[Cryptography]

Cryptography Session No.10
Summary 05-08-2022

Detailed Discussion on below points –

- Detailed explanation of Hybrid Key set up and the challenges faced – key distribution
- Brief on root poisoning attack
- Brief on IP snooping (phishing attack)
- Detailed description on MITM attack
- PKI (Public Key Infrastructure) – set up some infrastructure for public key –for this we have to trust on third party company – Certificate Authority (CA)
- CA verifies that, public key belongs to the server- sign a certificate
- For this the server creates a document or server certificate, places the company information and server public key.
- Server requests the CA to verify and sign the certificate – Certificate Signing Request (CSR)
- Format of certificate signed by CA is Chinese Remainder Theorem (CRT)
- Here the only challenge is getting the public key – so the final solution to this is root CA
- Importance of pre-installed public key – only way to get the CA public key
- Importance of Domain Name – CA to sign the certificate of server
- Here the only challenge is we have limited CA to sign millions of websites
- The root CA creates sub CA or intermediate CA to sign the certificates of servers then clients can have a secure communication with the servers
- First build root CA
    - Create private key

```
root@ip-172-31-42-1:/pki/rootca/private
[root@ip-172-31-42-1 ~]#
[root@ip-172-31-42-1 ~]#
[root@ip-172-31-42-1 ~]#
[root@ip-172-31-42-1 ~]# mkdir /pki
[root@ip-172-31-42-1 ~]# cd /pki
[root@ip-172-31-42-1 pki]# mkdir rootca
[root@ip-172-31-42-1 pki]# cd rootca
[root@ip-172-31-42-1 rootca]# pwd
/pki/rootca
[root@ip-172-31-42-1 rootca]# ls
[root@ip-172-31-42-1 rootca]# mkdir private
[root@ip-172-31-42-1 rootca]# ls
private
[root@ip-172-31-42-1 rootca]# cd private/
[root@ip-172-31-42-1 private]# openssl  genrsa -aes256  -out root-ca.key 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................+++
...+++
e is 65537 (0x010001)
Enter pass phrase for root-ca.key:
Verifying - Enter pass phrase for root-ca.key:
[root@ip-172-31-42-1 private]# l
```

- Create CSR and self-signed by root CA - CRT
  - To use the configuration file of root CA first install the software

```
[root@ip-172-31-42-1 rootca]# ls
private
[root@ip-172-31-42-1 rootca]# cd private/
[root@ip-172-31-42-1 private]# openssl  genrsa -aes256  -out root-ca.key 4096
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................+++
...+++
e is 65537 (0x010001)
Enter pass phrase for root-ca.key:
Verifying - Enter pass phrase for root-ca.key:
[root@ip-172-31-42-1 private]# ls
root-ca.key
[root@ip-172-31-42-1 private]# yum install  openssl-libs
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use subscripti
on-manager to register.

Red Hat Enterprise Linux 8 for x86_64 - AppStre 123 kB/s | 4.5 kB     00:00
Red Hat Enterprise Linux 8 for x86_64 - BaseOS  116 kB/s | 4.1 kB     00:00
Red Hat Ansible Engine 2 for RHEL 8 (RPMs) from 113 kB/s | 4.0 kB     00:00
RHUI Client Configuration Server 8               57 kB/s | 2.0 kB     00:00
```

