Poster Proposal: Protecting Query Privacy in Censorship Resistant Publication

Stan Gurtler*, Miti Mazmudar, and Ian Goldberg

University of Waterloo, Waterloo, ON N2L 3G1, Canada
{tmgurtler, miti.mazmudar, iang}@uwaterloo.ca

Abstract. From concerns over outright blocking of materials (such as with the Great Firewall of China) to tamper-resistance against adversaries who may seek to alter materials, censorship resistance at large seeks to solve the problem of access to materials which adversaries may attempt to prohibit. In particular, censorship resistant publication schemes such as CROPS [2] allow for publishers to produce material in a manner that censors are unable to take down, tamper with, or pressure a server to do the same. However, censorship resistant publication schemes to this point largely do not consider a censor's ability to put pressure on users themselves, to prevent them from seeking any such materials. If a censor can easily learn that a user within their reach attempts to access sensitive materials, the censor can enact punitive measures on such users for having accessed these materials, regardless of the censor's ability to directly prevent the access to the material. Until users are protected and guaranteed the ability to freely access materials, a document cannot be considered censorship resistant. To this end, we modify existing censorship resistant publication systems such that even malicious nodes acting as part of the system will learn nothing about the content of the queries that any user makes. This is done through a novel application of information-theoretic private information retrieval, used in combination with robust communication protocols [1] from previous work. This, when used with other techniques like Tor, gives the guarantee that a user may retrieve information from a publication system such that no censor can observe (or pressure a node into revealing) what they are retrieving.

Keywords: Censorship resistant publication · Private information retrieval · Distributed hash tables · Query privacy.

References

1. Backes, M., Goldberg, I., Kate, A., Toft, T.: Adding query privacy to robust DHTs. In: Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security. pp. 30–31. ASIACCS '12, ACM, New York, NY, USA (2012)
2. Vasserman, E.Y., Heorhiadi, V., Hopper, N., Kim, Y.: One-way indexing for plausible deniability in censorship resistant storage. In: Proceedings of the 2nd USENIX Workshop on Free and Open Communications on the Internet. USENIX, Bellevue, WA (2012)

* Presenting author