Data and Network Security

(Master Degree in Computer Science and Cybersecurity)

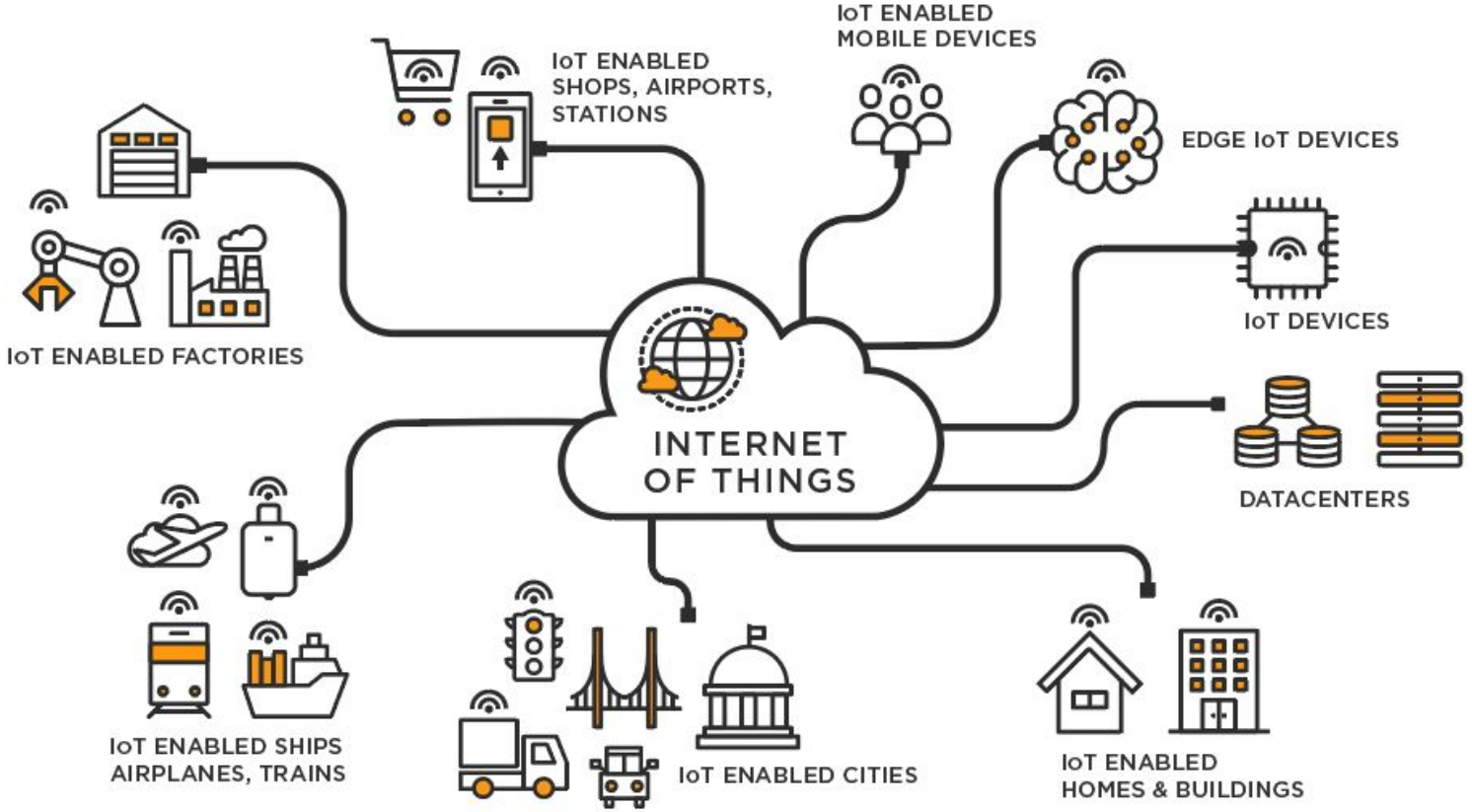
Lecture 8

SAPIENZA
UNIVERSITÀ DI ROMA

Outline for today

- Recap last lecture
- Exploring the dark web
- Geolocation-Based Profiling in the DarkWeb

Internet of Things (IoT)



Internet of Things (IoT) - Definition

Network of physical objects or "things" embedded with sensors, software, and other technologies that enable them to **connect and exchange data** with other devices and systems over the internet.

Creation of a seamless network where devices can communicate and interact with each other autonomously, leading to increased:

- efficiency,
- automation,
- improved decision-making.

IoT devices - a summary from security perspective

Attractive target
- Contain sensitive and private information

Easy to exploit
- Do not support complex security techniques

Amplify the attack impact
- Control physical environment
- Access personal information
- Spread to other interconnected devices

Remote attestation

Remote attestation:

- Security mechanism used to verify the integrity and trustworthiness of a device's software and hardware configuration remotely.

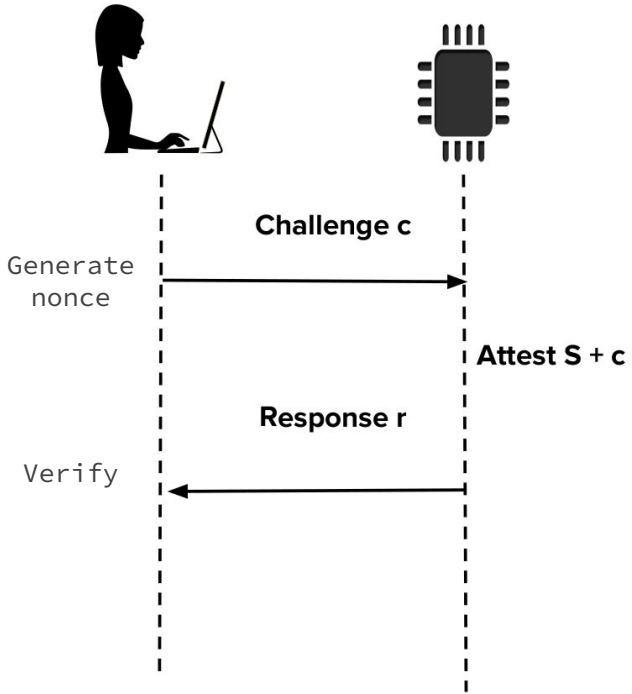
- This process allows a trusted entity, such as a server or a cloud-based service, to **assess whether an IoT device is running the expected software and hasn't been tampered with or compromised.**

Remote attestation - Overview

Challenge (Executed by Verifier)
- Outputs a random Challenge (nonce, timestamp, memory addresses, attestation routine)

Attest (Executed by Prover)
- Computes a small attestation response based on internal state S and challenge c

Verify (Executed by Verifier)
- Compared the response received from Prover with the expected state



Requirements of Remote attestation

Challenge (Executed by Verifier)
- Authentic, fresh, unpredictable

Attest (Executed by Prover)
- Authentic, Atomic, Unforgeable, Dynamic, Deterministic

Verify (Executed by Verifier)
- deterministic

Approaches of Remote attestation

Memory
- Static vs. Dynamic

Number of device
- Single vs. swarms

Design
- Software based, Hybrid, or Hardware

Remote attestation challenges - summary

- There is no single remote attestation protocol that checks all types of the memories in a IoT devices e.g., data variables, CPU registers
- Attestation is an overhead operation
- During the attestation, device stop the usual work
- The results of the attestation are not comprehensive
  - Attestation results are boolean claims (T or F). Do not give insights about the history of the device.
- Design of robust framework for mobile devices which allow them to join or leave the network while preserving the network integrity

