THE DEEP WEB

Presented by: Ángel Heredia Pérez

@Anthares101

CROSSVALE

INTEGRATE · AUTOMATE · DELIVER

THE DEEP WEB

ÁNGEL HEREDIA PÉREZ @ANTHARES101

THE DEEP WEB

ÁNGEL HEREDIA PÉREZ @ANTHARES101

THE DEEP WEB

ÁNGEL HEREDIA PÉREZ @ANTHARES101

THE DEEP WEB

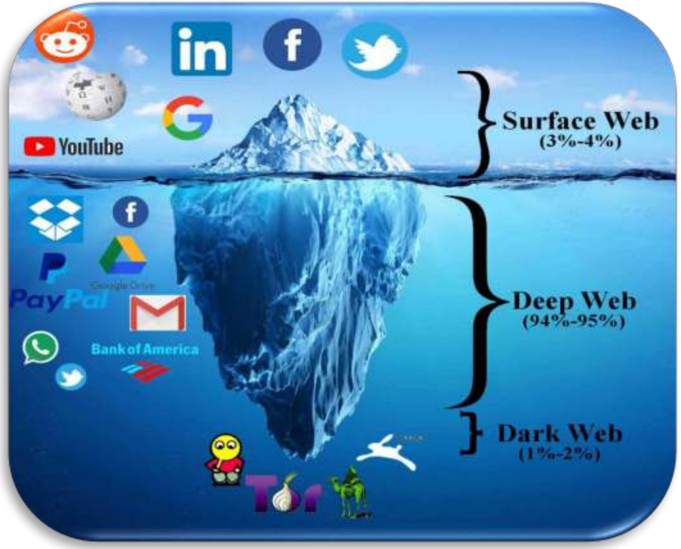


Image extracted from this Wapology article

THE DEEP WEB

Dark

TOR

TOR:

