Network Security (NetSec)

TECHNISCHE UNIVERSITÄT DARMSTADT

Summer 2015
Chapter 00: Organizational Issues
Module 03: Exam, Summer 2015

Prof. Dr.-Ing. Matthias Hollick

Technische Universität Darmstadt
Secure Mobile Networking Lab - SEEMOO
Department of Computer Science
Center for Advanced Security Research Darmstadt - CASED

Mornewegstr. 32
D-64293 Darmstadt, Germany
Tel.+49 6151 16-70922, Fax. +49 6151 16-70921
http://seemoo.de or http://www.seemoo.tu-darmstadt.de

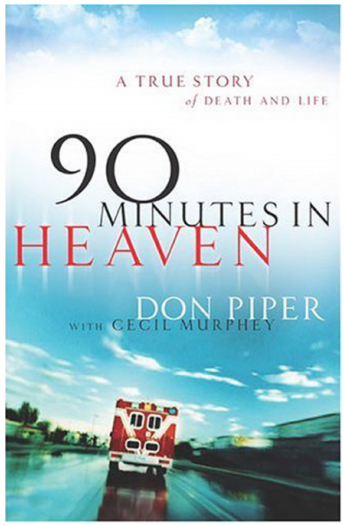
Prof. Dr.-Ing. Matthias Hollick
matthias.hollick@seemoo.tu-darmstadt.de

CASED

Organizational Issues

NetSec exam in a nutshell

- FRI, 24.07.2015, starting 13:15
- Room S206/030, S101/A01, S105/122 (see Moodle for your room)
- Written, 90min, closed book, English
- A valid student ID and a valid photo ID are required (i.e. a passport or a national identity card – your TU-Student card is not enough)
- A document-proof pen (no pencil, no red ink)



Source: imdb.com, sxc.hu, apple.com

Organizational Issues

NetSec exam in a nutshell

- FRI, 24.07.2015, starting 13:15
- Room S206/030, S101/A01, S105/122 (see Moodle for your room)
- Written, 90min, closed book, English (but answers in German are OK)
  - You will be given a set of problems/questions to work on
  - You can obtain 90 credits; i.e., roughly 1 credit per minute

Additionally:

- You have to register in TUCaN, if you are a "legacy" student, tell us (until 07.07.2015, 23:59)
- Consultation hours
  - WED July 15, 2015: S4|14, room 4.3.01, 13:30h to 15:00h
- Forum should be used for Q & A, we regularly monitor it
- Dates for results (only available in TUCaN) and "Klausureinsicht" will be announced on MOODLE in due time

Source: http://www.thisiscolossal.com/2015/06/new-paper-birds-and-wildlife-by-diana-beltran-herrera/

How Does the Exam Look Like?

[Source: xkcd.com]

How Does the Exam Look Like?

The exam covers the entire lectured material (lecture + exercise)

- You should have a thorough understanding of the lectured material and esp. be able to explain the workings of the discussed security protocols
- We know that learning 500++ slides of content is demanding. You definitely should not learn these by heart, but try to get the gist out of the slides
- In the lecture, we emphasized certain aspects – expect the exam to emphasize on these aspects as well
- The guest lecture on practical wireless network security ("Wi-Fi hacking") by Pedro Larbig, deepens the understanding of C06M03. C06M03 is relevant for the lecture as all other modules.
- The exercise is relevant for the exam!

How Does the Exam Look Like?

The exam covers the entire lectured material (lecture + exercise)

- ... continued from last slide
- The basic working of the presented TLS attacks is relevant: Freak, Shellshock, Heartbleed (some of this was live demonstrated in the lecture)
- Again: the exercise is relevant for the exam

The exam does *NOT* cover:

- The appendices of the lecture slides
  - Appendices are clearly marked.
- The additional readings on the course platform
- The distinguished lectures (CASED, MAKI)

Sample Problems

5.2. (3 points) IEE 802.11i introduced the Temporal Key Integrity Protocol (TKIP). Explain this data privacy mechanism. What does it improve compared to WEP?

- Avoids WEP's weak keys (Decorrelate WEP IV and per-packet key, no weak IVs)
- Replay protection (Sequence number instead of random number)
- Added message integrity function (Michael, provides only weak security, though)
- Fixes issues of WEP yet can be implemented on legacy HW

We like this answer! The part in parentheses are optional for the given number of credits.

- Paints the network in green (we consider this answer wrong)
- TKIP is temporal (so what?)
- IPSec can be used to secure network communication (does not answer the question)
- It uses AES encryption (does not apply for TKIP)

We are not happy with this answer

Sample Problems

4.3. (6 points) What are the differences between SPIT (SPam over IP Telephony) and SPAM? Describe 3 methods to prevent SPIT.

