KTH Datavetenskap
och kommunikation

DD2395 Computer Security
Exam 2012-01-10, 10.00 –13.00

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 29–31p. Good luck!

1 CIA. [3 points]

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

1b Which of these can message authentication codes provide? How does that work?

2 Cryptography. [1 point]

There is an assumption underlying the following algorithms that - given large enough numbers for the parameters - it is difficult for an attacker to do the computation necessary to break them. What is the computation an attacker needs to do that makes it hard to break

2a RSA public-key encryption?

2b Diffie-Hellman key exchange?

3 Web attacks. [2 points]

Pick 2 items from the following list and explain briefly what they are and what an attacker can do:

- Broken Authentication and Session Management
- Insecure Direct Object References
- Cross-Site Request Forgery (CSRF)
- Security Misconfiguration
- Insecure Cryptographic Storage
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Unvalidated Redirects and Forwards

4 Denial-of-service. [3 points]

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

4b Explain reflection and amplification.

5 Security principles. [1 point]

5a What is the principle of complete mediation?

5b Why is it important?

6 Access Control [2 points]

6a What is the main difference between discretionary and mandatory access control?

6b List and explain 2 advantages of role-based access control.

7 Multi-Level Security [2 points]

KTH wants to adopt a multi-level mandatory access control system to make sure upcoming exams are kept confidential.

7a Which system would you choose for this purpose and why? Bell La Padula, Clark Wilson, or Chinese Wall?

7b What difficulties can you foresee if such a system were adopted?

8 Software security. [3 points]

8a What does an attacker need to do to exploit a stack overflow vulnerability to make a program crash? What if the attacker wants to run their own code first?

8b For performance reasons, you'll have to use C for a program. As the programmer, what can you do to prevent buffer overflow attacks? Explain 2 techniques.

8c How can you avoid race conditions?

9 Malware. [3 points]

9a Viruses and worms go through different phases over their life-time; list and explain at least 3 of them.

9b What can botnets be used for? List and explain two uses for an attacker.

10 Authentication. [3 points]

10a List and explain 3 ways of attacking password-based authentication.

10b What are appropriate countermeasures for these?

11 Firewalls. [1 point]

11a What is the purpose of a demilitarized zone (DMZ)?

11b What does one typically put into a DMZ?

12 Intrusion Detection. [2 points]

12a What are advantages and disadvantages of signature-based detection versus anomaly detection?

12b Where would you place a honeypot? Explain why.

13 Consulting. [2 points]

How would you respond to the following statements? Come up with an argument for why this is or is not a good idea.

13a I prefer to log in as administrator or root, this way I don't have to type in my password so often.

13b I just implemented my own version of AES and made some changes and optimizations. Now it runs much faster!

13c As a system administrator, I make the default settings very secure for the users. If need be, they can be changed later.

13d When programming, I make sure to check user input against all the ways I can think of that it can go wrong. If I find a match, I raise an exception.

14 Social Engineering. [3points]

14a What is meant by the term "social engineering"?

14b List and describe 3 human tendencies of behavior that are commonly exploited by social engineers.

14c What countermeasures would you take to prevent such exploitations?