Design and security of an instant messaging service using Tor

Marvin FOURASTIE

Cours “Sécurité avancée”

Spring 2021

Motivations

Ensure secure and anonymous exchanges

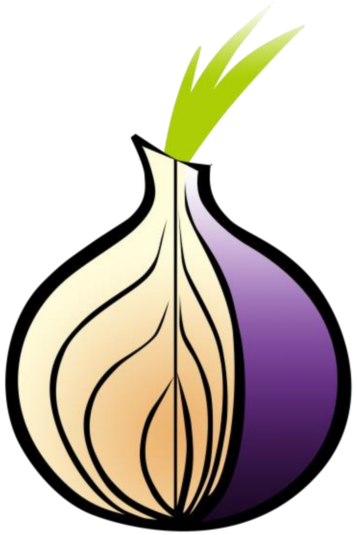
Use Tor to implement an instant messaging system

Study the pros and the cons of such a system

Tor

Onion routing

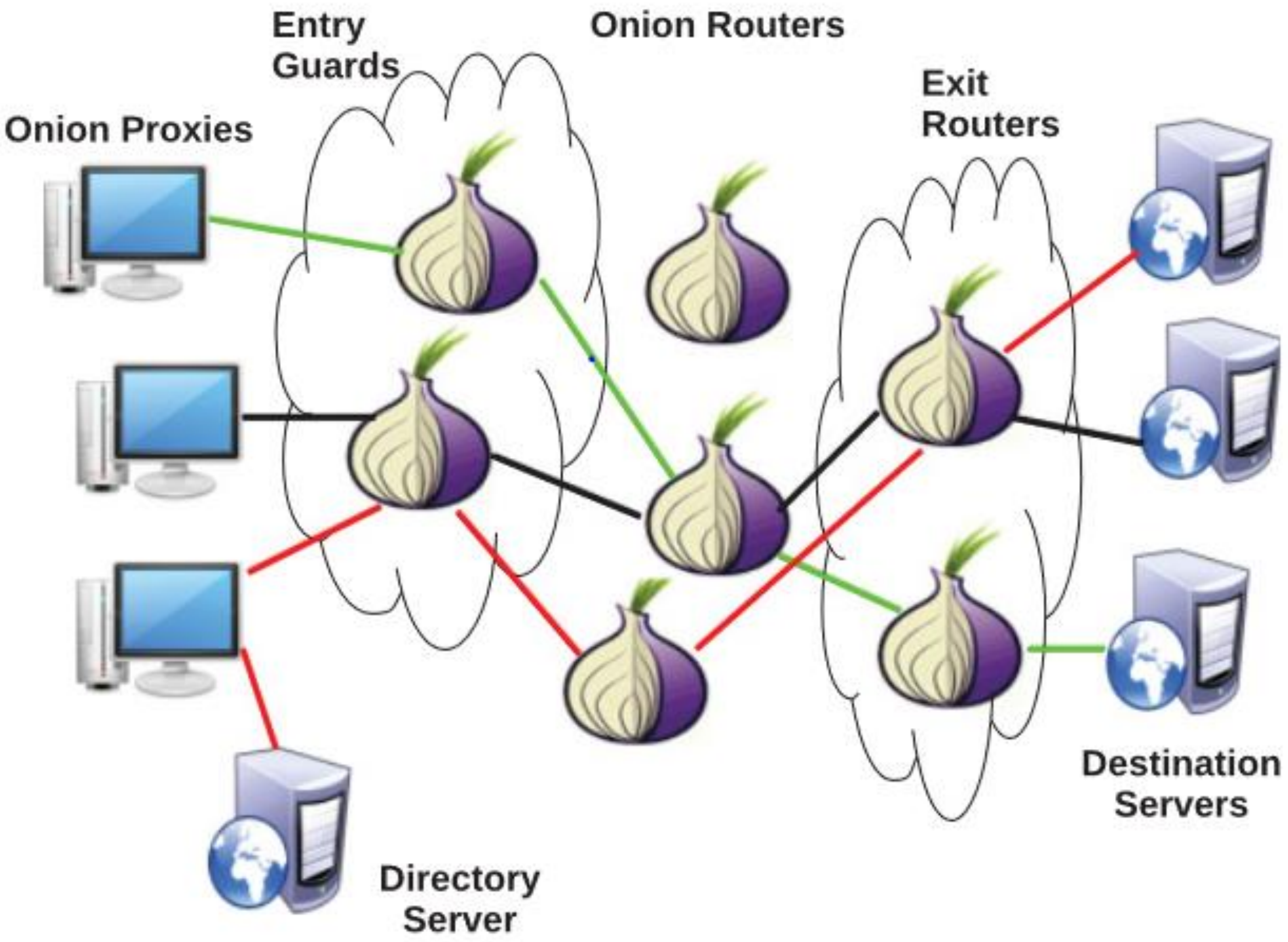
Usability



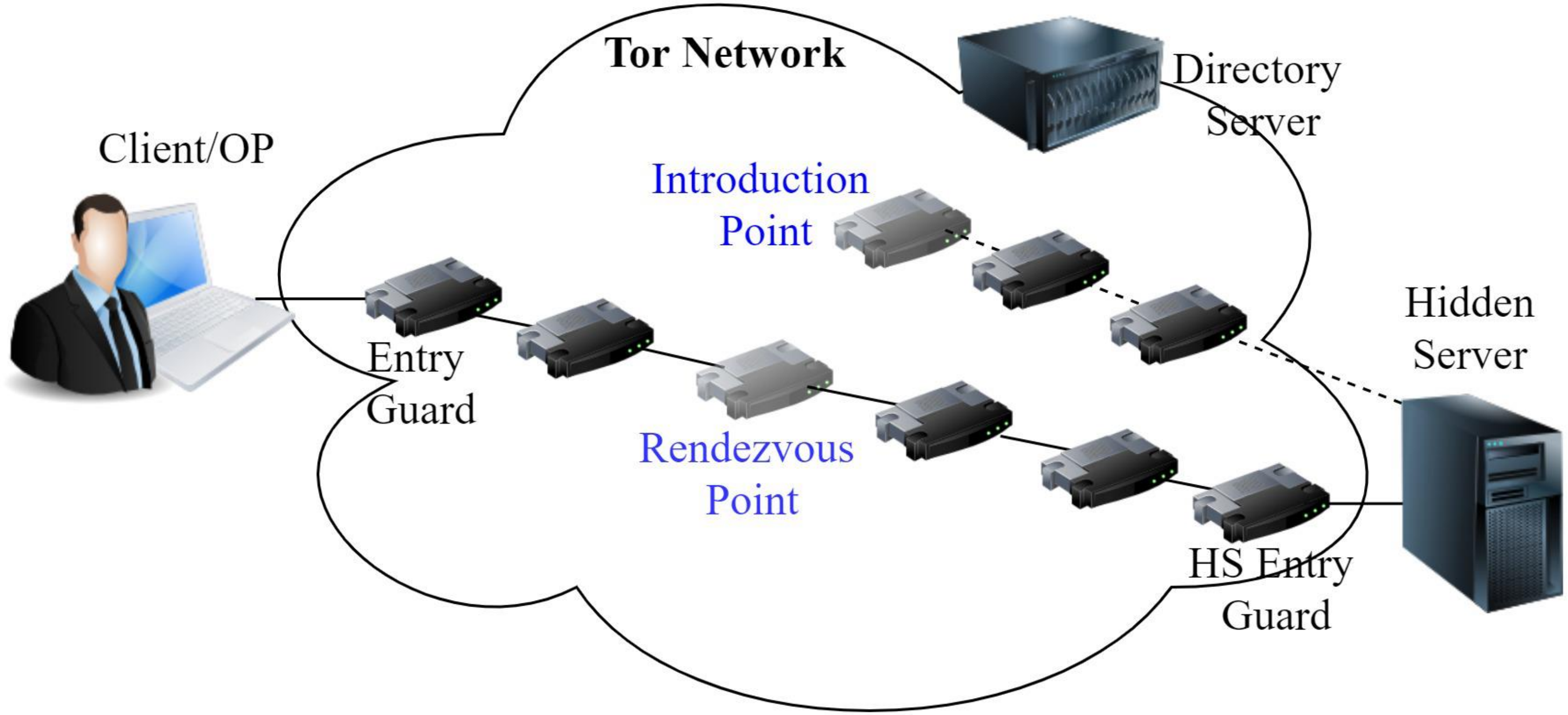
low-latency

Anonymity

Tor


Entry Guards
Onion Routers
Onion Proxies
Exit Routers
Destination Servers
Directory Server

Tor


Tor Network
Directory Server
Client/OP
Introduction Point
Hidden Server
Entry Guard
Rendezvous Point
HS Entry Guard