This year, this was not part of the lecture.
The distinguished lectures are NOT part of the exam!

Important points:

- Read carefully. There are TWO questions! Answer both!
- While you can give 4 or more methods, we will grade exactly as implied by the question, i.e., we will grade 3 methods and the corresponding description.
- We have described methods in the lecture. If you answer with a correct method that has not been discussed during the lecture, you will also get credits. However, please give enough reasoning/ explanation to help us understanding this solution. Just putting “SPIT-Cemetery” is not sufficient, even if such a (proprietary) tool/method exists.

Sample Problems

SECURE MOBILE NETWORKING

3.6. In the reading exercise, we discussed the paper „Design Failures of Transport Level Security“. The paper names the „Time-zone design problem“ as a key weakness. Please describe this weakness and name countermeasures as described in the paper.

Bear in mind, the exercise is an integral part of the lecture and, hence, the exam!

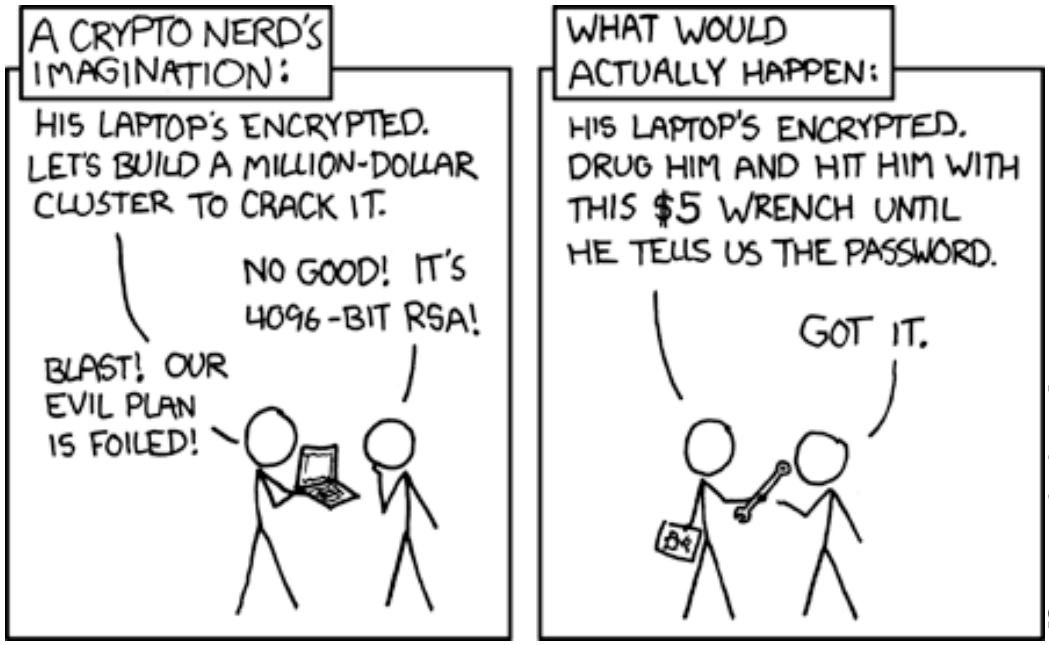
Important points:

- Again: read carefully. There are two subparts of the question (weakness and countermeasure)
- Describe only the scheme in question (we will ignore your answers, if they refer to the “packet-color design problem” or the “router-sleeps design problem”)
- A simple answer is fine with us:
  “The time-zone design problem describes that attacks are possible, if a TLS record is crossing the international data line from west to east. The proposed solution is to send packets by canoe from east to west.”

How Does the Exam Look Like?

Tipps

- I very much recommend to form teams during the preparation
- We know that time is short. This is, why we continually tried to engage you in the exercise/lecture
- Watch the recordings or consult a textbook if you have doubts. You need to understand the key aspects of the lecture
- It is important to understand pros/cons of the discussed algorithms
- It is important to know pitfalls in implementing security
- Again: the exercise is important



[Source: xkcd.com]

Contact

Prof. Dr.-Ing. Matthias Hollick
Department of Computer Science

SEEMOO
Mornewegstr. 32
64293 Darmstadt/Germany
matthias.hollick@seemoo.tu-darmstadt.de

Phone +49 6151 16-70920
Fax +49 6151 16-70921
www.seemoo.tu-darmstadt.de

Copyright Notice