Remote attestation - open issues

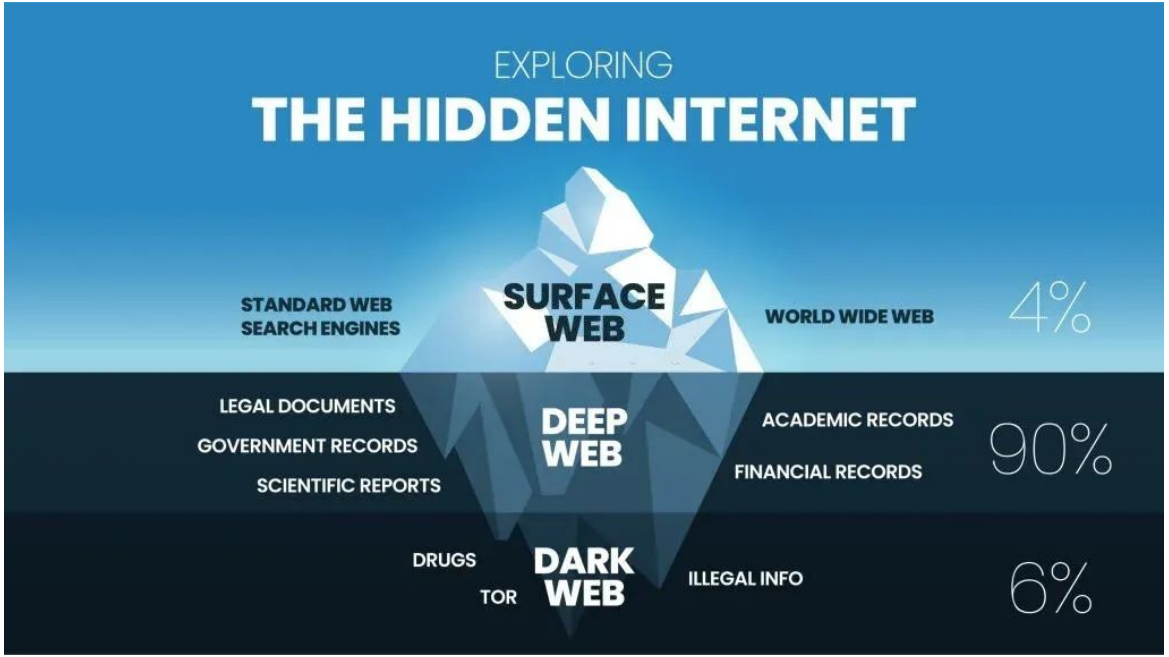
- Uninterrupted remote attestation e.g., medical device
- Efficient remote attestation for dynamic memory
- Attestation of distributed services
- Attestation of all types of memories
- Attestation of IoT devices in dynamic networks

Outline for today

- Recap last lecture
- Exploring the Dark Web
- Geolocation-Based Profiling in the DarkWeb

Layers of the web

- The surface web
- The deep web
- The dark web



Surface web

- Part of the internet that most of use use every day. (socials etc)
- Accessible through regular browsers (firefox, chrome, safari)
- Anytime/anywhere as long as you have internet access

Deep web

- Refers to part of the internet that is behind “closed doors”
- Accessible only from a group of people within an organization.

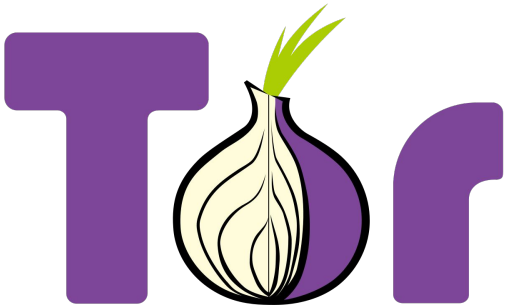
Deep web

- Refers to part of the internet that is behind “closed doors”
- Accessible only from a group of people within an organization.

- Credentials and permissions needed to access.
- Information can not be found by search engines

Dark web

- Accessible through the use of special browsers (e.g. Tor)
- Unregulated part of the internet
- No organization, business or government is in charge of the dark web or is able to enforce rules/policies



Origins of the dark web

- Known to have begun around 2000s

- Thesis project: Distributed decentralization information storage and retrieval system

- Aimed at the creation of a new way to anonymously communicate and share information

Dark side of the Web

Unlike the Surface Web, which consists of websites and pages that are indexed and easily accessible through search engines like Google, the Dark Web operates on overlay networks such as Tor (The Onion Router) or I2P (Invisible Internet Project). These networks use layered encryption to anonymize users and conceal their online activities.

Dark side of the Web

The Dark Web hosts a wide range of content, including anonymous communication platforms, underground marketplaces, forums, and websites offering illegal goods and services such as drugs, weapons, counterfeit documents, and hacking tools.

Dark side of the Web - harmful content

- Stolen information
- Drugs
- Stolen goods
- Disturbing content
- Terrorist content
- Hacking services
- Crypto based lottery tickets
- ….

Dark side of the Web

Note that not all content on the Dark Web is illicit; there are also legitimate uses such as:

- secure communication,
- whistleblowing,
- accessing censored information.

What is out there in the dark web?

- Black markets

The dark web is home to many black marketplaces where all sorts of goods can be sold/bought such as cheap netflix accounts, credit card numbers, weapons, drugs etc

What is out there in the dark web?

- Black markets

The dark web is home to many black marketplaces where all sorts of goods can be sold/bought such as cheap netflix accounts, credit card numbers, weapons, drugs etc

- Email services

Send emails to specific individuals that have to use same kinds of tools to send/receive also (e.g Tor)

What is out there in the dark web?

- File uploads/transfers

Secure file uploads and transfers are common on the dark web, as the network provides several layers of encryption on both files and connection.
These services are commonly used by journalists to share files that contain sensitive information

- Forums/Chat services

Message boards and chat room dedicated to topics that are not safe to discuss in other parts of the internet

What is out there in the dark web?

- Whistleblowing websites

Sensitive information is found/leaked on these sites.
Denouncing (anonymously) illegal activities of a company/nation etc.

- Link directories

Accessing a specific site you need to know the exact URL. In case of dark web these URLs are not easy to remember and usually are random strings.

A bit of notoriously “famous”

- The red room
- The silk road

A bit of notoriously “famous”

- The red room
  Livestream where criminals show kidnapped people and kill them on camera.
  Human parts are then cut for money.
  Transactions in crypto such as bitcoin
  Membership fees were also applied
  Luckily Cyber police continuously assist in taking down this kind of websites

A bit of notoriously “famous”

- The silk road
  - The first dark web market, known for selling drugs
  - Created by Ross Ulbricht
  - More than 1.2billion dollars in sales in cryptocurrency
  - Ross was arrested in 2013 in San Francisco
  - FBI tracked Ulbricht through some of his early requests to others in helping him to set up the site

Visiting the dark web

- Through the Tor network
- Then you need the appropriate links (known as .onion)
- onion.live

The Tor Project

- Aim at preserving online anonymity
  - Software
  - Network
  - protocol

- Open source
- Community of researchers, developers, users, and relay operators
- Funding from US DoD, Electronic Frontier Foundation, Voice of America, Google, NLnet, Human Rights Watch and more…

The Tor Project - History

- Mid 1990’s: The idea of “onion routing” was discovered by Paul Syverson
- Created by the U.S Naval Research Lab
- Developed in hopes of creating private internet connections
- Early 2000’s : Roger Dingledine (MIT Graduate) started the TOR project
- 2002: Officially released to the public
- 2008: Development of the TOR Browser began
- 2019: Tor Announced the release of the Tor Browser for Androids

Tor in a nutshell

- Tor uses onion routing system.
- Tor uses thousand of volunteer networks to direct traffic over internet so user identity can be kept hidden from network interceptor.
- Tor helps to reduce risk of traffic analysis by distributing transaction over several places so no single point can link to senders destination

