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

2013-08-21

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 36

Questions 10

Preliminary grades

The following grading criteria applies: 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.

(2p) 1. In 2011 a group of hackers, that calls themselves LulzSec, managed to do an SQL injection attack on Sony and with that retrieved over one million user accounts; including information such as their names, home address, passwords, email addresses et cetera. The CSO (Chief Security Officer) at Sony had apparently not taken a course in computer security, if he did, he must have cheated his way through the course, since all this information was stored in plain text. Explain in detail how they should have stored this information in their database to protect themselves against these kinds of attacks.

(1p) 2. 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.

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 chosen plaintext attack and for the second there is published a known-plaintext 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. A popular choice of encryption technique when using IPSec is AES-CTR or some versions of the CTR-mode.

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

(1p) (b) What are the advantages of using CTR instead of for example CBC with IPSec?

(6p) 5. 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.

$A \rightarrow AS : E_{A,AS}(Id_b)$
$A \leftarrow AS : E_{A,AS}(K_{ab}, E_{B,AS}(K_{ab}, Id_A))$
$A \rightarrow B : E_{B,AS}(K_{ab}, Id_A)$
$A \rightarrow B : E_{K_{ab}}(Message)$

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

(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 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 using a Gmail-account and don't want the contents of your e-mails to be subjected to NSA-screenings.

(2p) (b) You have moved to a mountain-top and your only means of communicating is through carrier pigeons with the help of the IPoAC (IP over Avian Carriers) protocol [2], and you need to ensure that only authorized people are able to read your messages.

(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 populace 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] 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.).

[2] D. Waitzman. Standard for the transmission of IP datagrams on avian carriers. RFC 1149 (Experimental), April 1990. URL `http://www.ietf.org/rfc/rfc1149.txt`. Updated by RFCs 2549, 6214.