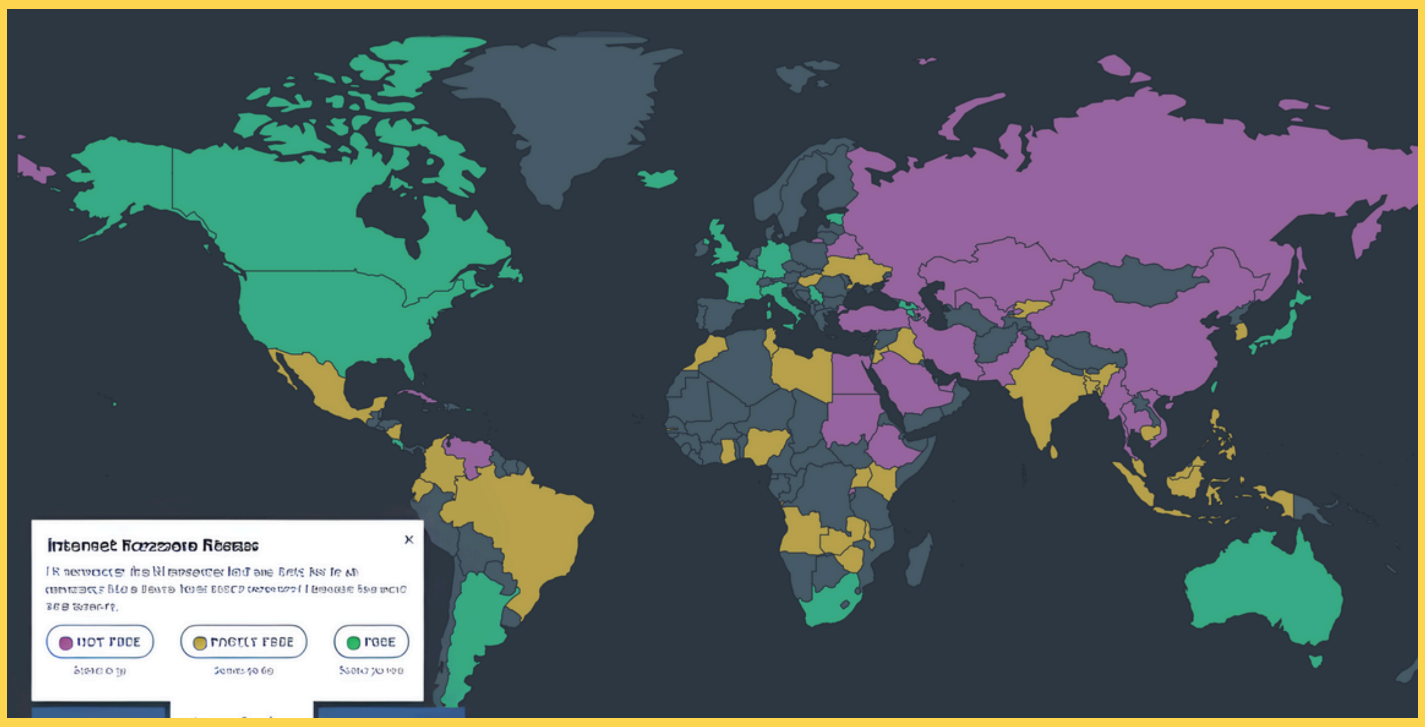
Semz: Anonymous and Secretive Messaging During Internet Censorship