Tor in a nutshell

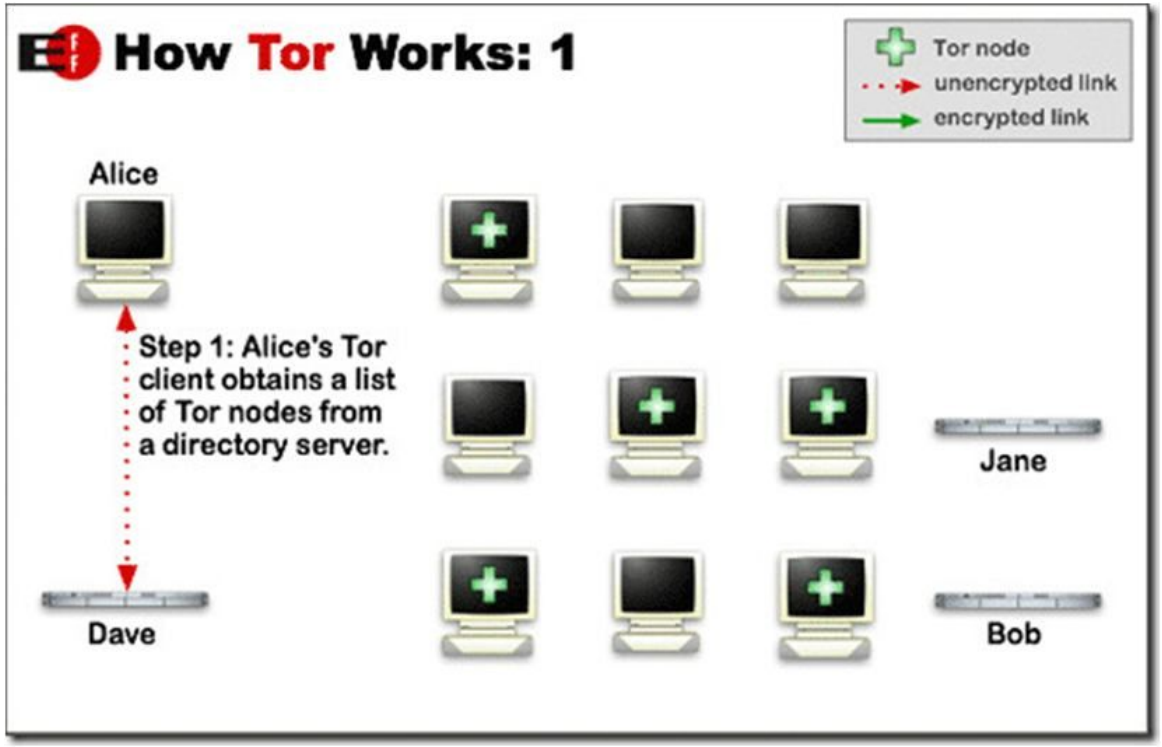
For example user A wants to send a packet safely to user B using Tor network.

Tor creates private network for this communication.

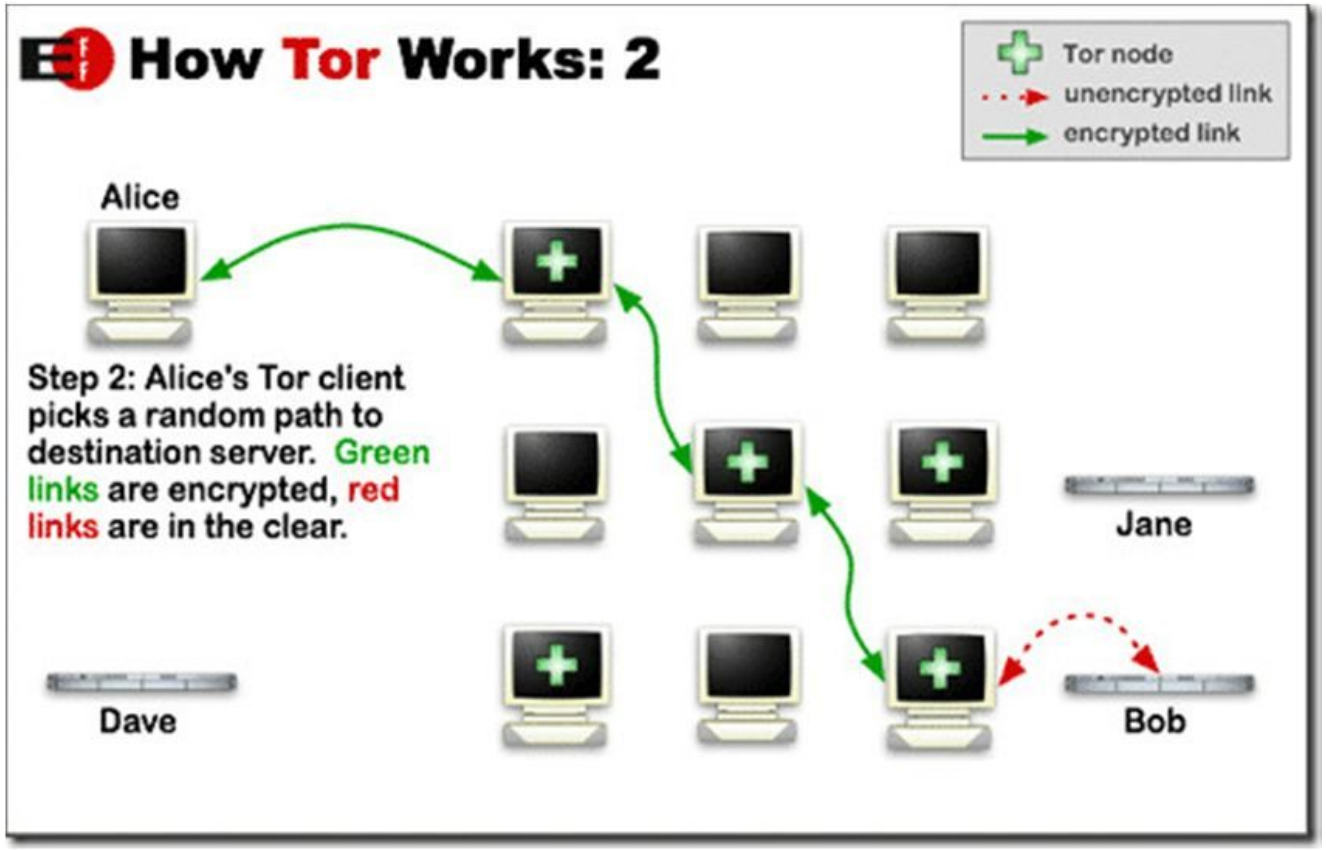
- First step is to identify available nodes. User A’s Tor client obtains list of Tor nodes from server. It picks random node for each time so pattern cannot be observed by interceptor.

- Client generates an encrypted message and which is sent to first node. The client on this node decrypts the first layer of encryption and identifies the next node. This will continue until the final node receives the location of the actual recipient, where it transmits an unencrypted message.

