Mittuniversitetet

MID SWEDEN UNIVERSITY

Final exam

DT116G Network Security

Daniel Bosk
daniel.bosk@miun.se
Phone: 060 - 14 8709

Lennart Franked
lennart.franked@miun.se
Phone: 060 - 14 8683

2013-01-09

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, do not write about subjects remotely related to the question.

Write your answers on separate sheets, not on the exam paper. Only write on one side of the sheets. Start each question on a new sheet. Do not forget to *motivate your answers.*

Make sure you write your answers clearly, if I cannot read an answer the answer will be awarded no points – even if the answer is correct. The questions are *not* sorted by difficulty.

Time 5 hours.

Aids Dictionary.

Maximum points 41

Questions 10

Preliminary grades

E $\geq$ 50%, D $\geq$ 60%, C $\geq$ 70%, B $\geq$ 80%, A $\geq$ 90%.

Questions

The questions are given below. They are not given in any particular order.

1. You have a web server configured with SSL. It was set up before your time, it has just worked so nothing needed to be changed. The SSL setup currently enables one cipher, and there has just been published a paper on a known-plaintext attack on this cipher.

   (3p) (a) You should be worried sick and be sleepless in the nights with this server setup running. Why?

   (1p) (b) What is your solution to the problem? The server has to be running.

2. When you communicate with your friends, to be sure that no one is trying to impersonate your friends you always sign your communication. Your friends want you to sign their newly generated keys. They send you these new keys in a message signed in with their old keys. Your friends use a simple MAC where

   (1p) (a) MD5,

   (1p) (b) SHA1, and

   (1p) (c) SHA256,

   respectively, are used as hash functions and the message digest is then signed with their old keys. Motivate the level of trust you would assign each new key.

3. (2p) Why would HMAC, using MD5 as a hash function, be better as a MAC than the usage example from previous question?

4. (6p) 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 implementations you have decided to implement your own version. You know that you need to decide upon an encryption algorithm and a cipher block mode.

   (a) Give pros and cons for using any of the following algorithms: RSA, 3DES, and AES.

   (b) Give pros and cons for using any of the following cipher block modes: CBC, CFB, and CTR.

5. (3p) 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?

6. (3p) 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.)

7. Given the three scenarios below, name *one service* and *one mechanism* that you can use to ensure the correct type of security. Your answer should *only* address that particular scenario.

   (2p) (a) You are sending a message to a friend and want to protect your message from passive attacks.

   (2p) (b) You have developed a piece of software and published it on the web. After a couple of months you find out that someone is redistributing a modified version of your software that contains a trojan horse. You want the users to use the correct version of your software.

   (2p) (c) When you arrive at work one day your boss calls you in to her office and informs you that she suspects that a disgruntled employee have been accessing sensitive information but she can't prove it. You want to prevent this from happening again.

8. (2p) Explain the difference between a circuit-level gateway and an application-level gateway.

9. (4p) In a Kerberos realm a server will allow users to access its services on the basis that the user can provide a valid Kerberos ticket. Explain why the server should trust such a user.

10. In the context of IPsec, explain the application of the following functions:

    (2p) (a) AH/ESP

    (2p) (b) Tunnel-mode

    (2p) (c) Transport-mode

    (2p) (d) SA/SAD

References

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