Servizi Onion

Dalla teoria all'implementazione

Leonardo Migliorelli[1]
leonardo.migliorelli@studenti.unicam.it

Computer Science @ Unicam

Tesi Unicam - Servizi Onion, dalla teoria dall'implementazione

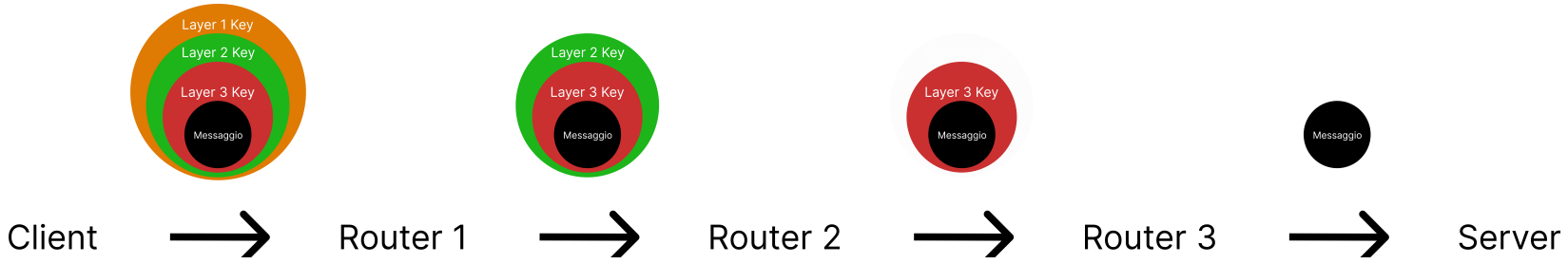
- Relatore: Marcantoni Fausto
  https://computerscience.unicam.it/marcantoni/
- Studente: Leonardo Migliorelli
  leonardo.migliorelli@studenti.unicam.it MAT. 113920

Indice

Introduzione

In questa tesi spiegheremo il funzionamento delle reti **Onion** e parleremo in particolare della rete **Tor**, in fine mostreremo com'è possibile implementare un **servizio Onion/Tor**.
Le reti Onion sono state create per risolvere le due più grandi vulnerabilità di Internet che gravano sulla **privacy** e sull'**anonimato**, ovvero l'**analisi del traffico** e le **intercettazioni**.
Una rete di questo tipo nasconde infatti gli indirizzi e il contenuto di ogni richiesta, consentendo all'utente di navigare in rete senza essere tracciato.

