A Browser-based Secure P2P Framework for Decentralized Online Social Networks

Andreas Disterhöft
Technology of Social Networks
University of Düsseldorf
Universitätsstr. 1, 40225 Düsseldorf, Germany
Email: disterhoeft@cs.uni-duesseldorf.de
Telephone: +49 211 81-14049

Kalman Graffi
Technology of Social Networks
University of Düsseldorf
Universitätsstr. 1, 40225 Düsseldorf, Germany
Email: graffi@cs.uni-duesseldorf.de
Telephone: +49 211 81-11692, Fax: +49 211 81-11638

***Abstract*—Online social networks figured out to be the main tool to communicate in the Internet. While current centralized solutions suffer from censorship, privacy violations and unwanted marketing of the users data, decentralized solutions, e.g. based on p2p technology, promise to overcome these limitations. The downside of p2p solutions is the need to install additional software, which is nowadays not accepted by users which are used to web-based applications. With WebRTC, standard browsers can communicate directly, which allows to construct secure p2p overlays. We present our WebRTC-based p2p framework with a social network application on top, which uses a heavily modified version of OpenChord to provide a decentralized public key infrastructure, secure communication patterns and a set of building blocks to create a social network. Our prototype application proved its efficiency in a real world scenario and can now be reached via webp2p.cs.uni-duesseldorf.de.**

I. Motivation

In these days the topic of surveillance is ubiquitous, mainly because of the insights through the classified information from the National Security Agency, the NSA, leaked by Edward Snowden. Current applications like Facebook and WhatsApp, which offer communication over the Internet, can be easily monitored and / or are defeatable, mainly as a client / server architecture is used. Those centralized solutions dominate in the Internet and their providers are using the user's data for marketing purposes and also have an obligation to hand over information to national security organizations.

In contrast to the client / server architecture a peer-to-peer (p2p) solution provides direct communication between users without any centralized instance and is able to scale with increasing number of participants as their storage capacity, computation power and bandwidth is shared among others. One viable option to prevent surveillance is the use of secured p2p networks. Unfortunately, current solutions such as LifeSocial [1], PeerSoN [2] or Safebook [3] come with the limitation that potential users have to install software, which already might be a barrier. Such a barrier hinders users from testing a p2p software and limits the grow of the user base.

With the introduction of WebRTC it is possible to establish an encrypted direct multimedia communication between browser instances. So this creates the opportunity to accomplish secured p2p networks based on browsers without the need of installing additional software, as popular browsers like Chrome and Firefox already implement WebRTC. In addition, client-side software updates are not necessary as the latest code in form of HTML5 and JavaScript files is retrieved or updated on refreshing the web page. Various sources might host the software.

All in all with the help of WebRTC a framework based on a p2p overlay can be and was created, which is user-friendly and can not be monitored by third parties. In Section II we want to briefly present our realization of this concept. Section III gives a short state of our software, points out which features are implemented and states what exactly we demonstrate.

II. Demonstrator

In this section, we concisely present and point out the main features of our web-based p2p framework. Figure 1 shows the modular structure of the software, which comprises of five elements: (1.) the communication layer for p2p networking, termed Web-Open-Chord, (2.) the application layer providing a basic layer and (3.) selected social networking applications such as a friend list, a video chat and a storage-supported chat. A graphical user interface (4.) is used for interaction as well as a (5.) monitoring component is active to create performance evaluation information for debugging and scientific purposes.

A. Web-DHT-Overlay Module

The main part of the software is the Web-DHT-Overlay Module, which contains the p2p overlay logic and the basic application support. This module's task is to establish direct browser-to-browser connections, use these connections to implement a Chord DHT and provide all security related functions, such as authentication, secure communication and access control. We decided to use the *PeerJS* library at the communication layer which encapsulates the WebRTC API and provides an easy access to WebRTC features like establishing connections to remote peers supported by rendezvous nodes and start data transmission or audio/video (AV) streaming. This is used by our heavily modified version of OpenChord to provide a full decentralized overlay, churn handling, security, robustness and a usable basis for social applications on top. As we extended the open source implementation of OpenChord, our software is also distributed under GNU GPL v2. One of the the most crucial changes is the use of asymmetric cryptography in order to apply public key as the *Chord ID*. The public key is derived deterministically from the user name and password as proposed in [4]. Among others, this change resulted in the

