Prof. Dr. Thorsten Strufe
Stefanie Roos
{strufe,roos}@cs.tu-darmstadt.de

Fachgebiet Peer-to-Peer Netzwerke
Fachbereich Informatik
Technische Universität Darmstadt

Exercise 12

for **Peer-to-Peer Networks** - winter term 2012/2013

(29.01.2013)

Deadline for submission: 05.02.2013 1:30 PM

Guidelines

- Exercises annoted by **G#** are intended to be discussed and solved in class without grading, whereas exercises annoted with **H#** are supposed to be solved in groups and be handed in for grading.
  This does not mean, that ungraded exercises are less important.
- Please submit your solutions until the beginning (1:30 PM) of the next exercise in the coming week. Solutions can either be dropped in the letterbox in front of A110 or handed in personally on the beginning of the exercise. **Electronic submission is no more allowed!**
- Note that points are only given if your solution is clearly legible. Unreadable submissions will not be rated! (Machine written submissions are allowed)
- Written assignments are to be solved in groups of 2-3 participants while programming assignments have to be done in groups of four to six participants.
- Always annotate your solutions on the handed in sheet with names and matriculation numbers. If you have privacy concerns, you are allowed to omit your name and tell it to us personally.
- Please subscribe to the mailing list:
  `https://mail.rbg.informatik.tu-darmstadt.de/mailman/listinfo.cgi/p2p-lecture-ws12`
- By submitting any processed exercises or program code you hereby commit to the "Grundregeln der wissenschaftlichen Ethik am Fachbereich Informatik" (see also `http://www.informatik.tu-darmstadt.de/de/sonstiges/plagiarismus/`).
  This especially means, that you should always write in your own words. However if you use external materials, you have to cite them correctly.
  We will not accept solutions that only rely on literal citations.

G#12.1 Security in Online Social Networks (OSNs)

a) Centralized OSNs

It has been suggested to encrypt OSN data. Does that solve the privacy problems resulting from having one trusted authority?

b) P2P OSNs

In contrast to having a centralized system, a P2P system can be used as an OSN. Which privacy related problems emerge in such a system?

c) Social Overlays

In Social Overlays, people only directly communicate with trusted parties. This provides a high level of security, since in theory even the membership in such a system is concealed to strangers. However, the network cannot be structured by choosing links to enable fast routing as e.g. in a DHT. Can you think of ways to store and locate data efficiently?

H#12.1 Online Social Networks (OSNs)

a) Definition (3 Points)

Give a definition of Online Social Network.

b) OSN stakeholders (6 Points)

Describe the stakeholders in OSNs. Why are these parties interested in OSNs? What do they gain from them?

H#12.2 To DHT or not to DHT? (12 Points)

Consider the following scenarios. Would you use a DHT in its original form? Explain why or why not. If not, can you imagine ways to modify the typical DHT behavior for the specific application? If so, which DHT would you use?

i. The network should provide responder anonymity, i.e. the node that is responsible for a certain service/object cannot be guesses easily

ii. File-sharing

iii. A censorship-resilient network, i.e. it should not easily be possible to remove content

iv. Instant messaging

v. Large database distributed over thousands of machines

vi. Wireless sensor network

H#12.3 Q&A

Think of questions you have regarding the content of the class and send them to Stefanie Roos until Feb 10th.