Poster: Incentivized Censorship Resistance with Payment Contracts

Cecylia Bocovich, John A. Doucette, Ian Goldberg
University of Waterloo, School of Computer Science
{cbocovic, j3doucet, iang}@uwaterloo.ca
Waterloo, Ontario N2L 3G1, Canada

***Abstract*—We propose Lavinia, a censorship resistant publishing system that incentivizes document storage through the use of an anonymous, distributed, time-locked payment system. This has the advantage of allowing the publisher to decide whether a document is worth storing, and for how long, instead of relying on public interest or an appointed editorial board. We give a description of related work in censorship resistant publishing and the incentives in our system for honest participation with the use of payment contracts.**

I. Introduction

Censorship of information is a long-standing problem that has often been countered by technological solutions. The printing press was the first such innovation, and a notable feature of the technology was that, in principle, any individual could produce and disseminate many copies of whichever documents they preferred. The only important impediment to using a printing press was the acquisition of enough capital to purchase the requisite raw materials and labour. As noted by Anderson [1], modern technologies like the Internet have in some significant way regressed from this model. Although the Internet has made the distribution and mirroring of content easier and more cost effective than physical printing, it is also much easier to control. For example, China's great firewall [2] is a much more practical censorship strategy than searching the contents of every physical document entering a country. The Digital Millennium Copyright Act in the United States similarly provides an extremely flexible and versatile tool for commercial interests to censor digital content from the web [3].

Anderson's eternity service [1] outlines a conceptual framework for building censorship-resistant publishing systems in the context of modern digital communications. However, despite myriad attempts to build similar systems, many of which *do* provide strong censorship resistance, we are still removed from the model of the printing press: existing systems impose barriers above and beyond simply paying for the needed raw materials and labour.

We propose a new censorship resistant publishing model: one that attempts to realize a proper digital printing press akin to Anderson's eternity service. Our new system allows a publisher to issue payments that ensure widespread availability of a document, without requiring any further action. We expand on previous work on censorship resistance to provide anonymity and plausible deniability for participating servers, and make use of recent innovations in cryptocurrencies [4] to provide additional incentives that strengthen the robustness of our system and encourage honest participation.

II. Related work

There have been many attempts to realize the eternity service. One such attempt is Publius [5]. Content in Publius is stored on a static, predetermined set of servers as an encrypted document and a set of key shares. The content can be deleted and updated with a password known to the original publisher. Despite the usefulness of update functionality, this additional feature presents a significant risk to the publisher, because it creates a strong incentive for censors to determine the original publisher's identity and force them to take down the document. Additionally, Publius' centralized design is vulnerable to censorship by government agencies; shutting down a predetermined set of servers is sufficient to shut down the service.

Dagster [6] and Tangler [7] take an alternative approach to censorship resistance by 'tangling' content together, so that removal of a censored document renders a large number of unrelated documents unreadable. This system also provides servers with plausible deniability of the content they are hosting, making them less susceptible to coercion and "rubber-hose" attempts to drop content.

Freenet [8] is a popular censorship resistant system that uses decentralization to mitigate the possibility of government crackdowns. Servers in Freenet each donate storage space and act as nodes in the system, caching and serving content as it is requested. The mechanics of Freenet that make it efficient cause more popular (i.e., more frequently accessed) documents to be cached, and less popular documents to be dropped from the system. This scenario is not ideal for censorship resistance, as popular documents may not be in as high a need for censorship resistance as unpopular content.

Free Haven [9] is an alternative decentralized design that allows unpopular content to remain available in the face of powerful censors. This system stores secret shares of a document on a collection of servers, called the servenet. These shares are associated with a with a keyword, $H(PK_{doc})$ accessible by broadcasting a request for this key to the entire servenet. Each server maintains plausible deniability of the content they are hosting, and a level of anonymity through the use of an anonymous communication channel. The novel reputation system Free Haven employs holds servers accountable for maintaining and serving document shares, and a trading system encourages honest participation by allowing servers to decide which documents they are comfortable with hosting and hand off documents that may be in danger to a server better suited to the task.

The system most closely related to ours is the Censorship Resistant Overlay Publishing System (CROPS) [10], which uses a secure distributed lookup system to store shares of documents across a large set of users. Individual servers lack sufficient information to reconstruct the content stored on their machines. At the same time, CROPS allows outside users to retrieve documents quite easily by querying the system with only a single keyword. Like Freenet however, CROPS does not properly incentivize users to provide storage to the network. When deletion decisions must be made, CROPS uses curated garbage collection to prevent the deletion of important, yet unpopular documents. This still does not realize a digital printing press akin to Anderson's goals [1]. Users cannot store content that the editorial board deems to be uninteresting or offensive, unless it is also popular.

III. Our Contribution

We introduce Lavinia, an improved design for a censorship-resistant publishing system. Lavinia uses an audit-payment system to ensure document availability for arbitrary storage times and to encourage honest participation. Its decentralized design provides anonymity, plausible deniability for participating servers, and resistance to powerful government censors.

