

Link Us If You Can: Enabling Unlinkable Communication on the Internet

Zhenbo Xu¹ Wei Yang* Yang Xu Ajin Meng
Jianhua Liu Qijian He Liusheng Huang

School of Computer Science and Technology
University of Science and Technology of China

SECON, 2018



Outline

- 1 Introduction
 - online communication privacy
- 2 HTor
 - overview
 - challenges
- 3 Evaluation
- 4 Application scenario



Outline

- 1 Introduction
 - online communication privacy
- 2 HTor
 - overview
 - challenges
- 3 Evaluation
- 4 Application scenario



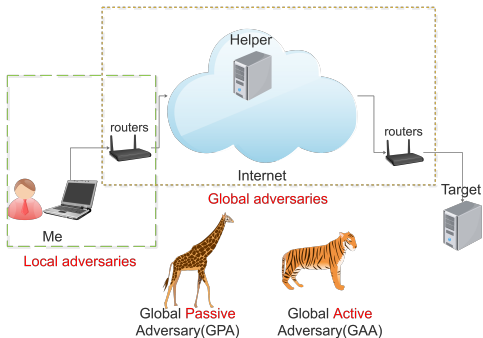
Hide our traces/identities

Why difficult?

Protect online privacy = Never online



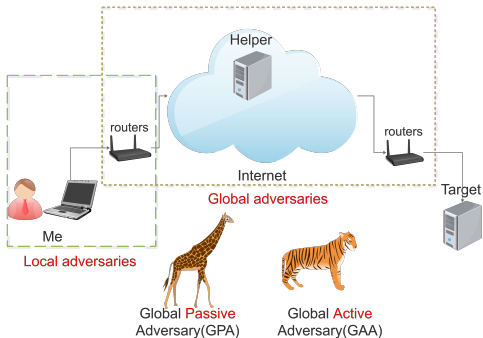
Roles in this privacy battle on online communication



What to protect?

- content?

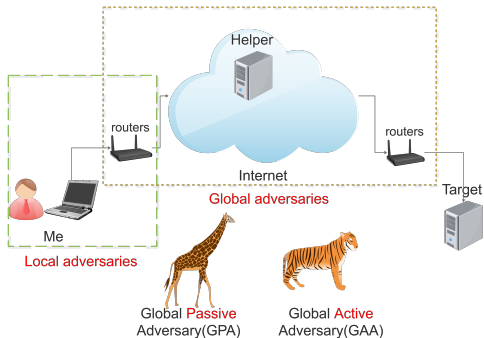
Roles in this privacy battle on online communication



What to protect?

- content?
- identity?

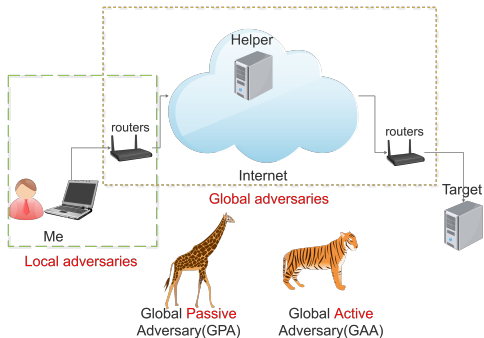
Roles in this privacy battle on online communication



What to protect?

- content?
- identity?
- or, behavior?

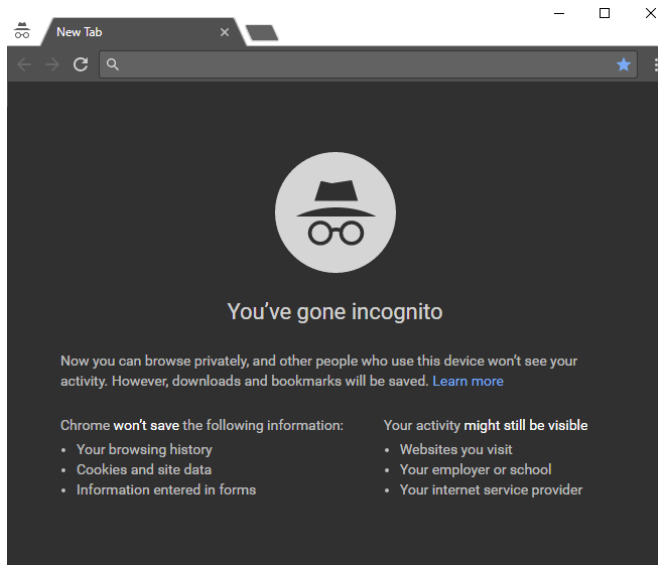
Roles in this privacy battle on online communication



What to protect?