Goals

Anonymity of the users

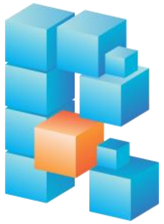
Messages encryption

No centralised server

Related Work

“Classical” instant messaging →

Synchronous messaging on Tor →



Asynchronous messaging on Tor → ATHiCC

Our implementation

Create cells

Set up the circuit

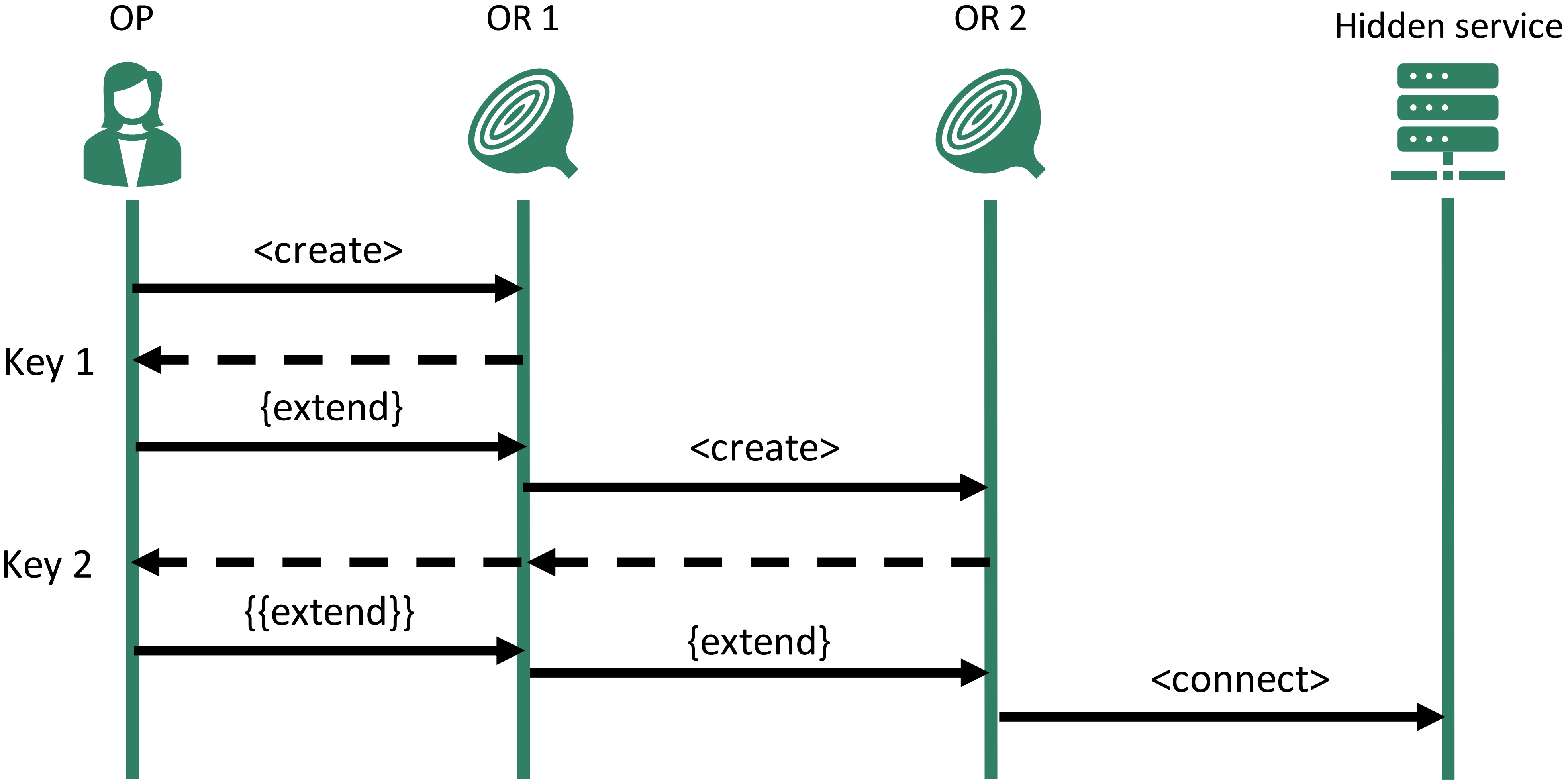
