<table>
<thead>
<tr>
<th>Kurskod</th>
<th>Provkod</th>
<th>Tentamensdatum</th>
</tr>
</thead>
<tbody>
<tr>
<td>DT116G</td>
<td>T108</td>
<td>2018-08-30</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Kursnamn</th>
<th>Datateknik GR (B), Nätverkssäkerhet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provnamn</td>
<td>Tentamen</td>
</tr>
<tr>
<td>Ort</td>
<td>Sundsvall</td>
</tr>
<tr>
<td>Termin</td>
<td>H18</td>
</tr>
<tr>
<td>Ämne</td>
<td>Datateknik</td>
</tr>
</tbody>
</table>
Final Exam
DT116G Network Security
Lennart Franked
lennart.franked@miun.se
Phone: 010 142 8633
2018-08-30

Instructions
Carefully read the questions before you start answering them. Note the time limit of the exam and plan your answers accordingly. Only answer the question. The questions are not sorted by difficulty. Clearly show which answer you are giving your solution to. *Always motivate your answers and show your calculations.*

Time 5 hours.
Exam Aids .
Maximum points 30
Questions 10

Preliminary grades
The following grading criteria applies: E ≥ 30%, D ≥ 45%, C ≥ 60%, B ≥ 75%, A ≥ 90%. Scoring will be based on level of depth shown in your answer. To pass this exam you must have shown proficient knowledge in all the intended learning outcomes (ILO) covered in this exam. Each questions ILO affiliation is shown as (ILO: #).

Covered ILO
This exam covers the following Intended Learning Outcomes (ILO)

- ILO: 1 – account for the mostly used protocols for encryption, digital signatures and certificates
- ILO: 2 – explain how to build a network that provides secure operation and protection for users,
- ILO: 3 – apply secure communication protocols over the Internet
Questions

The questions below are not given in any particular order.

1. (ILO: 1) Explain the following types of attacks on a symmetric encryption scheme:
   - Ciphertext only
   - Known plaintext
   - Chosen plaintext

2. (ILO: 1) A few years back Mozilla held public discussions on whether to include or exclude Telias-
   Sonera CA-certificates from its web browser Firefox. This was due to TeliaSonera having dealings
   with certain non-democracies and purportedly supplied surveillance equipment to said governments.
   Mozilla is right to exclude TeliaSonera certificates if these accusations stand true, explain why this
   is an issue (from a technological perspective).

3. (ILO: 1) When we talk about different hash algorithms, we mention properties that they must follow
   in order to be useful for integrity and authentication mechanisms. One of them is strong collision
   resistance, that is, it must be computationally infeasible to find a pair \((x, y)\) such that \(H(x) = H(y)\).
   Explain why this is a vital property for a hash algorithm.

4. (ILO: 2) Paranoia just struck you. Hence, you are thinking about implementing full-disk encryption
   on your systems. Because of fear for government trap-doors in already packaged software implementa-
   tions you have decided to implement your own version. You know that you need to decide upon
   an encryption algorithm.
   - Discuss advantages and disadvantages with the following encryption algorithms: RSA, 3DES, and
     AES.

5. (ILO: 2) An organisation has a spam filter employed to filter all incoming email to the organisation’s
   employees.
   - As what type of firewall would you classify this spam filter? (This includes an explanation why.)
   - Give an overview of what other types of firewalls exist and how they work.

6. (ILO: 2) Describe the following modes of operation for block encryption, explain using both text
   and figures
   - ECB
   - CBC
   - CFB
   - CTR

7. (ILO: 2) For computer aided exams where the exam is taken by opening a particular webpage in the
   web browser, explain how you can use a rule-based NIDS such as Snort to detect cheaters.
   (Note that you do not have to provide syntactically correct Snort-rules which can be loaded into
   Snort without error.)

8. (ILO: 3) You just finished reading RFC 5998 [rfc5998] “Extension for EAP in IKEv2”, you tell your
   friend about this, however your friend haven’t a faintest idea what you are talking about. Explain
   to your friend in as much detail as you can
   - what IKEv2 is and what it is used for.
   - what EAP is and what it is used for.
   - what benefits you would get for running EAP in IKEv2.
9. (ILO: 3) You have a friend who is currently taking a course on Network Security. He is preparing for the final exam and have just finished reading about GPG. He calls you and asks "Hi friend, how are you? You've already taken the course on Network Security", you never told him you haven't taken the exam yet, "can you explain how Kerberos, X.509, and GPG relates to each other? I don't understand why we need three systems which does kind of the same thing."

Explain to your friend
- how Kerberos works,
- how X.509 works in comparison to Kerberos, and finally
- how GPG works in comparison to Kerberos and X.509.

10. (ILO: 3) Cloud computing has stopped being a trend and can now be found as a part of most companies IT-architecture. Besides using cloud services for running software or using it for storage it has now become more and more common we put our security out on the cloud as well. This is called SecaaS. What does this actually mean? Name four services that can be offloaded on the cloud along with a short

References