- content?
- identity?
- or, behavior?
- unlinkable communication


Existing Popular Solutions



The screenshot shows a Chrome browser window with a dark theme. The address bar contains navigation icons (back, forward, refresh, search) and a star icon for bookmarks. The main content area features a large circular icon with a hat and glasses, representing the Incognito mode. Below the icon, the text reads "You've gone incognito". A paragraph explains that browsing is private but downloads and bookmarks are saved, with a "Learn more" link. Two columns of information are provided: one listing what Chrome won't save (browsing history, cookies, forms) and another listing what activity might still be visible (websites visited, employer/school, internet service provider).

New Tab

← → ↻ 🔍 ☆ ⋮



You've gone incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. [Learn more](#)

Chrome **won't save** the following information:

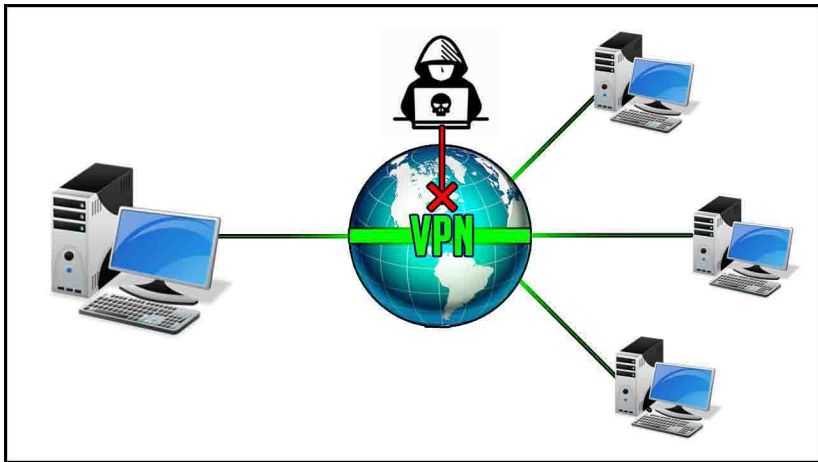
- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity **might still be visible**

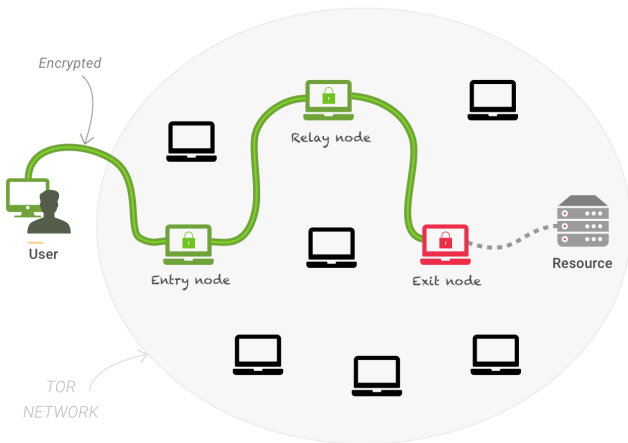
- Websites you visit
- Your employer or school
- Your internet service provider



Existing Popular Solutions



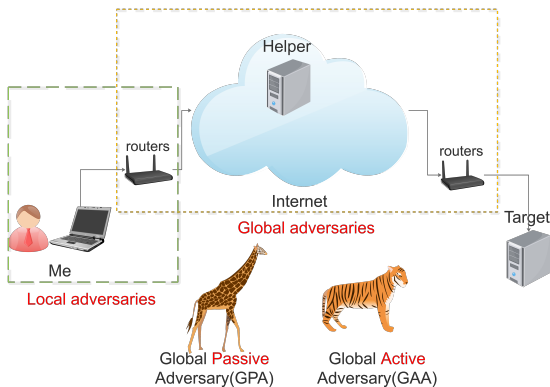
Existing Popular Solutions



Introduction

online communication privacy

How to mask our online behaviors (or say, to keep unlinkability)?



