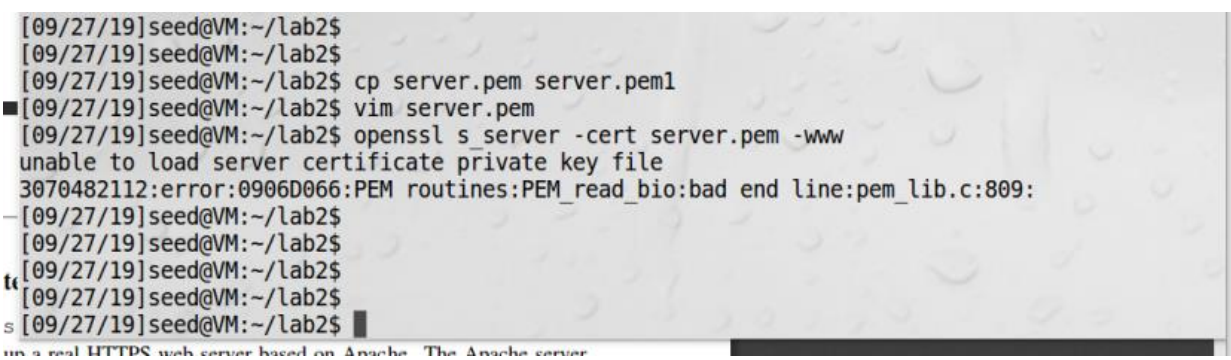
Added exception in firefox for seedpkilab2018.com:4433

Here is command and screenshot of website



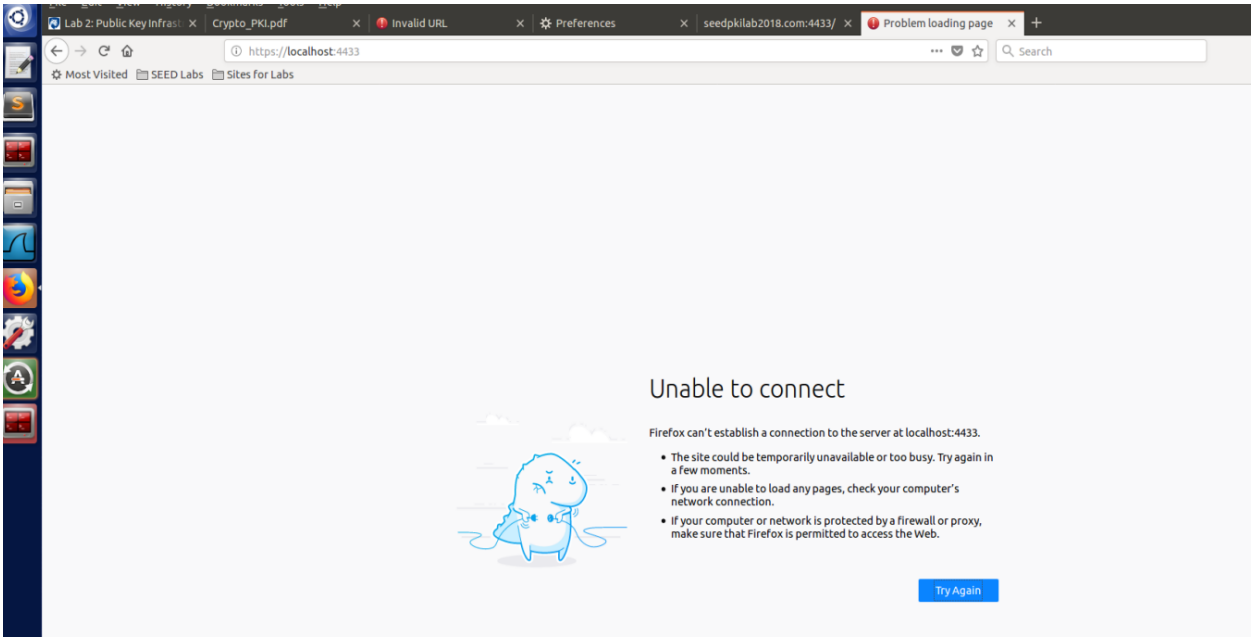
Task3.1 Edited One byte in server.pem

Observation: openss server started giving error and it didn't start



Task 3.2 : Try to open https://localhost:4433

Observation: though seedpkilab2018.com and localhost both are pointing to same ip address 127.0.0.1 but website doesn't open for localhost because openssl server is running with seedpkilab2018 domain and it doesn't recognize localhost domain name.



