Mittuniversitetet
MID SWEDEN UNIVERSITY

Försättsblad Prov Original

Kurskod	Provkod	Tentamensdatum
DT116G	T108	2018-04-04

Kursnamn	Datateknik GR (B), Nätverkssäkerhet
Provnamn	Tentamen
Ort	Sundsvall
Termin	V18
Ämne	Datateknik

Mittuniversitetet
MID SWEDEN UNIVERSITY

Final Exam

DT116G Network Security

Lennart Franked
lennart.franked@miun.se
Phone: 010 142 8683

2018-04-04

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 $\geq 9p$, D $\geq 13p$, C $\geq 18p$, B $\geq 22p$, A $\geq 27p$. 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.

(3p) 1. *(ILO: 1)* Explain the following terms, give an example of a threat that can compromise what it stands for, and give an example of a countermeasure for that threat.

- Confidentiality
- Integrity
- Authentication

(3p) 2. *(ILO: 1)* According to [**Lucks2005hc**], in 2005 it took a few hours on an ordinary PC to find a colliding message M', which still makes sense, for a given message M, where both messages have the same MD5 digest. Hypothetically, we report the grades on this exam by email over an unsecured wireless network and sign it using a MAC based on MD5. The MAC works like this, we compute the message digest for the message using MD5 and then sign this digest with our public key. Hence you cannot change the digest in the message should you intercept it.

Why is this a bad idea for reporting grades?

(3p) 3. *(ILO: 1)* A user connects to your web server using an SSL connection secured by an X.509-certificate. How can the user be sure that it is the correct server?

(3p) 4. *(ILO: 2)* Below follows a simple authentication protocol based on symmetric encryption. This protocol allows for two nodes in a network to securely communicate. With the help of a trusted third party that shares symmetric keys with all of the involved parties two participants can set up a communication channel.

$$
\begin{aligned}
A &\rightarrow AS\colon E_{A,AS}(ID_b) \\
AS &\rightarrow A\colon E_{A,AS}(K_{A,B}, E_{B,AS}(K_{A,B}, ID_A)) \\
A &\rightarrow B\colon E_{B,AS}(K_{A,B}, ID_A) \\
A &\rightarrow B\colon E_{K_{A,B}}(M)
\end{aligned}
$$

Name at least three vulnerabilities on this protocol, and rewrite the protocol to fix these.

(3p) 5. *(ILO: 2)* Your pointy-haired boss comes to you and says he wants you to set up WPA2 Enterprise in his home. You, being a very obedient employee who 'needs the money', will of course do this. However, you are a very lazy person, so you try to avoid this.

Explain to your boss why this is unnecessary to have in his home but good in the office.

(3p) 6. *(ILO: 2)* Explain the difference between a circuit-level gateway and an application-level gateway.

(3p) 7. *(ILO: 3)* In the context of IPsec, explain the application of the following functions:

- AH/ESP
- Tunnel-mode
- Transport-mode
- SA/SAD

(3p) 8. *(ILO: 3)* Storing data in the cloud have become more and more common, however in order to ensure that the data in rest are secure, encryption should be used. Explain the practical problems with encrypting the data that is in rest in the cloud and give one suggestion of how to solve this.

(3p) 9. *(ILO: 3)* You have a large amount of raw data that you need to send to a colleague, it is important that both the confidentiality and integrity of the data is not compromised during the data transmission, you also want to ensure that only your colleaugue will be able to read the information and that your colleauge will be able to verify that the data received is infact from you.

Explain how you would solve this using a *combination* of the different security mechanisms that you have read about during this course.

(3p) 10. *(ILO: 3)* The SSL architecture contains four protocols spanned across two layers. Name two protocols and explain their purpose.