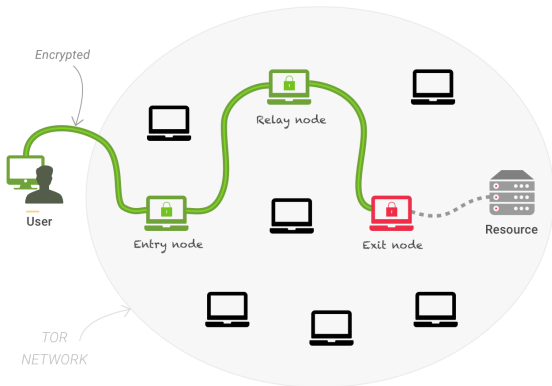
- relay & encryption (Tor, VPN, HTTPS)



Introduction

online communication privacy

How to mask our online behaviors (or say, to keep unlinkability)?



- relay & encryption (Tor, VPN, HTTPS)
- end-to-end correlation attack / tagging attack / website fingerprinting



How can we make out traffic unlinkable?

- First, import delay. If your message is delivered without delay, global watchers can easily follow the message.

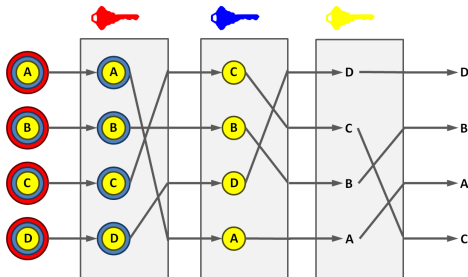


Figure: Mix network (threshold and shuffle)



How can we make our traffic unlinkable?

- First, import **delay**. If your message is delivered without delay, global watchers can easily follow the message.
- **sleeper attack**.

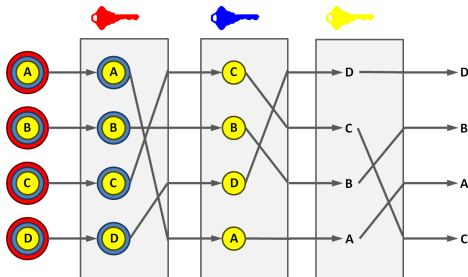


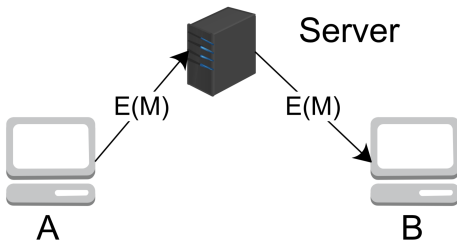
Figure: Mix network (threshold and shuffle)



How can we make our traffic unlinkable?

- Second, cut off the **direct** link. Find a service provider.

III. Service providers (SPs)



A sends $E(M)$ to B by SPs

Figure: Service providers (encryption and a large anonymity set)



How to prevent various attacks/interventions from global adversaries?

Why almost all anonymous networks are vulnerable?

- Rely on other participants to ensure correct communication. But participants can actively ruin the security of anonymous networks.



How to prevent various attacks/interventions from global adversaries?

Why almost all anonymous networks are vulnerable?

- Rely on other participants to ensure correct communication. But participants can actively ruin the security of anonymous networks.
- Service providers are apparent targets waiting for attacks and analysis. An anonymous network client usually behaves differently because it interacts with relay nodes rather than true websites.



If there exists a service provider

Faced with GPA/GAA, the SP can satisfy:

- It does not appear to provide communication services.
- A large anonymity set.
- Previous messages can be denied.



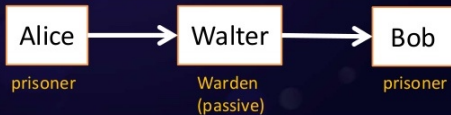
Outline

- 1 Introduction
 - online communication privacy
- 2 HTor
 - overview
 - challenges
- 3 Evaluation
- 4 Application scenario



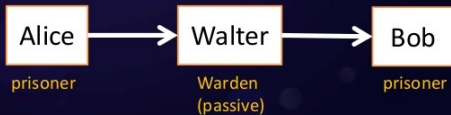
Covert channel

Prisoner model:



Covert channel

Prisoner model:

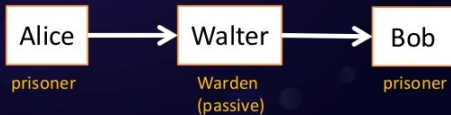


- **Covert channel** is defined as any manner of transferring data by means that were not intended for that purpose.



