VAST: Versatile Anonymous System for Web Users

Outline

- Conclusions
- VAST security analysis
- Performance
- Design and draft of the method implementation
- VAST system overview
- Providing anonymity - state of the art
- Introduction to the current techniques of...
Third Party Proxy Servers

Current Solutions

Pros / Reasons for Popularity
- Further research and motivation to
- Cons / Motivation to

- Re-require for system realization
- Simplicity and relativity low costs
- Navigation
- Insufficient delays of web
- Easy access to the service
- Identity data
- High efficiency in hiding users
- User’s privacy protection
- WWW system relieved to block off
- Filling the technical loophole in

Anonymizer, Magnaent Proxy, Reverse Proxy, SaveWeb

Examples:

- Popular techniques: Third Party Proxy Servers

1/4

Current Solutions

2/4
<table>
<thead>
<tr>
<th><strong>Pros / Advantages over</strong></th>
<th><strong>Cons / Reasons for</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Encrypts traffic</td>
<td>- Requires substantial infrastructure - high cost</td>
</tr>
<tr>
<td>- Single proxies</td>
<td>- Possibility of proxies collaborating</td>
</tr>
<tr>
<td>- Decentralization of information</td>
<td>- Serious delays of Web navigation</td>
</tr>
<tr>
<td>- Elimination of basic types of traffic</td>
<td>- Knowledge about users' Web activity</td>
</tr>
<tr>
<td>- Safety of traffic</td>
<td></td>
</tr>
</tbody>
</table>

**Chaining with Encryption**

**Current Solutions**

![Diagram showing chaining with encryption technique scheme]

**Encryption / Adaptation of Chaining MIXNET**

- Safer but more theoretical technique: Chaining with...
Main principles:

- Facility to implement outside laboratories – Relatively low costs
- Accessibility – no additional requirements from users
- Retention of speed (minimalization of performance differences)
- Preventing risks of traffic analysis attacks
- Providing versatile anonymity (including service provider and also preserving advantages of single third party proxy servers)

Versatile Anonymous System for Web Users

**VAST**

"'Tecumseh'"

— Charles Mark (1838-1927)

No civilized barbarian trenches for gain.
Unnamed save in mute Nature's inventory
Rich in wild grasses numbnesses, and flowers

The prairie realm — VAST 

ocean's paraphrase —
VAST Primary Elements Overview

Proxy

- Provides user interface
- But without user interface
- Dummy traffic generator
- Anonymous proxies
- Similar to popular Java applet residing in Web

VAST Proxy Elements Concept

- Open source code of agent applet
- Secure connection between client and proxy
- Dummy traffic of dummy traffic
distributions as a source
- Web search
- Anonymity achievable versatile
- Use of free time to
- Only one proxy node
- Generation of dummy traffic
- Specific technique
Proxy Functions

- Blocking Java applets from destination Web server
- Blocking scripts and programs from destination Web server
- Blocking cookies from destination Web server

- Destination Web server
- Optional encrypting communication between VAST proxy and
  proxy – resources URL addresses among others
- Encrypting all data transmitted between VAST agent and VAST
  IP address among others
- Hiding all user's identifiable data from destination Web server

Agent Functions

- Graphical Interface
  - Presentation of source anonymity level and communication with user by
  - Resources downloaded by user and resources downloaded by simulator
  - Analysis of a level of user anonymity as a result of a proportion between
  - Generation of pages chosen by user (skipping dummy traffic pages)
  - Receiving resources from proxy, dividing resources between group of pages
  - Receiving configuration parameters from user and transmitting them to proxy
  - Generation of URL (Uniform Resource Locator) addresses as a background for
  - Simulation of URL Web activity
  - Communication with proxy server secured by SSL/TLS protocol (secure)
Illustration of traffic seen by the user

1/3

Dummy Traffic - Example

Session - will be used rest of this presentation a shorter name – other by links from transactions pages. In the transactions can be connected with each transactions generated by user – where all transactions generated from HTTP transactions.

Subject session - collection of Web session.

Graphic files (e.g. HTML files and contained elements, e.g. responses which represent a single Web requests and corresponding server response)

Web transaction - a series of HTTP client transactions.

Symbols of:

- Web transaction
- Session
- Subject session
- Web album
... but the proxy server cannot distinguish which transactions were requested by the user.

It is possible to distinguish only particular sessions...
Groups of Risk Sources

VAST Security

VAST Performance

content

Delays induced by VAST system in comparison to traditional proxy server

acceptable delays (similar to delays present in traditional anonymous proxy server)
Traffic Analysis Attacks

VAST Security and Privacy

VAST: Full protection thanks to specific dummy traffic generation mechanism

̴ timing attack

̴ message volume attack

̴ attacker: observation of the transfer volume (i.e., message volume) and correlation of input and output

̴ attacker: observation of communication time through linking of potential end points and points of correlation between beginning and/or ending of an event in each possible end point

̴ VAST: hiding based on specific architecture of proxy from the destination server’s point of view

̴ from the VAST service provider’s point of view

̴ from the others Internet users’ point of view

̴ hiding based on SSL/TLS protocol and hiding based on SSL/TLS protocol

̴ from the local environment point of view

2/2
Conclusions

Traffic Analysis Attacks

VAST Security and Analysis

- Protection against traffic analysis attacks
- Low cost of service implementation
- High performance
- Private data of users
- Disabling service provider (and all other parties) to access to
The main system features include:

- It is a comprehensive technique which overcomes weaknesses
- Distant proxy
generates dummy traffic in the relationship between local agent and
The novel idea is utilization of Web search engines resources to
versatile anonymity
VAST provides protection of Web user's privacy by granting
References

I. Margasinski, K., Zyzyszkowski, P., edn. 200
Poland
Institute of Telecommunication
Warsaw University of Technology
Igor Margasinski, Krzysztof Zyzyszkowski

Thank you for your interest!