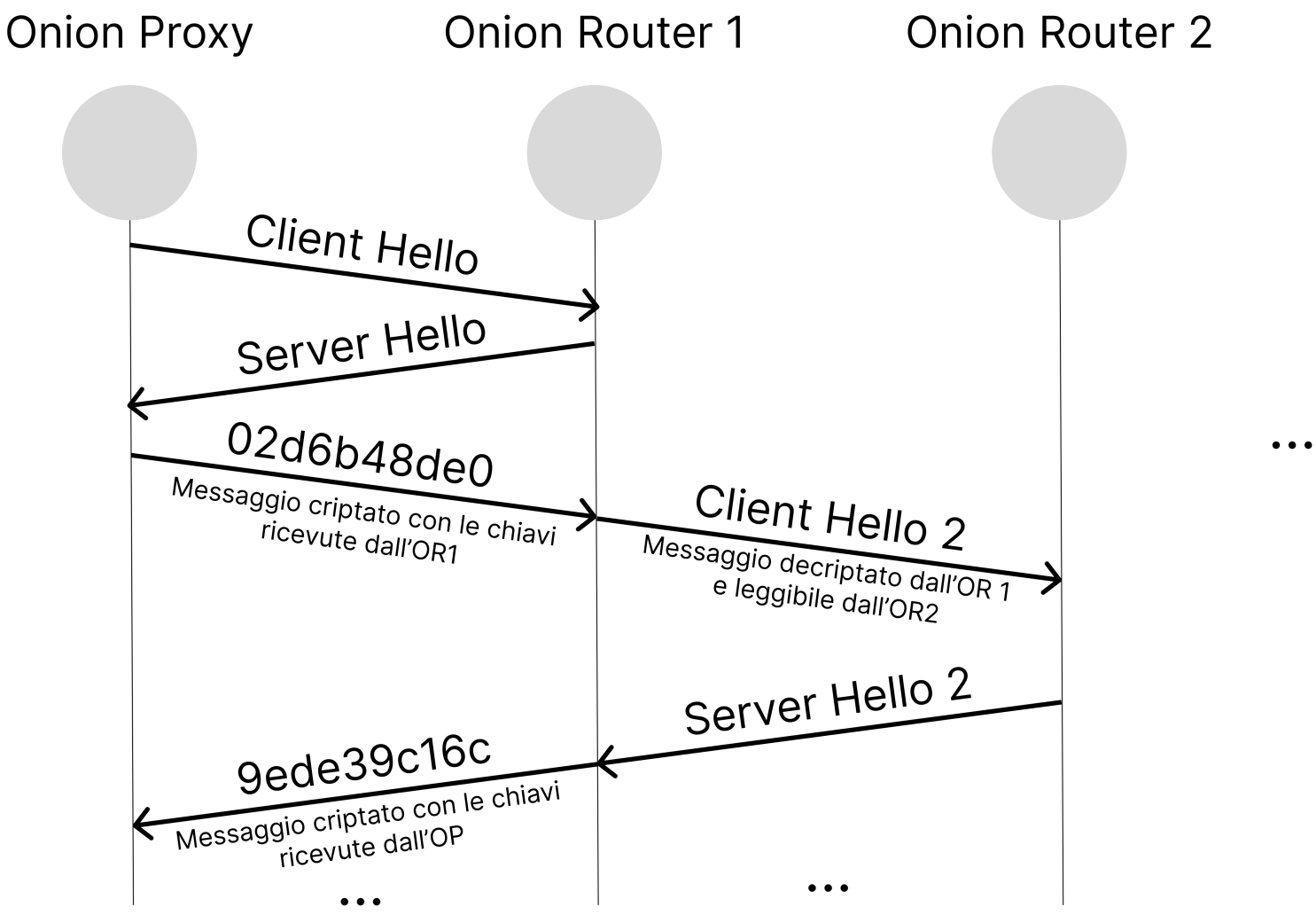
Onion Routing



La rete Onion è una rete distribuita composta da nodi chiamati **Onion Router**, collegati tra loro tramite i circuiti creati dai client/proxy.
Ogni pacchetto che passa nel circuito viene decriptato in maniera sequenziale dai relativi nodi prima di essere inoltrato all'exit node che si occupa di instradare il pacchetto nella classica rete Internet.
Grazie a questo meccanismo nessun nodo conosce contemporaneamente l'indirizzo del mittente e del destinatario

Creazione del circuito

La generazione del circuito è un processo **iterativo** e **progressivo** in cui il proxy server sceglie i nodi del circuito. A partire dal primo nodo viene instaurata una connessione **TLS** e vengono scambiate le **chiavi simmetriche** tramite un processo **asimmetrico** (in maniera simile allo scambio di chiavi di HTTPS), successivamente si usano queste chiavi per cifrare il messaggio che verrà inviato al primo nodo che lo decripta e inoltra al secondo nodo.
Questo processo continua fino all'exit node, a questo punto il circuito è completo e può iniziare a trasmettere i pacchetti.


Onion Proxy
Onion Router 1
Onion Router 2
Client Hello
Server Hello
02d6b48de0
Messaggio criptato con le chiavi ricevute dall'OR1
Client Hello 2
Messaggio decriptato dall'OR 1 e leggibile dall'OR2
Server Hello 2
9ede39c16c
Messaggio criptato con le chiavi ricevute dall'OP
...
...
...