Mittuniversitetet
MID SWEDEN UNIVERSITY

Försättsblad Prov Original

Kurskod	Provkod	Tentamensdatum
DT116G	T106	2019-04-24

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

Mittuniversitetet
MID SWEDEN UNIVERSITY

Final Exam

DT116G Network Security

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

2019-04-24

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 Pen and Paper.

Maximum points 27

Questions 9

Preliminary grades

The following grading criteria applies: E $\geq$ 30%, D $\geq$ 45%, C $\geq$ 60%, B $\geq$ 75%, A $\geq$ 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.

(3p) 1. *(ILO: 1)* Account for what it means that a hash function is:

- preimage resistant
- second preimage resistant
- collision resistant

(3p) 2. *(ILO: 1)* Draw the exchange, and explain the purpose of each message, when an EAP supplicant wants to gains access to a network through an EAP authenticator and an authentication server such as RADIUS.

(3p) 3. *(ILO: 1)* Explain the following types of attacks on a symmectric encryption scheme:

- Ciphertext only
- Known plaintext
- Chosen plaintext

(3p) 4. *(ILO: 2)* Given the following Kerberos exchange where client C want to get access to server V through the authentication server AS:

C $\rightarrow$ AS:	$\mathrm{ID}_C \| \mathrm{P}_C \| \mathrm{ID}_V$
AS $\rightarrow$ C:	Ticket
C $\rightarrow$ V:	$\mathrm{ID}_C \|$Ticket

Ticket $= E(K_v, [\mathrm{ID}_C] \| \mathrm{AD}_C) \| \mathrm{ID}_V$

Name and explain three problems that allows an attacker to use this protocol. For each problem you mention, you must also show how this can be corrected.

(3p) 5. *(ILO: 2)* WEP has been long considered not secure. When data is sent over WEP the confidentiality of the data is based upon the RC4 stream cipher. To replace WEP another security standard called WPA was introduced. WPA is also based on the RC4 stream cipher but is considered safer than WEP, why is this?

(3p) 6. *(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.

(3p) 7. *(ILO: 3)* Explain when it is appropriate to apply a security mechanism on the network layer, transport layer and application layer. What security mechanism is used where? Name at least one downside of that security mechanism.

(3p) 8. *(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) 9. *(ILO: 3)* A popular choice of encryption technique when using IPSec is AES-CTR or some versions of the CTR-mode.

- What does AES-CTR mean? Explain on a technical level, not just state what it is short for.
- What are the advantages of using CTR instead of for example CBC with IPSec?

References

[1] William Stallings. *Network security essentials : applications and standards.* 4. ed. Upper Saddle River, N. J.: Prentice Hall, 2010. ISBN: 0-13-706792-5 (pbk.)

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