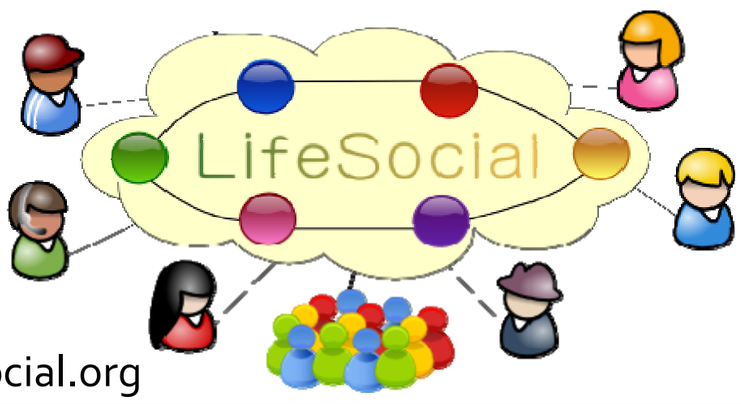
Kalman Graffi, Patrick Mukherjee, Burkhard Menges, Daniel Hartung, Aleksandra Kovacevic, Ralf Steinmetz
Technische Universität Darmstadt, Germany, and the Norwegian Information Security Laboratory
Contact: graffi@kom.tu-darmstadt.de , www.lifesocial.org

Practical Security in P2P-based Social Networks

LifeSocial.KOM – A Secure P2P-based Social Online Network



www.lifesocial.org

Problem Statement

Peer-to-Peer-based Social Online Networks are an emerging trend

Security issues will be crucial for its success

- Authentication and secure communication and peer / user lookup
- Fine grained data access control – for individual users and groups

Contributions in the Paper

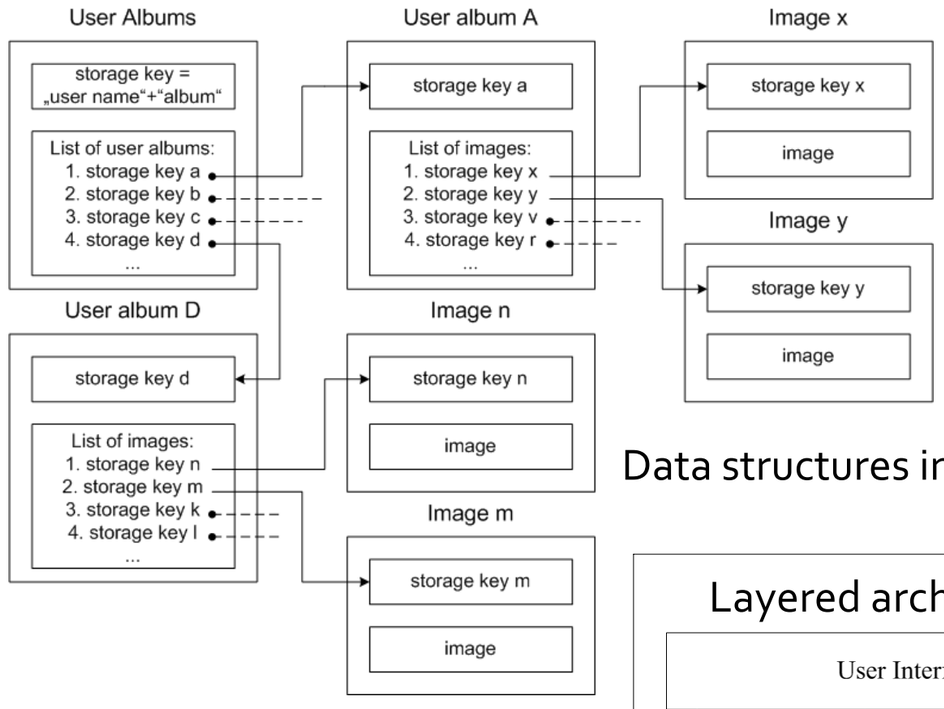
General security solution for P2P-Social Online Networks based on DHTs

