The Complete Studyguide for DT116G Network Security

Lennart Franked
lennart.franked@miun.se

Daniel Bosk
daniel.bosk@miun.se

studyguide.tex 1530 2013-12-11 10:52:12Z lenfra

Contents

1 Aims

This course covers the procotols, architectures and applications that is used in todays network to ensure confidentiality, integrity and availability. You will get a well-founded understanding for the mechanisms needed to provide a secure networking environment.

After completing this course you will fulfill the following requirements:

- Have an understanding of how to use a public–private key-pair.
- Know how to use implementations of asymmetric ciphers.

- Be able to distribute your own key and retrieve other public keys using publicly available key servers.
- Be able to use steganography as a way to hide messages.
- Demonstrate ability to detect and possibly prevent attacks on a network.
- Reflect and discuss the importance of network security, or consequences of lack thereof, in society.

2 Overview

This course will primarily use Stallings [8], this study guide will contain all reading instructions that are covered in this course, togheter with a recommended timetable.

2.1 Schedule

You will find a summary of the course schedule in Table 1 on the next page. You are free to follow this schedule, but the lectures are given at those times and the deadlines are mandatory.

The reading instructions are found below, in the following sections.

2.2 Introductory lecture

The lecture introduces the material of the course and the area of network security. It provides an overview of chapter 1 “Introduction” in *Network security essentials : applications and standards* [8] and certain contents from chapter 1 “What is security engineering?” in *Security engineering : a guide to building dependable distributed systems* [1].

2.3 Secret-key cryptography

The lecture essentially covers “En introduktion till kryptografi” [2], chapter 2 “Symmetric Encryption and Message Confidentiality” in *Network security essentials : applications and standards* [8], and chapter 5 “Cryptography” in *Security engineering : a guide to building dependable distributed systems* [1].

You should then solve problems 2.1, 2.2, 2.12, 2.13 and 2.14 in [8].

2.4 Public-key cryptography

The lecture covers chapter 3 “Public-Key Cryptography and Message Authentication” in [8] and the remaining parts of chapter 5 “Cryptography” in [1].

After this you should solve problems 3.1, 3.2, 3.5, 3.7, 3.8, 3.9 and 3.10 in [8].

Course Week	**Chapter**
1	Introductory lecture
2	Lecture on secret-key cryptography Lecture on public-key cryptography Tutoring
3	Lecture on key distribution and authentication Tutoring
4	Lecture on network access control and cloud security Lecture on SSL/TLS Tutoring
5	Lecture on wireless security Tutoring
6	Lecture on email security L1 Privacy of Communication S2 Ethics in Computer Networks Tutoring
7	Lecture on IPsec Seminar on ethics Tutoring
8	Lecture on intrusion detection L3 Intrusion Detection Systems Lecture on firewalls Tutoring
9	Tutoring
10	Exam

Table 1: Timetable based on course given at 50 percent study rate.

2.5 Key distribution and authentication

The lecture covers chapter 4 “Key Distribution and User Authentication” in [8] and chapter 3 “Protocols” in [1].

When you are done studying the material you should solve problems 4.1, 4.2, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, and 4.11 in [8].

2.6 Network access control and cloud security

The lecture covers chapter 5 “Network Access Control and Cloud Security” in [8]. When finished reading the chapter, you should solve problems 5.2 and 5.3 in [8], note however that in 5.3 instead of writing a brief paper, publish the URL in the forum along with a brief summary of the what the video addresses.

2.7 Transport-level security

The lecture covers chapter 6 “Transport-level Security” in [8]. To make sure you have fully understood the chapter, you should solve problems 6.1, 6.2 and 6.3 in [8].

2.8 Wireless network security

The lecture covers chapter 5.1 - 5.3 and chapter 7 “Wireless Network Security” in [8]. To check that you have fully understood these chapters, you should solve problems 7.1, and 7.2

2.9 Electronic mail security

The lecture covers chapter 8 “Electronic Mail Security” in [8] and the RFC document “Analysis of Threats Motivating DomainKeys Identified Mail [3]

When you have finished reading this chapter, you should solve problems 8.6 - 8.8 in [8].

2.10 L1 Privacy of communication

Before starting this assignment you should have read chapters 1–4 and 8 in *Network security essentials : applications and standards* [8].

For the second part of this assignment you should read *OpenPuff v4.00 Steganography & and Watermarking* [6] to fully understand how steganography works in practice.

During this assignment you should consult the documentation [5, 6, 9] for instructions on how to use the specific softwares.

2.11 IP security

The lecture covers chapter 9 “IP Security” in [8]. You should also read section 1 in [4] as a complement to the course literature, to help you grasp the Internet Key Exchange protocol. To check that you have fully understood this chapter, you should solve problems 9.3, 9.6, 9.8 and 9.10.

