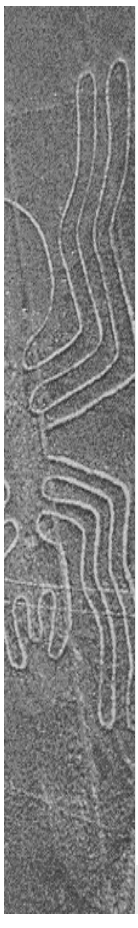
Web Privacy: an Essential Part of Electronic Commerce

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

International Interdisciplinary Conference on Electronic Commerce
ECOM-03



Outline

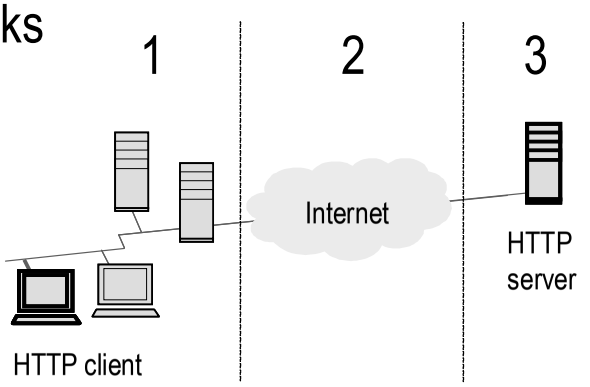
- **Privacy risks**
- **Current solutions** –

  client-side utilities, third party proxy servers, P3P, chaining with encryption
- **Our proposal**

  VAST system
- **VAST performance**

Classification of privacy risks (1/2)

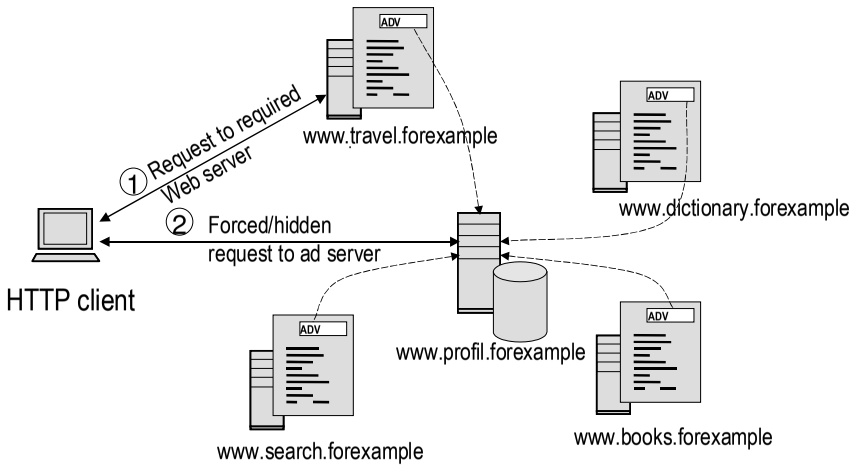
1. Internal Risks - Internet service providers, LAN administrators, employers, other third parties
2. Communication Link Originated Risks
   - *sniffing*



Three groups of privacy risks

Classification of privacy risks (2/2)

3. Web Server Originated Risks - server administrators, ad servers, banner ad networks



Web users profiling scheme

Current Solutions

- Client-side Utilities
  personal firewalls, system cleaners, cookie managers, banner ad blockers, trojan horses detectors
- Third Party Proxy Servers
  Anonymizer, Magusnet Proxy, Rewebber, Surfola, SafeWeb
- New Protocol
  Platform for Privacy Preferences Protocol
- Adaptation of Chaining with Encryption Technique
  Onion Routing, Crowds, Freedom

Vast system overview

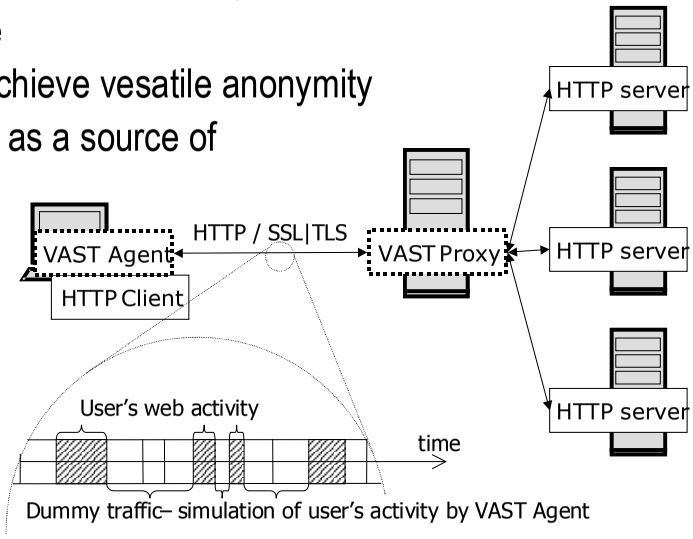
- **V**ersatile **A**nonymous **S**ys**T**em for Web Users
- Original system developed at Institute of Telecommunication, Warsaw University of Technology