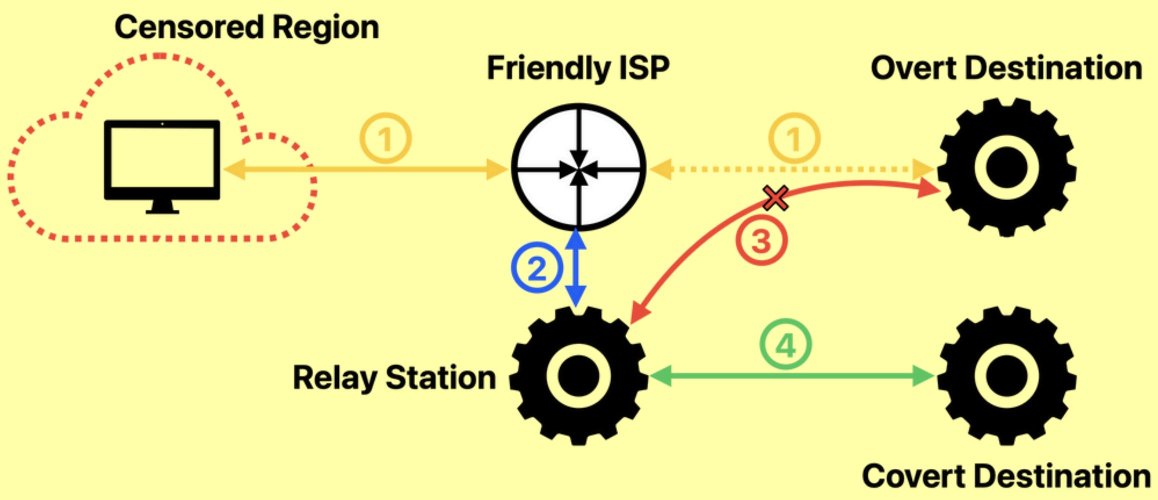
Internet Censorship is Widespread



- A **worldwide** issue
- Many methods to circumvent censorship have been created
- Due to many reasons, such as: **political instability**, **elections**, or **protests**

Decoy Routing

- Use a friendly ISP to evade censorship
- Requests look like they are intended for the overt destination, so they won't get blocked

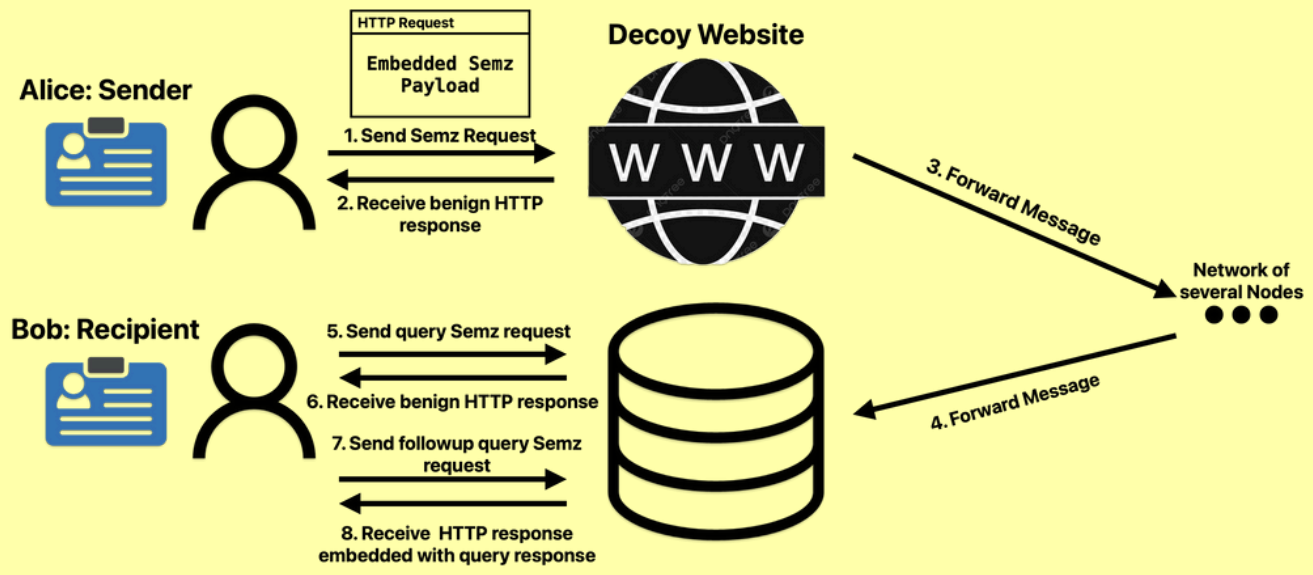


Decoy Routing is hard to deploy, as
cooperating ISPs are hard to find!!!

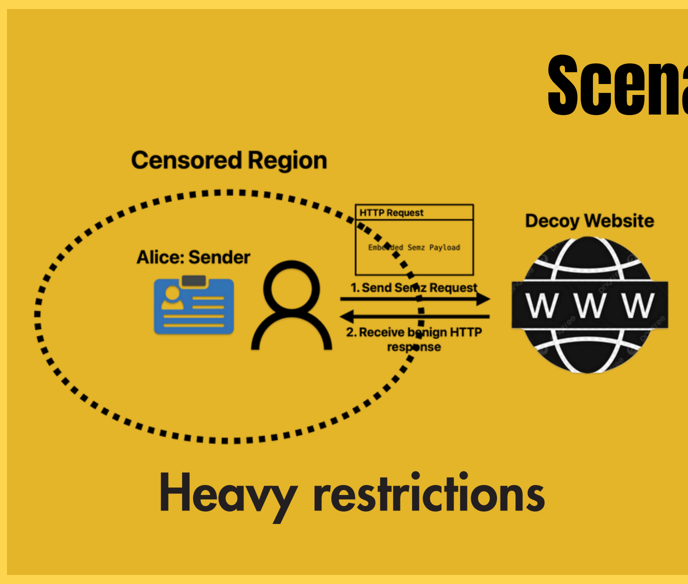
How can we fix the deployability of Decoy Routing?