Lavinia's design stems from that of CROPS [10]; however, we eliminate the need for garbage collection and an editorial board by providing economic incentives for the prolonged storage of unpopular content. In place of the editorial board, we introduce a content-oblivious audit system that rewards servers for producing document shares, and auditors for ensuring document availability.

A publisher incentivizes the system to keep her document by constructing payment contracts for each document share. She constructs a contract for each share D_i, at each time t_j she wishes her document to be checked for availability. For example, she might decide that she wishes her document to be checked for availability once a month for 2 years. She must then construct 24 contracts for each document share she uploads to the system. These contracts will be distributed amongst special participants in the system, known as auditors, and will reimburse both the server responsible for hosting the share, and the auditor responsible for ensuring its availability for the current time period.

To ensure that her document is audited during each time period, we need a way of time-locking these payments. The server and auditor should not be paid before each time period begins, and they should not be able to audit the document ahead of time. To accomplish this, we use a combination of bitcoin's built-in time-lock feature [4] and sequences of temporary bitcoin addresses for each document share. In order for the auditor at time t_j to unlock the bitcoin signing key for their temporary account, they must have information from the bitcoin transaction posted by the previous auditor at time t_{j-1}.

We enforce the timed release of information with the time-lock feature in bitcoin. The auditor at time t_{j-1} cannot move their bitcoins from the temporary account to their own personal account until time t_{j-1} has passed. Upon posting this transaction, they are required by the bitcoin scripting language to release information to the next auditor at time t_j that unlocks the latter's temporary account. With the knowledge gained from this transaction, the next auditor in the sequence is able to compute the private key for their own temporary account and perform an audit of the document share. Each auditor is incentivized to keep the information necessary to perform the next audit a secret until their audit time; if they release it ahead of time, they run the risk of compromising their private account and forfeiting their payment to the next auditor in the sequence. Conversely, if they wait until they are allowed to move their bitcoins to a private account, their payment will be safe from the next auditor with high probability.

There are some challenges with this method. The dependence on an auditor for a previous time period introduces a vulnerability in our scheme. If an auditor at time t_j fails to complete their transaction, all auditors following will be unable to perform their audit and receive remuneration for their work. This would eventually result in the document share being dropped from the system. We address this problem by constructing burn scripts. Auditors have the ability to burn bitcoins from the previous audit and their own, receiving a fraction of the funds they would normally receive. This allows the next auditor in the chain to resume business as usual, and ensures the document remains in the system.

IV. Evaluation

Although not shown here, we have proved that the self-interest of servers and auditors results (game theoretically) in normal, honest execution of the Lavinia protocol. We also show that our system is secure against a subset of malicious users. We are currently in the process of a proof-of-concept implementation to provide data on the efficiency and robustness of our system.

References

[1] R. Anderson *et al.*, "The Eternity Service," in *Pragocrypt 1996*, 1996, pp. 242–252.

[2] P. Winter and S. Lindskog, "How the Great Firewall of China is blocking Tor," in *Proceedings of the 2nd USENIX Workshop on Free and Open Communications on the Internet*, 2012.

[3] J. M. Urban and L. Quilter, "Efficient Process or Chilling Effects—Takedown Notices under Section 512 of the Digital Millennium Copyright Act," *Santa Clara Computer & High Tech. LJ*, vol. 22, p. 621, 2005.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008, [Online]. Available: http://bitcoin.org/bitcoin.pdf.

[5] M. Waldman, A. D. Rubin, and L. F. Cranor, "Publius: A robust, tamper-evident, censorship-resistant, web publishing system," in *9th USENIX Security Symposium*, 2000, pp. 59–72.

[6] A. Stubblefield and D. S. Wallach, "Dagster: Censorship-resistant publishing without replication," Houston, TX, USA, Tech. Rep. TR01-380, 2001.

[7] M. Waldman and D. Mazieres, "Tangler: a censorship-resistant publishing system based on document entanglements," in *Proceedings of the 8th ACM conference on Computer and Communications Security*. ACM, 2001, pp. 126–135.

[8] I. Clarke, O. Sandberg, B. Wiley, and T. W. Hong, "Freenet: A distributed anonymous information storage and retrieval system," in *Designing Privacy Enhancing Technologies*. Springer, 2001, pp. 46–66.

[9] R. Dingledine, M. J. Freedman, and D. Molnar, "The Free Haven Project: Distributed Anonymous Storage Service," in *In Proceedings of the Workshop on Design Issues in Anonymity and Unobservability*, 2000, pp. 67–95.

[10] E. Y. Vasserman, V. Heorhiadi, Y. Kim, and N. Hopper, "Censorship resistant overlay publishing," Minneapolis, MN, USA, Tech. Rep. 11-027, 2011.