Key exchanges

Extend cells

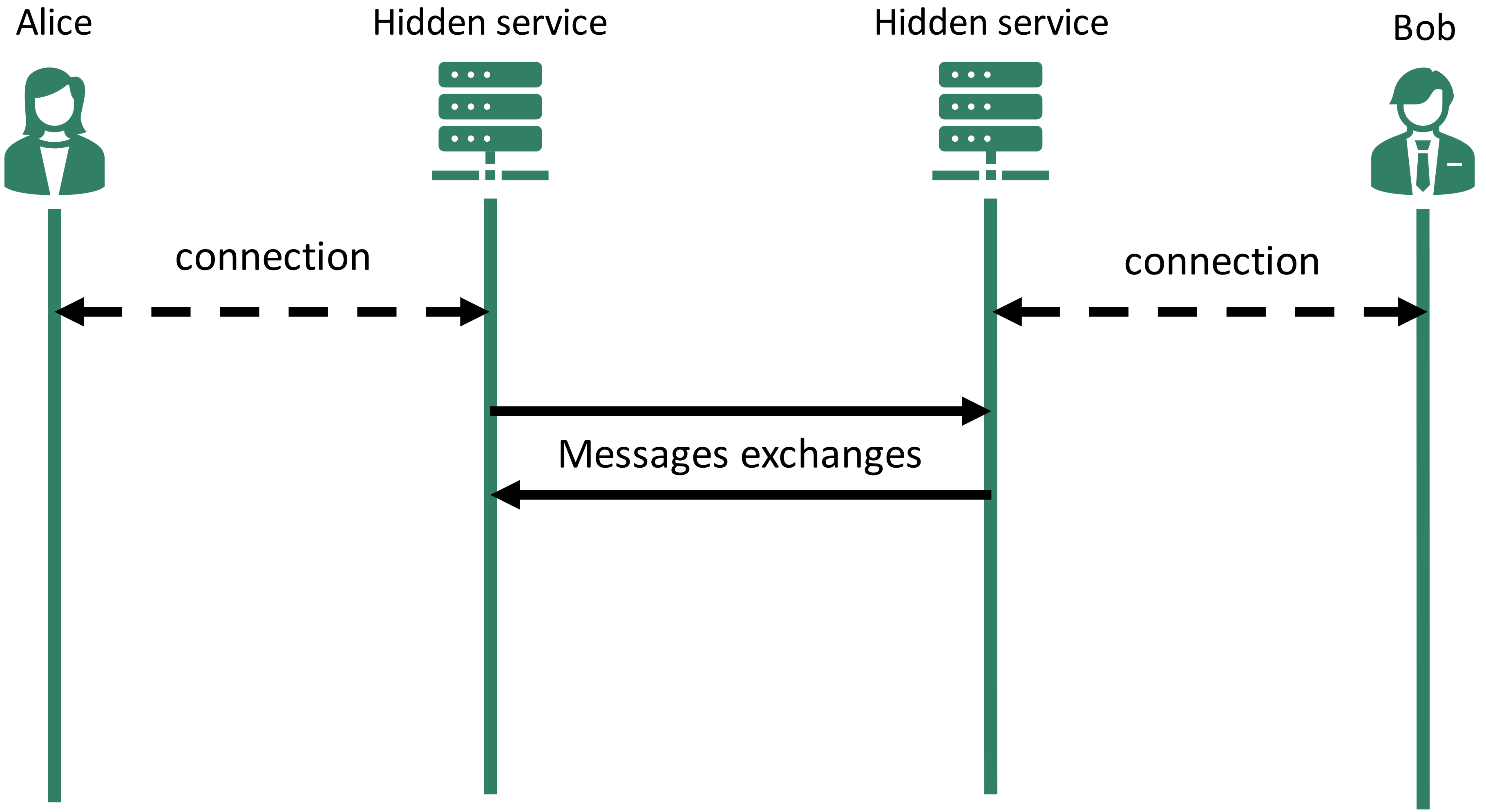
Extend circuit by one hop

Use create cell to add an OR

Our implementation



Our implementation



Security of the system: Defenses

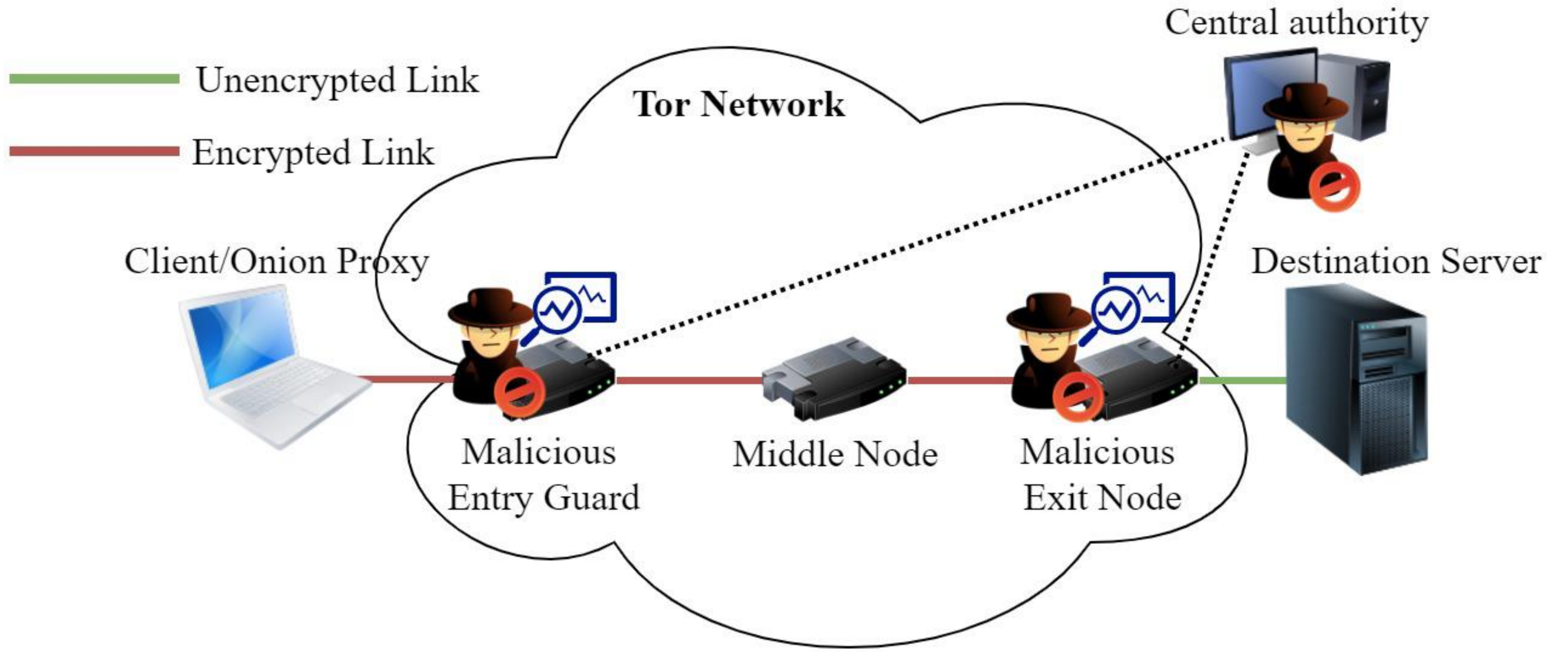
Perfect forward secrecy

Rendezvous points
and hidden service

End-to-end
