中国科学院研究生院学报 2011, 28(5) 659-667 DOI: ISSN: CN:

本期目录 | 下期目录 | 过刊浏览 | 高级检索   [打印本页] [关闭]

论文

一种基于Web通信行为的抗审查隐蔽通信协议

谭庆丰, 时金桥, 郭莉, 王啸

中国科学院计算技术研究所信息安全研究中心,北京市信息内容安全技术国家工程实验室, 北京 100190

摘要:

以往基于TCP/IP协议或HTTP协议的隐蔽通信方式通常是利用协议本身各个字段的特点,将信息隐藏在协议的各个字段中.这种方式往往会具有某种结构特征,而基于计时的隐蔽通信又往往具有某种流模式.基于非对称通信理论和马尔科夫模型的Web行为预测,提出一种基于Web通信行为的抗流量审查隐蔽通信协议.重点描述隐蔽通信协议和原型系统,并分析协议的安全性.测试结果表明,该方法具有很高的效率和安全性.

关键词: 隐蔽通信 抗审查 Web通信行为

A censorship-resistant covert communication protocol based on Web communication behavior

TAN Qing-Feng, SHI Jin-Qiao, GUO Li, WANG Xiao

Information Security Research Center, Institute of Computing Technology, Chinese Academy of Sciences; Chinese National Engineering laboratory for Information Security Technologies, Beijing 100190, China

Abstract:

The existing covert communication method based on TCP/IP or HTTP often utilizes characteristics of protocol and hides extra data in specific fields of protocol header. Such a method leaves some obvious signatures. However, timing-based covert communications have some kind of traffic pattern. We propose a censorship-resistant covert communication protocol based on Web communication behavior, which combines dynamic asymmetric communication and Markov model-based Web usage prediction. In this paper we focus on covert communication protocol, prototype system, and security of the protocol. The test results show that our method has high performance and safety.

Keywords: covert communication censorship-resistant Web communication behavior

收稿日期 2010-08-07 **修回日期** 2010-11-07 **网络版发布日期**

DOI:

基金项目:

国家重点基础研究发展计划(973)项目(2007CB311100)资助

通讯作者:

作者简介:

作者Email: tanqingfeng@software.ict.ac.cn

扩展功能

本文信息

- Supporting info
- PDF(998KB)
- [HTML全文]
- 参考文献[PDF]
- 参考文献

服务与反馈

- 把本文推荐给朋友
- 加入我的书架
- 加入引用管理器
- 引用本文
- Email Alert
- 文章反馈
- 浏览反馈信息

本文关键词相关文章

- 隐蔽通信
- 抗审查
- Web通信行为

本文作者相关文章

PubMed

参考文献:

[1] Handel T, Sandford M. Hiding data in the OSI network model // Anderson R. Information Hiding Workshop (IH 1996). Cambridge, UK: Springer, LNCS, 1996, 1174: 23-38.

[2] Murdoch S, Lewis S. Embedding covert channels into TCP/IP //Proc 7th Information Hiding Workshop. 2005.

[3] Cabuk S, Brodley C, Shields C. IP covert timing channels: Design and detection // Proceedings of the 2004 ACM Conference on Computer and Communications Security. 2004.

[4] Anonymizer . http://www.anonymizer.com.

[5] Dingledine R, Mathewson N, Syverson P. Tor:the second-generation onion router // Proceedings of the 13th USENIX Security Symposium. 2004.

[6] JAP Anonymity & Privacy . http://anon.inf.tu-dresden.de/.

[7] I2P Anonymous Network . http://www.i2p2.de.

[8] Adler M, Maggs B. Protocols for asymmetric communication channels // Proceeding of 39th IEEE Symposium on Foundations of Computer Science(FOCS). Palo Alto, CA, 1998.

[9] Gagie T. Dynamic asymmetric communication
[J]. Information Processing Letters, 2008, 108(6):352-355.

[10] Feamster N, Balazinska M, Harfst G, et al. Infranet: circumventing Web censorship and surveillance //Proceedings of the 11th USENIX Security Symposium. 2002:247-262.

[11] Xing D S, Shen J Y. A new Markov model for Web access prediction
[J]. Computing in Science and Engineering, 2002, 4(6):34-39.

[12] Brian, Davison D. Learning Web request patterns //Web Dynamics: Adapting to Change in Content, Size, Topology and Use. Springer, 2004:435-460.

[13] Deshpande M, Karypis G. Selective Markov model for prediction Web page access
[J]. ACM Transaction on Internet Technology, 2004, 4(2):163-184.

本刊中的类似文章