SICUREZZA NELLE RETI a. a. 2012/13 – Riassunto Onion Routing

by Salvatore Fresta

Per **Onion Routing** si intende la tecnica per rendere anonima la comunicazione su una rete o comunque per rendere difficile il tracciamento. I dati vengono cifrati dal mittente ed inviati tramite diversi nodi di rete chiamati **onion router** al reale destinatario. Esattamente come quando si sbuccia una cipolla, ogni onion router che riceve il pacchetto decifra la propria parte che contiene le informazioni di routing, le interpreta ed inoltra il pacchetto all'onion router specificato. Tutto questo fino ad arrivare all'ultimo nodo, chiamato **exit node**, che inoltrerà il pacchetto al dovuto destinatario.

Quindi ogni nodo intermediario non dispone di adeguate informazioni per riconoscere mittente, destinatario e dati. Ognuno conosce solo un'informazione parziale che garantisce un ottimo livello di anonimato. Naturalmente una rete del genere decade un poco in prestazioni.

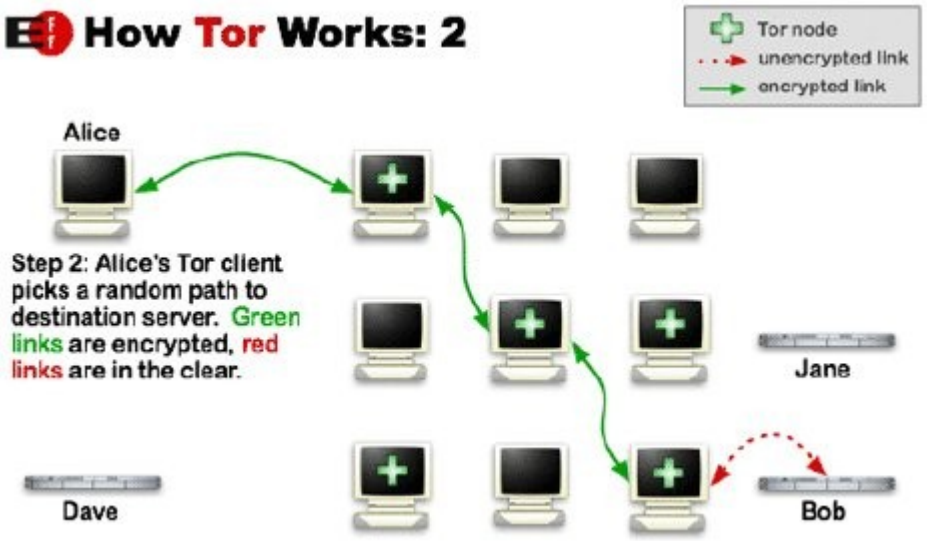
Gli onion router costituiscono il **mix di Chaum**: un mix riceve i messaggi di lunghezza fissa, li cripta, aspetta di averne un numero sufficiente per un buon livello di anonimato e li inoltra ad altri mix in ordine arbitrario.

Uno dei progetti più significativi di Onion Routing è **TOR**, acronimo di **The Onion Router Project**.

Funzionamento di TOR:

1. Alice vuole comunicare con Bob. Avvia il client TOR (chiamato **Onion Proxy**) che per prima cosa riceve una **lista di onion router** da un *directory server*.

2. A questo punto il client TOR **costruisce un circuito random** utilizzando alcuni degli onion router della lista. Il traffico tra gli onion router sarà cifrato utilizzando TSL mentre sarà in chiaro quello tra **exit node** (scelto in base alle **exit policy**) e Bob.



Solitamente **ogni minuto** viene aggiornato il circuito in modo da offrire un alto livello di anonimato.

È facile intuire che, a meno di sistemi di autenticazione a livello applicativo, sarà impossibile anche per Bob conoscere il reale mittente, in quanto egli vede i pacchetti come se fossero inviati dall'exit node.

Ogni nodo **conosce solo il nodo precedente e quello successivo**, quindi anche se in mezzo ci sta qualche nodo malevolo (per tracciare il traffico ad esempio), questo non sarà in grado di conoscere l'informazione in quanto rimane sconosciuta la reale origine e la reale destinazione. Inoltre i pacchetti, come già detto, sono cifrati.

Per raggiungere buoni livelli di **efficienza**, tutte le richieste effettuate dal client nello stesso minuto viaggiano attraverso lo stesso circuito (**multiplexing**).

I nodi che operano da *directory server* **devono essere trusted**, altrimenti possono fornire informazioni false al fine di tracciare il traffico.

Ogni onion router ha una **long-term key** utilizzata per l'identificazione ed una **short-term key** utilizzata in ogni sessione TSL che garantisce la PFS (**Perfect Forward Secrecy**), ovvero una volta terminata la sessione le chiavi cambieranno e non sarà possibile per un onion router rivedere il traffico. Quindi non è possibile ricostruire il traffico tra router diversi.

I pacchetti TOR si chiamano **celle**.

Per proteggere eventuali informazioni personali, ontenuti all'interno dei pacchetti applicativi, da terzi alla fine del circuito, è necessario utilizzare un **protocol cleaner** come Privoxy.