

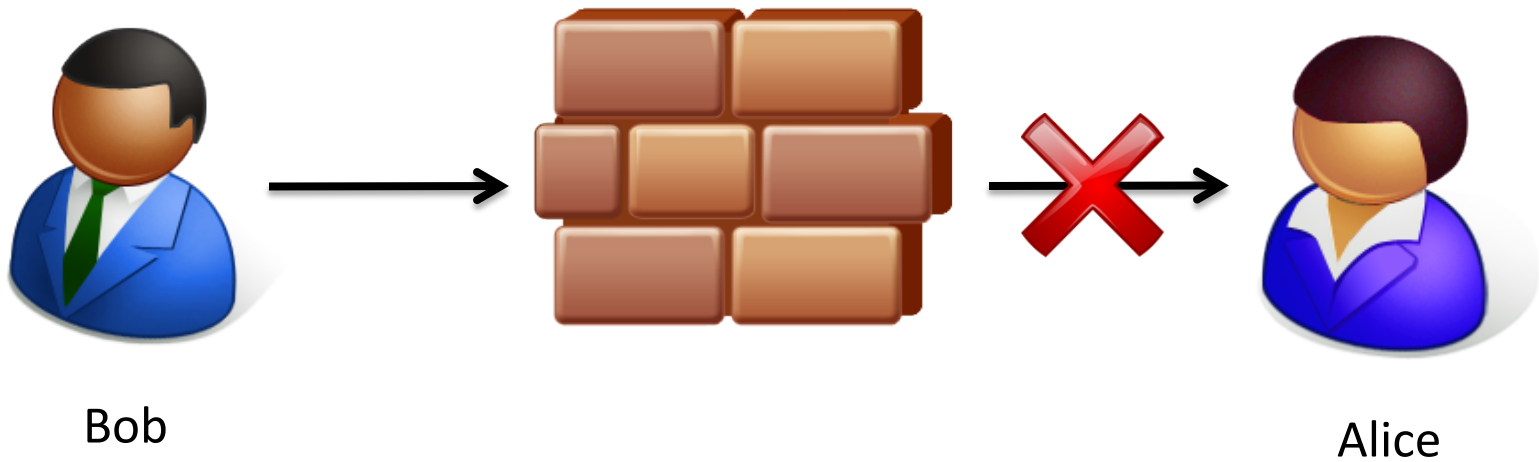
# Facade: High-Throughput, Deniable Censorship Circumvention Using Web Search

Ben Jones, Sam Burnett, Nick Feamster,  
Sean Donovan, Sarthak Grover, Sathya Gunasekaran,  
and Karim Habak