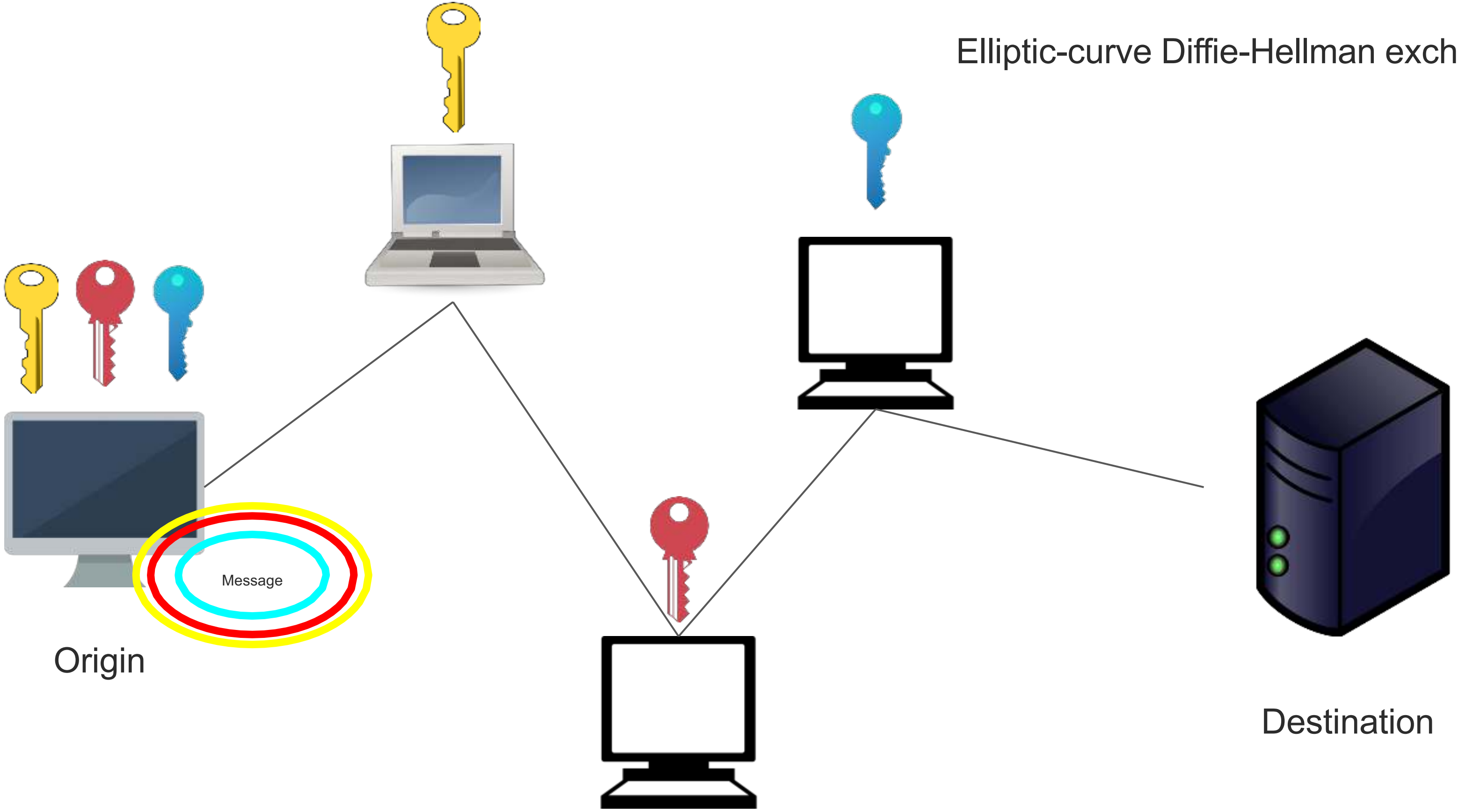
AN ONION ROUTING IMPLEMENTATION

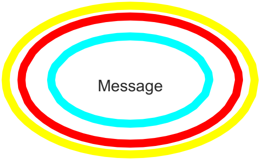
TorProject.org

ÁNGEL HEREDIA PÉREZ @ANTHARES101

WHAT IS ONION ROUTING?

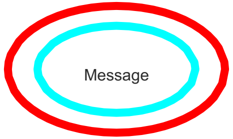
Elliptic-curve Diffie-Hellman exchange





Origin

Destination

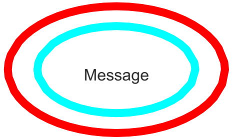


Message

Origin

Destination

Origin



Destination

Origin

Message

Destination

Message

Origin

Destination

Message

Origin

Destination

Message

Origin

Destination

Message

⚠

No encryption

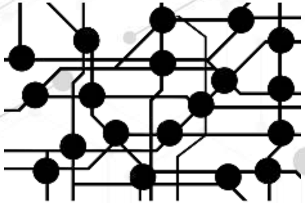
Origin

Destination

Tor®
TorProject.org

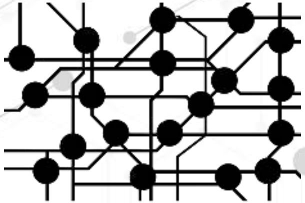
TOR CIRCUITS

Are formed by Tor using 3 relays (or nodes). The client will connect to the destination using this circuit through a local proxy



TOR CIRCUITS

A Tor circuit is considered “dirty” once used and after 10 minutes of this usage, if no traffic is using it, the circuit is refreshed