integrity checking

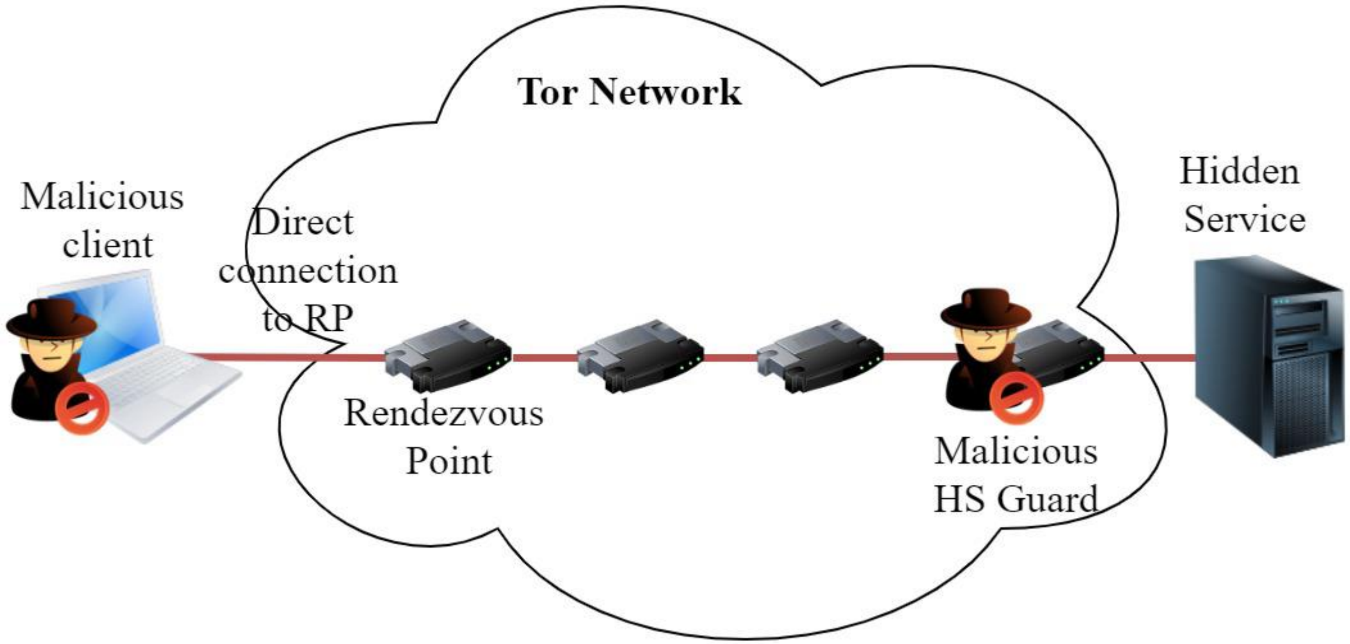
Security of the system: Attacks

Entry and exit routers



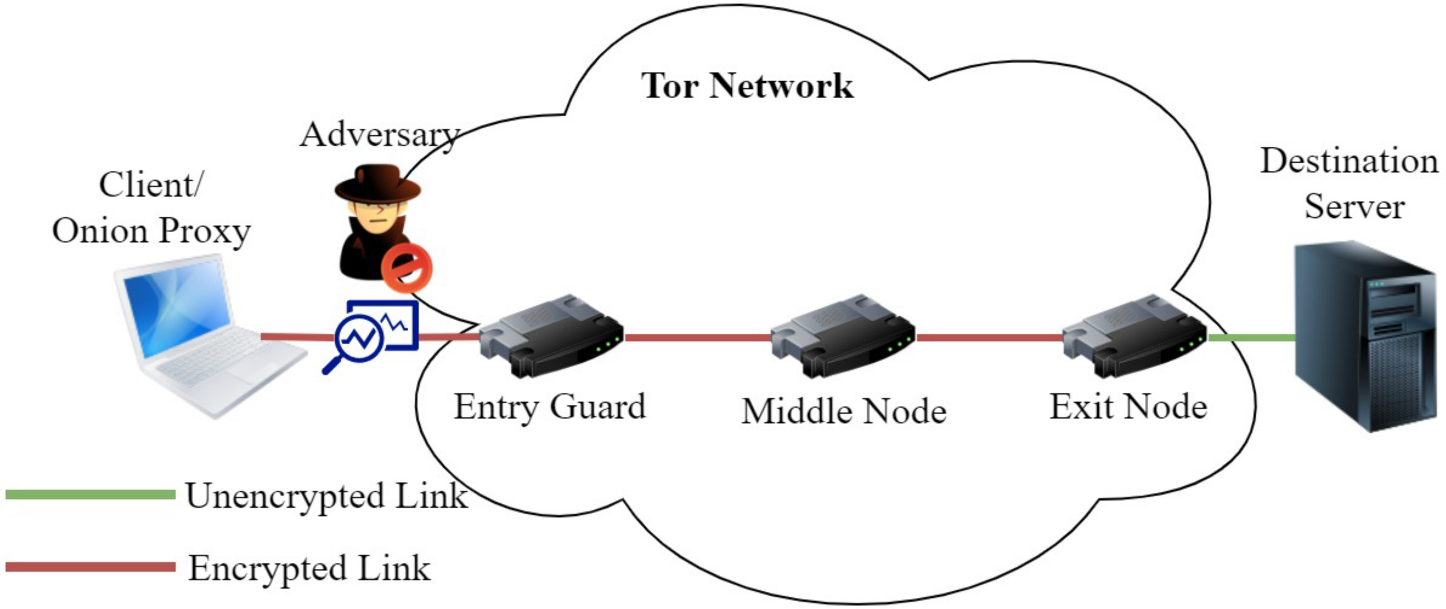
Security of the system: Attacks

OP/Server



Security of the system: Attacks

Side channels



Future works

Missing features of Tor

Asynchronous messaging

Implement end-to-end encryptions

Analyse, large scale tests

Conclusion

✓

Ensure anonymity

Synchronous/asynchronous messaging

Easy to run

✗

Hard to prevent abuses

Some security issues

A large-scale usage seems difficult

Design and security of an instant messaging service using Tor

Marvin FOURASTIE

Cours “Sécurité avancée”

Spring 2021