*Georgia Institute of Technology*

FOCI 2014

# Censorship is a common problem



# Difficult to hide that you are using Tor



**Tor is supposed to hide you online. In this Harvard student's case, it did the opposite.**



Bob



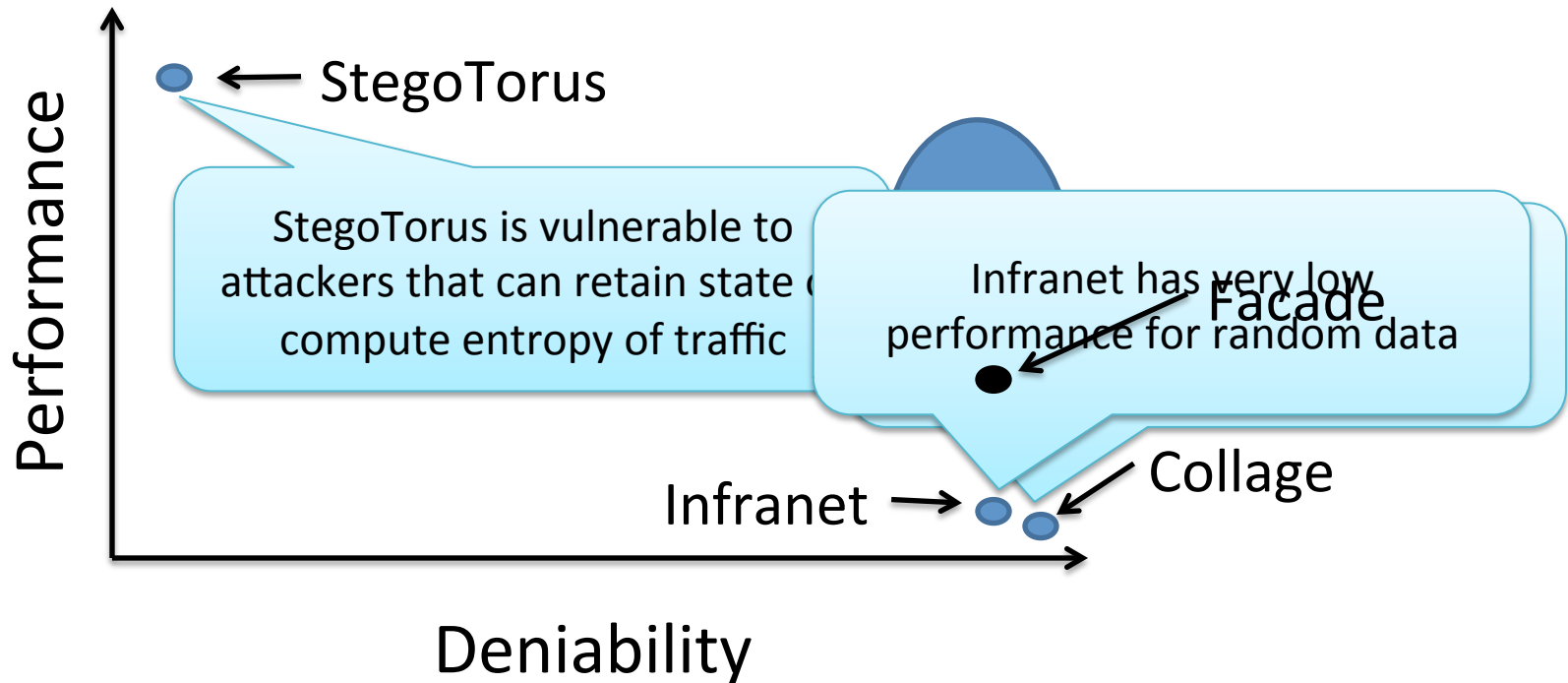
Alice

HTTP circumvention tools are necessary or they soon will be



The image shows a screenshot of a web browser. The top part of the browser window displays the Tor logo, which consists of the letters 'T', 'o', and 'r' in purple, with a purple onion bulb in the center of the 'o'. Below the logo are navigation buttons for 'HOME', 'ARCHIVES', and 'AI'. The main content area of the browser shows an article from Ars Technica. The article title is 'Iran reportedly blocking encrypted Internet traffic'. The author's name is 'Bob'. The article text begins with 'The Iranian government is reportedly blocking access to websites that use the ...'. The Ars Technica logo is visible in the top left of the article content. The article is categorized under 'LAW & DISORDER / CIVILIZATION & DISCONTENT'. The navigation bar includes 'MAIN MENU', 'MY STORIES:', 'FORUMS', 'SUBSCRIBE', and 'JOBS'. The article is dated 'Posted February 10th, 2012' and includes tags like 'filtering', 'positive futures', and 'Rev'.

