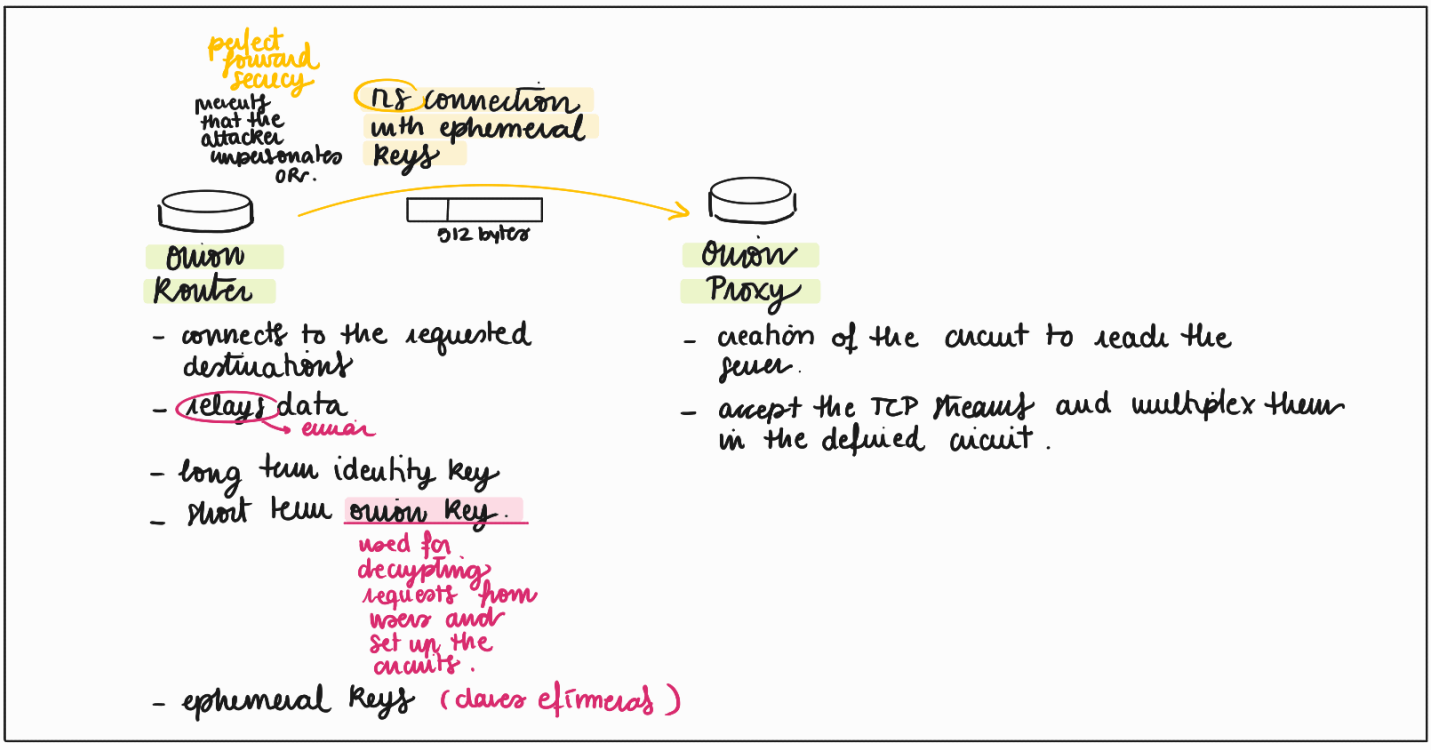
TOR implementation documentation → overlay network

→ Each OR maintains TLS with another OR.

OR = onion router

→ **Onion Proxy** : creation of the circuit across the network
(local software)



Onion Router
- connects to the requested destinations
- relays data (email)
- long term identity key
- short term onion key.
  used for decrypting requests from users and set up the circuits.
- ephemeral keys (does efimeral)

Onion Proxy
- creation of the circuit to reach the server.
- accept the TCP streams and multiplex them in the defined circuit.

Packets / Cells

2	1	509
CircID	CMD	Data

each circuitID has a different value depending on the connection it traverses.

CircID : circuit identifier

CMD : what to do with the payload.

0/1/2/3 (2nd byte) **Control cells** : they are always interpreted by the node that receives

0	• padding : Keepalive
1 | 2	• create / created : create new circuit
3	• destroy : Tear down the circuit.

