Network Security
Summer 2015
Exercise 1, Sheet 2

TECHNISCHE UNIVERSITÄT DARMSTADT

Prof. Dr.-Ing. Matthias Hollick
Secure Mobile Networking Lab — SEEMOO
https://www.seemoo.de

Goal

This reading exercise aims to familiarize you with both reading and critically discussing research papers and the topics covered therein. The paper will give you an insight into research in network security.

Deadline

The hard deadline for this exercise is **Wednesday 29th April, 2015, 23:00:00**. Late submissions are subject to the following penalty: (1) up to 1 day late: you will obtain 50 % of the achieved points; (2) up to 2 days late: you will obtain 25 % of the achieved points; (3) more than 2 days late: you will obtain zero points.

Bonus system

We decided to install a credit-based bonus system in our course. We will hand out credits in certain exercises if you (the students) deliver first-rate performance. Within the relevant exercises we will document the detailed requirements to obtain the bonus. Throughout the entire course 280 credits can be obtained in our bonus system. If you score at least 230 credits, you are eligible for a 0.7 grade bonus in the final exam. If you score between 190 and 229 credits, you are eligible for a 0.3 grade bonus. Below 190 credits we will not issue any bonus.

How to solve this exercise

Within this exercise sheet up to 20 bonus credits can be obtained. The obtainable credits are directly related to the credits given with the respective questions. You may choose to answer questions totaling *up to* 25 credits. If you provide answers to more questions, the additional answers will not be graded. This has two implications: (1) It does not help you to answer all questions to achieve full credit. (2) You can achieve full credit by providing excellent answers to questions worth 20 credits.

We want you to provide answers in a **brief and concise** manner. You might receive a penalty if you provide information that is not relevant to answering the questions. You can take the number of credits per question as an estimator of how elaborate you should be.

Upload the answers in Moodle in a plain text file (no Word, no obscure file formats, just ASCII text) following the naming conventions: *ex01s2-lastname_firstname.txt*. Replace *lastname* and *firstname* with your personal information. Please write down each answer in a new line and refer to the question you are answering. Do not include any additional white spaces or non answer items. Also do not use any markup or formatting language such as HTML, Markdown or LaTeX.

Problem 1.3 Answers (Bonus: 20 credits)

Below we list general and more advanced questions related to the paper *Users Get Routed: Traffic Correlation on Tor by Realistic Adversaries* from the previous exercise (Problem 1.3).

a) (1 credit) What is Tor used for?

b) (1 credit) What is a Tor relay? What types are there?

c) (1 credit) What are the main contributions of this paper?

d) (1 credit) Which well-known attack is Tor vulnerable to? How does it work in principle?

e) (1 credit) Briefly summarize the adversary model considered in the paper.

f) (1 credit) What is *Tor Metrics*?

g) (1 credit) What is a Monte Carlo simulation?

h) (1 credit) In the Internet, what is an Autonomous System (AS)?

i) (1 credit) What does DE-CIX do?

j) (2 credits) How does Tor attempt to anonymize its users' traffic??

k) (2 credits) How does the adversary model compare to the ones used in other works on onion routing?

l) (2 credits) Why are "security metrics" needed? Explain with an example.

m) (2 credits) What is the main function of the Tor path simulator (TorPS)? Explain w.r.t. the Tor network model and client model.

n) (2 credits) How is the "network adversary" different from the other adversary type presented in the paper w.r.t. mounting an attack?

o) (2 credits) Why do the authors "omit ASes which contain clients, or destinations for a given client and activity, from the set of adversaries?"

p) (2 credits) How strong is the "network adversary" compared to the "relay adversary"?

q) (3 credits) How does user behavior affect their security in Tor?

r) (3 credits) What is the intend of the different user models presented in the paper?

s) (3 credits) What is the trade-off for a resource-constrained adversary when allocating bandwidth to guard and exit relays? How does bandwidth resources relate to the adversary's power?

t) (3 credits) What is the significance of Figures 2a-2c?

u) (3 credits) What is the impact of alternative path selection strategies on security?

v) (4 credits) Explain and compare how the two adversary types attempt to compromise a user's privacy.