# We need to target new points on performance/deniability curve

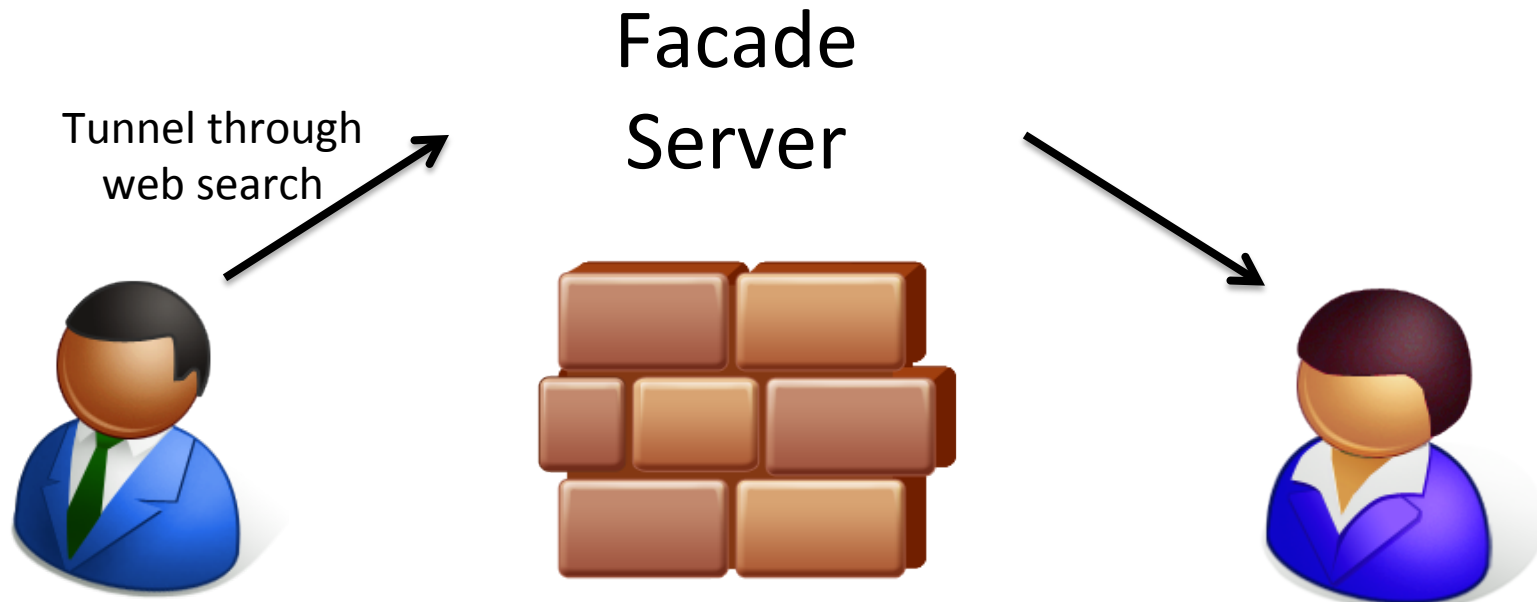


Note: graph drawn for emphasis, not to scale

# Research Problems

- How can we create deniable, HTTP covert channels?
- Can we get the deniability of Infranet with better performance for encrypted data uploads?

# Our Solution



- Everyone searches the web and search has dozens of bits of entropy
- Let's use this entropy to hide information

# Outline

- Motivation
- Facade protocol
- Evaluation



# Threat Model

- Our target censor can:
  - Detect and block all protocols other than HTTP
  - Store some state (several HTTP request/ response pairs)
    - Ex: detect that information in cookies has not been set by the server
  - Censor can operate in-path
    - Ex: create error conditions to fingerprint client or server

# Facade Overview

- Facade encodes information in web search
- Real users browse and search at the same time so Facade encodes information in browsing and search
- Note: Facade server must have sufficient cover search traffic to maintain deniability

# Encoding data in search

- Encode information in the path string with a dictionary encoding
- The dictionary is a mapping from data to English
- Example:  
<http://www.example.com/?q=banana+law>  
encodes the string “hello”