→ Establishing a Public Key Infrastructure for peer / user authentication

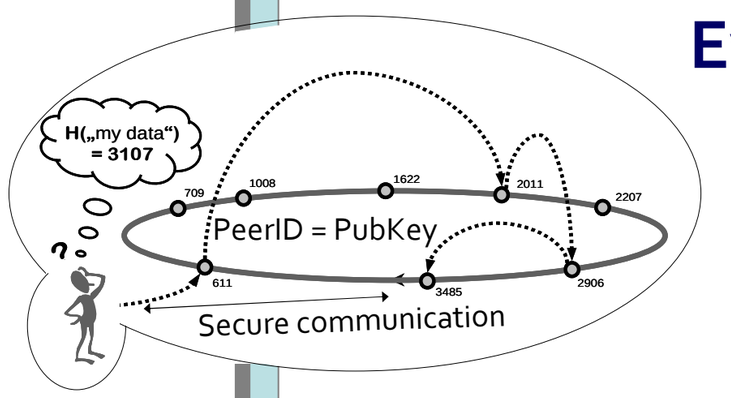
→ Secure (authenticated, confidential, ...) peer-to-peer communication

→ Access Control (read, write) and user access rights management

Secure Social Data Management



Data structures in the DHT



Evaluation

MESSAGE ENCRYPTION DATA AND TIME OVERHEAD

Msg. Size (bytes)	Encryp. Msg. Size (bytes)	Overhead abs. (bytes)	Overhead rel. (%)	En-/Decryp. Time (ms)
895	2794	1899	212,18	10 / 9
995	2906	1911	192,06	10 / 8
1395	3306	1911	136,99	11 / 9
1895	3802	1907	100,63	12 / 9
2895	4794	1899	65,60	14 / 10
3895	5802	1907	48,69	13 / 9
5895	7802	1907	32,35	12 / 8
10895	12794	1899	17,43	11 / 9

Overhead for Secure Peer-to-Peer Communication

- Data overhead per message ~ 2kb
- Time overhead ~ 10 msec

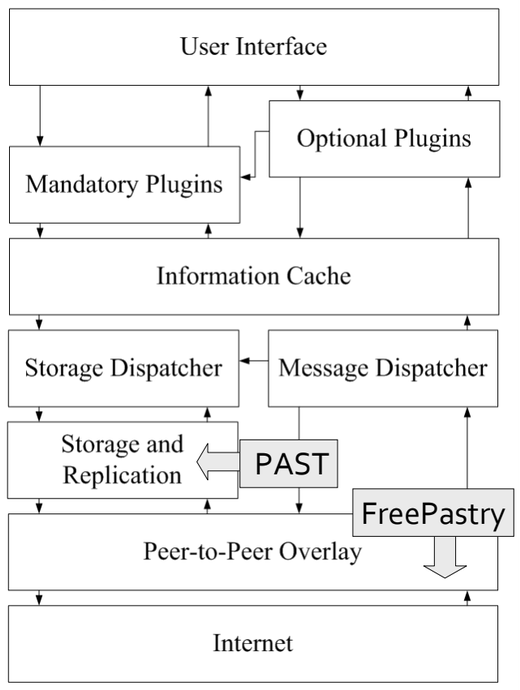
SHAREDITEM ENCRYPTION DATA OVERHEAD

Privil. Users	Item Size (bytes)	Encryp. Item Size (bytes)	Overhead abs. (bytes)	Overhead rel. (%)	En- / Decryption (ms)	Key Wrap. ping (ms)
1	346697	348159	1462	0,42	15 / 20	1
10	346715	351892	5177	1,49	25 / 21	4
50	346819	368524	21705	6,26	34 / 20	19
100	346969	389318	42349	12,21	54 / 19	37
200	347269	430922	83653	24,09	89 / 20	73