  - Configuration file of root CA copied to another folder

```
  Verifying        : openssl-libs-1:1.1.1k-7.el8_6.x86_64                3/4
  Verifying        : openssl-libs-1:1.1.1k-6.el8_5.x86_64                4/4
Installed products updated.

Upgraded:
  openssl-1:1.1.1k-7.el8_6.x86_64      openssl-libs-1:1.1.1k-7.el8_6.x86_64

Complete!
[root@ip-172-31-42-1 private]#
[root@ip-172-31-42-1 private]# cd /etc/pki/tls/
[root@ip-172-31-42-1 tls]# ls
cert.pem  certs  ct_log_list.cnf  misc  openssl.cnf  private
[root@ip-172-31-42-1 tls]# vim openssl.cnf
-bash: vim: command not found
[root@ip-172-31-42-1 tls]# vi openssl.cnf
[root@ip-172-31-42-1 tls]#
[root@ip-172-31-42-1 tls]# ls
cert.pem  certs  ct_log_list.cnf  misc  openssl.cnf  private
[root@ip-172-31-42-1 tls]# cd
[root@ip-172-31-42-1 ~]# cp /etc/pki/tls/openssl.cnf   /pki/rootca/
[root@ip-172-31-42-1 ~]# cd /pki/rootca/
[root@ip-172-31-42-1 rootca]# ls
openssl.cnf  private
[root@ip-172-31-42-1 rootca]#
```

```
[root@ip-172-31-42-1 tls]# vi openssl.cnf
[root@ip-172-31-42-1 tls]#
[root@ip-172-31-42-1 tls]# ls
cert.pem  certs  ct_log_list.cnf  misc  openssl.cnf  private
[root@ip-172-31-42-1 tls]# cd
[root@ip-172-31-42-1 ~]# cp /etc/pki/tls/openssl.cnf   /pki/rootca/
[root@ip-172-31-42-1 ~]# cd /pki/rootca/
[root@ip-172-31-42-1 rootca]# ls
openssl.cnf  private
[root@ip-172-31-42-1 rootca]# pwd
/pki/rootca
[root@ip-172-31-42-1 rootca]# ls
openssl.cnf  private
[root@ip-172-31-42-1 rootca]# vim openssl.cnf
-bash: vim: command not found
[root@ip-172-31-42-1 rootca]# yum  install vim -y
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use subscripti
on-manager to register.

Last metadata expiration check: 0:02:35 ago on Fri 05 Aug 2022 05:09:49 PM UTC.
```

```
Running transaction
  Preparing        :                                                        1/1
  Installing       : vim-filesystem-2:8.0.1763-19.el8_6.4.noarch            1/4
  Installing       : vim-common-2:8.0.1763-19.el8_6.4.x86_64                2/4
  Installing       : gpm-libs-1.20.7-17.el8.x86_64                          3/4
  Running scriptlet: gpm-libs-1.20.7-17.el8.x86_64                          3/4
  Installing       : vim-enhanced-2:8.0.1763-19.el8_6.4.x86_64              4/4
  Running scriptlet: vim-enhanced-2:8.0.1763-19.el8_6.4.x86_64              4/4
  Running scriptlet: vim-common-2:8.0.1763-19.el8_6.4.x86_64                4/4
  Verifying        : gpm-libs-1.20.7-17.el8.x86_64                          1/4
  Verifying        : vim-enhanced-2:8.0.1763-19.el8_6.4.x86_64              2/4
  Verifying        : vim-filesystem-2:8.0.1763-19.el8_6.4.noarch            3/4
  Verifying        : vim-common-2:8.0.1763-19.el8_6.4.x86_64                4/4
Installed products updated.

Installed:
  gpm-libs-1.20.7-17.el8.x86_64
  vim-common-2:8.0.1763-19.el8_6.4.x86_64
  vim-enhanced-2:8.0.1763-19.el8_6.4.x86_64
  vim-filesystem-2:8.0.1763-19.el8_6.4.noarch

Complete!
[root@ip-172-31-42-1 rootca]# vim openssl.cnf
[root@ip-172-31-42-1 rootca]#
```

- Specify the folder name

```
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             = /pki/rootca           # 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 certs with same subject.
new_certs_dir   = $dir/newcerts         # default place for new certs.

certificate     = $dir/cacert.pem       # The CA certificate
serial          = $dir/serial           # The current serial number
crlnumber       = $dir/crlnumber        # the current crl number
                                        # must be commented out to leave a V1 CR
L
-- INSERT --                                              61,19-30      14%
```

