DeSyPs

A decentralized, sybil-resistant, pseudonymous online discussion platform

Sebastian Friebe, Martin Florian
Institute of Telematics
Karlsruhe Institute of Technology
{friebe,florian}@kit.edu

Problem domain: privacy, sybil-resistance, censorship-resistance, peer-to-peer connectivity

1 Presented technologies

DeSyPs is a decentralized, sybil-resistant, pseudonymous online discussion plattform. It is a prototype application that showcases the individual building blocks *Peer-Tor-Peer* (PTP) [1] and *BitNym* [2].

1.1 BitNym

BitNym is a trusted-third-party-independent and sybil-resistant pseudonymization and pseudonym change system. It is is based on the use of cryptocurrency blockchains as general-purpose, append-only bulletin boards. More specifically, it leverages the security of the Bitcoin [3] network.

The issuing of pseudonyms is an established approach for protecting the privacy of users while limiting access and preventing sybil attacks. To prevent pseudonym deanonymization through continuous observation and correlation, frequent and unlinkable pseudonym changes must be enabled. Unlike BitNym, established approaches for realizing sybil-resistant pseudonymization and pseudonym change are either inherently dependent on trusted third parties or involve significant computation overhead at end-user devices.

1.2 Peer-Tor-Peer (PTP)

PTP is a Java library that enables the rapid development of peer-to-peer applications for Android devices and desktop systems. In addition to enabling non-local peer-to-peer connectivity even in the presence of restrictive middleboxes, PTP realizes the pseudonymity, undetectability, confidentiality, integrity and authenticity of resulting communication channels.

PTP uses Tor [4], which is an infrastructure-based mix network, i.e., anonymization is provided by a network of dedicated relays (often high-bandwidth servers) that are reachable from the public Internet (i.e., are not firewalled or behind NAT). Using Tor hidden services, users can become reachable via the Tor network without disclosing their true IP address. For registering hidden services and accepting connections, only outbound connections must be made by clients. Thus, using hidden services, peers are able to connect to each other independently of any restrictive firewalls or NAT middleboxes, as long as outbound connections to Tor relays are possible. This is highly relevant in currently deployed cellular networks where the establishment of direct communication links between users is often impossible. PTP provides a comfortable abstraction for Tor and Tor hidden services and handles tasks like (peudonymous) authentication, message serialization and multiplexing, connection managament and message retransmission.

2 What will be demonstrated?

DeSyPs is a decentralized and pseudonymous online discussion platform. The application can be used to take part in discussions created by other users or to start own discussions. These discussions are designed as chat rooms in which all users are able to participate. In addition to contributing to the discussion via text messages, participants can use the integrated poll feature to vote on relevant topics. All of these interactions are also open to the demonstrators' audience. To demonstrate a more realistic multiple-user use case, several automatic chat bots are permanently engaged in a DeSyPs discussion, to which audience members can contribute.

The communication between DeSyPs participants takes place over a peer-to-peer network realized through the PTP library. Due to this, all communication is protected so that attackers can't determine which participant takes part in which discussions. Furthermore, the decentralized design provides censorship-resistance since no single individual is able to impede the participation of other users or censor the discussion or resulting votes.

Without protecting a platform like DeSyPs using additional measures, attackers could launch sybil attacks by using numerous sybil identities, influencing discussions and distorting votes. To provide sybil-resistance while maintaining its decentralized nature, DeSyPs uses the BitNym system. Participants in discussions have to possess a valid BitNym pseudonym created and verifiable by BitNym. To provide anonymity, the pseudonyms can be mixed an arbitrary number of time before being used in DeSyPs.

For the demonstration, relevant parts of the Bitcoin (testnet) blockchain are visualized on an additional monitor. The visualization displays the blocks which store pseudonyms, when the pseudonyms have been created and with which pseudonyms they have been mixed since then to increase the anonymity set. The audience is able to interact with this visualization by selecting single pseudonyms, which highlights the pseudonyms that have been mixed into the selected pseudonym. It can be observed that even when the original owners of the pseudonyms are known, it is not possible to determine which of the highlighted pseudonym owners is the current owner of the selected pseudonym.

3 Technical details

State of the software:

- PTP is feature complete and can be used in other applications. Development of improvements is still ongoing. Note that there hasn't been an independent security audit of the software, so an application in security- and privacy-critical scenarios is not advised.
- BitNym exists as a proof-of-concept prototype. A generically usable library and API is currently in development. When finished, the library will allow other applications to use the features provided by BitNym, i.e., sybil-resistant pseudonym registration, validation and mixing.
- DeSyPs is a prototype application developed mainly to showcase PTP and BitNym.

Platform requirements:

- PTP: Java VM, working Tor client, Internet connectivity (tested on Ubuntu Linux, Windows and Android)
- BitNym prototype: Java VM, Internet connectivity (tested on Ubuntu Linux)
- BitNym visualization: Modern web browser
- DeSyPs: Java VM, desktop manager, working PTP and BitNym (tested on Ubuntu Linux)

Envisioned licensing scheme for all demo components: LGPL (open for discussion)

4 References

References

[1] Martin Florian, Timon Hackenjos, and Simeon Andreev. Peer-tor-peer. https://github.com/kit-tm/ptp.

[2] Martin Florian, Johannes Walter, and Ingmar Baumgart. Sybil-resistant pseudonymization and pseudonym change without trusted third parties. In *Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society*, WPES '15, pages 65–74, New York, NY, USA, 2015. ACM.

[3] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. http://nakamotoinstitute.org/bitcoin/, October 2008.

[4] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th Conference on USENIX Security Symposium - Volume 13*, SSYM'04, pages 21–21, Berkeley, CA, USA, 2004. USENIX Association.