

VAST: Versatile Anonymous System for Web Users

Igor Margasiński, Krzysztof Szczypiorski
 Warsaw University of Technology
 Institute of Telecommunications
 Poland

10th International Multi-Conference on
 Advanced Computer Systems – ACS'2003

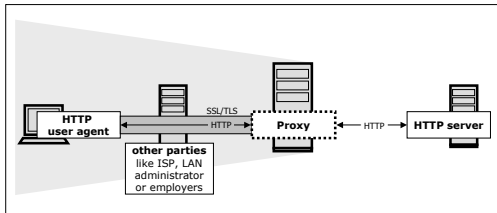
Outline

- ◆ Introduction to the current techniques of providing anonymity – state of the art
- ◆ VAST system overview
- ◆ Design and draft of the method implementation
- ◆ Performance
- ◆ VAST security analysis
- ◆ Future work

Current Solutions

1/4

- popular techniques: **Third Party Proxy Servers**



Third Party Proxy Server scheme

examples:

Anonymizer, Magusnet Proxy, Rewebber, Surfola, SafeWeb

Current Solutions

2/4

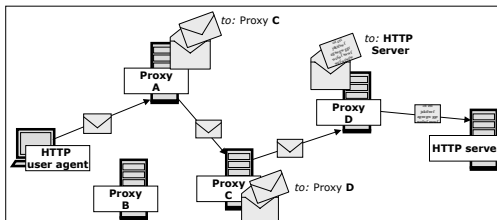
Third Party Proxy Servers

Pros / reasons for popularity	Cons / motivation to further research
<ul style="list-style-type: none"> ◆ filling the technical loop-hole in WWW system related to lack of user's privacy protection ◆ high efficiency in hiding user's identity data ◆ easy access to the service ◆ insignificant delays of Web navigation ◆ simplicity and relatively low costs required for system realization 	<ul style="list-style-type: none"> ◆ access to information about all user's Web activity ◆ centralization of information about personal Web activity ◆ possibility of tracking by traffic analysis ◆ limitation of sets of elements which can be downloaded (Java, JavaScript etc.)

Current Solutions

3/4

- safer but more theoretical techniques: **Chaining with Encryption / Adaptation of Chaum's MIXNET**



Chaining with Encryption technique scheme

examples:

Onion Routing, Crowds, Freedom ← first commercial implementation

Current Solutions

4/4

Chaining with Encryption

Pros / advantages over single proxies	Cons / reasons for unpopularity
<ul style="list-style-type: none"> ◆ decentralization of information about user's Web activity ◆ elimination of basic types of traffic analysis attacks 	<ul style="list-style-type: none"> ◆ serious delays of Web navigation ◆ possibility of proxies collaboration ◆ expensive infrastructure - high financial investments required

VAST

*The prairie realm – vast ocean's paraphrase –
Rich in wild grasses numberless, and flowers
Unnamed save in mute Nature's inventory
No civilized barbarian trenched for gain.*

— Charles Mair (1838-1927)
"Tecumseh"

VAST

Versatile Anonymous SysTem for Web Users

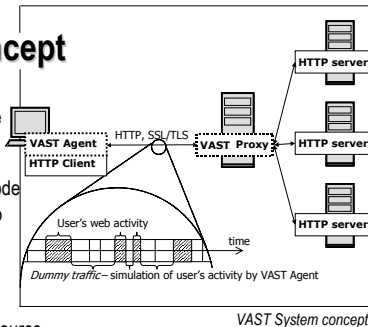
Original system developed and implemented at Warsaw University of Technology, Poland.

Main principles:

- ◆ preservation of all advantages of single third party proxy servers
- ◆ providing versatile anonymity (including service provider and also preventing risks of traffic analysis attacks)
- ◆ retention of speed (minimalization of performance differences between VAST usage and traditional browsing)
- ◆ accessibility – no additional requirements from users
- ◆ facility to implement outside laboratories – relatively low costs

VAST Concept

- ◆ Specific technique of dummy traffic generation
- ◆ Only one proxy node
- ◆ Use of free time to achieve versatile anonymity
- ◆ Web search engines and dictionaries as a source of dummy traffic
- ◆ Secure connection between client and proxy
- ◆ Open source code of agent applet



VAST System concept

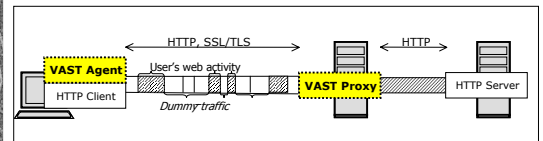
VAST Primary Elements Overview

Agent

- ◆ Java applet residing in Web browser
- ◆ dummy traffic generator
- ◆ provides user interface