*The prairie realm – **v a s t** ocean's paraphrase –*
Rich in wild grasses numberless, and flowers
Unnamed save in mute Nature's inventory
No civilized barbarian trenched for gain.

———
"Tecumseh", Charles Mair (1838-1927)

Vast concept

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



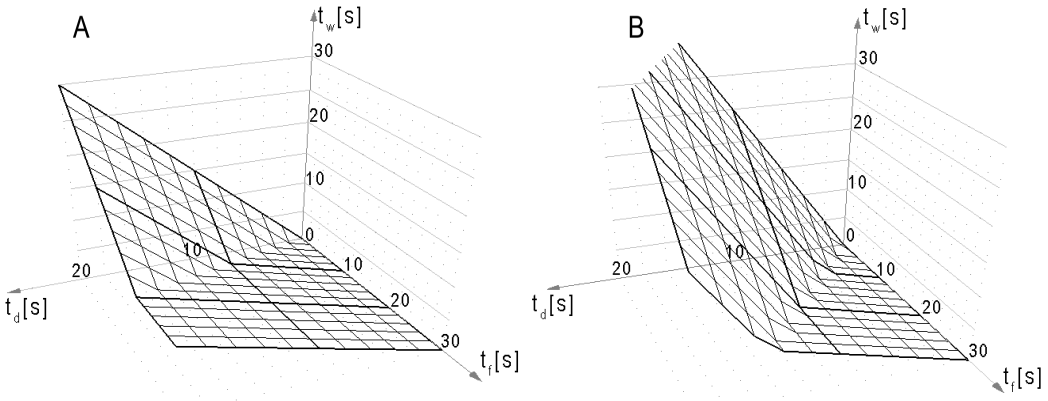
VAST system scheme

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 Webage downloading induced by VAST system in comparison to traditional proxy server



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

Summary

- Today's popular tools are not perfect
- VAST overcomes weaknesses of existing systems
- Specific *dummy traffic* generation technique may be in some cases viewed as its weakness

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 Vol. 24 no 2 (1981) 84 - 88
3. Cranor, L., Langheinrich, M., Marchiori, M., Presler-Marchall, M.: The Platform for Preferences 1.0 (P3P 1.0) Specification, W3C Recommendation (2002)
4. Dierks T., Allen C.: The TLS-Protocol Version 1.0. RFC 2246 (1999)
5. Ferneyhough, C.: Online Security and Privacy Concerns on the Increase in Canada, Ipsos-Reid (2001)
6. Fielding, R., Gettys, J.,Mogul, J., Frystyk, H., Masinter, L., Leach, P., Berners- Lee T.: HyperText Transfer Protocol – HTTP/1.1. RFC 2616 (1999)
7. Goldberg, I., Shostack, A.: Freedom Network 1.0 Architecture and Protocols. Zero-Knowledge Systems. White Paper (1999)
8. Goldschlag, D. M., Reed, M. G., Syverson, P. F.: Onion Routing for Anonymous and Private Internet Connections. Communications of the ACM Vol. 42 no 2 (1999) 39-41
9. Krane, D., Light, L., Gravitch D.: Privacy On and Off the Internet: What Consumers Want. Harris Interactive (2002)
10. Kristol, R., Montulli, L.: HTTP State Management Mechanism. RFC 2965 (2000)
11. Martin, D., Schulman, A.: Deanonymizing Users of the SafeWeb Anonymizing Service. Privacy Foundation, Boston University (2002)
12. Presler-Marshall, M.: The Platform for Privacy Preferences 1.0 Deployment Guide, W3C Note (2001)
13. Reiter, M.K., Rubin, A.D.: Crowds: Anonymity for Web Transactions. ACM Transactions on Information and System Security (1998) 66-92
14. Syverson, P. F., Goldschlag, D. M., Reed, M. G.: Anonymous Connections and Onion Routing. IEEE Symposium on Security and Privacy (1998)