You use Semz!

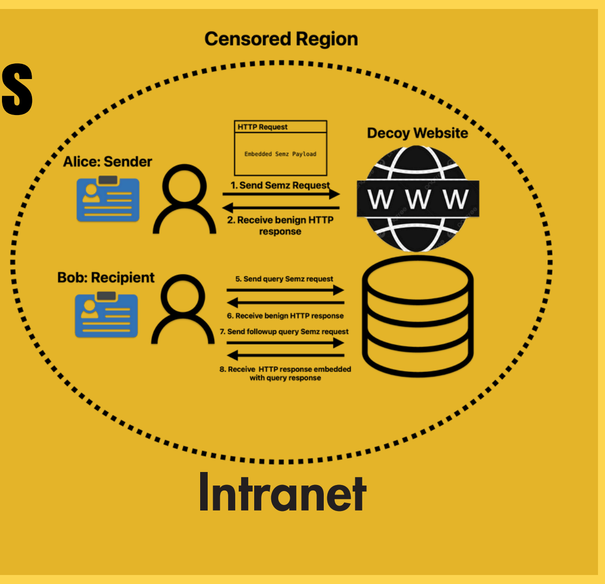
Workflow


Alice: Sender
HTTP Request
Embedded Semz Payload
Decoy Website
1. Send Semz Request
2. Receive benign HTTP response
3. Forward Message
Network of several Nodes
Bob: Recipient
5. Send query Semz request
6. Receive benign HTTP response
7. Send followup query Semz request
8. Receive HTTP response embedded with query response
4. Forward Message