Proxy

- ◆ similar to popular anonymous proxies
- ◆ but without user interface



VAST System elements

Agent Functions

- ◆ communication with proxy server secured by SSL/TLS protocol (Secure Socket Layer / Transport Layer Security)
- ◆ simulation of user Web activity
- ◆ generation of URL (Uniform Resource Locator) addresses as a background for addresses requested by user
- ◆ receiving configuration parameters from user and transmitting them to proxy
- ◆ requesting pages selected by user and pages selected by simulator
- ◆ receiving resources from proxy, dividing resources between group of pages chosen by user and dummy traffic pages
- ◆ presentation of pages chosen by user (skipping dummy traffic pages)
- ◆ analysis of a level of user anonymity as a result of a proportion between resources downloaded by user and resources downloaded by simulator
- ◆ presentation of actual anonymity level and communication with user by graphic interface

Proxy Functions

- ◆ hiding all user's identifiable data from destination Web server – IP address among others
- ◆ encrypting all data transmitted between VAST agent and VAST proxy – resources' URL addresses among others
- ◆ optional encrypting communication between VAST proxy and destination Web server
- ◆ blocking cookies from destination Web server
- ◆ blocking scripts and programs from destination Web server
- ◆ blocking Java applets from destination Web server

Dummy Traffic - Basic Definitions

- ♦ **Web transaction** – a series of HTTP client requests and correspondent server responses, which represent a single Web page (HTML files and contained elements, i.e. graphic files)
- ♦ **Subject session** – collection of Web transactions generated by user – where all transactions can be connected with each other by links from transactions pages. In the rest of this presentation a shorter name – session – will be used

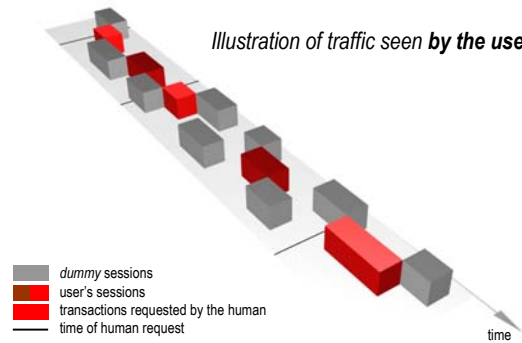


Symbols of web transaction (A) and subject session (B)

Dummy Traffic - Example

1/3

Illustration of traffic seen by the user



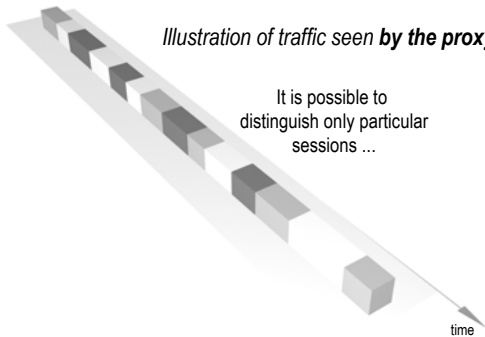
grey dummy sessions
red user's sessions
red transactions requested by the human
time of human request

Dummy Traffic - Example

2/3

Illustration of traffic seen by the proxy

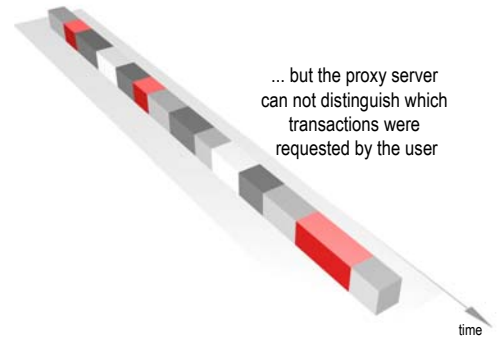
It is possible to distinguish only particular sessions ...