2.12 S2 Ethics in computer networks

Before starting this assignment you should have read Chapter 14 (online chapter) in “Network Security Essentials” [8], or Chapter 24 (online chapter) in “Cryptography and Network Security” [7].

2.13 Intrusion detection

The lecture gives an overview of chapter 11 “Intruders” in [8] and chapter 21 “Network Attack and Defense” in [1].

When you have reviewed the material you should solve problems 11.2, 11.3, 11.4, 11.6, and 11.9 in [8].

2.14 L3 Intrusion Detection

Before starting this assignment you should have read chapters 10 to 13 in Stallings [8]. You should also read chapters 1, 2.1, 2.4, 2.5, 2.9, 3.1-3.4 in the Snort documentation [10].

2.15 Firewalls

The lecture covers chapter 12 “Firewalls” in [8] and the remaining parts of chapter 21 “Network Attack and Defense” in [1]. After reading this chapter, check your understanding by solving problems 12.1, 12.4, 12.5, 12.6 and 12.10

3 What if I am not done in time?

The deadlines on this course are of great importance. You must have completed the introductory assignment within its deadline. If you do not do this you will be deregistered from the course and your place will be open to other students.

For seminars there will be three sessions during the course, if you cannot make it to any of those you will have to return the next time the course is given; i.e. up to a year later. All of these sessions will be in the course schedule (in the Student Portal).

If you miss a deadline for the preparation for a seminar session, then you have to go for the next seminar even if the first seminar is not passed yet. If you miss all three you have to return the next time the course is given.

Written assignments are graded once during the course, at the latest shortly after the deadline of the assignment. After the course your are offered two more attempts within a year. In total you have three chances for having your assignments graded over the period of a year. After that you should come back the next time the course is given.

No tutoring is planned after the end of the course, i.e. after the last tutoring session scheduled in the course schedule. If you are not done with your assignments during the course and want to be guaranteed tutoring you have to reregister for the next time the course is given. Reregistration is a lower priority class of applicants for a course, all students applying for the course the first time have higher priority – this includes reserves too.

If you by the end of the course have a majority of the assignments left undone you will have to reregister for the course the next time it is given. Whether you have completed the majority of the assignments or not is up to the teacher to decide. Talk to the teacher to see if you have to reregister or can just hand in the missing assignments.

Thus, if you feel that you will not be done with the course on time, it is better to stop the course at an early stage. If you register a break within three weeks of the course start, you will be in the higher priority class of applicants the next time you apply for the course. You can register such a break yourself in the Student Portal.

References

[1] Ross J. Anderson. *Security engineering : a guide to building dependable distributed systems*. 2nd ed. Indianapolis, IN: Wiley, 2008. ISBN: 978-0-470-06852-6 (hbk.) URL: `http://www.cl.cam.ac.uk/~rja14/book.html`.

[2] Daniel Bosk. "En introduktion till kryptografi". 2013. URL: `http://ver.miun.se/courses/infosak/compendii/introcrypt.pdf`.

[3] J. Fenton. *Analysis of Threats Motivating DomainKeys Identified Mail (DKIM)*. RFC 4686 (Informational). Internet Engineering Task Force, Sept. 2006. URL: `http://www.ietf.org/rfc/rfc4686.txt`.

[4] C. Kaufman, P. Hoffman, Y. Nir, and P. Eronen. *Internet Key Exchange Protocol Version 2 (IKEv2)*. RFC 5996 (Proposed Standard). Updated by RFCs 5998, 6989. Internet Engineering Task Force, Sept. 2010. URL: `http://www.ietf.org/rfc/rfc5996.txt`.

[5] Werner Koch. *Using the GNU Privacy Guard*. Mar. 2012. URL: `http://www.gnupg.org/documentation/manuals/gnupg.pdf`.

[6] Eng. Cosimo Oliboni. *OpenPuff v4.00 Steganography & and Watermarking*. July 2012. URL: `http://embeddedsw.net/doc/OpenPuff_Help_EN.pdf`.

[7] William Stallings. *Cryptography and network security : principles and practice*. 6th ed. Pearson Education, 2013. ISBN: 978-0-273-79335-9.

[8] William Stallings. *Network security essentials : applications and standards*. 5th ed. International Edition. Pearson Education, 2013. ISBN: 978-0-273-79336-6.

[9] The Gpg4win Initiative. *The Gpg4win Compendium*. Aug. 2010. URL: `http://wald.intevation.org/frs/download.php/775/gpg4win-compendium-en-3.0.0-beta1.pdf`.

[10] The Snort Project. *SNORT Users Manual*. May 2013. URL: `http://s3.amazonaws.com/snort-org/www/assets/166/snort_manual.pdf`.