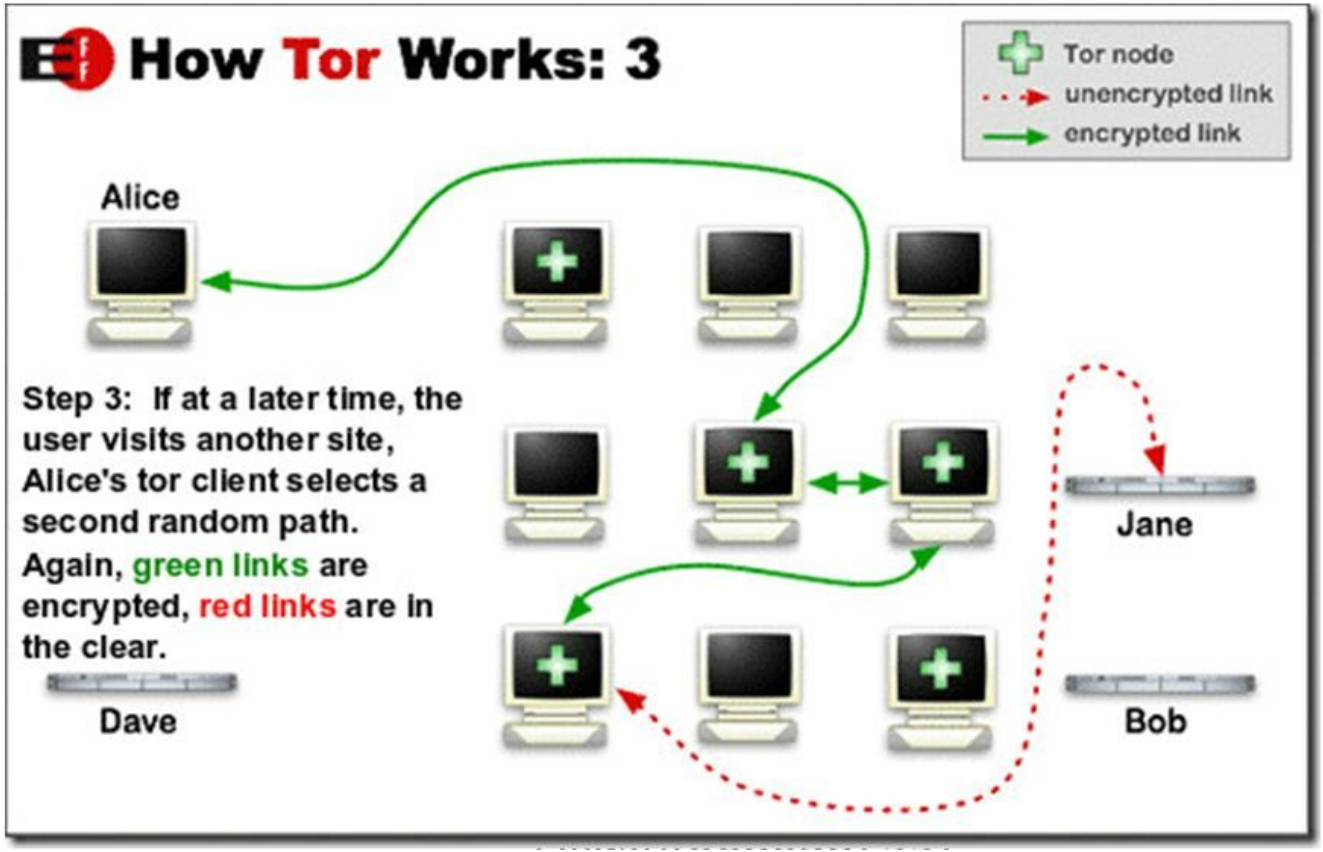
Tor in a nutshell



Tor in a nutshell



Tor in a nutshell

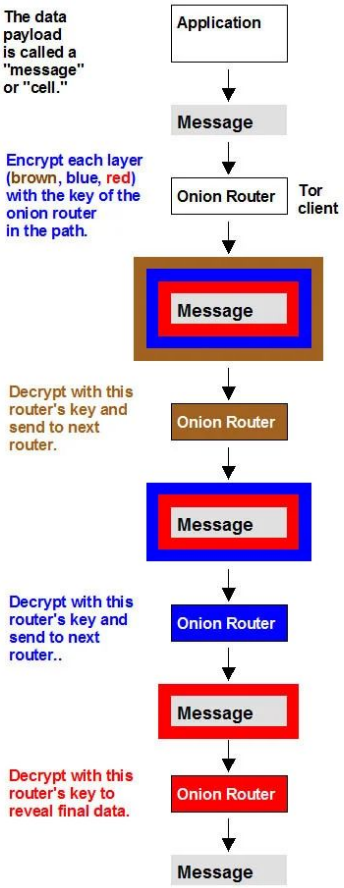


The onion routing

- Onion routing connection has three phases:
  - Connection set up,
  - data movement
  - Connection tear down.

The onion routing

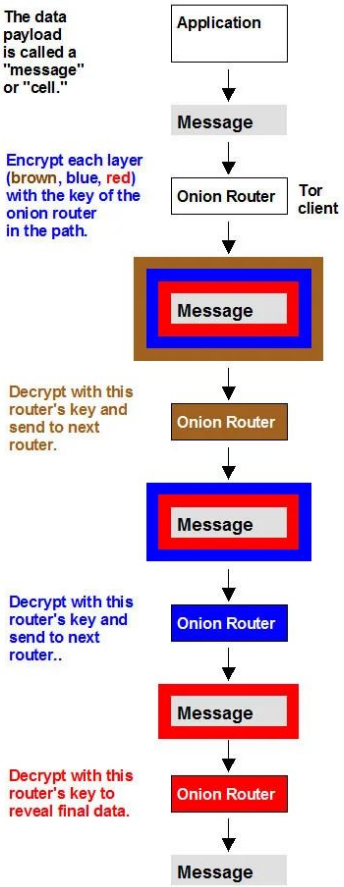
First phase starts when initiator creates an onion, it is layered data structure which specifies properties of connection at each point.



The onion routing

First phase starts when initiator creates an onion, it is layered data structure which specifies properties of connection at each point.

Initiator determines number of onion routers(nodes) to be used in the communication and creates Onion packet by having multiple encryption using public key of onion router(node)

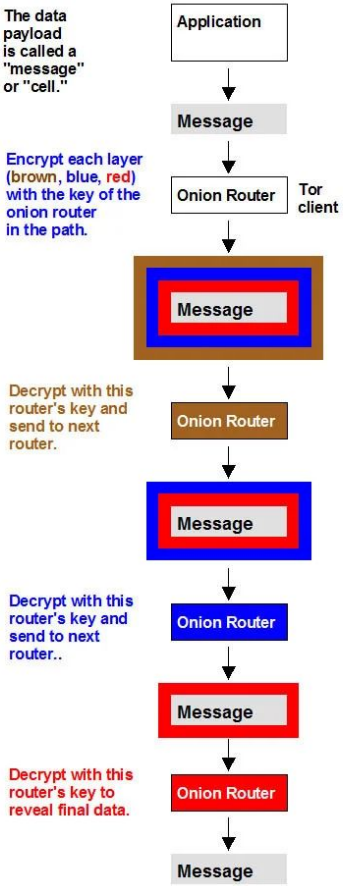


The onion routing

First phase starts when initiator creates an onion, it is layered data structure which specifies properties of connection at each point.

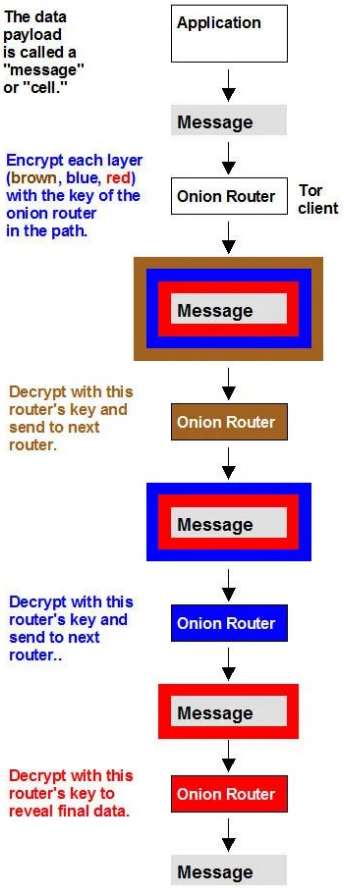
Initiator determines number of onion routers(nodes) to be used in the communication and creates Onion packet by having multiple encryption using public key of onion router(node)

Each node has information about only 2 nodes: sender and receiver. Each node peels the layer of onion, they use their public key to decrypt the data and can obtain information about where they should send the packet.