Covert channel

Prisoner model:

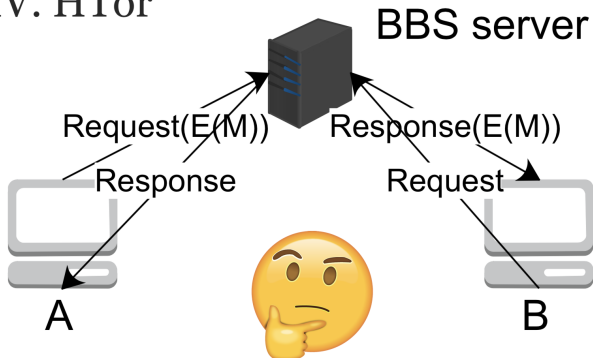


- **Covert channel** is defined as any manner of transferring data by means that were not intended for that purpose.
- We do not want network watchers to think that I'm communicating with the service provider.



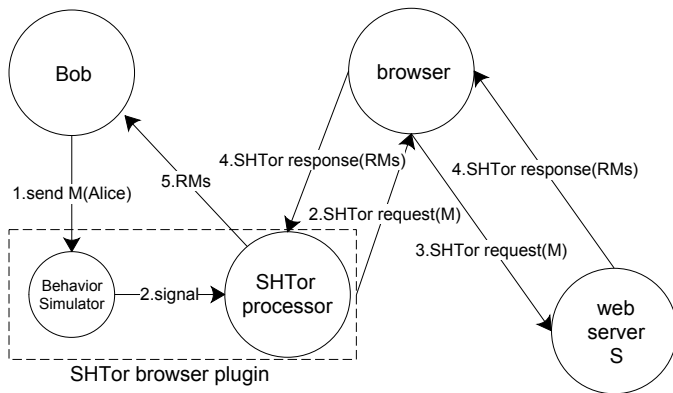
Work flow

IV. HTor



A sends E(M) to B by browsing web pages

Work flow



Outline

- 1 Introduction
 - online communication privacy
- 2 HTor
 - overview
 - **challenges**
- 3 Evaluation
- 4 Application scenario



How to build covert channels in HTTP request?

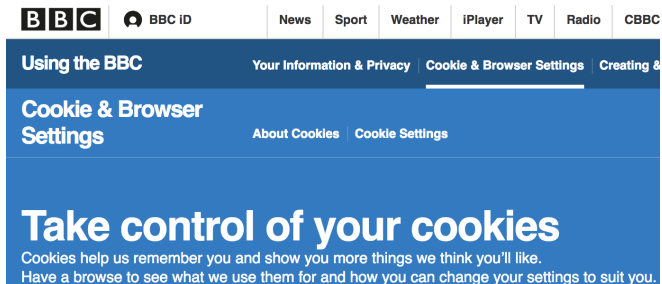
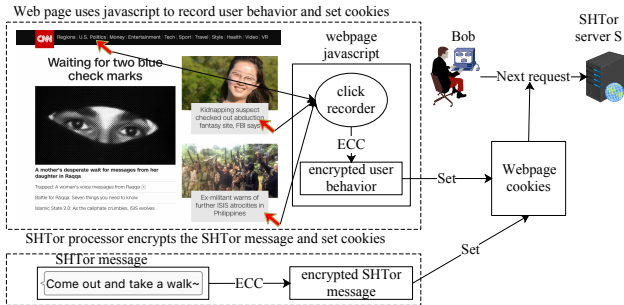


Figure: Covert channel design in HTTP requests

- More and more companies use cookie profiling (personalized marketing) to record user behaviors as visitors move across pages on your website.



How to build covert channels in HTTP request?



- For normal visitors, the website collects records of user behaviors and encrypt them into session cookies. For HTor users, a hidden message is expanded to the same length and also encrypted into session cookies.



How to build covert channels in HTTP response?

You may also like



Figure: Covert channel design in HTTP responses

- There are many ways to build covert channels in HTTP responses as the content in HTTP response is large enough to hide several messages.



