KTH Datavetenskap
och kommunikation

DD2395 Computer Security
Re-Exam 2011-06-01, 14.00 –17.00

This is a closed-book exam, no material (books, articles, laptops, phones, or any other electronic devices, etc.) permitted. Please answer in English if you can, only answer in Swedish if you must. Grading is according to the following preliminary point allocations. E 16–19p, D 20–22p, C 23–25p, B 26–28p, A 29–30p. Good luck!

1 CIA. [3 points]

1a Explain the components of the CIA model: Confidentiality, Integrity, Availability.

1b Which of these does encryption provide?

1c Which of these do message authentication codes provide?

2 Digital envelopes. [2 points]

2a How do digital envelopes work? Describe all the necessary steps.

2b What are they used for?

3 E-Mail. [2 points]

To secure e-mail, we used gpg in a lab exercise. Alice heard about that and now wants to do the same to exchange e-mails with Bob. Which keys does she need to have in the following cases and what for?

3a Alice sends an e-mail to Bob and signs it.

3b Alice receives an encrypted and signed e-mail from Bob.

3c Alice wants to send an e-mail to Bob but prevent Carol from reading it.

3d Alice suspects that Carol has been sending e-mails to Bob pretending that they come from Alice. Alice wants to avoid that.

4 Denial-of-service. [3 points]

4a What is a denial-of-service attack?

4b Describe two different examples and how they work.

5 Security principles. [1 point]

5a What is the principle of least privilege?

5b Why is it important?

6 Web attacks. [3 points]

6a Explain briefly how SQL injection works and how to defend against it.

6b What is the main difference between cross-site scripting and cross-site request forgery attacks?

7 Access Control [3 points]

Alice has started a legal consulting company. She wants to make sure that access to resources are secure and no one unauthorized can get to sensitive data of her clients.

7a How would you advise her to organize access control in the company, taking into account that the company is growing fast and new employees come and go?

7b It is important to Alice that client confidentiality is kept and she does not want information from competing clients leak to each other. How can she do this?

8 Software security. [3 points]

8a What happens in buffer overflow attacks?

8b What are canaries and how can they help against buffer overflow attacks?

8c Name and explain two strategies of defensive programming.

9 Malware. [3 points]

9a Viruses and worms can disguise themselves in various ways to avoid detection. One way is polymorphism. How does it work? Name two other ways for avoiding detection.

9b What are trojan horses? What are they used for?

10 Authentication. [3 points]
Usual authentication systems verify passwords with the help of their hashes stored in protected files.

10a What is the purpose of storing password hashes rather than the passwords themselves?

10b Why should we protect the access to the password hashes?

10c What is the purpose of salts?

11 Firewalls. [1 point]
Bob wants to set up a firewall for his home network. He is risk averse and wants to be sure that no unwanted traffic gets in, even if that means that some legitimate traffic does not get through, either. What should be the default setting of his firewall?

12 Honeypots. [1 point]
Give two reasons for deploying honeypots.

13 Social Engineering. [2points]

13a What is meant by the term “social engineering”?

13b Describe one example of social engineering and what could be done beyond general education to prevent it from succeeding.