# Making search deniable with OpenSearch

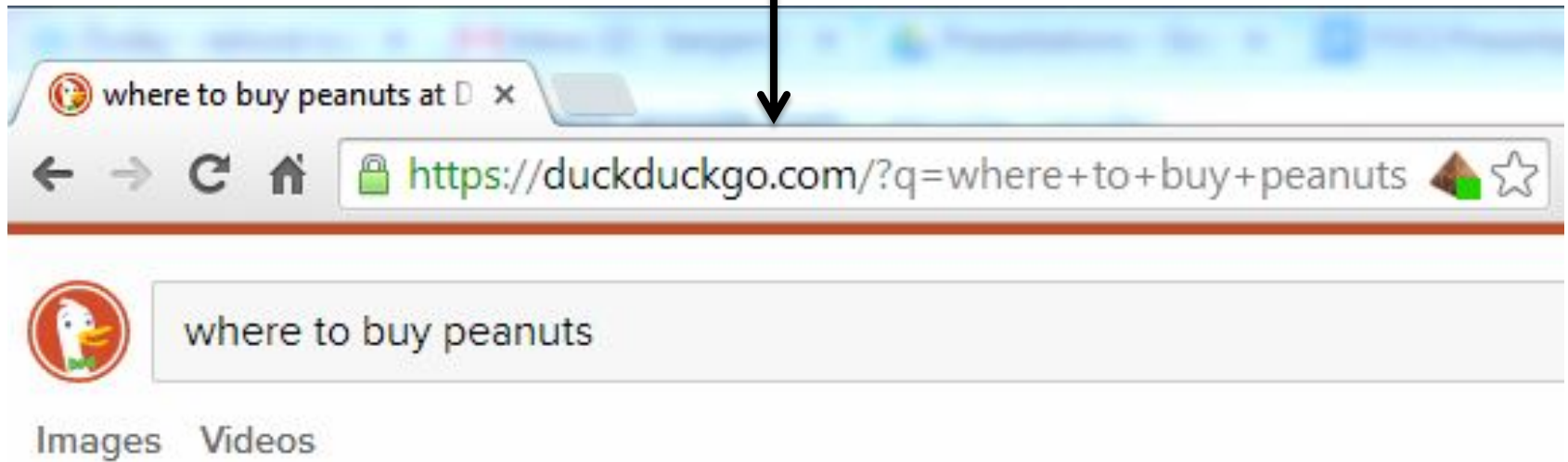
- What is it?
  - Specification for sending search requests
- How does it work?
  - Encodes query into a URL
- Why are we using it?
  - Widely deployed: Chrome, Baidu, Yandex, etc.

# OpenSearch Example

Query: where to buy peanuts



URL: <https://duckduckgo.com/?q=where+to+buy+peanuts>



# System Overview

0. User makes request for `http://www.epochtimes.com`

Framing Layer

1. Facade breaks request into chunks for transmission

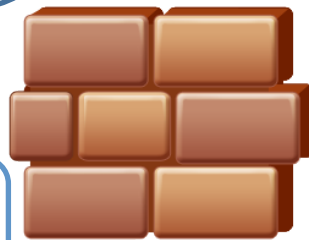
URL Encoding

2. Facade client sends the first chunk `http://www.epochtimes.com`

Facade Client

Encode "epochtimes.com" as `http://example.com/q=shoe+coffee`

Censor



Facade

8. Facade server makes request for `http://www.epochtimes.com` and returns the content via an image encoding

Framing Layer

7. Facade server assembles the first chunks together

URL Encoding

6. Facade server decodes the first chunk

Facade Server

# Outline

- Motivation
- Facade protocol
- **Evaluation**

# Performance Evaluation: Methods

- Evaluated entropy of a search request using AOL search corpus
- 20 million queries from 650k users
- Get the average information content (entropy) per query



# Performance Evaluation: Results

Tool	Entropy Per Request (bits)	Request Rate to Equal 256kbps	Deniability Set
Facade	<sup>1</sup> ~78	3,300	HTTP+Search
Infranet	<sup>2</sup> 3	85,300	HTTP+Browse
StegoTorus	<sup>3</sup> 12000	21	HTTP

<sup>1</sup> The paper contains an error wherein the entropy is reported with log base e instead of 2

<sup>2</sup> Infranet entropy computed with parameters from paper, i.e. 8 links per page, so  $\log_2(8)=3$  bits

<sup>3</sup> StegoTorus entropy calculated based upon Base64 encoding 2000 characters per URL

# Future Work: Tradeoffs

- Tune performance/deniability with dictionary choices
  - Per user/site dictionaries
  - Dictionaries with joint PDFs

# Conclusion

- Facade: an HTTP covert channel that balances performance and deniability by improving upload performance
- Get Facade (in development) from <https://github.com/ben-jones/facade>
- Contact me: Ben Jones [bjones99@gatech.edu](mailto:bjones99@gatech.edu)