The onion routing

Receiver can use its public key and finally obtain plain text. Once connection is established bi-directional communication is possible. When data is sent back from the receiver to sender layering occurs in reverse direction.



Outline for today

- Recap last lecture
- Exploring the dark web
- Geolocation-Based Profiling in the DarkWeb

Geolocation-Based Profiling in the DarkWeb

End goal: To geolocate anonymous crowds of the DarkWeb forums

Geolocation-Based Profiling in the DarkWeb

End goal: To geolocate anonymous crowds of the DarkWeb forums

We will see:

- how to decompose the global profile of posting of the Dark Web forum into components that uncover the geographical origin of the crowd.
- detecting the native language of anonymous Dark Web users, starting from their posts in English

Building Reliable User and Region Profiles from User Activity Traces

How can we build profiles of users from a given known population starting from their activity traces?

The traces can be of any kind: posts, comments to posts, messages exchanged, access times, or a mix of them.

Building Reliable User and Region Profiles from User Activity Traces

Determine whether a user is or is not typically active at a given hour of the day.

Profile P_u

- Represented by an array of 24 elements, one per hour.

- $P_u[h]$, $h \in \{0, \ldots, 23\}$, is the fraction of daily online posting activity done by user u during hour h.

Building Reliable User and Region Profiles from User Activity Traces

Profile P_u

- Represented by an array of 24 elements, one per hour.
- $P_u[h]$, $h \in \{0, \ldots, 23\}$, is the fraction of daily online posting activity done by user u during hour h.

- $a_u(d,h)$ indicates whether user u has posted in the h^{th} hour of day d

User profile

Profile P_u

- Represented by an array of 24 elements, one per hour.
- $P_u[h]$, $h \in \{0, \ldots, 23\}$, is the fraction of daily online posting activity done by user u during hour h.

- $a_u(d,h)$ indicates whether user u has posted in the h^{th} hour of day d.

User profile is defined as follows:

$$P_u = \{P_u[h] | h \in \{0, \ldots, 23\}, P_u[h] = \frac{\sum_d a_u(d,h)}{\sum_{d,h'} a_u(d,h')}\}$$

User profile

Profile P_u

- Represented by an array of 24 elements, one per hour.
- $P_u[h]$, $h \in \{0, \ldots, 23\}$, is the fraction of daily online posting activity done by user u during hour h.

- $a_u(d,h)$ indicates whether user u has posted in the h^{th} hour of day d.

Profile P_u is the distribution of user u activity throughout the day on the target forum.

$$P_u = \{P_u[h] | h \in \{0, \ldots, 23\}, P_u[h] = \frac{\sum_d a_u(d,h)}{\sum_{d,h'} a_u(d,h')}\}$$

Where do we start?

To build reliable region profiles we need to start off from datasets that are rich enough to reflect the behavioral patterns of the users and that include verified information on their location

Where do we start?

To build reliable region profiles we need to start off from datasets that are rich enough to reflect the behavioral patterns of the users and that include verified information on their location.

Twitter livestream data of 2016

- 2% of total tweets
- 6 million users whose home country is known from their profile

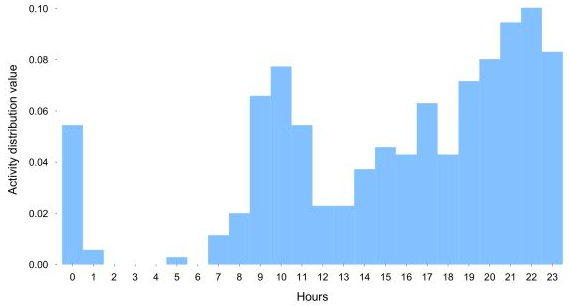
Base dataset

Using this dataset and the above methodology it was possible to build profiles for 14 countries or states:

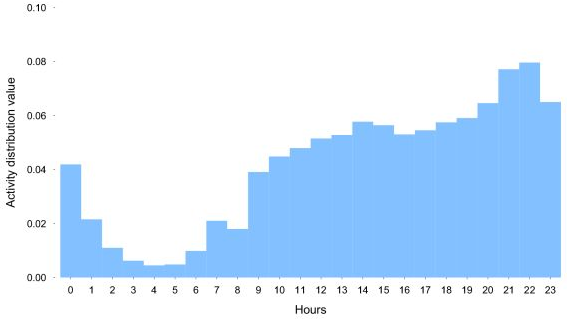
- Brazil,
- California,
- Finland,
- France,
- Germany,
- Illinois,
- Italy,
- Japan,
- Malaysia,
- New South Wales (Australia),
- New York
- Poland
- Turkey
- UK

Country/State	Users (#)	Country/State	Users (#)
Brazil	3,763	Japan	3,745
California	2,868	Malaysia	1,714
Finland	73	New South Wales	151
France	2,222	New York	1417
Germany	470	Poland	375
Illinois	794	Turkey	1,019
Italy	734	United Kingdom	3,231

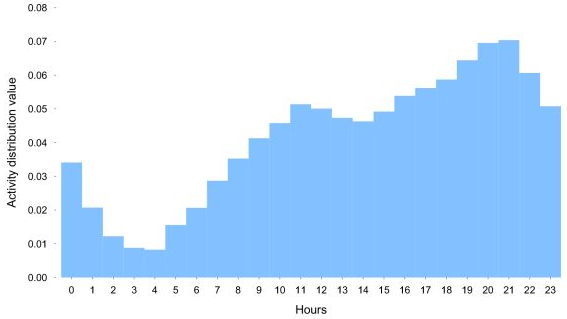
A users profile



(a) Profile of a German user.

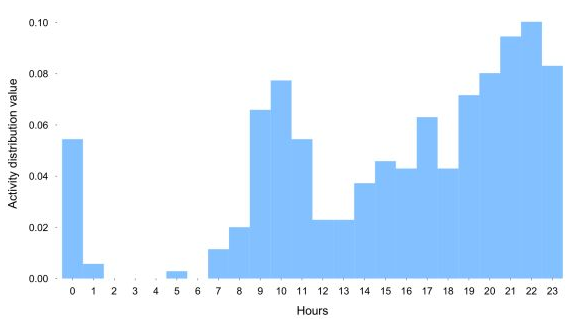


(b) Twitter dataset of the German population (local time UTC + 1).

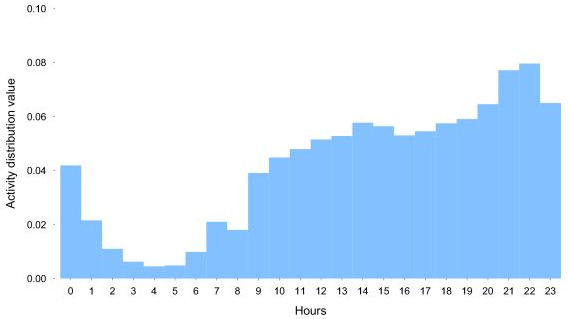


(c) Entire Twitter dataset (UTC).

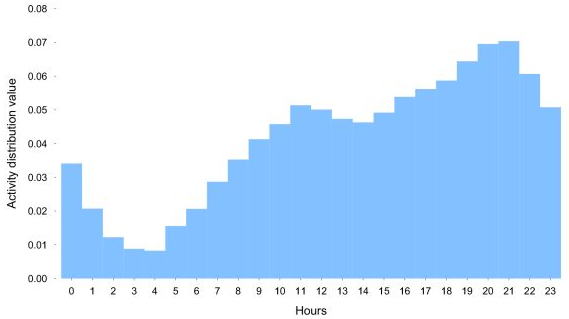
A users profile



(a) Profile of a German user.