Task 4:

To enable our website seedpkilab2018 in apache server (along with ssl), edited both file in /etc/apache2/site-available/ directory:

Add our website in hosted website:

```
</VirtualHost>
<VirtualHost *:80>
        ServerName http://www.csrflabattacker.com
        DocumentRoot /var/www/CSRF/Attacker
</VirtualHost>
<VirtualHost *:80>
        ServerName http://www.repackagingattacklab.com
        DocumentRoot /var/www/RepackagingAttack
</VirtualHost>
<VirtualHost *:80>
        ServerName http://www.seedlabclickjacking.com
        DocumentRoot /var/www/seedlabclickjacking
</VirtualHost>
<VirtualHost *:80>
        ServerName http://www.seedpkilab2018.com
        DocumentRoot /var/www/seedpkilab2018
        DirectoryIndex index.html
</VirtualHost>
                                                                    60,1          Bot
```

Added server key and certificate location in SSL file:

```
#        this only for browsers where you know that their SSL implementation
#        works correctly.
#   Notice: Most problems of broken clients are also related to the HTTP
#   keep-alive facility, so you usually additionally want to disable
#   keep-alive for those clients, too. Use variable "nokeepalive" for this.
#   Similarly, one has to force some clients to use HTTP/1.0 to workaround
#   their broken HTTP/1.1 implementation. Use variables "downgrade-1.0" and
#   "force-response-1.0" for this.
# BrowserMatch "MSIE [2-6]" \
#               nokeepalive ssl-unclean-shutdown \
#               downgrade-1.0 force-response-1.0

        </VirtualHost>
<VirtualHost *:443>
ServerName seedpkilab2018.com
DocumentRoot /var/www/seedpkilab2018
DirectoryIndex index.html
SSLEngine On
SSLCertificateFile      /home/seed/lab2/server.pem
SSLCertificateKeyFile   /home/seed/lab2/server.key
</VirtualHost>
</IfModule>

vim: syntax=apache ts=4 sw=4 sts=4 sr noet                                  142,1
```

Test configuration, Enable ssl and restart the server.

```
[09/27/19]seed@VM:~$ cd lab2
[09/27/19]seed@VM:~/lab2$ vim /etc/apache2/sites-available/
000-default.conf  default-ssl.conf
[09/27/19]seed@VM:~/lab2$ vim /etc/apache2/sites-available/
000-default.conf  default-ssl.conf
[09/27/19]seed@VM:~/lab2$ vim /etc/apache2/sites-available/000-default.conf
[09/27/19]seed@VM:~/lab2$ sudovim /etc/apache2/sites-available/000-default.conf

sudovim: command not found
[09/27/19]seed@VM:~/lab2$ sudo vim /etc/apache2/sites-available/000-default.conf

[09/27/19]seed@VM:~/lab2$ sudo vim /etc/apache2/sites-available/default-ssl.conf

[09/27/19]seed@VM:~/lab2$ ls
ca.crt  index.txt       openssl.cnf  server.crt  server.pem1
ca.key  index.txt.attr  private      server.csr  task3
certs   index.txt.old   serial       server.key  task4
crl     newcerts        serial.old   server.pem
[09/27/19]seed@VM:~/lab2$ sudo vim /etc/apache2/sites-available/default-ssl.conf

[09/27/19]seed@VM:~/lab2$ mkdir /var/www/seedpkilab2018
mkdir: cannot create directory '/var/www/seedpkilab2018': Permission denied
[09/27/19]seed@VM:~/lab2$ sudo mkdir /var/www/seedpkilab2018
[09/27/19]seed@VM:~/lab2$ sudo vim /var/www/seedpkilab2018/index.html
[09/27/19]seed@VM:~/lab2$ sudo apachectl configtest
AH00112: Warning: DocumentRoot [/var/www/seedlabclickjacking] does not exist
AH00558: apache2: Could not reliably determine the server's fully qualified doma
in name, using 127.0.1.1. Set the 'ServerName' directive globally to suppress th
is message
Syntax OK
[09/27/19]seed@VM:~/lab2$ sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create s
elf-signed certificates.
To activate the new configuration, you need to run:
  service apache2 restart
[09/27/19]seed@VM:~/lab2$ sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
  service apache2 reload
[09/27/19]seed@VM:~/lab2$ sudo service apache2 restart
[09/27/19]seed@VM:~/lab2$
```

Open our new website

SEED Project | Assignments: Fall 2019 | Topic: Clarifications on | Crypto_PKI.pdf | seedpkilab2018.com/

https://seedpkilab2018.com

Most Visited | SEED Labs | Sites for Labs

SEED LAB PKI 2019, THIS IS LANDING PAGE

Task5:

In this section we will see how MIMA doesn't work with PKI.

Let suppose attacker try to poison the DNS with its own ip address, So when user actually visit "fakebook.com" (**not facebook.com**), that server will server him a certificate. Now 2 cases can happen:

1) The presented certificate(by server) is genuine but not for "fakebook.com" may be for gmail.com, in that case user browser will detect that servername is not matching with user URL so It will report the fail certificate verification.
2) If Attacker present a forged certificate, in that case User browser wont be able to verify that certificate with preinstalled CA's certificate in user browser. In this case too user will get the certificate failure warning.

