java peer not authenticated

作者：yp
原文链接：https://ld246.com/article/1520826650219
来源网站：链滴

记录一下发起https请求时候的异常问题.已经配置了忽略证书,还是跳不过去.

```
Ignoring unavailable cipher suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

Ignoring unavailable cipher suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
Ignoring unavailable cipher suite: TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
Ignoring unsupported cipher suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
Ignoring unsupported cipher suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
Ignoring unsupported cipher suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
Ignoring unsupported cipher suite: TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
Ignoring unsupported cipher suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
Ignoring unsupported cipher suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
Ignoring unsupported cipher suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
Ignoring unsupported cipher suite: TLS_RSA_WITH_AES_256_CBC_SHA256
Ignoring unavailable cipher suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
Ignoring unsupported cipher suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
Ignoring unsupported cipher suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
Ignoring unavailable cipher suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA
Ignoring unsupported cipher suite: TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
Ignoring unsupported cipher suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
Ignoring unsupported cipher suite: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
Ignoring unavailable cipher suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
Ignoring unavailable cipher suite: TLS_RSA_WITH_AES_256_CBC_SHA
Ignoring unsupported cipher suite: TLS_RSA_WITH_AES_128_CBC_SHA256
main, setSoTimeout(1500000) called
Allow unsafe renegotiation: false
Allow legacy hello messages: true
Is initial handshake: true
Is secure renegotiation: false
%% No cached client session
*** ClientHello, TLSv1
RandomCookie:  GMT: 1503981715 bytes = { 30, 214, 241, 201, 151, 196, 225, 2, 254, 129, 209,
96, 155, 197, 121, 224, 34, 239, 163, 38, 142, 242, 208, 240, 178, 60, 126, 97 }
Session ID:  {}
Cipher Suites: [TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128
CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA, TL
_ECDH_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_DSS
WITH_AES_128_CBC_SHA, TLS_ECDHE_ECDSA_WITH_RC4_128_SHA, TLS_ECDHE_RSA_WITH_R
4_128_SHA, SSL_RSA_WITH_RC4_128_SHA, TLS_ECDH_ECDSA_WITH_RC4_128_SHA, TLS_ECDH
RSA_WITH_RC4_128_SHA, TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_RSA_W
TH_3DES_EDE_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDH_ECDSA_WITH_3DES
EDE_CBC_SHA, TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_C
C_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA, SSL_RSA_WITH_RC4_128_MD5, TLS_EMPTY
RENEGOTIATION_INFO_SCSV]
Compression Methods:  { 0 }
Extension elliptic_curves, curve names: {secp256r1, sect163k1, sect163r2, secp192r1, secp224r
, sect233k1, sect233r1, sect283k1, sect283r1, secp384r1, sect409k1, sect409r1, secp521r1, sect
71k1, sect571r1, secp160k1, secp160r1, secp160r2, sect163r1, secp192k1, sect193r1, sect193r2
 secp224k1, sect239k1, secp256k1}
Extension ec_point_formats, formats: [uncompressed]
***
main, WRITE: TLSv1 Handshake, length = 149
main, READ: TLSv1 Alert, length = 2
main, RECV TLSv1 ALERT:  fatal, handshake_failure
```

原文链接：java peer not authenticated

```
main, called closeSocket()
main, handling exception: javax.net.ssl.SSLHandshakeException: Received fatal alert: handsha
e_failure
main, IOException in getSession():  javax.net.ssl.SSLHandshakeException: Received fatal alert:
andshake_failure
main, called close()
main, called closeInternal(true)
main, called close()
main, called closeInternal(true)
```

ssl请求的debug日志.

最后升级了下httpclient的jar包到4.5.4版本后解决了问题