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

2013-04-25

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 33

Questions 10

Preliminary grades

The following grading criteria applies: E $\geq$ 50%, D $\geq$ 60%, C $\geq$ 70%, B $\geq$ 80%, A $\geq$ 90%; with no question awarded zero points.

Questions

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

(2p) 1. According to Lucks and Daum [1], 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?

(1p) 2. Why would HMAC, using MD5 as a hash function, be better as a MAC (but still not good) than the usage example from question 1?

3. Your company bought a license for a proprietary software suite. The security of this software is based on two ciphers; for the first there is published a known-plaintext attack and for the second there is published a ciphertext-only attack.

(2p) (a) What does this mean?

(1p) (b) Management forces you to use this software as they spent hard money on it. You are to send critical information to another office over the highly insecure network called the Internet, which of the two ciphers will you use?

(2p) (c) If the choice of crypto mechanisms was totally up to you, how would you do to ensure yourself that the transfer is perfectly correct – that is, both integrity and confidentiality is ensured.

4. The organisation you work for does all its crypto with DES-CBC.

(2p) (a) What does DES-CBC mean? Explain on a technical level, not just state what it is short for.

(1p) (b) Do you see any problems with this approach?

(3p) 5. Last week Mozilla held public discussions on whether to include or exclude TeliaSonera 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).

(2p) 6. 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 active 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 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. An organisation has a spam filter employed to filter all incoming email to the organisation's employees.

(2p) (a) As what type of firewall would you classify this spam filter? (This includes an explanation why.)

(3p) (b) Give an overview of what other types of firewalls exist and how they work.

(3p) 9. In a Kerberos realm a server will allow users to access its services on the basis that the user can provide a valid service-granting ticket. Explain why the server should trust such a user and provide its service.

(3p) 10. There is a trend among the populus to use the term "VPN-tunnel". Their purpose of using this service is to avoid surveillance of their habits on the Internet.

In essence, this is accomplished by having all your traffic routed through someone else, and thus have your doings associated with another IP-address – the same address as many others using the same service.

Explain how this is accomplished using IPsec.

References

[1] Stefan Lucks and Magnus Daum. Hash collisions (the poisoned message attack), 2005. URL `http://th.informatik.uni-mannheim.de/people/lucks/HashCollisions/`.

[2] 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.).