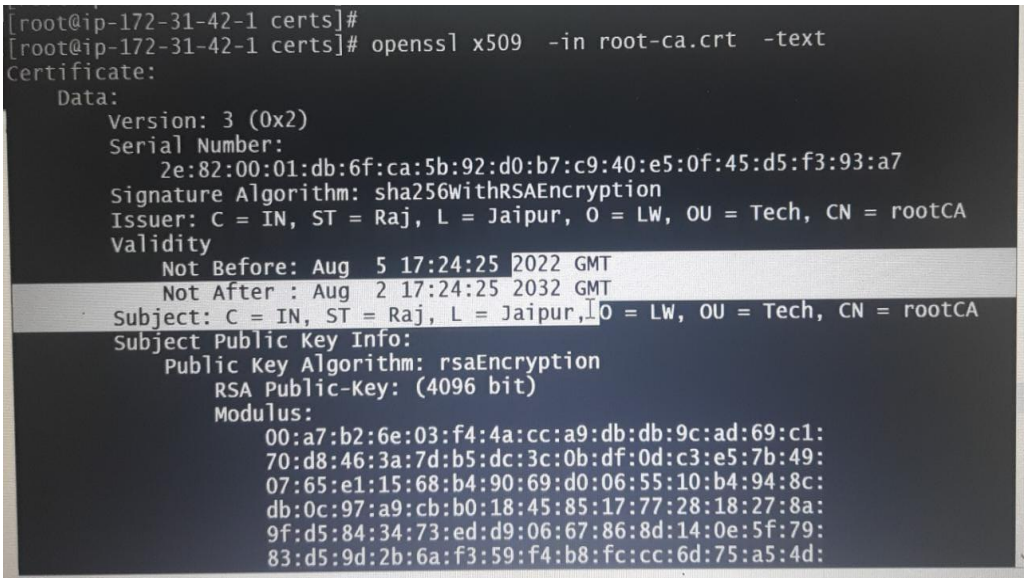
```
  vim common 2:8.0.1763-19.el8_6.4.x86_64
  vim-enhanced-2:8.0.1763-19.el8_6.4.x86_64
  vim-filesystem-2:8.0.1763-19.el8_6.4.noarch

Complete!
[root@ip-172-31-42-1 rootca]# vim openssl.cnf
[root@ip-172-31-42-1 rootca]# pwd
/pki/rootca
[root@ip-172-31-42-1 rootca]# vim openssl.cnf
[root@ip-172-31-42-1 rootca]# pwd
/pki/rootca
[root@ip-172-31-42-1 rootca]# mkdir newcerts
[root@ip-172-31-42-1 rootca]# vim openssl.cnf
[root@ip-172-31-42-1 rootca]# mkdir certs
[root@ip-172-31-42-1 rootca]# vim openssl.cnf
[root@ip-172-31-42-1 rootca]# touch index.txt
[root@ip-172-31-42-1 rootca]# vim openssl.cnf
[root@ip-172-31-42-1 rootca]#
[root@ip-172-31-42-1 rootca]# echo 01 > serial
[root@ip-172-31-42-1 rootca]# cat serial
01
[root@ip-172-31-42-1 rootca]# ls
certs  index.txt  newcerts  openssl.cnf  private  serial
[root@ip-172-31-42-1 rootca]#
```

- Root CA creates their own CSR with self-signed

```
[root@ip-172-31-42-1 rootca]# echo 01 > serial
[root@ip-172-31-42-1 rootca]# cat serial
01
[root@ip-172-31-42-1 rootca]# ls
certs  index.txt  newcerts  openssl.cnf  private  serial
[root@ip-172-31-42-1 rootca]# openssl  req  -config openssl.cnf   -key private/r
oot-ca.key    -new  -days 3650 -sha256 -x509 -extensions  v3_ca  -out certs/roo
t-ca.crt
Enter pass phrase for private/root-ca.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) [XX]:IN
State or Province Name (full name) []:Raj
Locality Name (eg, city) [Default City]:Jaipur
Organization Name (eg, company) [Default Company Ltd]:LW
Organizational Unit Name (eg, section) []:Tech
Common Name (eg, your name or your server's hostname) []:rootCA
Email Address []:
[root@ip-172-31-42-1 rootca]#
```

- To view the CRT in standard format



Important Links –

Hash13 link for Extra Sessions and session recording - https://learning.hash13.com/

Community Link to post Query, Doubts and share your blogs - https://hash13-community.circle.so/home