Scenarios



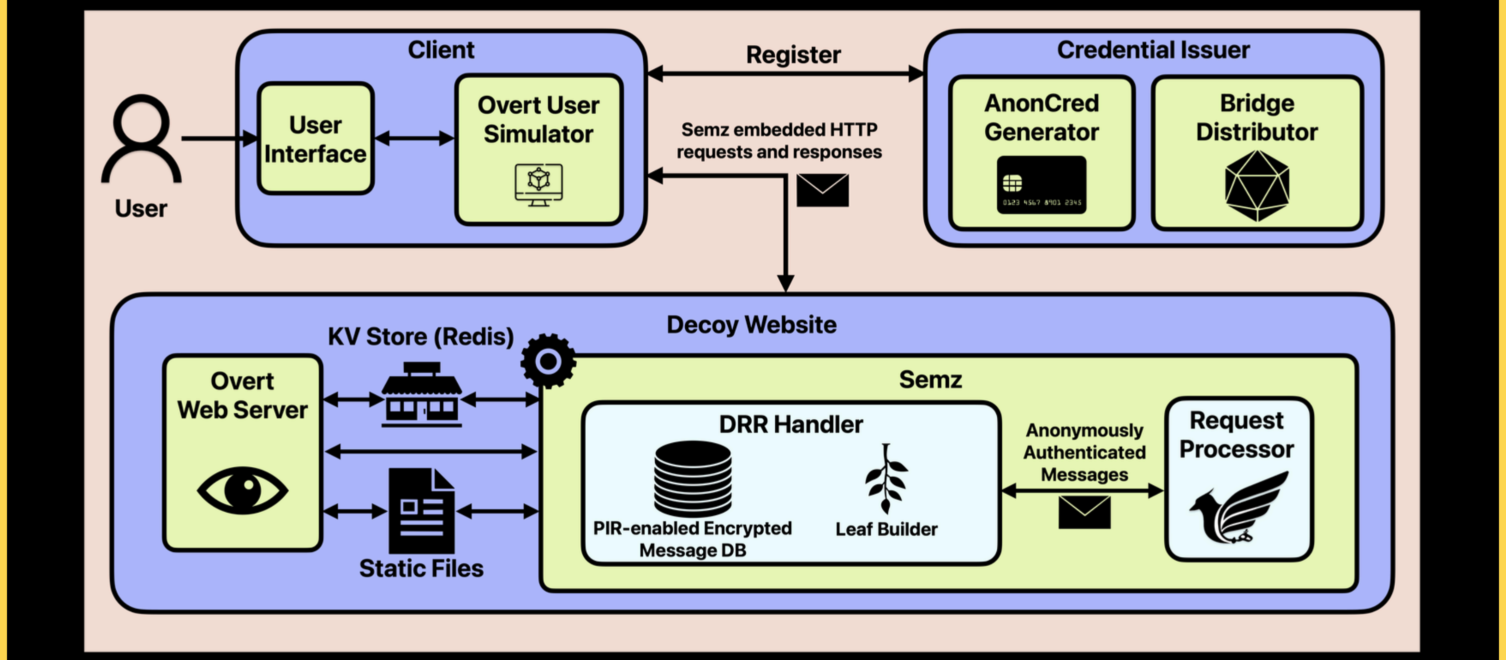
Heavy restrictions


Censored Region
Alice: Sender
HTTP Request
Embedded Semz Payload
1. Send Semz Request
2. Receive benign HTTP response
Decoy Website
Bob: Recipient
5. Send query Semz request
6. Receive benign HTTP response
7. Send followup query Semz request
8. Receive HTTP response embedded with query response

Intranet

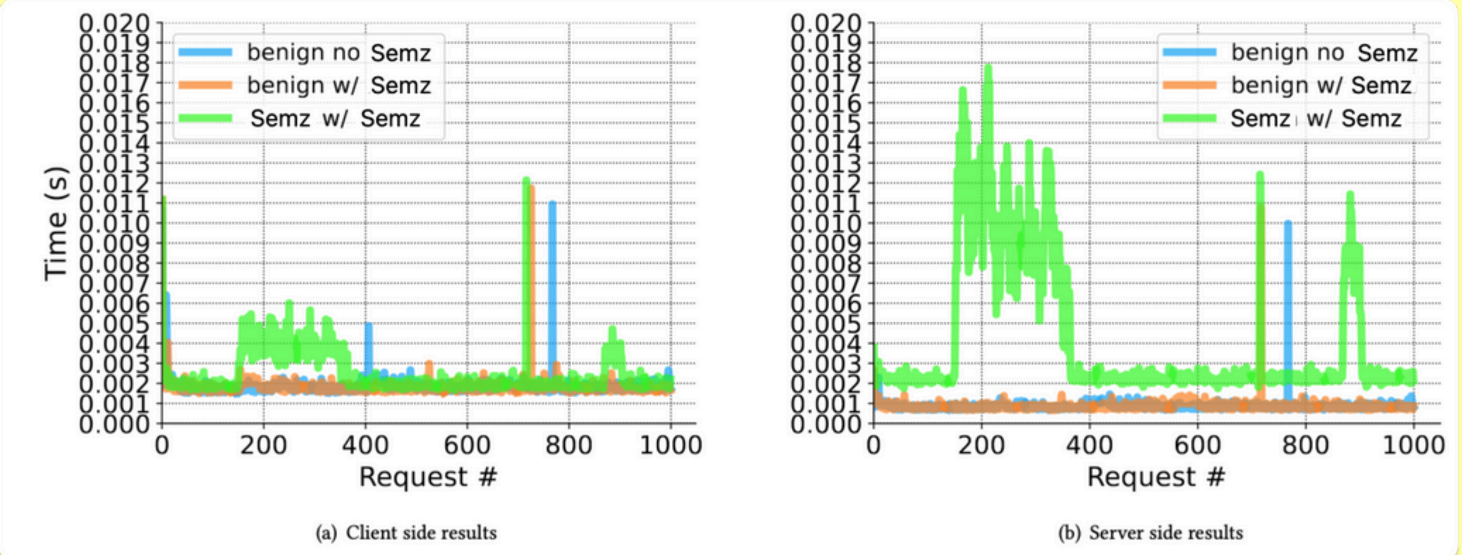
Architecture

- Semz aims for improved **deployability** by using **websites** to send traffic
- Semz **thwarts behavior analysis** attacks by mimicking a benign user's behavior
- Semz **resists traffic analysis** attacks by embedding data in the leaf nodes of webpage data (e.g., media files)
- Decoy Websites process Semz requests **after** responding to the encapsulating HTTP request to **evade timing attacks**



Preliminary Evaluation

- Semz poses **minimal overhead** on websites
- Semz does **not** meaningfully change request processing times



(a) Client side results

(b) Server side results

Conclusion and Future Work

- We design Semz, a new *censorship circumventing messaging system* that enables users to **anonymously** and **secretly** send messages in **heavily censored regions**
- We demonstrated that Semz poses **minimal overhead on websites**
- Future work will focus on performing **additional evaluation** to further evaluate Semz's resilience to **traffic** and **behavioral** fingerprinting

Semz is a work in progress

Please do not hesitate to share you thoughts and ideas

UNIVERSITY OF WATERLOO | DAVID R. CHERITON SCHOOL OF COMPUTER SCIENCE

Sina Kamali
sinakamali@uwaterloo.ca