

Deep Web

Mikel Egaña Aranguren

mikel-egana-aranguren.github.io

mikel.egana@ehu.eus



Deep Web

<https://doi.org/10.5281/zenodo.4302267>

<https://github.com/mikel-egana-aranguren/EHU-SGSSI-01>



Zer da Deep Web?

Ohiko sare ezaguna (Clearnet):

- Helbide ezagunek osatzen dute (adibidez: www.ehu.eus)
- HTML edukiak indexatuta daude eta bilaketak egiteko aukera ematen dute, interesatzen zaiguna aurkitzeko

Zer da Deep Web?

Internet bidez zuzenean eskuratu ezin diren eduki guztiekin osatzen dute Deep Web (Internet sakona)

Uste da existitzen den eduki guztitik:

- %10 Clearnet-en dago (ezagutzen dugun internet)
- 90% Deep Web-en

Zer da Deep Web?

Deep Web-ko edukia:

- Informazio konfidentziala edo babestua (bilatzaileek ez dute indexatzen, eta ezin da zuzenean eskuratu):
 - Osasun-erregistroak
 - Erregistro akademikoak
 - Bankuko datuak
 - ...

Zer da Deep Web?

Deep Web-ko edukia:

- Informazio "soltea": estekatuta ez dagoen HTML artxiboa, adibidez
- HTML ez diren formatuetan nabigatzaile batek irakurri ezin duen informazioa
- Eduki argitaraezina (Zentsura): libreki argitaratu ezin diren edukiak, ekar ditzakeen ondorioengatik

Zer da Deep Web?

Deep Web-ko edukia:

- Legez kanpoko edukia eta/edo eduki desatsegina (Darknet)
 - Arma, droga eta pertsonen trafikoa
 - Material pedofiloa
 - Malwarea
 - Hacker, mertzenario eta abarren alokairua
 - Snuff pelikulak

Zer da Deep Web?

Web mailak

- 1 maila: Webgune oso ezagunak eta publiko guztientzakoak
- 2 maila: Webgune ezezagunak eta gune pornografikoak
- 3 maila (Hemen Deep Web hasten da): Pribatutasuna eta anonimotasuna behar ditu (eduki sentsibleak)
- 4 maila: Proxy bat behar du. Maila arriskutsua (legez kanpoko edukiak)
- 5 maila: Gobernuaren eta militarren sekretuak
- ???

Sarbideak

Deep Web-era sartzeko, software berezi bat behar da, pribatutasuna, anonimotasuna eta proxy lana egingo dituena

Deep Webeko hainbat edukitarako sarbidea emango duten aukera desberdinak daude: TOR, I2P, Freenet, Zeronet

TOR

The Onion Router (TOR)

Nabigazio-sare anonimoa

Saretik doazen paketeen jatorria eta helmuga ezkutatzen ditu

TOR

The Onion Router (TOR)

The FBI couldn't get my husband to decrypt his Tor nodes, so they told a judge he used his GRAPHICS DRIVER to access the "dark web" and jailed him PRE TRIAL for 3 years

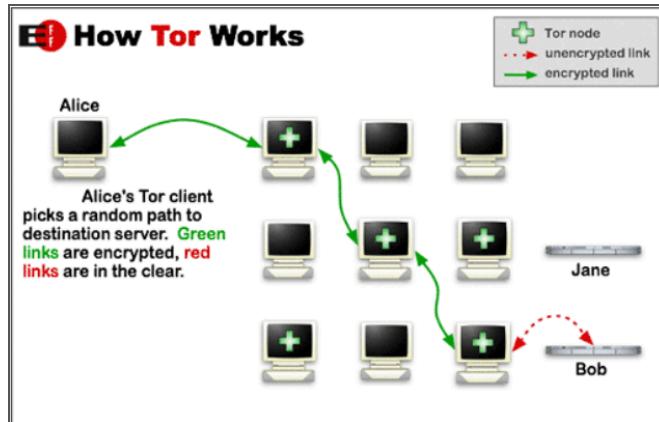
TOR

TOR sisteman sartzeko software espezifiko bat behar da:

- TOR Browser: web nabigatzailea
- Tails (The Amnesic Incognito Live System): USB baten exekutatzen den sistema eragilea

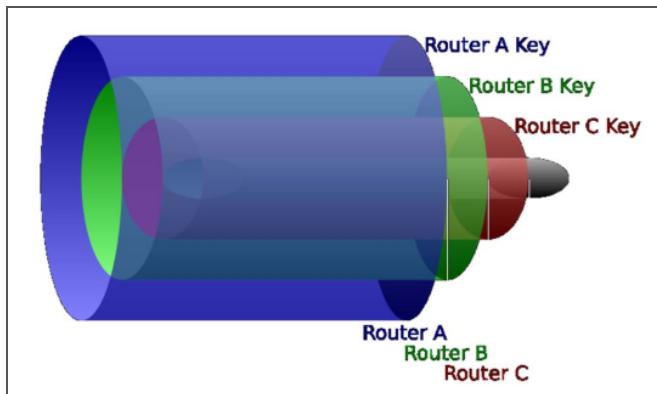
TOR

Konexio bat egin behar den bakoitzean, bide aleatorio bat kalkulatzen da nodoen artean



TOR

Informazioa geruzatan zifratzen da (tipula bat bezala) nodoen gako publikoekin; horrela, nodo bakoitzak hurrengo nodoa soilik zein den daki, ez bide osoa



TOR

TOR sarea erabiliz, beste era batera eskuraezinak izango ziren URL-tara jo daiteke:

- .onion domeinua
- URL alfanumerikoak: <http://3g2upl4pq6kufc4m.onion/>

TOR

Edukiak aurkitzeko, bilatzaile espezifikoak edo URLak biltzeko guneak erabili behar dira:

- Torch bilatzailea (<http://xmh57jrznw6insl.onion/>)
- The Hidden Wiki (<http://kpvz7ki2v5agwt35.onion>)