To demonstrate this, we will use second option from above 2 option's.

1) Create a new CA & its certificate. Create a public key for fakebook.com and host on same apache server.

```
tsa_policy1 = 1.2.3.4.1
tsa_policy2 = 1.2.3.4.5.6
tsa_policy3 = 1.2.3.4.5.7

####################################################################
[ ca ]
default_ca      = CA_default            # The default ca section

####################################################################
[ CA_default ]

dir             = /home/seed/lab2/new_ca                # Where everything is kept
certs           = $dir/certs            # Where the issued certs are kept
crl_dir         = $dir/crl              # Where the issued crl are kept
database        = $dir/index.txt        # database index file.
#unique_subject = no                    # Set to 'no' to allow creation of
                                        # several ctificates with same subject.
new_certs_dir   = $dir/newcerts         # default place for new certs.

certificate     = $dir/cacert.pem       # The CA certificate
```

Generate key and get verified by our fake CA.

```
[09/28/19]seed@VM:~/.../new_ca$
[09/28/19]seed@VM:~/.../new_ca$ openssl req -new -x509 -keyout ca.key -out ca.crt -config openssl.cnf
Generating a 2048 bit RSA private key
..............................................+++
.............................................................+++
writing new private key to 'ca.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:PENN
Locality Name (eg, city) []:STATE
Organization Name (eg, company) [Internet Widgits Pty Ltd]:fakebook.com
Organizational Unit Name (eg, section) []:fakebook
Common Name (e.g. server FQDN or YOUR name) []:fakebook.com
Email Address []:fakebook@fakebook.com
[09/28/19]seed@VM:~/.../new_ca$
[09/28/19]seed@VM:~/.../new_ca$
[09/28/19]seed@VM:~/.../new_ca$
[09/28/19]seed@VM:~/.../new_ca$ openssl genrsa -aes128 -out server.key 1024
Generating RSA private key, 1024 bit long modulus
............................................................++++++
...............................++++++
e is 65537 (0x10001)
Enter pass phrase for server.key:
Verifying - Enter pass phrase for server.key:
[09/28/19]seed@VM:~/.../new_ca$ openssl req -new -key server.key -out server.csr -config openssl.cnf
Enter pass phrase for server.key:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:PENN
Locality Name (eg, city) []:STATE
Organization Name (eg, company) [Internet Widgits Pty Ltd]:fakebook.com
Organizational Unit Name (eg, section) []:fakebook
Common Name (e.g. server FQDN or YOUR name) []:fakebook.com
```

