TDTS21 – Advanced Networking [vt 2021 version of the course]
Final Examination deadline: 18:00 on Friday, June 4, 2021
Total Marks: 40
Grade Requirements: Three (26/40); four (32/40); and five (38/40).
Instructor: Niklas Carlsson

General instructions [2021]

- Read all instructions carefully (including these)!!!! Some questions have multiple tasks/parts. Please make sure to address *all* of these.
- The total possible marks granted for each question are given in parentheses. The entire test will be graded out of 40. This gives you 10 marks per hour, or six minutes per mark, **plan your time accordingly**.
- This examination consists of a total of 6+1 = 7 questions. Check to ensure that this exam is complete.
- When applicable, please explain how you derived your answers. Your final answers should be clearly stated.
- Type answers electronically; no marks will be given for handwritten answers that cannot be read easily.
- Where a discourse or discussion is called for, be concise and precise.
- If necessary, state any assumptions you made in answering a question. However, remember to read the instructions for each question carefully and answer the questions as precisely as possible. Solving the *wrong* question may result in deductions! It is better to solve the *right* question incorrectly, than the *wrong* question correctly.
- Please write your **name**, exam code, page numbers (even if the questions indicate numbers as well), etc. at the top/header of each page. (This ensures that marks always can be accredited to the correct individual.)
- Please answer in English, and try to only use Swedish or ”Swenglish” if needed to complement your answers when uncertain about language.
- Most questions are designed to be answered using concrete example figures/tables. Please try to be as precise as possible.

2021 exam

- Answers should be submitted per email, to the examiner, as a single pdf file.
- Please type answers in English. No handwritten answers are allowed.
- Figures can be drawn by hand or by computer. If you draw by hand, please scan (or take a photo) and insert into the file you use to generate your pdf.
- You must answer all questions yourself; no group work or outside help is allowed.
- Do not copy-paste text from other sources.
- Finally, **you must fill out and sign the compliance statement** at the end of the exam.

Good luck with the exam!

Question 1: Intro and address basics (10 points)

Consider a scenario in which you view a video on the YouTube website. Assume that the video is served from a datacenter located in eastern USA and you are located on the LiU campus. Furthermore, consider the IPv4 packets associated with the video transfer, including both requests and video content.

First, please draw an image of the end-to-end data path and briefly (but clearly!) explain using this figure how the following five addresses are (a) obtained by the involved parties [including what protocols/processes are involved and how they work] and (b) used to achieve end-to-end Internet routing of the packets: (i) your IP address, (ii) your MAC address, (iii) the YouTube servers IP address, (iv) Google's AS number(s), and (v) LiU's AS number. (Please clearly indicate each of the 10 cases associated with this question and address them one-by-one.)

Second, explain which of these addresses are used in the control plane and which are used in the data plane.

Third, please show the address-related header information associated with a "packet" sent from your computer to the above YouTube server (using HTTPS) when it passes your network interface card. The image should clearly indicate how encapsulation is done and should include MAC addresses, IP addresses, port numbers, and web-related addresses. Here, also indicate what addresses would be visible (and not visible) to wireshark or other packet analyzer (when using HTTPS). You are encouraged to setup and use a real Wireshark example to answer this question (although not a must).

Finally, using the above example, please explain how (or why not) your computer can learn about the YouTube servers (i) host name, (ii) IP addresses, and (iii) MAC address.

Question 2: TCP basics (4 points)

Use figures and examples to illustrate why TCP's additive increase and multiplicative decrease (AIMD) mechanism provides some stability and fairness.

Question 3: BGP basics and trends (6 points)

First, please draw a figure that clearly shows an example where BGP may result in a sub-optimal routing path and use the figure to explain why BGP would result in a sub-optimal route in this case. Second, please show and explain how some content providers' use of peering agreements has changed over time and the impact that this has had on the "distances" observed on the Internet. Third, please show and explain (using a n example scenario) how an AS can perform an interception attack on a prefix.

Question 4: TCP and QUIC (8 points)

First, use a figures and example numbers to illustrate how Cubic TCP differs from TCP Reno under some example scenario. Your example scenario should illustrate all phases of a typical TCP connection and should cover both the initial handshake phase as well as loss events detected using both duplicate ACKs and timeouts.

Second, list and briefly explain the key ideas behind (i) BBR, (ii) compounded TCP, and (iii) QUIC. Please be concise and use a sentence or two per bullet.

Question 5: Tail statistics (6 points)

First, please explain how a heavy-tailed distribution relates to an exponential distribution and support your answer with figures that compare well-selected example distributions that illustrate your answer. Here, please generate plots that include examples of both types and that illustrate the key differences. Datasets can either be real data or datasets you generate yourself (e.g., using the definition of the distribution). Second, please list and explain at least two papers from the class that considered heavy-tailed distributions, and give an example distribution for one such distribution per paper.

Question 6: Third-party services and tracking (6 points)

First, use the literature from the course to explain (i) how modern websites are built up, (ii) who deliver this content, (iii) how parallelism typically is achieved, and (iv) how a user may be tracked across a series of websites. Second, please discuss performance and privacy implications associated with the above aspects. Please describe these implications using a simple but concrete example scenario, ideally using a figure or two. Third, please provide concrete examples and discuss how a few example websites (or categories of websites) may differ with regards to these tradeoffs. For this question, please use Wireshark, Chrome's inspect function, or similar tool.

Bonus (only on original exam)

Question 7: HTTPS, Certificates, and MITM attacks (6 points)

Please use a clear step-by-step figure explaining how you can execute a HTTPS interception, or man-in-the-middle (MITM) attack, on a client that accidentally has agreed to trust your root certificate. In this question, please clearly show the certificates being communicated (using public-key crypto) **and** the basic Diffie-Hellman key exchanges. Your figure should clearly show the use of public keys, certificate chains, and the creation of shared secrets. Ideally, to make things more concrete, please also include a concrete example based on an example website from which you extract the certificate, domain name, identify the public key used, the root that the "bad" entity may have managed you to trust. For examples of "bad" websites that you could use for this example, please feel free to leverage a suitable example certificate from badssl.com.

Mandatory: Statement of compliance

Finally, you are required to sign and send back (scan/photo), together with the exam, a text with the following declaration:

I hereby solemnly declare that during the TDTS21 exam, June 4th 2021, I did not cheat or plagiarize text, and that all work presented here was done by myself without any consultation with people by phone, chat, or any other means during the exam. (The course instructors being the only exception.)

Good luck!!