TOR CELLS

Tor send information in packets of 512 bytes each. This packets are called cells

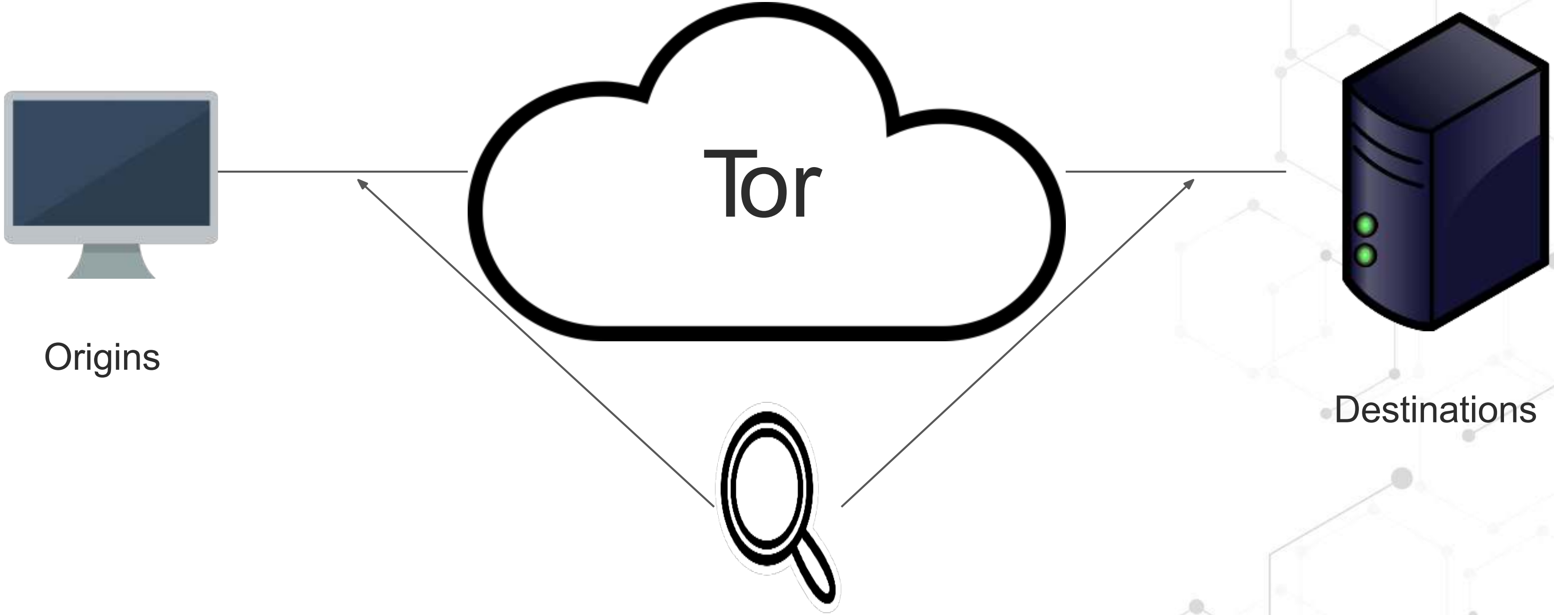
TOR NODES TYPES

- Guard and middle relay 🌐⚠
- Exit relay 🌐⚠🔨
- Bridge ~~🌐~~

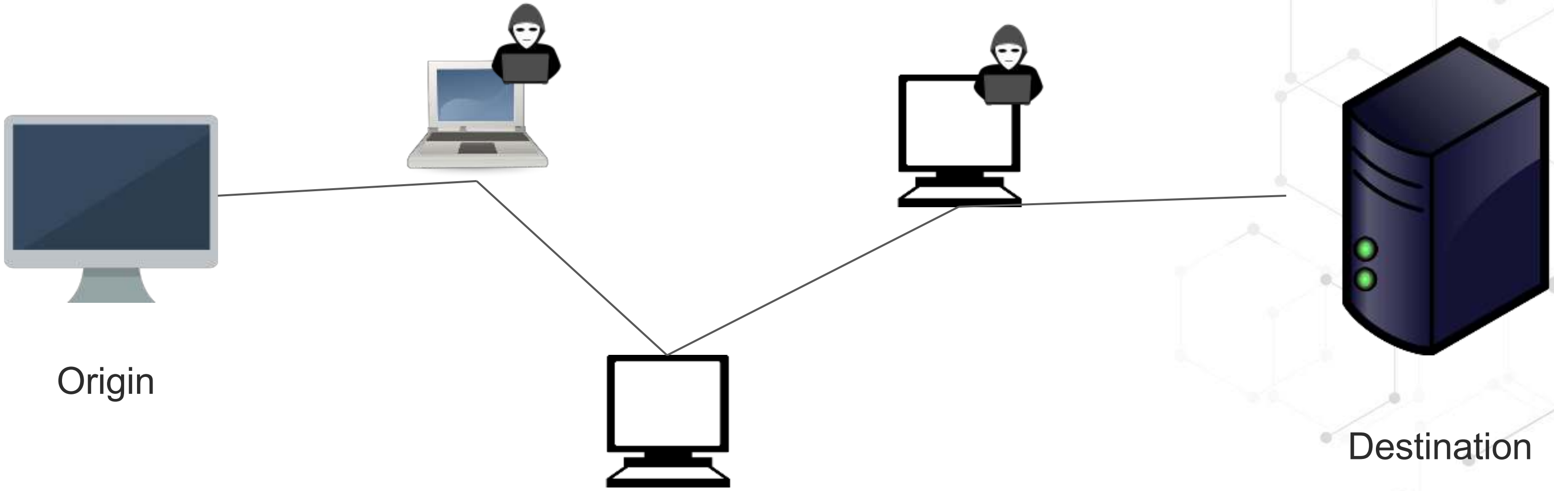
TOR VULNERABILITIES

ÁNGEL HEREDIA PÉREZ @ANTHARES101

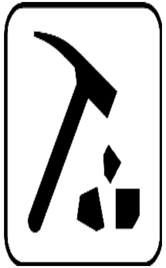
TRAFFIC ANALYSIS



