Riffle (anonymity network)

Riffle is an anonymity network developed by researchers at MIT and EPFL as a response to the problems of the Tor network.

Riffle employs a privacy-enhancing protocol that provides strong anonymity for secure and anonymous communication within groups. The protocol is designed using the anytrust model, which ensures that even if colluding servers attempt to compromise the privacy of the group, they cannot do so if at least one server in the group is honest.[1]

Like Tor, it utilizes onion routing.[2] According to MIT's Larry Hardesty, researchers at MIT and the Qatar Computing Research Institute demonstrated a vulnerability in Tor's design.[3]

To achieve its goals, Riffle implements two distinct protocols: the Hybrid Shuffle protocol for sending and Private Information Retrieval (PIR) for receiving.[4]

For sending information, Riffle uses a hybrid shuffle, consisted of a verifiable shuffle and a symmetric-key algorithm. The Hybrid Shuffle protocol consists of a setup phase and a transmission phase. During the setup phase, a slow verifiable shuffle based on public key cryptography is used, while an efficient shuffle based on symmetric key cryptography is used during the transmission phase.[4] Messages sent over Riffle are not forwarded if they have been altered by a compromised server. The server has to attach proof in order to forward the message. If a server encounters unauthenticated messages or different permutations, it exposes the signed message of the previous server and runs the accusation protocol to ensure verifiability without requiring computationally intensive protocols during transmission phases.[4]

For receiving information it utilizes multi-server Private Information Retrieval. All servers in the system share a replicated database, and when a client requests an entry from the database, they can cooperatively access it without knowing which entry they are accessing.[4]

The main intended use-case is anonymous file sharing. According to the lead project researcher, Riffle is intended to be complementary to Tor, not a replacement.[5]

See also

- Anonymous web browsing
- Internet censorship circumvention

- Internet privacy
- Onion routing
- Tor (anonymity network)
- RetroShare

References

1. Uchill, Joe (2016-07-11). "Researchers tout new anonymity network" (https://thehill.com/policy/cybersecurity/287255-researchers-tout-new-anonymity-network) . *TheHill*. Retrieved 2021-02-12.
2. Francisco, Iain Thomson in San. "Meet Riffle, the next-gen anonymity network that hopes to trounce Tor" (https://www.theregister.com/2016/07/13/riffle_next_gen_anonymity/) . *www.theregister.com*. Retrieved 2021-02-12.
3. Larry Hardesty (11 July 2016). "How to stay anonymous online" (https://news.mit.edu/2016/stay-anonymous-online-0711) . MIT News.
4. Kwon, Albert; Lazar, David; Devadas, Srinivas; Ford, Bryan (1 April 2016). "Riffle: An Efficient Communication System With Strong Anonymity" (http://people.csail.mit.edu/devadas/pubs/riffle.pdf) (PDF). *Proceedings on Privacy Enhancing Technologies*. **2**: 115–134. doi:10.1515/popets-2016-0008 (https://doi.org/10.1515%2Fpopets-2016-0008) . hdl:1721.1/128773 (https://hdl.handle.net/1721.1%2F128773) .
5. "Building a new Tor that can resist next-generation state surveillance" (https://arstechnica.com/information-technology/2016/08/building-a-new-tor-that-withstands-next-generation-state-surveillance/) . *Ars Technica*. 2016-08-31. Retrieved 2021-02-12.

External links

- Riffle code at GitHub (https://github.com/kwonalbert/riffle)

This Internet-related article is a stub. You can help Wikipedia by expanding it (https://en.wikipedia.org/w/index.php?title=Riffle_(anonymity_network)&action=edit).