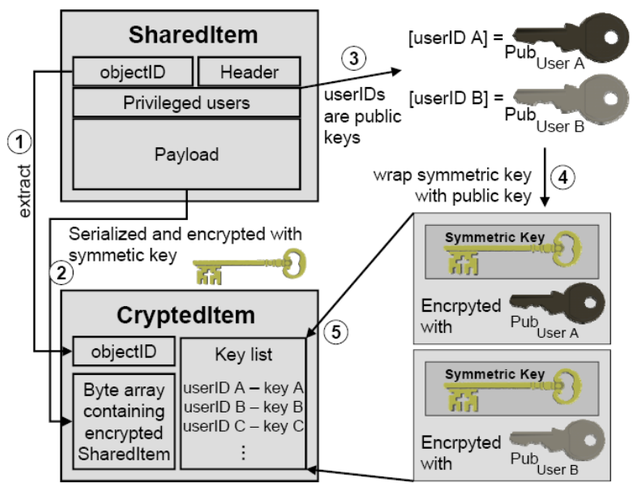
Overhead for Access Control

- Data and time overhead is related to number of privileged users

Layered architecture



Secure data structures



Outlook

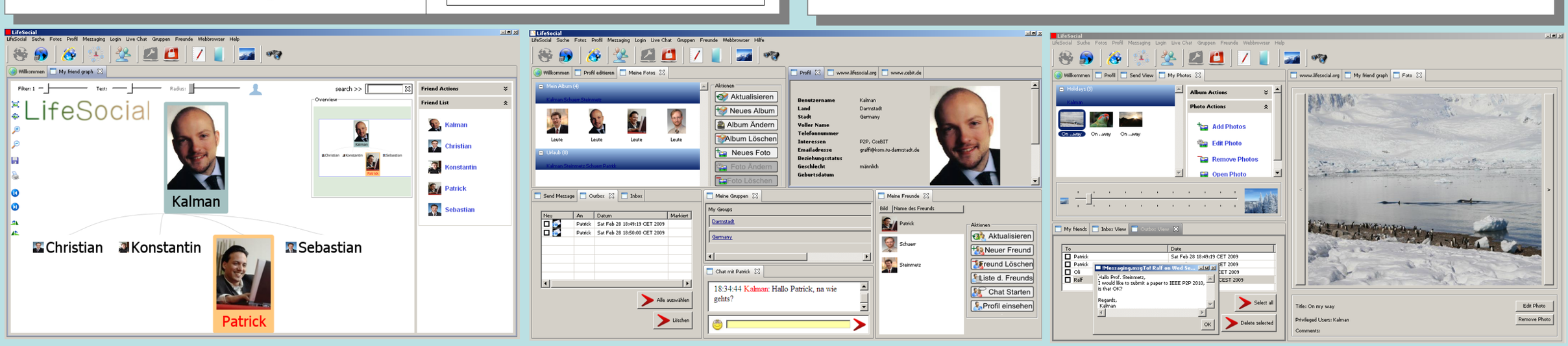
Monitoring and management of the quality of the running system

- Allows to see and control the quality metrics of the system

Further security extensions: deletion enforcement, detection of illegal content

Extension of more Plugins for user-to-user interaction: games, whiteboard

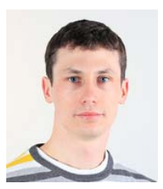
Deployment in a Alpha / Beta test



LifeSocial.KOM - P2P-based Social Online Network - K. Graffi et al., „A Distributed Platform for Multimedia Communities“, IEEE ISM 2008 - www.lifesocial.org

Department of Electrical Engineering and Information Technology
Multimedia Communications Lab - KOM
TECHNISCHE UNIVERSITÄT DARMSTADT
Dipl.-Math., Dipl.-Inform. Kalman Graffi
Kalman.Graffi@KOM.tu-darmstadt.de
Merckstr. 25
64283 Darmstadt
Germany
Phone +49 (0) 6151/164959
Fax +49 (0) 6151/166152
www.kom.tu-darmstadt.de


Kalman Graffi

Patrick Mukherjee

Daniel Hartung

Aleksandra Kovacevic

Ralf Steinmetz

Multimedia Communication Lab (KOM)
Technische Universität Darmstadt, Germany

Real Time Systems Lab (ES)
Technische Universität Darmstadt, Germany

The Norwegian Information Security Lab
Gjøvik University College, Norway