4 **Relay cells** : carry end-to-end stream data

ethhak

2	1	2	6	2	1	498
CircID	Relay	StreamID	Checksum	Relay Length	CMD	Data

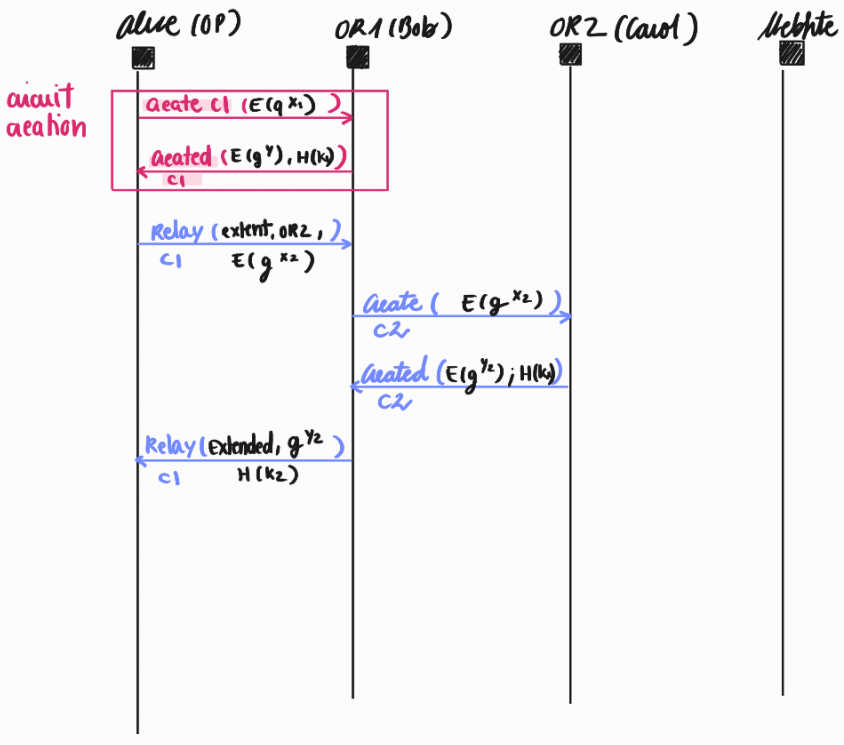
relay header

StreamID : many streams can be multiplexed over a circuit

4	• relay data : data flowing down
5	• relay begin : open a stream
6	• relay end : close a stream
7	• relay teardown : close a broken stream
8	• relay truncate : tear down only a part of the circuit
9	• relay sendme : congestion control.
10	• relay drop : long-range dummies

circuits & streams

1 circuit / TCP stream — Onion Routing



① Circuit creation RSA

- C_{AB} : circID — chosen by Alice
- g^x : payload A
  - diffie-hellman handshake
- g^y ; $k = g^{xy}$: payload B

② Send Relay Extent to make the circuit reach further.

- CBC : circID — chosen by Bob, we need to tell Alice

g = prime number = 29

p = prime number = 4751

a = random

$A = g^a \bmod (p)$

\n = tab (1 byte)

512 bytes for one packet

Cybersecurity Overview Project Meeting

Stack overflow

→ Real application
→ Several mechanisms
→ Explore buffer over

How to generate to rob attack

not implement defense technique

Sum of defense techniques

extend the lab with more countermeasures
read documentary
brute force

Research paper
implement one technique, not create it by 0

Javascript isolation

↳ deserialized code

Onion encryption

→ some VPN, how this

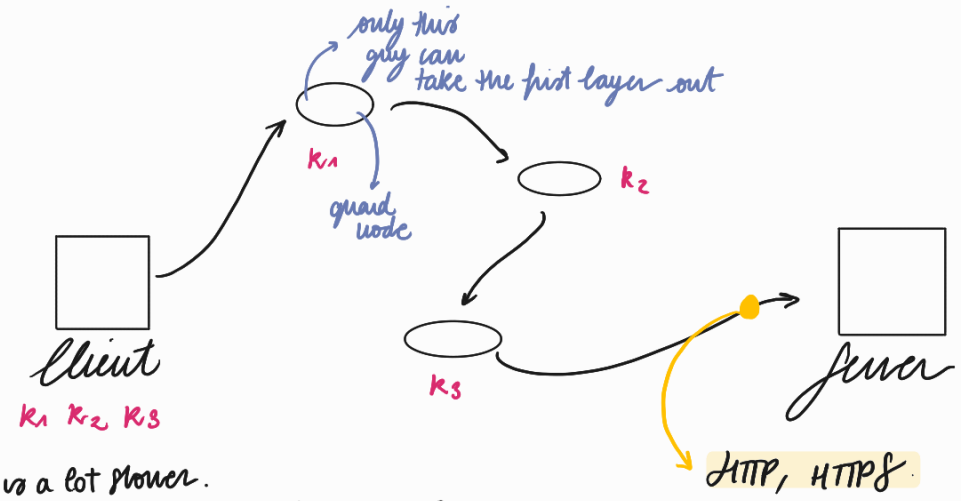
DDoS

→ Show there is a substantial work.

→ not large amount of resource

Supervision meeting

↳ choose a topic and some papers on it



- it is a lot slower.
- an onion router shall have ↑↑ BW.