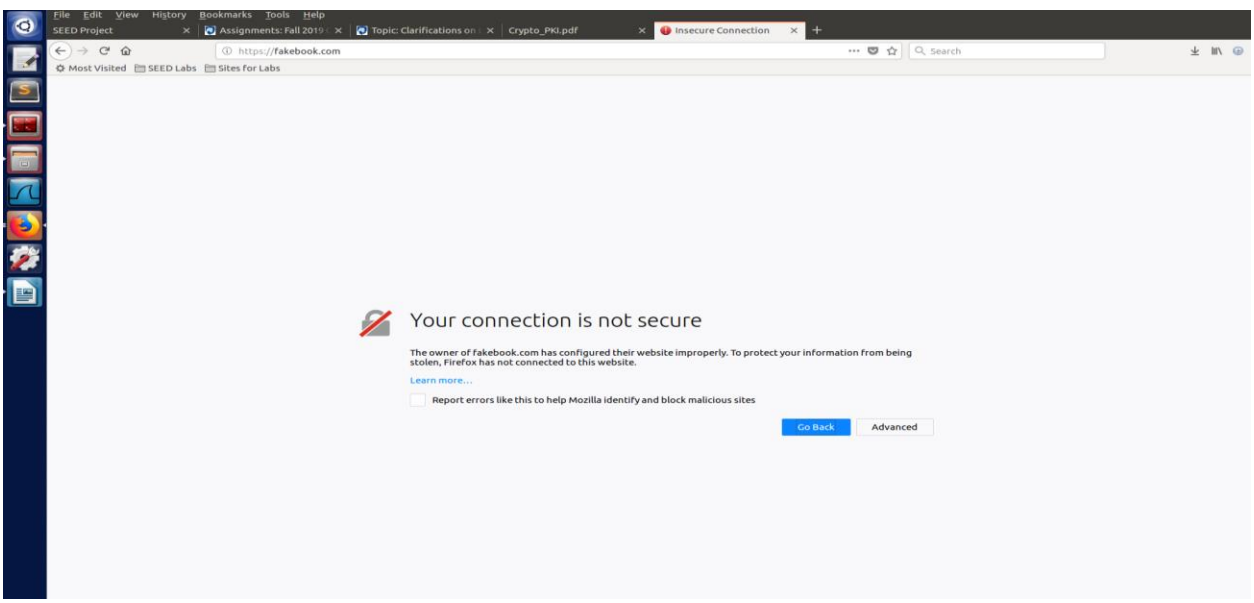
```
Email Address []:fakebook@fakebook.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:extra
An optional company name []:fakebook
[09/28/19]seed@VM:~/.../new_ca$
[09/28/19]seed@VM:~/.../new_ca$
[09/28/19]seed@VM:~/.../new_ca$
[09/28/19]seed@VM:~/.../new_ca$
[09/28/19]seed@VM:~/.../new_ca$
[09/28/19]seed@VM:~/.../new_ca$ openssl ca -in server.csr -out server.crt -cert ca.crt -keyfile ca.key -config openssl.cnf
Using configuration from openssl.cnf
Enter pass phrase for ca.key:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: Sep 28 23:46:41 2019 GMT
            Not After : Sep 27 23:46:41 2020 GMT
        Subject:
            countryName               = US
            stateOrProvinceName       = PENN
            organizationName          = fakebook.com
            organizationalUnitName    = fakebook
            commonName                = fakebook.com
            emailAddress              = fakebook@fakebook.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                69:F4:13:51:0F:52:12:27:95:22:96:DB:F6:DC:F9:2D:1B:FC:8E:65
            X509v3 Authority Key Identifier:
                keyid:5A:C4:DA:83:63:14:D5:84:6F:AB:84:ED:7A:C7:57:9B:8D:42:A2:63

Certificate is to be certified until Sep 27 23:46:41 2020 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
[09/28/19]seed@VM:~/.../new_ca$
[09/28/19]seed@VM:~/.../new_ca$
[09/28/19]seed@VM:~/.../new_ca$
```

Now add this(keys and certificate) to apache server and do DNS poising:

```
</VirtualHost>
<VirtualHost *:443>
   ServerName fakebook.com
   DocumentRoot /var/www/fakebook
   DirectoryIndex fakebook.html
   SSLEngine On
   SSLCertificateFile      /home/seed/lab2/new_ca/server.pem
   SSLCertificateKeyFile   /home/seed/lab2/new_ca/server.key
</VirtualHost>

</IfModule>

# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

```
127.0.0.1       www.csrflabelgg.com
127.0.0.1       www.csrflabattacker.com
127.0.0.1       www.repackagingattacklab.com
127.0.0.1       www.seedlabclickjacking.com
127.0.0.1       SEEDPKILab2018.com
#172.217.6.229  fakebook.com
127.0.0.1       fakebook.com
~
~
~
~
```

When user visit fakebook.com and we will present forged CA certificate then we can see browser is not able to verify it.

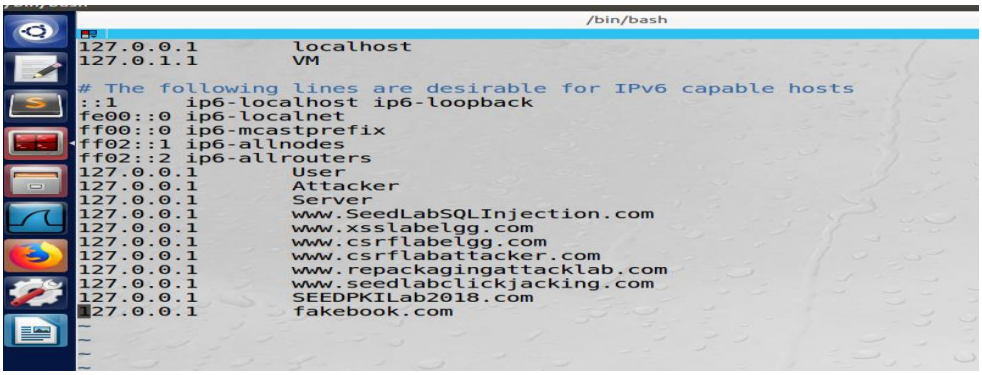


When poisoning for gmail ip address: it will also result in same as above, certification and domain name will fail the verification.

Task 6:

We have seen in task 5 that the certificate generated by attacker didn't match the preinstalled CA's certificate. In this task we will assume that CA's private key is compromised and now attacker will be able to create certificate which can be verified in browser.

Since we can't get versign or other CA's private key to create certificate which can be accepted by browser, so we have to add our CA's certificate in browser. Hence all traffic will be redirected to attacker server and he can present his key to user and decrypt the messages.



Here is Fakebook which look like facebook