How to build covert channels in HTTP response?

You may also like



Figure: Covert channel design in HTTP responses

- There are many ways to build covert channels in HTTP responses as the content in HTTP response is large enough to hide several messages.
- Exploiting static files as carriers are suspicious.



How to build covert channels in HTTP response?

You may also like



Figure: Covert channel design in HTTP responses

- There are many ways to build covert channels in HTTP responses as the content in HTTP response is large enough to hide several messages.
- Exploiting static files as carriers are suspicious.
- User-specific contents are much better. Thanks to personalized marketing, some contents like ADs or personalized suggestions can be user-specific without suspicion. We can build covert channels on them at will.



Deniable communication over HTTP

Simply changing keys for each message (one-time-pad) does not work in HTTP due to two reasons

- Stateless. Every HTTP request should be sent before HTTP response is received.
- The server can not proactively send messages to clients no matter how many messages are waiting for that client.



Deniable communication over HTTP

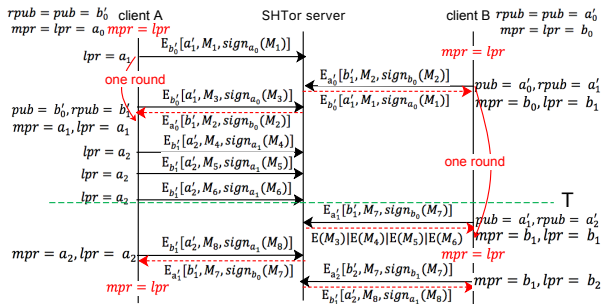


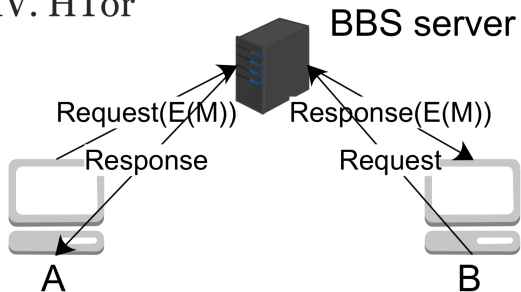
Figure: One-round-pad



Simple HTor: unlinkability against GPA

HTor has reliable security against GPA, keep **covert**, and ensure **K-unlinkability** and **Deniability**.

IV. HTor



A sends E(M) to B by browsing web pages

Figure: Simple HTor.



Unlinkable communications over unreliable servers

Against GAA:

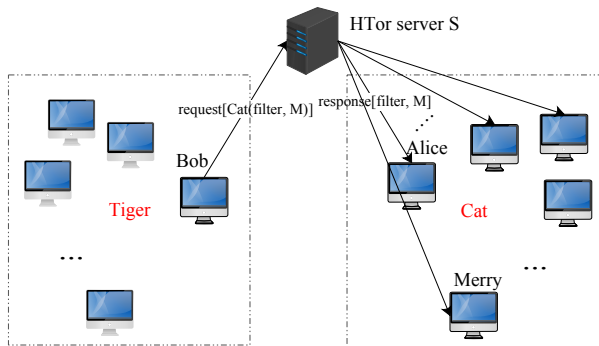


Figure: HTor group mechanism.



Advantages/Disadvantages

The advantages of HTor Over Tor:

- Coverttness.
- Deniability.
- Unlinkability against global adversaries.

The disadvantages of HTor:

- Message delays.
- Limited message length.

