

Invisible Internet Project a.k.a. I2P

Antonis Kouzoupis

Athens CryptoParty #0

November 11, 2012



Outline

Introduction

More I2P

- Key Concepts

- Sending a Message

Gimme something

- Applications

- Installation

The end

- References

- Thank you!

I2P is

- an anonymous network (Captain Obvious)
- a decentralized resilient network
- scalable
- end-to-end encrypted
- in active development since Feb 2003
- mostly written in Java
- currently in version 0.9.3
- open source
- **not Tor**



Key Concepts

It's essential to clarify some key concepts:

- Router
- Destination
- Tunnel
- netDb
- Garlic routing



Router

- The software that every I2P node should run
- The “thing” that participates in the network
- Traffic routing
- Transportation
- Encryption – Decryption

Destination

- Cryptographic identifiers
- Anonymous Endpoints
- Associated with applications
- Destinations are connected to routers
- Each user will have several local destinations on their router

Tunnel

- A unidirectional path through routers
- Layered encryption is used – each of the routers can decrypt only one layer
- Two types of tunnels:
 - **Inbound** Inbound tunnels bring messages to the tunnel creator. First router is the Inbound Endpoint and the last one is the Inbound Gateway
 - **Outbound** Outbound tunnels send messages away from the tunnel creator. First router is the Outbound Gateway and the last one is the Outbound Endpoint

Tunnel

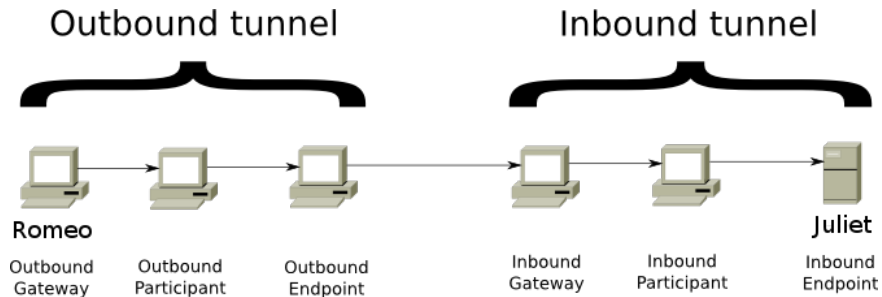


Figure: I2P Tunnels

netDb

- Network Database (so what?)
- Share network metadata
- Custom structured DHT based on the Kademlia algorithm
- Two types of metadata:
 - **routerInfo** Data necessary for contacting a particular router
 - **leaseSets** Data necessary for contacting a particular destination

Garlic Routing

- Variant of *onion* routing
- Each router decrypts only one layer of the message
- Bundle together multiple messages
- Difficult to perform traffic analysis



GARLEK

The Story

Let's unfold the story...

- Romeo and Juliet is a very loving couple
- Their families – Montagues and Capulets – are arch enemies
- They decide to communicate over I2P
- So they both install I2P

The Story

Let's unfold the story...

- Romeo and Juliet is a very loving couple
- Their families – Montagues and Capulets – are arch enemies
- They decide to communicate over I2P
- So they both install I2P

The Story

Let's unfold the story...

- Romeo and Juliet is a very loving couple
- Their families – Montagues and Capulets – are arch enemies
- They decide to communicate over I2P
- So they both install I2P

The Story

Let's unfold the story...

- Romeo and Juliet is a very loving couple
- Their families – Montagues and Capulets – are arch enemies
- They decide to communicate over I2P
- So they both install I2P



The Story

Let's unfold the story...

- Romeo and Juliet is a very loving couple
- Their families – Montagues and Capulets – are arch enemies
- They decide to communicate over I2P
- So they both install I2P

Building a tunnel

First of all, Juliet should build an outbound tunnel.

- Juliet does a lookup in the netDb to collect routerInfo
- Then she sends a build message to the first node
- The later forwards the message to the next node

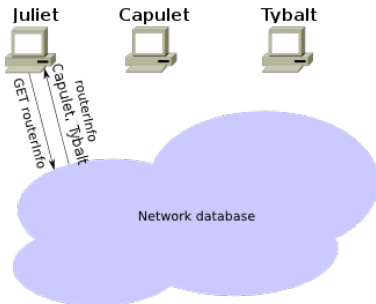


Figure: Build a tunnel

Building a tunnel

Then, the tunnel is ready

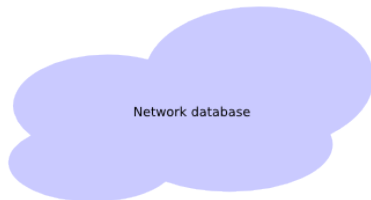
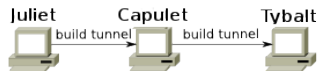


Figure: **Build a tunnel**

Send the message

- Juliet does a lookup in the netDb to find Romeo's leaseSet
- Picks one outbound tunnel and sends the message with instructions for Romeo's inbound tunnel gateway
- Romeo's inbound tunnel gateway receives the message and forwards it to Romeo's router

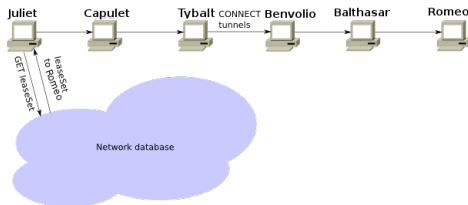


Figure: Sending the message

Applications

I2P provides a plethora of applications. Each application make its own anonymity, latency and throughput trade-offs.

- **Web Browsing** http & https proxy
- **Chat** IRC, I2P-Messenger
- **File Sharing** I2PSnark, iMule, Robert
- **E-mail** susimail, I2P-Bote
- **Blog** Syndie
- **Distributed Data Store** Tahoe-LAFS over I2P
- ...

Installation

- ✓ Download the latest build
- ✓ `java -jar i2pinstall_x.x.x.jar [-console]`
- ✓ Port forward necessary ports
- ✓ Configure bandwidth settings
- ✓ Add subscriptions to your addressbook

References

- `www.i2p2.{de,i2p}`
- `forum.i2p`
- `zzz.i2p`
- `killyourtv.i2p`
- `satori-wiki.i2p`
- `#i2p, #i2p-help @ {freenode, I2P}`

Thank you!

Q&A

Anonymity is not Boolean