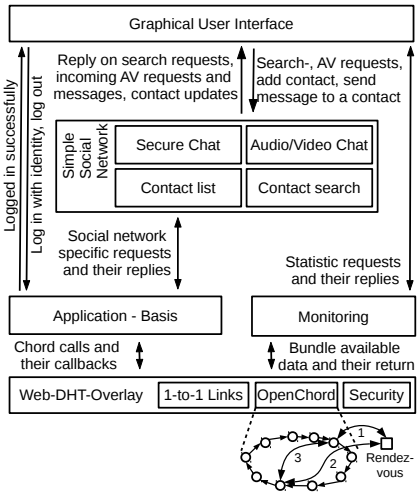

Fig. 1. Architecture

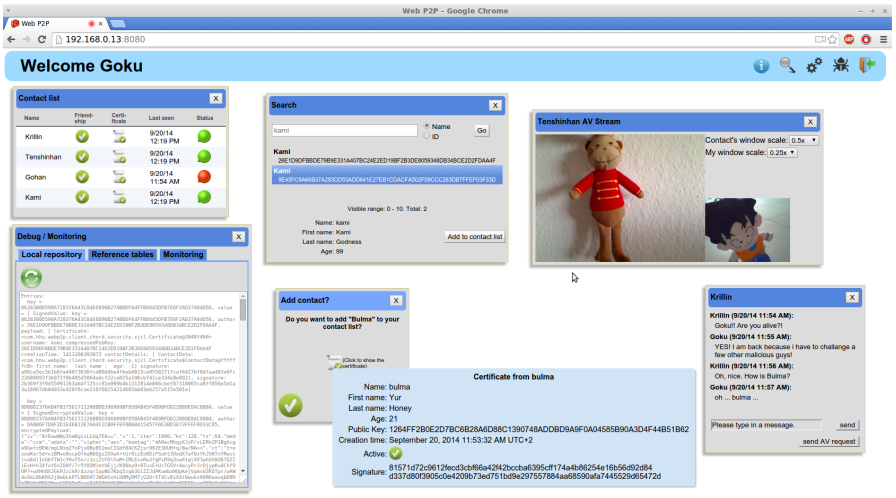

Fig. 2. Window-based GUI

ability to send encrypted messages by using the receiver's public key and create a signature, which the receiver can verify. To support user search in the Chord ring, we introduced self-signed certificates which each peer has to store at well-defined places in the DHT. So the user search is equivalent to the search of a user's certificate. An implemented access control mechanism of the DHT entries ensures that for example none of the certificates are overridden by unauthenticated users.

B. Monitoring Module for Performance Evaluation Purposes

To keep track of performance statistics, we introduced the monitoring layer. Each message carries all information necessary for monitoring statistics on the bandwidth utilization, hop count, delay, message type and nodes involved in routing. Please note, that the automatically aggregation and gathering of statistics is only active during the evaluation of our prototype.

C. Application Coordination Module

The application module is the entry point, supporting the coordination / multiplexing of multiple applications on top of the overlay. Its task is to instantiate and coordinate the other modules, loading the configuration on startup and forwarding social communication requests to the Chord module. This configuration is loaded from the web-server in order to keep all joining peers up-to-date. Please note, that the web-server is not an essential part of the system. Several web-servers might host the code. Once the configuration is obtained, all other modules are loaded.

D. Simple Social Networking Module

The simple social networking module currently contains four sub-modules: contact management, contact search, secure single chat and audio / video chat. The contact management provides information about the contacts of a user, namely the user name, corresponding public key, time last seen, online status and accepted friendship flag. In order to have the contacts and chat logs consistently available from any device, the contact list is saved as an encrypted DHT entry every few (configurable) minutes and whenever the user logs out. The contact search mainly implements the certificate search mentioned above and a search based on the user name. The secure single chat provides a text-based chat with a contact and the AV chat offers the opportunity to start an AV call with a contact, which is played by a HTML5 video element.

E. Graphical User Interface Module

The GUI communicates with the social networking, application and monitoring modules in order to delegate the requests the user initiates. Figure 2 shows a screenshot of the GUI from the view of a logged in user. Below the header with the buttons 'about', user search, settings, debug / monitoring and log out, there are a few open windows. 1.) *contact list* contains all contacts with their online status and time last seen 2.) *search* uses the certificate-based search of Chord to find and add contacts by their user name or public key 3.) *AV stream* shows an accepted AV stream with a contact on the left-hand side and the own video stream on the bottom right (both streams can be scaled) 4.) *debug / monitoring* which presents the local repository (local DHT entries), reference tables (routing tables) and monitoring information on request 5.) *add contact dialog* on receiving a contact request containing the certificate and buttons to answer the request and 6.) *chat* window displaying a chat with a contact.

III. State and Future Work

The demonstrator stated in Section II is a prototype and in an early stage. Our future work on this include plans to increase the overall performance of the platform, extend the functionality with features like data transfer, group chat, shared file systems and even multiplayer games. On the conference we plan to demonstrate our framework by logging in into our framework, show typical social media scenarios like chatting and AV streaming. The audience may interact by joining the session, as the framework will be publicly available via webp2p.cs.uni-duesseldorf.de.

References

[1] K. Graffi, C. Gross, D. Stingl, D. Hartung, A. Kovacevic, R. Steinmetz, LifeSocial.KOM: A Secure and P2P-based Solution for Online Social Networks, in: Proc. of IEEE Int. Consumer Communications and Networking Conf. (CCNC), 2011.

[2] S. Buchegger, D. Schiöberg, L.-H. Vu, A. Datta, PeerSoN: P2P Social Networking: Early Experiences and Insights, in: Proc. of ACM EuroSys Workshop on Social Network Systems (SNS), 2009.

[3] L. A. Cutillo, R. Molva, M. Önen, Safebook: A Distributed Privacy Preserving Online Social Network, in: Proc. of Int. Symp. on World of Wireless, Mobile and Multimedia Networks (WOWMOM), 2011.

[4] K. Graffi, P. Mukherjee, B. Menges, D. Hartung, A. Kovacevic, R. Steinmetz, Practical Security in P2P-based Social Networks, in: Proc. of IEEE Int. Conf. on Local Computer Networks (LCN), 2009.