CCEAP-based Sample Exercises

Provided by Zillien/Wendzel, Worms University of Applied Sciences.

Please note:

- You can see a list of possible CCEAP client options by running: `client -h`.
- For some covert channels, you may have to run CCEAP multiple times if you wish to send different hidden messages (e.g. a `0' bit, followed by a `1' bit). However, CCEAP itself is not focusing on the hidden meaning, at all.
- In several cases, there is not just one correct answer but multiple ways to achieve a correct answer.

I. Creation of a Covert Channel using a particular Pattern:

a) Create a covert channel using the *Value Modulation* pattern.
(hint: -d option)

Sample solution:
client.exe -d ABC (0 bit)
client.exe -d abc (1 bit)

b) Create a covert channel using the *Sequence Modulation pattern.*
(hint: -o option)

Sample solution:
client.exe -o 0,6,0/1,7,0 -> 0
client.exe -o 0,7,0/1,6,0 -> 1

c) Create a covert channel using the *Artificial Retransmission* pattern.
(hint: -p option)

Sample solution:
client.exe -l 10 -p 11 -c 20 (re-transmits the packet with the seq. no. 11)

d) Create a hybrid covert channel using the patterns *Size Modulation* and *Reserved/Unused*.

Sample solution:
client.exe -u 1 (writing a `1' byte into the unused header field)
client.exe -u 2 -o 1,2,3 (writing a `2' into the unused header field and increasing packet size due to the added options header)

e) Create a hybrid covert channel that uses the patterns *Interpacket Times* and *Artificial Packet Loss*.

Sample solution:
client.exe -t 1005,1005 –c 3 -> Set the inter-arrival time to 1005ms and transfer 3 packets (no artificial loss)
client.exe -t 205,1005 –x 2 –c 3 ->Exclude the packet with sequence number `2' and reduce the first inter-arrival time to 205ms.

II. Determining the patterns based on a given traffic recording:

a) The CCEAP server provides the following output of the traffic that it received.
Which pattern(s) were used?

```
received data (12 bytes):
> time diff to prev pkt: 0
> sequence number:       12
> destination length:    0
> dummy value:           0
> destination + padding: XXXXXXXX
> number of options:     0

received data (12 bytes):
> time diff to prev pkt: 1005
> sequence number:       10
> destination length:    0
> dummy value:           0
> destination + padding: XXXXXXXX
> number of options:     0

received data (12 bytes):
> time diff to prev pkt: 1005
> sequence number:       18
> destination length:    0
> dummy value:           0
> destination + padding: XXXXXXXX
> number of options:     0

received data (12 bytes):
> time diff to prev pkt: 1005
> sequence number:       16
> destination length:    0
> dummy value:           0
> destination + padding: XXXXXXXX
> number of options:     0
```

Solution:

PDU Order Pattern (& Artificial Pkt. Loss Pattern), also the traffic could be understood as such that it used the Inter-arrival Time Pattern.

b) The server output is now as follows. Which pattern(s) can you find?

```
received data (12 bytes):
> time diff to prev pkt: 0
> sequence number:       1
> destination length:    0
> dummy value:           0
> destination + padding: XXXXXXXX
> number of options:     0

received data (12 bytes):
> time diff to prev pkt: 500
> sequence number:       2
> destination length:    0
> dummy value:           0
> destination + padding: XXXXXXXX
> number of options:     0

received data (12 bytes):
> time diff to prev pkt: 500
> sequence number:       2
> destination length:    0
> dummy value:           0
> destination + padding: XXXXXXXX
> number of options:     0

received data (12 bytes):
> time diff to prev pkt: 500
> sequence number:       3
> destination length:    0
> dummy value:           0
> destination + padding: XXXXXXXX
> number of options:     0
```

```
received data (12 bytes):
> time diff to prev pkt: 1000
> sequence number:       4
> destination length:    0
> dummy value:           0
> destination + padding: XXXXXXXX
> number of options:     0

received data (12 bytes):
> time diff to prev pkt: 500
> sequence number:       5
> destination length:    0
> dummy value:           0
> destination + padding: XXXXXXXX
> number of options:     0

received data (12 bytes):
> time diff to prev pkt: 500
> sequence number:       6
> destination length:    0
> dummy value:           0
> destination + padding: XXXXXXXX
> number of options:     0

received data (12 bytes):
> time diff to prev pkt: 500
> sequence number:       7
> destination length:    0
> dummy value:           0
> destination + padding: XXXXXXXX
> number of options:     0
```

Solution:

The Rate or the Inter-arrival Time Pattern was used.
Also, the Artificial Retransmission Pattern was used.