Publius (publishing system)

Publius was an attempted communication protocol developed by Lorrie Cranor, Avi Rubin and Marc Waldman to give individuals the ability to publish information on the web anonymously and with a high guarantee that their publications would not be censored or modified by a third party. The experiment terminated sometime in 2001 with no significant results. The name of the system was chosen to reflect the joint pen name of the authors of *The Federalist Papers*.[1]

Design goals

The nine design goals of the Publius development team were:[2]

- Censorship resistance: decreasing the chance that a third party will manage to modify or delete the published materials.
- Tamper evident: unauthorized changes are traceable.
- Source anonymous: there is no way to tell who published the material once it is available on the web.
- Updatable: publishers are allowed to modify or delete their material.
- Deniable: third parties participating in publishing the materials lacks the responsibility for the hosted content.
- Fault tolerant: system should function even when some involved third parties are faulty or malicious.
- Persistent: there is no expiration date for published materials.
- Extensible: support for future protocol extensions or growth in the number of publishers.
- Freely available: all software tools required for the system should be out of charge.

Technical details

The Publius web system consisted of the following agents:

- Publishers - participants who publish their content on the web.
- Servers - which host the publishers' content on the web (considered as part of the third parties).
- Retrievers - participants who browse the web content published by the publishers.

Publius limited file sizes to 100 kilobytes.[3][4] Files on Publius could reference other files, allowing users to upload works larger than 100 kilobytes, if the file format allowed it (e.g., upload HTML, PDF, or PostScript files referencing outside images or fonts).

The Publius system relied on a static list of web servers. When a publisher wished to add a piece of content to the Publius network, publisher first encrypted it using a random 100 kilobyte symmetric key. This key was split into parts such that a minimum number of shared parts were required for the reconstruction of the content (see also Secret sharing).

Reception

The system opened in July 2000 for a two-month trial.[5] The system was intended to make censorship by governments more difficult by spreading parts of documents among multiple decentralized locations[5] and as such was a forerunner of later file sharing systems. The issues those later systems had with copyright violations and objectionable content were also foreseen with Publius.[6][3] The ability of the system to distribute communication content without allowing for restriction or identification of the original uploader was called destabilizing.[7]

The system encrypts a document and divides it into fragments, or keys, that reside on multiple randomly selected servers. Though the document can be split into many keys, only a few are required to reconstruct the document so the information can be decrypted and viewed.

During the trial period, Publius project had 50 computers in their network, including servers at the Center for Democracy and Technology and Xerox PARC.[4]

The project hasn't been updated since the initial trial.[1]

References

1. Waldman, Marc; Rubin, Aviel D.; Cranor, Lorrie Faith. "Publius Censorship Resistant Publishing System" (https://cs.nyu.edu/~waldman/publius/) . Retrieved 26 November 2019.
2. Waldman, Marc; Rubin, Aviel D.; Cranor, Lorrie Faith (2000). *Publius: A robust, tamper-evident, censorship-resistant, web publishing system* (https://www.usenix.org/legacy/publications/library/proceedings/sec2000/waldman.html) . 9th USENIX Security Symposium (https://www.usenix.org/legacy/publications/library/proceedings/sec2000/) . Session Chair: Ian Goldberg.
3. "New software promotes online anonymity" (https://web.archive.org/web/20000815065624/http://www.techserver.com/noframes/story/0,2294,500223018-500319451-501797953-0,00.htm

l) . 2000-08-15. Archived from the original (http://www.techserver.com/noframes/story/0,2294,500223018-500319451-501797953-0,00.html) on 2000-08-15. Retrieved 2021-04-18.

4. "Peer-to-Peer - We've Only Just Begun" (https://web.archive.org/web/20011217091230/http://www.thestandard.com/article/display/0,1151,17757,00.html) . 2001-12-17. Archived from the original (http://www.thestandard.com/article/display/0,1151,17757,00.html) on 2001-12-17. Retrieved 2021-04-18.
5. Sorid, Daniel (26 July 2000). "Divided Data Can Elude the Censor" (https://archive.nytimes.com/www.nytimes.com/library/tech/00/07/circuits/articles/27next.html) . *New York Times*. Retrieved 26 November 2019.
6. Akin, David (4 July 2000). "Censor-resistant Web system raises thorny questions: Online publishing: Publius system may lead to anonymous Web content". *National Post*.
7. Gibbs, W. Wayt (October 2000). "Speech without Accountability". *Scientific American*. London: Springer Nature.