(b) Twitter dataset of the German population (local time UTC + 1).

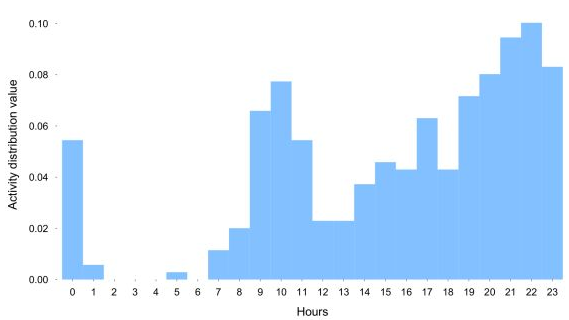


(c) Entire Twitter dataset (UTC).

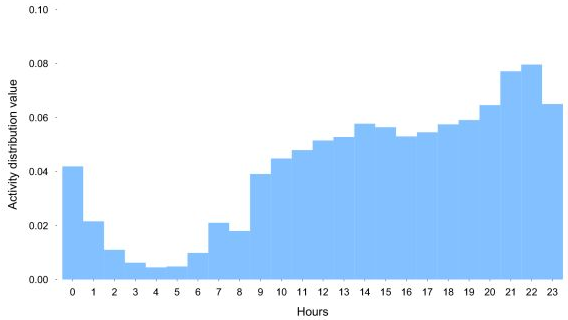
In both profiles we can easily distinguish the night as the hours of lower activity (the interval between 1:00 (1am) and 7:00 (7am)).

The activity of the German user has a first peak in the morning, drops during lunch time, and starts to grow again from the early afternoon to the evening, following a typical daily rhythm.

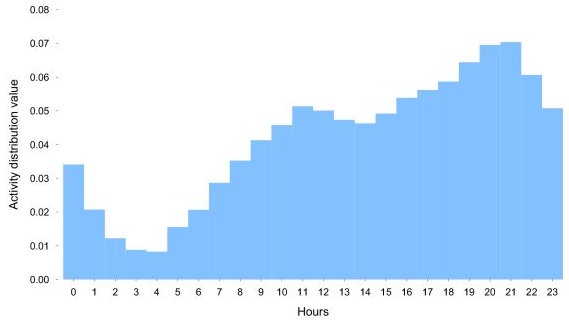
Correlation between countries/states



(a) Profile of a German user.



(b) Twitter dataset of the German population (local time UTC + 1).

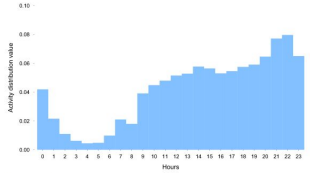


(c) Entire Twitter dataset (UTC).

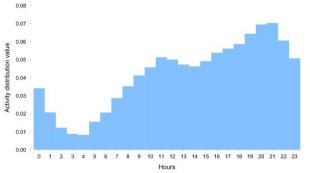
Profile of large crowds coming from different timezones are brought to the local Timezone (UTC), their profiles are almost identical.

- **use the general profile as the common baseline, properly shifted to the right timezone.**

Placing anonymous users to time zones



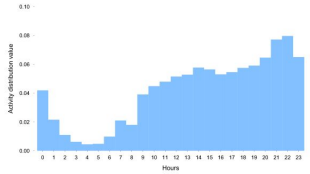
(b) Twitter dataset of the German population (local time UTC + 1).



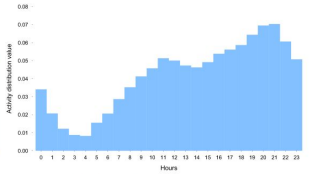
(c) Entire Twitter dataset (UTC).

Rationale: Users of the same region typically have a profile that is very close to that of the corresponding time zone crowd, and further away from crowds of different timezones.

Placing anonymous users to time zones



(b) Twitter dataset of the German population (local time UTC + 1).

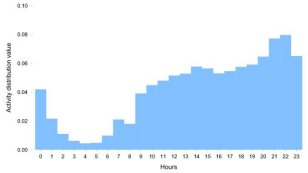


(c) Entire Twitter dataset (UTC).

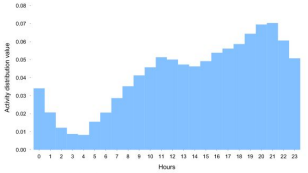
Rationale: Users of the same region typically have a profile that is very close to that of the corresponding time zone crowd, and further away from crowds of different timezones.

- For every member of an anonymous crowd, we compare his profile with that of all different timezone profiles
- geolocate that member to the timezone whose activity profile is **less distant**

Placing anonymous users to time zones



(b) Twitter dataset of the German population (local time UTC + 1).



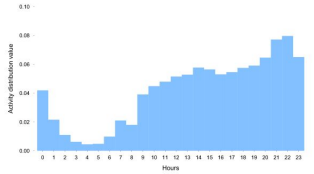
(c) Entire Twitter dataset (UTC).

Rationale: Users of the same region typically have a profile that is very close to that of the corresponding time zone crowd, and further away from crowds of different timezones.

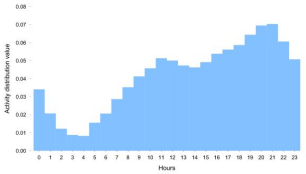
- For every member of an anonymous crowd, we compare his profile with that of all different timezone profiles
- geolocate that member to the timezone whose activity profile is **less distant**

Less Distant ->The one for which it takes less effort to transform the single user profile into by both shifting and moving probability mass.

Distance measure



(b) Twitter dataset of the German population (local time UTC + 1).



(c) Entire Twitter dataset (UTC).

Earth Mover's distance:

Given two distributions of earth mass spread on the same space, the EMD measures the least amount of work to move earth around so that the first distribution matches the second.

Less Distant ->The one for which it takes less effort to transform the single user profile into by both shifting and moving probability mass.

Single Country placement - Twitter dataset

Earth Mover's distance:

Given two distributions of earth mass spread on the same space, the EMD measures the least amount of work to move earth around so that the first distribution matches the second.

Less Distant ->The one for which it takes less effort to transform the single user profile into by both shifting and moving probability mass.

Single Country placement - Twitter dataset - Germany

For every timezone, compute the fraction of the population with profiles falling into Germany's timezone according to the EMD.

Observations:

- Despite common nationality, the habits of two different people are not exactly the same. For example, youngsters tend to go to sleep later than older people, parents wake up earlier than teenagers, and so on.

Single Country placement - Twitter dataset - Germany

For every timezone, compute the fraction of the population with profiles falling into Germany's timezone according to the EMD.

Observations:

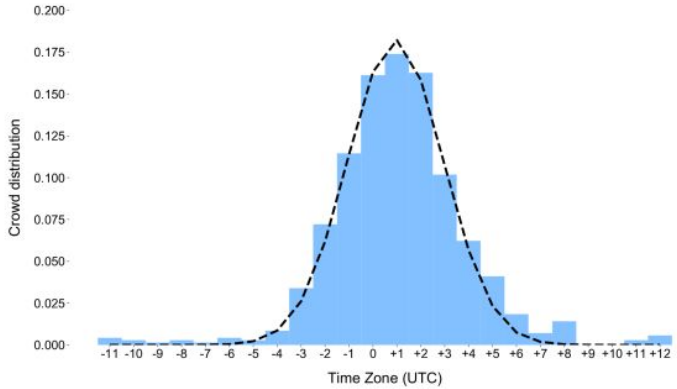
- Despite common nationality, the habits of two different people are not exactly the same. For example, youngsters tend to go to sleep later than older people, parents wake up earlier than teenagers, and so on.

Expectation
Expect a large number of the German crowd to fall under the timezone of Germany,
Expect that a portion of the crowd will be placed in neighbor timezones.