Dummy Traffic - Example

3/3

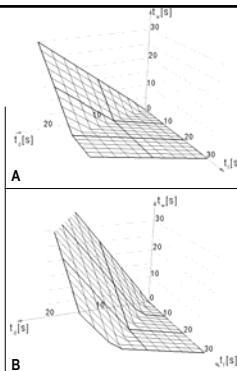
... but the proxy server can not distinguish which transactions were requested by the user



VAST Performance

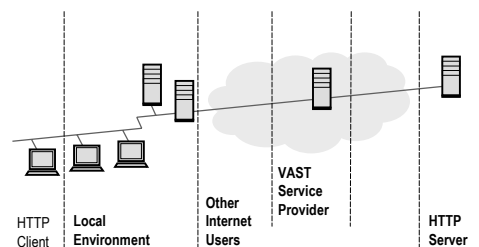
- t_d – average time of downloading of single Webpage
- t_f – average time of familiarizing with page content
- t_w – average delay in Webpage downloading induced by VAST system in comparison to traditional proxy server

acceptable delays (similar to delays present in traditional anonymous proxy server systems) occur when users spend some time ($t_{f,nt}$) familiarizing with Webpage content



Delays induced by VAST system in comparison to traditional proxy server (A – one dummy session, B – two dummy sessions)

VAST Security – Groups of Risk Sources



VAST Security in Particular Groups

- ◆ From the **local environment** point of view
 - hiding based on *SSL/TLS* protocol
- ◆ From the **others Internet users** point of view
 - hiding based on *SSL/TLS* protocol and masking based on *dummy* traffic
- ◆ From the **VAST service provider's** point of view
 - masking based on *dummy* traffic
- ◆ From the **destination Web server** point of view
 - hiding based specific architecture of proxy

VAST Security and Traffic Analysis Attacks

1/2

- ◆ **timing attack**
 - Attacker:** observation of communication time through linking of potential end points and searching for correlations between beginning and/or ending of an event in each possible end point
 - VAST:** full protection thanks to specific dummy traffic generation mechanism
- ◆ **message volume attack**
 - Attacker:** observation of the transfer volume (i.e. message volume) and correlation of input and output
 - VAST** system fills periods of user's inactivity with dummy traffic - separation of particular messages from encrypted link between agent – proxy server is then practically impossible

VAST Security and Traffic Analysis Attacks

2/2

- ◆ **flooding attack**
 - Attacker:** sending a large number of messages – flooding – or messages with certain characteristics by other system users
 - VAST** protects against this attack because of the form of the message sent to the proxy server itself. Even after an effective isolation of user's message, it is still unknown which requests are generated by machine and which come from human
- ◆ **linking attack**
 - Attacker:** long-term observation
 - VAST** does not offer an effective protection against this kind of attack; However, it is possible to enhance the VAST system and include a mechanism providing effective protection against long-term linking attack - transformation of agent Java applet into a Java program – *local* proxy

Conclusions

- ◆ VAST provides protection of Web user's privacy by granting versatile anonymity
- ◆ The novel idea is utilization of Web search engines resources to generate *dummy* traffic in the relation between local agent and distant proxy
- ◆ It is a comprehensive technique which overcomes weaknesses of existing systems
- ◆ The main system features include:
 - disabling service provider (and all the other parties) to access to private data of users
 - high performance
 - low costs of service implementation
 - protection against traffic analysis attacks

Thank you for your interest!

Igor Margasiński, Krzysztof Szczypiorski
Warsaw University of Technology
Institute of Telecommunication
Poland

e-mail: {I.Margasinski,K.Szczypiorski}@tele.pw.edu.pl

References

1. Berners-Lee, T., Fielding, R., Frystyk, H. Hypertext Transfer Protocol – HTTP/1.0. RFC 1945, 1996.
2. Chaum, D. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM, 1981.
3. Dierks T., Allen C. The TLS-Protocol Version 1.0. RFC 2246, 1999.
4. Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., Berners-Lee T. HyperText Transfer Protocol – HTTP/1.1. RFC 2616, 1999.
5. Goldberg, I., Shostack, A. Freedom Network 1.0 Architecture and Protocols. Zero-Knowledge Systems. White Paper, 1999.
6. Goldschlag, D. M., Reed, M. G., Syverson, P. F. Onion Routing for Anonymous and Private Internet Connections. Communications of the ACM, 1999.
7. Krane, D., Light, L., Gravitch D. Privacy On and Off the Internet: What Consumers Want. Harris Interactive, 2002.
8. Kristol, R., Montulli, L. HTTP State Management Mechanism. RFC 2965, 2000.
9. Martin, D., Schulman, A. Deanonimizing Users of the SafeWeb Anonymizing Service. Privacy Foundation, Boston University, 2002.
10. Reiter, M.K., Rubin, A.D. Crowds: Anonymity for Web Transactions. ACM Transactions on Information and System Security, 1997.
11. Syverson, P. F., Goldschlag, D. M., Reed, M. G. Anonymous Connections and Onion Routing. IEEE Symposium on Security and Privacy, 1997.