KTH Datavetenskap
och kommunikation

DD2395 Computer Security
Exam 2010-03-18, 09.00 –14.00

This is a closed-book exam, no material (books, articles, laptops, phones, etc.) permitted. Write your answers directly on the exam paper, and put your name, etc. on each page according to the general instructions for exams. If you run out of space, you can use extra paper.

To pass this exam you have to pass the first part, that means a Pass grade on at least 6 questions in the first part.

The second part will determine the grade according to the following preliminary point allocations. D – 14p, C – 19p, B – 23p, A – 29p, provided that the first part has resulted in a Pass grade. Good luck!

Part I

1 CIA.

Explain the components of the CIA model: Confidentiality, Integrity, Authenticity. Which of these does encryption provide?

2 Authentication.
Describe two fundamentally di´erent conceptual approaches that can be used for user authentiaction. Be concise: One sentence each should su˘ ce.

3 Intrusion Detection.
What is a honeypot? What is it used for?

4 Access control.
True or false? Justify your answer in one sentence: Access control matrices can represent anything that is represented by access control lists.

5 Bu´er overflow.
Explain briefly what bu´er overflow attacks are and how to defend against them.

6 Malicious software.
What is the di´erence between a virus and a worm? What do they have in common?

7 Security principles.
What is the principle of least privilege? Why is it important?

Part II

8 MAC v. Digital Signatures.
Message authentication codes (MAC) and digital signatures both serve to authenticate the content of a message. Which of the following best describes how they di´er?

a) A MAC can be verified based only on the message, but a digital signature can only be verified with the secret key used to sign the message.

b) A MAC can be verified based only on the message, but a digital signature can only be verified with the public key of the party that signed the message.

c) A MAC can only be verified with the secret key used to generate it, but a digital signature can be verified based only on the message.

d) A MAC can only be verified with the secret key used to generate it, but a digital signature can be verified with the public key of the party that signed the message.

9 Cryptography. [1 point]
What advantage does public-key encryption o´er over secret-key encryption?

10 E-Mail. [1 point]
True or false? Justify your answer in one sentence: Suppose I generate a RSA public and private key pair, and I publish the public key. Then that's all I need to be able to send you a securely encrypted email.

11 Defaults. [3 points]

11a Which is generally safer (from a security point of view), a firewall with a "default deny" policy or a firewall with a "default allow" policy? Why?

11b Many spam filters can be configured to either use a whitelist or a blacklist. Name one advantage of using a whitelist instead of a blacklist for your spam filter.

11c Name one disadvantage of using a whitelist (compared to a blacklist) for your spam filter.

12 Firewalls. [3 points]

Explain the strengths and weaknesses of each of the following firewall deployment scenarios in defending servers, desktop machines, and laptops against network threats:

a A firewall at the network perimeter (i.e., where the network meets the Internet)

b Firewalls on every end host machine.

c A network perimeter firewall and firewalls on every end host machine.

13 Web Attacks. [4 points]

13a List 3 common attacks on web applications.

13b Pick one of these attacks and describe how it works.

13c What would be an appropriate counter-measure to this attack?

14 DoS. [2 points]

The software company Snoracle is selling a new defense against DDoS attacks. Their software looks at the source IP address on all incoming packets, and if it finds any IP address that accounts for more than 1% of traˇ c over the last hour, it installs an entry in the router that blocks all packets from that address for the next 24 hours. Their marketing folks are claiming that this will stop all DDoS attacks cold in the water. Is this a good solution to the problem? Give one reason why or why not.

15 Social Engineering. [2points]

What is meant by the term “social engineering”? Describe one example of social engineering and what could be done to prevent it from succeeding.

16 Security consulting. [4 points]

You have been hired by a company to review the communication confidentiality design created in house. Obviously the designers have not taken DD2395. Identify two of the worst security design errors and describe the problems caused by each of these errors.

In the SecureComm architecture, we avoid the overheads of installing a public-key infrastructure (PKI) by relying on a simpler approach of manually distributed shared keys between all pairs of communicators. Since the organization only has 25 communicators which will eventually grow to 50 over the next five years or so, we feel this approach will cost less in software and time than dealing with a full PKI solution. The keys will be passed to communicators via a separate channel such as a CD or thumb drive, so the sensitive key will not be sent in the clear. The master key file includes all the pairwise shared keys, and it can be stored on the central server. It will be stored under a very restrictive access control, so only members of the Administrative group can access the file to add or distribute keys. The master key file also provides a natural key escrow benefit. If an employee loses his or her key or leaves the organization, the administrator can access the appropriate keys from the master key file to access his or her networked conversations. The shared key will be used in a block encryption algorithm designed by us called SuperCrypt. The algorithm is more sophisticated than AES, plus it has the benefit that it is proprietary so the attacker will not be able to attack the structure of the encryption algorithm.

17 RSA. [3 points]
Alice is setting up a RSA key pair. She has selected p=13 and q=11

17a What is n?

17b What is Œ(n)?

17c What values can be posted publicly and still preserve the security of the key pair?

17d What RSA operation would Alice apply to a message m to convince Bob that she originated m?

17e Alice has picked a session key k. Assume Alice already has access to Bob's public key. How should Alice compose a message to Bob to pass the session key while preserving confidentiality and integrity of data and identity?

18 Software security. [2 points]
What can we do to make code safe? Give 2 example strategies.

19 Policy. [4 points] Alice and Bob work as attourneys and use the "chinese wall" policy. The o˘ ce has 6 companies as clients, numbered 1 to 6.
Each company has 3 objects: a business plan P, an internal budget B, and a public (sanitized) annual report R. We use $P_1; B_1; R_1$ for client 1's objects, and so forth.
We have three groups. Within the groups, there is no conflict, but between the groups there are conflicts of interest: $COI_1 = f1; 2g; COI_2 = f3; 4g; COI_3 = f5; 6g$.
Alice specializes on COI_3 and does not have reading rights for the private (unsanitized) objects belonging to the companies in the other COIs. Bob starts out with reading rights to everything. Alice and Bob now try to execute, in order, the following operations. Which ones are accepted and which ones are not? Explain why.

1. Alice tries to read from P_5

2. Alice tries to read from B_2

3. Bob tries to read from P_3

4. Bob tries to write to B_1

5. Alice tries to write to B_6

6. Bob tries to read from B_4

7. Alice tries to read from R_1

8. Bob tries to read from B_2