NEFARIOUS RELAYS



0 DAY VULNERABILITY

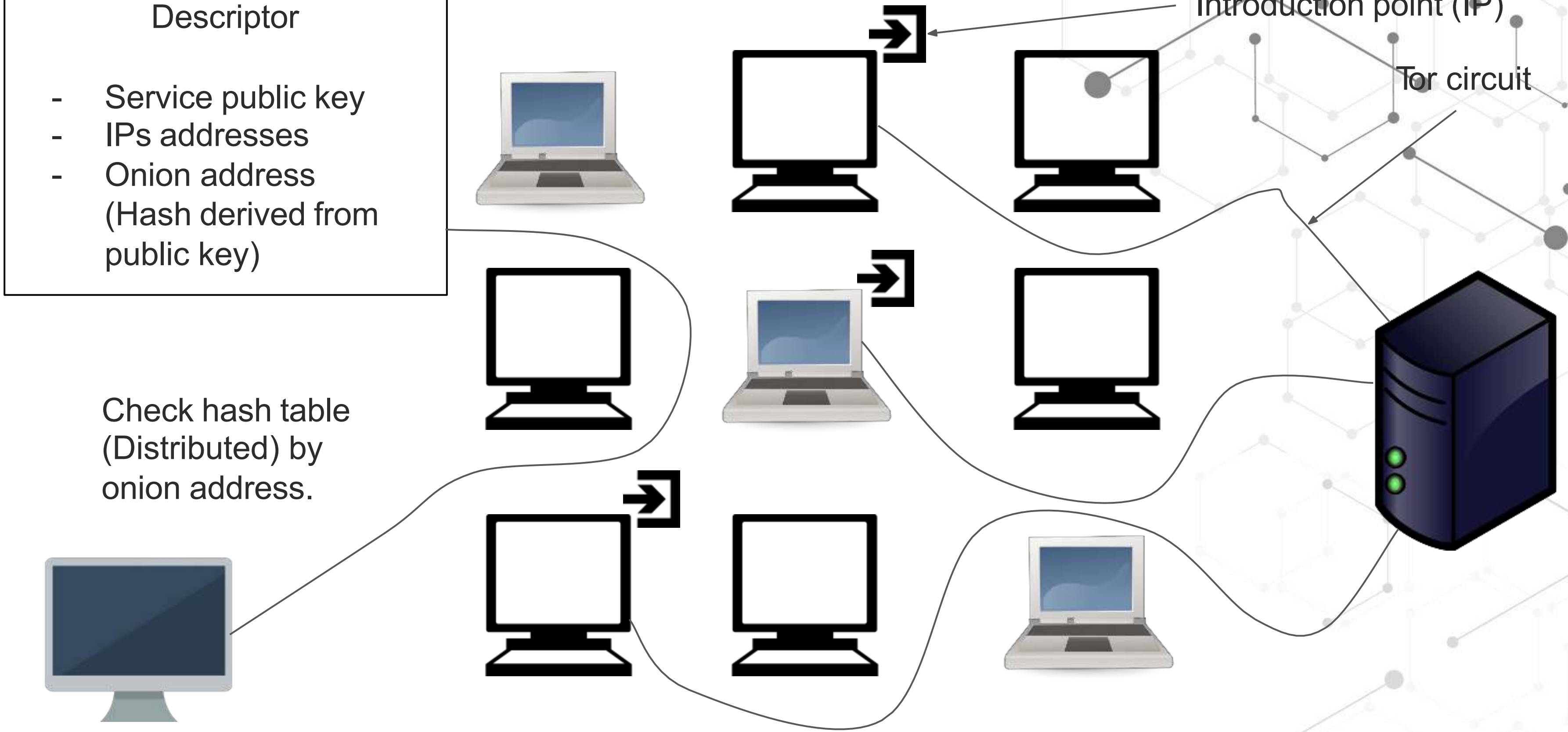


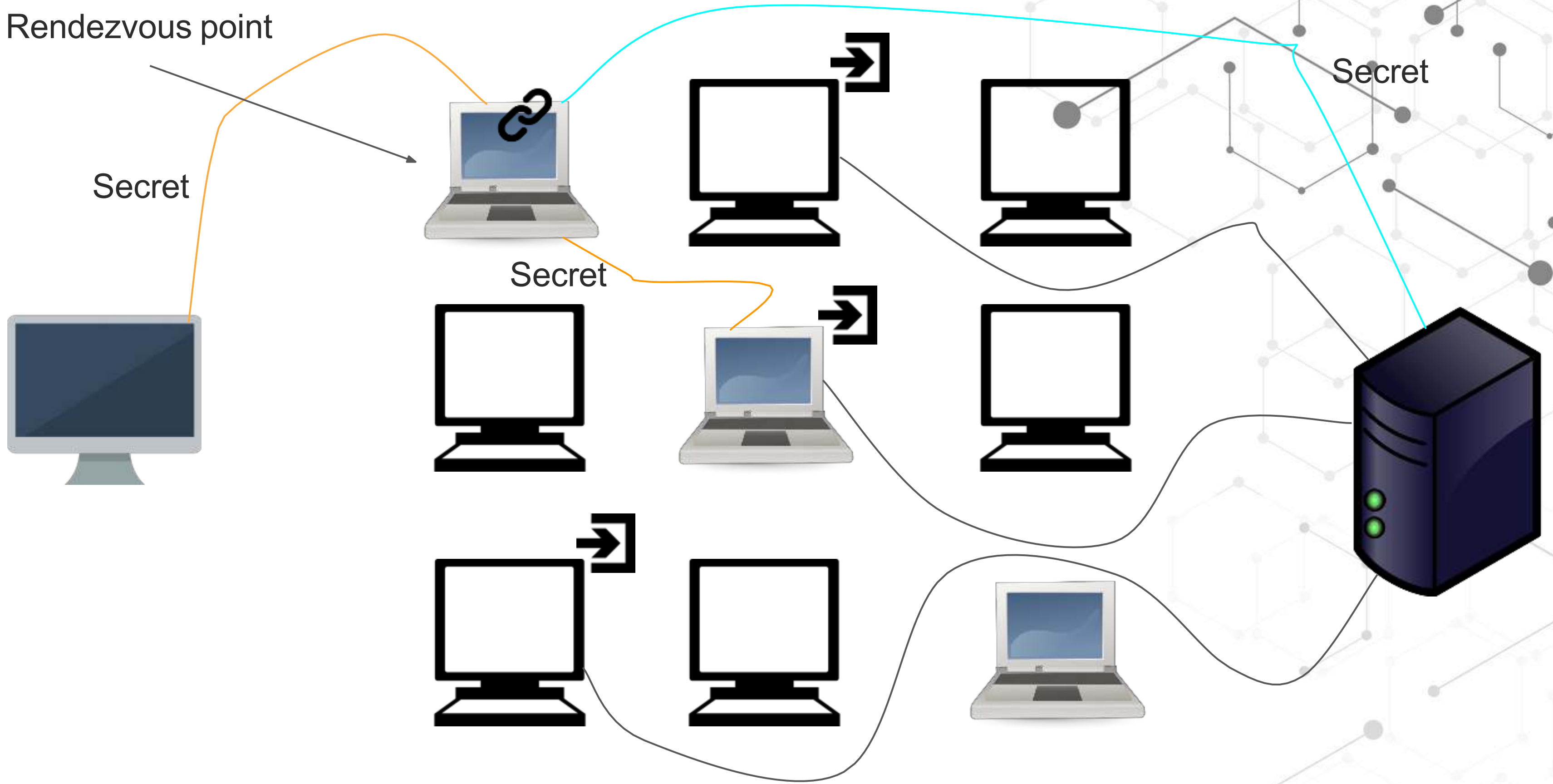
TOR SECRET SERVICES

Server Hidden Service Descriptor

- Service public key
- IPs addresses
- Onion address (Hash derived from public key)

Check hash table (Distributed) by onion address.




Rendezvous point
Secret
Secret
Secret

SINGLE ONION

If the server doesn’t need anonymity we can skip the tor circuit between the server and the rendezvous point

DOCUMENTATION

How long Tor circuits stay alive

How TOR Works- Computerphile

EXTRA BITS: Onion Routing - Computerphile

TOR Hidden Services - Computerphile

Tor documentation

THANK YOU! 😄

ÁNGEL HEREDIA PÉREZ @ANTHARES101

CROSSVALE™
INTEGRATE·AUTOMATE·DELIVER