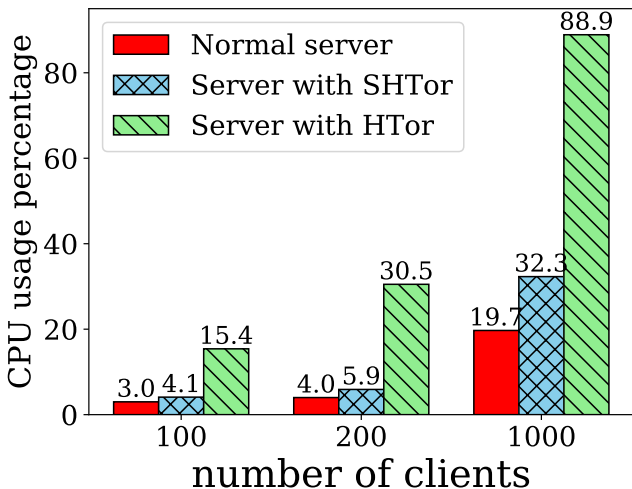


Implementation

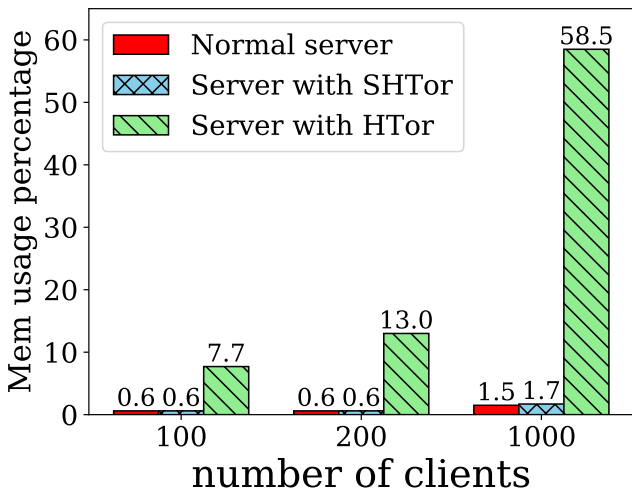
- Resource consumption.
- Message delays.



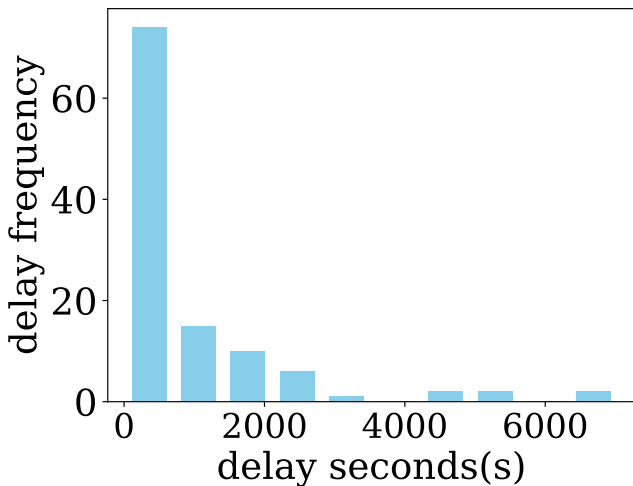
Resource consumption



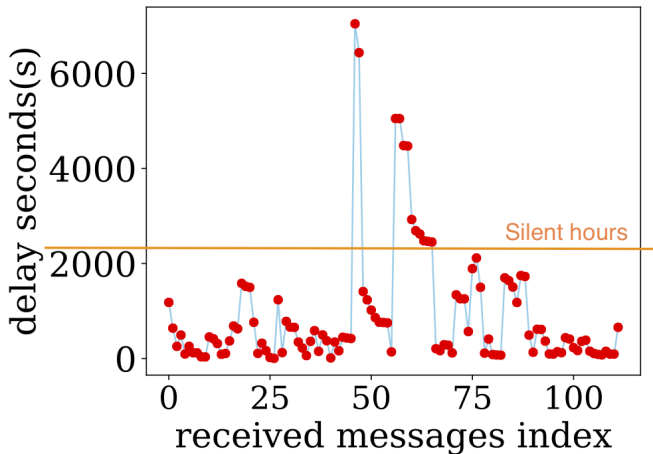
Resource consumption



Delay



Delay



About behavior simulator

If you make sure you are not being monitored by GAA:

No need to use BS to scheduler your messages. Send HTTP requests at will.

If you are not sure:

Do use BS to simulate your browsing behavior to completely avoid suspicion.



No need to rely on HTTP protocol

We choose HTTP because HTTP is everywhere and thus is very suitable to be a carrier to build covert channels.

The key insight of HTor is to **exploit covert channels** to design a covert, easy-to-reach, scalable and anonymous network.



Use HTor in suitable scenarios

Do not use HTor if you:

- don't care online communication privacy.
- want instant messaging. Message delay is inherent in HTor.

Please try HTor if you:

- want to communicate with someone without any traces and suspicions.
- rely on your own website (Personal website or corporate website) to achieve secure communications.



Thank You!