Single Country placement - Twitter dataset - Germany

For every timezone, compute the fraction of the population with profiles falling into Germany's timezone according to the EMD.

Expectation
Expect a large number of the German crowd to fall under the timezone of Germany,
Expect that a portion of the crowd will be placed in neighbor timezones.

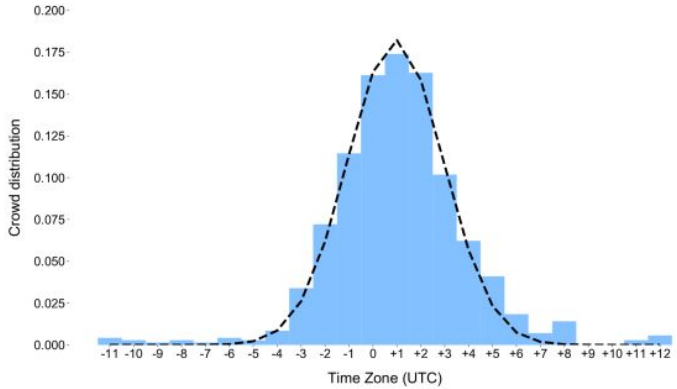


(a) German

Single Country placement - Twitter dataset - Germany

Observation:

- There is a peak at UTC + 1 timezone, that covers Germany, while the values drop for timezones further away.
- Most importantly, we observe that the crowd placement follows a Gaussian distribution

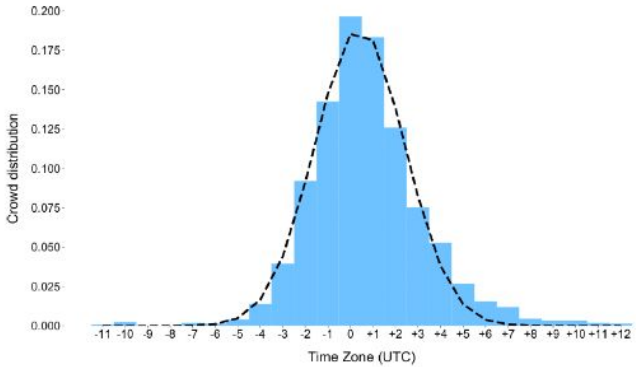


(a) German

Single Country placement - Twitter dataset - France

Observation:

- There is a peak at UTC + 1 timezone, that covers France, while the values drop for timezones further away.
- Most importantly, we observe that the crowd placement follows a Gaussian distribution

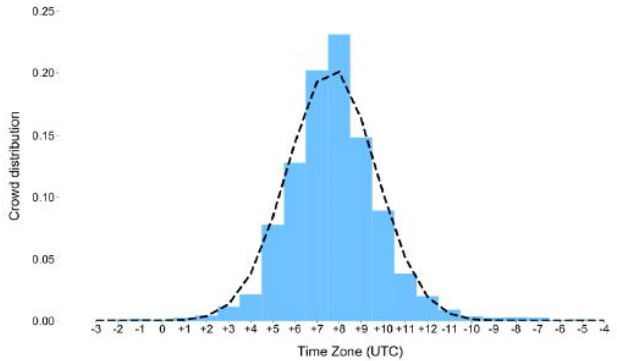


(b) French

Single Country placement - Twitter dataset - Malasyia

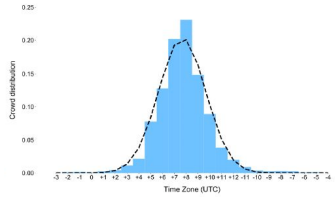
Observation:

- There is a peak at the country's timezone, that covers Malaysia, while the values drop for timezones further away.
- Most importantly, we observe that the crowd placement follows a Gaussian distribution



(c) Malaysian

Single Country placement - Conclusion

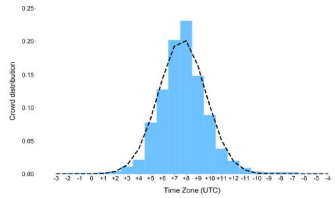


(c) Malaysian

Observation:

- The previously mentioned behaviour is seen in all countries considered in the twitter dataset

Single Country placement - Conclusion



(c) Malaysian

Observation:

- The previously mentioned behaviour is seen in all countries considered in the twitter dataset

Conclusion:

To geolocate a given crowd of people from the same, unknown region, it is enough to build the corresponding activity profiles placement through the EMD distance and curve-fit the resulting distribution with a Gaussian.

The center of the Gaussian will uncover the timezone of the unknown region and thus the geolocation of the crowd.

Multiple Country placement

Users access a given site from multiple different regions.

Since single region crowds follow a Gaussian distribution, we expect that the mixture of multiple region populations exhibits a profile that follows a Gaussian mixture model.

Uncovering the Gaussian distributions (i.e. mean and standard deviation) allows us to correctly place the members of mixed-country crowds in the corresponding geolocations.

Multiple Country placement

Users access a given site from multiple different regions.

Since single region crowds follow a Gaussian distribution, we expect that the mixture of multiple region populations exhibits a profile that follows a Gaussian mixture model.

Uncovering the Gaussian distributions (i.e. mean and standard deviation) allows us to correctly place the members of mixed-country crowds in the corresponding Geolocations.

We do not know the number of different crowds a priori.

Multiple Country placement

To address this issue, we can utilize Expectation-Maximization with the standard deviation observed empirically for the Gaussian fitting curves of single-region placement distributions.
EM is an iterative algorithm used as the standard to estimate the maximum likelihood parameters of a given model.

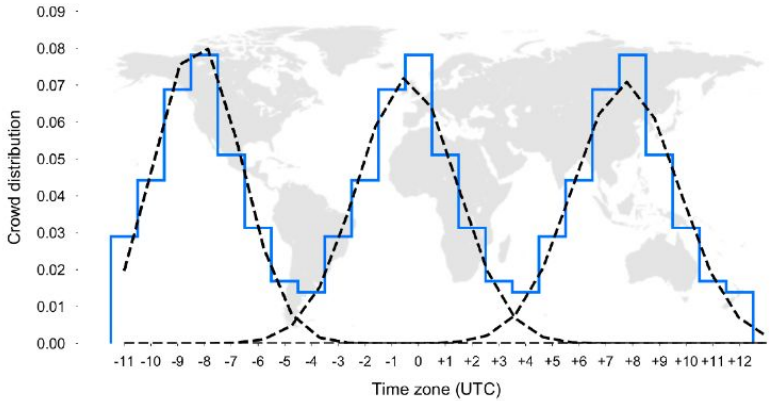
In our case, the model is the Gaussian mixture, and the components are the Gaussian curves.

Gaussian fitting metrics.

Dataset	Average	Standard deviation
Malaysian Twitter	0.009	0.013
German Twitter	0.009	0.009
French Twitter	0.008	0.010
Synthetic dataset (a)	0.011	0.010
Synthetic dataset (b)	0.012	0.010
CRD Club	0.007	0.006
Italian DarkNet Community	0.014	0.016
Dream Market forum	0.011	0.008
The Majestic Garden	0.009	0.011
Pedo support community	0.012	0.010
Baseline	0.081	0.070

Multiple Country placement

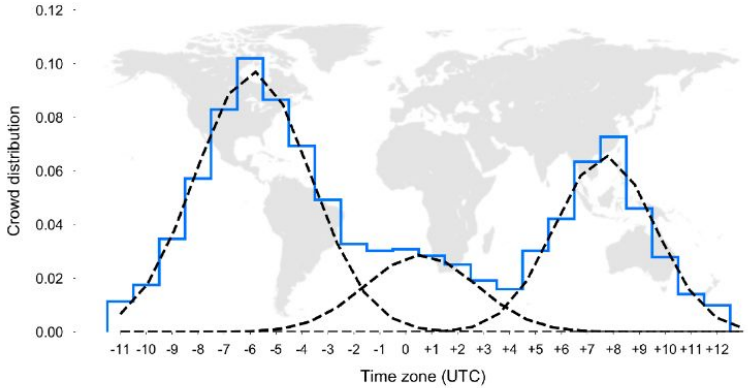
To address this issue, we can utilize Expectation-Maximization with the standard deviation observed empirically for the Gaussian fitting curves of single-region placement distributions.
EM is an iterative algorithm used as the standard to estimate the maximum likelihood parameters of a given model.
In our case, the model is the Gaussian mixture, and the components are the Gaussian curves.



