Cmpe 277: (Certificate Pinning) Man in the middle.

**Method of testing:** Pin the certificate and a public key for a specific URL say <https://www.google.com>. For this generate a keystore with all the certificates from [www.google:443](http://www.google:443) CA and in project. Later enter a different url which is issued from a different CA. Check if the initial pinned certificate would reject it. So by entering a different url <https://www.yahoo.com> which is issued from a different CA, a certificate and public key mismatch is displayed.

**Steps followed:**

1. Get the google CA certificate chain lists:

Swetha-RKs-MacBook-Pro:maninthemiddle swethark$ openssl s\_client -connect <www.google.com:443>

CONNECTED(00000003)

depth=2 /C=US/O=GeoTrust Inc./CN=GeoTrust Global CA

verify error:num=20:unable to get local issuer certificate

verify return:0

---

Certificate chain

0 s:/C=US/ST=California/L=Mountain View/O=Google Inc/CN=<www.google.com>

i:/C=US/O=Google Inc/CN=Google Internet Authority G2

1 s:/C=US/O=Google Inc/CN=Google Internet Authority G2

i:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA

2 s:/C=US/O=GeoTrust Inc./CN=GeoTrust Global CA

i:/C=US/O=Equifax/OU=Equifax Secure Certificate Authority

---

2. Retrieve the entire certificate for host (“<www.google.com:443>”) and store in mygooglecertfile.pem

openssl s\_client -showcerts -connect <www.google.com:443> </dev/null 2>/dev/null|openssl x509 -outform PEM >mygooglecertfile.pem

3. Using my cacert i,e mygooglecertfile.pem as an input, generate a keystore containing our CAs. This is done in code.

4. So for any of the incoming SSL connection, get the CA list of Trusted chains that is given as an input to checkServerTrusted() method

5. Check if the chain[0] public key is same as our keystore CA issued certificate. If its same, then it is issued from a trusted CA. If exception, then the certificate is not from trusted CA.

Application specific Logs: Logs for valid URL input (https://www.google.com)

/newSslSocketFactory-chain.length %s(15343): 3

I/System.out(15343): ca=CN=www.google.com, O=Google Inc, L=Mountain View, ST=California, C=US

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*(15343): \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

D/MY CA publicKey-(15343): 

I/System.out(15343): MY CA subject =CN=www.google.com, O=Google Inc, L=Mountain View, ST=California, C=US

I/System.out(15343): MY CA issuer =CN=Google Internet Authority G2, O=Google Inc, C=US

D/Received Chain[0] publicKey-(15343): 

I/Choreographer(15343): Skipped 46 frames! The application may be doing too much work on its main thread.

I/System.out(15343): chain[0] subject =CN=www.google.com, O=Google Inc, L=Mountain View, ST=California, C=US

I/System.out(15343): CA issuer =CN=Google Internet Authority G2, O=Google Inc, C=US

I/Choreographer(15343): Skipped 31 frames! The application may be doing too much work on its main thread.

I/Choreographer(15343): Skipped 53 frames! The application may be doing too much work on its main thread.

D/Received Chain[1] publicKey-(15343): 

I/System.out(15343): chain[1] subject =CN=Google Internet Authority G2, O=Google Inc, C=US

I/System.out(15343): CA issuer =CN=GeoTrust Global CA, O=GeoTrust Inc., C=US

I/Choreographer(15343): Skipped 35 frames! The application may be doing too much work on its main thread.

D/Received Chain[2] publicKey-(15343): 

I/System.out(15343): chain[2] subject =CN=GeoTrust Global CA, O=GeoTrust Inc., C=US

I/System.out(15343): CA issuer =OU=Equifax Secure Certificate Authority, O=Equifax, C=US

D/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*(15343): \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Logs for second Forbidden URL input (<https://www.yahoo.com>)

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*(15343): \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

D/MY CA publicKey-(15343): 

I/System.out(15343): MY CA subject =CN=www.google.com, O=Google Inc, L=Mountain View, ST=California, C=US

I/System.out(15343): MY CA issuer =CN=Google Internet Authority G2, O=Google Inc, C=US

I/Choreographer(15343): Skipped 48 frames! The application may be doing too much work on its main thread.

D/Received Chain[0] publicKey-(15343): 

I/Choreographer(15343): Skipped 89 frames! The application may be doing too much work on its main thread.

I/Choreographer(15343): Skipped 55 frames! The application may be doing too much work on its main thread.

I/System.out(15343): chain[0] subject =CN=www.yahoo.com, OU=Information Technology, O=Yahoo Inc., L=Sunnyvale, ST=California, C=US

I/System.out(15343): CA issuer =CN=VeriSign Class 3 Secure Server CA - G3, OU=Terms of use at https://www.verisign.com/rpa (c)10, OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US

D/Received Chain[1] publicKey-(15343): 

I/System.out(15343): chain[1] subject =CN=VeriSign Class 3 Secure Server CA - G3, OU=Terms of use at https://www.verisign.com/rpa (c)10, OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US

I/Choreographer(15343): Skipped 40 frames! The application may be doing too much work on its main thread.

I/System.out(15343): CA issuer =CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US

D/Received Chain[2] publicKey-(15343): 

I/System.out(15343): chain[2] subject =CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US

I/Choreographer(15343): Skipped 47 frames! The application may be doing too much work on its main thread.

I/System.out(15343): CA issuer =OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US

D/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*(15343): \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Screenshots:**









