Clasnif: uno sniffer di immagini JPEG

Claudio Santini (407978)

Descrizione

Clasnif è uno sniffer che cerca i byte di inzio/fine delle immagini JPEG all'interno di segmenti TCP/IP attraverso l'algoritmo di Boyer-Moore-Horsepool e salva nella directory corrente le immagini trovate (dà una idea rapida dei siti che stanno visitando gli utenti sulla rete).
Di default il programma sta in ascolto di pacchetti TCP sulla porta 80 (filtrati con pcap_compile), e quando trova i byte di inizio frame JPEG (`jpeg_soi 0xFFD8`) inzia a memorizzare i segmenti passanti su quella connessione in una lista di buffer (`struct list_t`) fino a che non trova i byte di fine (`jpeg_eoi`), oppure fino all'avvento di un timeout, o del superamento della dimensione massima consentita.
Le connesioni vengono memorizzate in una hash table implementata dalla libreria uthash e ricavate utilizzando come chiave la combinazione di ip e porte sorgente/destinazione.
Nel caso di perdita di pacchetti, il l'algoritmo fa del suo meglio; si distinguono diversi casi:

- viene perso il pacchetto contente l'inzio dell'immagine (jpeg_soi): l'immagine viene persa.
- viene perso il pacchetto contente jpeg_eoi: l'immagine scade per timeout e non viene salvata.
- viene perso uno o più pacchetti del corpo dell'immagine, dunque l'immagine viene salva con qualche imperfezione.

Testing

Il programma è stato compilato con gcc 4.3.3 (precompilato per Ubuntu) e con libpcap 0.8.

Per verificarne il funzionamento basta generare con un qualunque browser del traffico HTTP contenente immagini JPEG (ad esempio basta visitare un sito con qualche jpeg).

Se viene lanciato senza parametri il programma cerca l'interfaccia di rete di default di pcap (tipicamente eth0) , altrimenti inzia l'ascolto sull'interfaccia specificata. Ad esempio

```
claudio@laptop:~/workspace/clasnif$ make
gcc -Wall -pedantic -lpcap clasnif.c -o clasnif
claudio@laptop:~/workspace/clasnif$ sudo ./clasnif ath0
[sudo] password for claudio:
Device: ath0
Image saved in 0.jpg
Image saved in 1.jpg
Image saved in 2.jpg
Image saved in 3.jpg
Image saved in 4.jpg
Image saved in 5.jpg
[...]
```

Per avere informazioni aggiuntive durante l'esecuzione è sufficiente ricompilare il codice con l'opzione -DDEBUG:

```
claudio@laptop:~/workspace/clasnif$ gcc -DDEBUG -lpcap clasnif.c -o clasnif
```

```
claudio@laptop:~/workspace/clasnif$ sudo ./clasnif ath0
claudio@laptop:~/workspace/clasnif$ sudo ./clasni ath0
Device: ath0
packet 1
---------------------------------
packet 2
---------------------------------
packet 3
---------------------------------
packet 4
ether: >> 0 1a ... 8 0
ip: >> 45 0 ... 37 2a
tcp: >> d9 26 ... 0 0
header->len=806 hlen=66 datalen=740
data: >> 47 45 ... d a
---------------------------------
[…]
```

Il programma salva le immagini che trova nella directory corrente, con nomi del tipo N.jpg, dove N è un contatore intero crescente.