(a) Synthetic dataset modelling the behavior of Malaysian users in three different timezones: UTC, California, and Australia.

Multiple Country placement

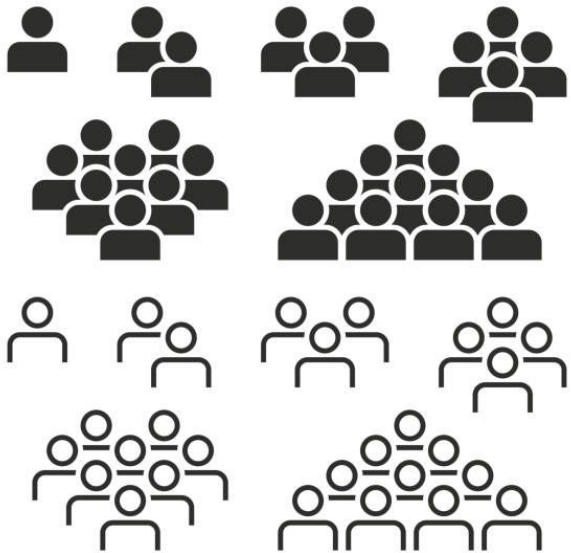
To address this issue, we can utilize Expectation-Maximization with the standard deviation observed empirically for the Gaussian fitting curves of single-region placement distributions.
EM is an iterative algorithm used as the standard to estimate the maximum likelihood parameters of a given model.
In our case, the model is the Gaussian mixture, and the components are the Gaussian curves.



(b) Synthetic dataset: Illinois, German, and Malaysian users.

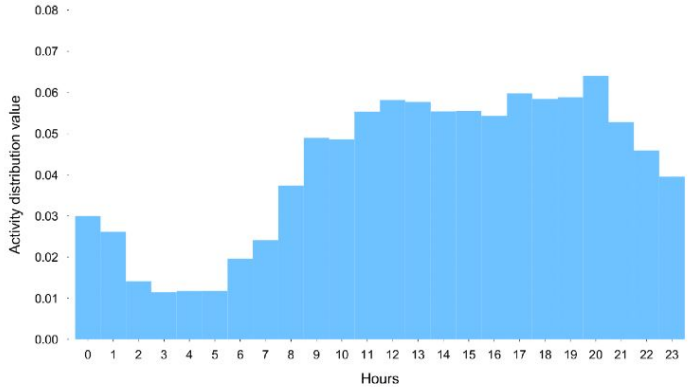
Geolocation in action - The Darkweb

- We need some DarkWeb groups
- Possibly some that we know the underlying information
- Unknown ones

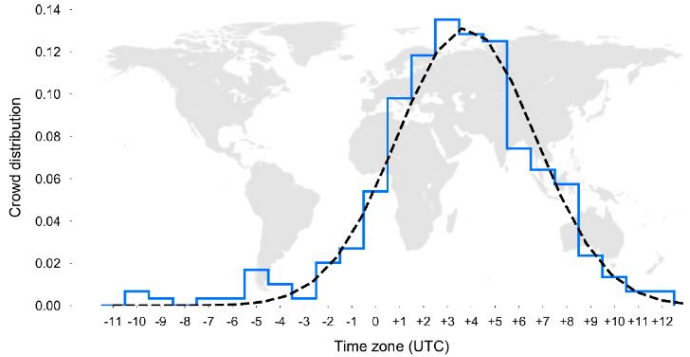


Geolocation in action - The Darkweb

- CRD Club, is mostly in Russian,
- Italian DarkNet Community (IDC) is the forum of the homonymous Italian marketplace in the Dark Web.



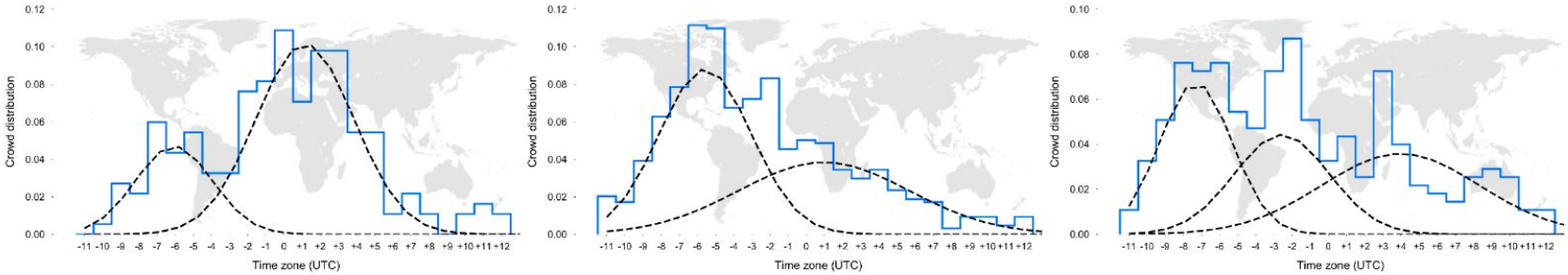
(a) Regional profile (UTC + 3).



(b) Gaussian distribution.

Geolocating unknown DarkWeb communities

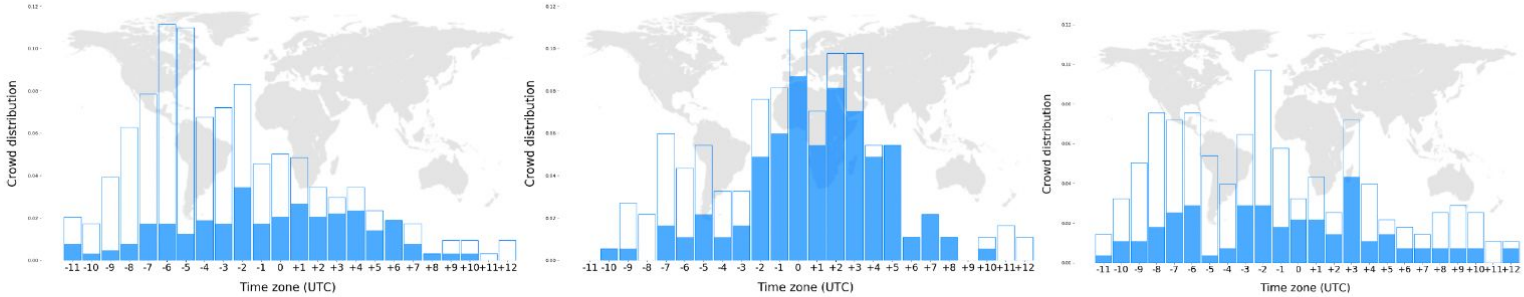
- Dream Market
- Majestic garden
- Pedo support community



(a) Dream Market forum. (b) The Majestic Garden. (c) Pedo support community.

Geolocating unknown DarkWeb communities

- Not native vs native english speakers distribution?



(a) The Majestic Garden forum. (b) The Dream Market forum. (c) The PedoSupport Community forum.

Reading Material

1. The onion routing Link-1
2. Geolocation-Based Profiling in the DarkWeb: Link-2