Computer Security 1, COMPGA01, 2010-11

Answer ALL questions. 2.5 hours.

Answers should be short, straightforward and clear. 100 marks total.

Marks for each part of each question are indicated in square brackets

Calculators are NOT permitted

Question 1. Questions about network security.

1. A workstation with an IP address of 10.0.0.1 carries out a ping 10.0.0.2 command. Shown below (in order) is the network traffic on the LAN (Local Area Network). The commands between square brackets are written in an informal way making them easier to understand for the reader.

step 1 10.0.0.1 sends [ARP who-has? 10.0.0.2] to the LAN broadcast address.

step 2 10.0.0.2 replies [ARP is-at 0A:BC:00:00:00:1F] to 0A:BC:00:00:00:1A

step 3 10.0.0.1 sends ping packet to 10.0.0.2

Answer the following five sub-questions:

(a) What does the acronym MAC stand for? What is the main purpose of it? This is in the context of this exercise (not in cryptology and not in access control theory).

(b) How many bits does it have in wired networks (Ethernet)?

(c) Security-wise, is it better to have this MAC value implemented in hardware or as a software feature?

(d) What is the MAC destination address in the ping packet in the example above?

(e) What is the MAC address of the workstation initiating the ping request?

[5 marks]

2. An attacker notices that a particular network request "Request A" from a client to a software application running on a server is always 30 bytes long (including UDP headers, IP headers and Ethernet headers). In response to this request, the server always provides the reply "Reply B", which is 600 bytes long (also including UDP+IP+Ethernet headers). The attacker decides to spoof the IP address of the client and use this as the source IP address when sending many requests of type "Request A" to the server. We assume that all communication between the client and the server is based on UDP (User Datagram Protocol). If the attacker has 1 Mbits/s of outgoing bandwidth, assuming he can use all of it to mount an attack against a victim, and neglecting any additional overheads, how much of the victim's bandwidth will be used by the attack?

[3 marks]

3. What is a firewall? State at least 3 and at most 5 key fundamental principles of computer security which apply to firewalls and elsewhere. For each of these principles explain using one example, or in one way, how firewalls may reflect, play a certain role in, or help to implement, the application of this principle.

[4 marks]

4. For each of the following three words: X = Software, Hardware or Stateful explain a) what X means as an adjective in a context of firewalls. b) What is one thing which is good and positive about it, mostly from the security perspective. c) What is one thing which is problematic or dangerous about it, again from the security perspective. Overall we expect 9 answers.

[4 marks]

5. Explain the term DMZ in the context of network security.

[2 marks]

[Total 18 marks]

Question 2. Questions about computer security, data security, cryptography, storage and management of confidential data, passwords and keys.

Prof. Sandwich has email client software installed on a local PC, which always connects to his company's mail servers situated in a DMZ through and over the classical SMTP protocol. Before Prof. Sandwich can use his PC, he enters his password, which is unknown and assumed to follow a probability distribution with high entropy.

1. List between 3 and 4 essential requirements or recommendations for the secure storage of this password on the local hard drive.

   [3 marks]

2. Assume that the entropy of his password is as high as 80 bits. Is this enough? Assuming that passwords are NOT reused in multiple systems, what else do we need to look at? Given several different probability distributions with entropy being equal to 80 bits, can some of these distributions be much weaker and how?

   [3 marks]

3. Explain how dropping the privileges can be used to protect an email application against a rogue email containing an exploit.

   [3 marks]

4. Is SMTP traffic encrypted and are emails sent by Prof. Sandwich encrypted and authenticated?

   [2 marks]

5. Can a hacker somewhere on the wider Internet (outside Prof. Sandwich's company) use an ARP poisoning attack to intercept his SMTP traffic?

   [2 marks]

6. If we choose some sort of a secure SMTP extension (could be based either on SSL, SSH, Kerberos or other protocol) what is a necessary **trusted setup** condition which should not be forgotten at the moment of installing or configuring the email system?

   [2 marks]

Question 2 continued.

Prof. Sandwich sometimes uses PGP, GNUPG as a plug-in for his email software.

7. Explain what is the meaning of Hybrid Encryption.

[2 marks]

8. Why, when sending an encrypted email message with PGP, do we want to add ourselves to the recipient list?

[2 marks]

Question 2 continued.

One day Prof. Sandwich lost his private key but he still has the corresponding public key. His hard drive crashed due to a mechanical fault, and he cannot recover all the data, but he still has the hard drive and it was neither stolen nor otherwise compromised. He decided not revoke this key because he is too busy and he is confident that it was never compromised.

9. Provide some advice about how to really destroy the data on a hard drive so that he can be confident the nobody will recover his private key. Provide one argument to the effect that destruction is in this case arguably better or more secure than revocation.

[2 marks]

10. On the next day Prof. Sandwich was able to restore his computer, his emails and his settings to work back again from his backups, but the private key was never a part of his backups. Can he still send encrypted emails? Can anyone decrypt any of the encrypted emails sent to him?

[2 marks]

11. What does he need to do now, to be able to recover all the benefits of having a secure email system? What assumptions and maybe related hardware requirements would we like to have here or/and what could go wrong with a process of secure key **generation**? We omit problems related to secure key storage and trust/certificates.

[2 marks]

12. How can this private key be securely stored on a hard drive (not using any special hardware or smart cards)? What security remains if his computer is now stolen or hard drive partition cloned? Can you propose one extra enhancement?

[3 marks]

[Total 28 marks]

Question 3. Explain in detail the following notions, definitions, technical terms or acronyms. Between 2 and 10 lines of explanation are expected for each sub-question.

1. Memory protection, segmentation and paging.

   [4 marks]

2. A Trusted Path Mechanism.

   [2 marks]

3. DEP and NX bits. Why or how it became an 'NX bit' to be set and not an 'X bit' to be disabled?

   [2 marks]

4. Explain step by step a typical code injection attack with buffer overflow and stack smashing. The student may draw a pictures with text heap and stack, and explain what happens at different stages.

   [10 marks]

5. Explain how the concept of $W \oplus X$ can be used to prevent these buffer overflow attacks.

   [2 marks]

6. Explain how ASLR and Random Canaries can be used to prevent these buffer overflow attacks.

   [4 marks]

[Total 24 marks]

Question 4. Questions about Biba model.

1. Explain the term MAC in the context of access control theory (not in cryptography and not in networking).

   [2 marks]

2. Given a lattice and a totally ordered set, write a definition of the Bell-LaPadula or Biba product lattice.

   [3 marks]

3. In Biba model, explain what is the semantics or our understanding of what it means for a file to be at a high integrity level in some lattice.

   [2 marks]

4. Explain in terms of information flow, the mandatory requirements in Biba model. Give a correct interpretation of the two main rules regarding reading and writing.

   [3 marks]

5. Consider the set of integrity levels $L = \{low, admin, kernel\}$, where $kernel > admin > low$. Furthermore consider the set of categories Cat containing

   $$Cat = \{HRandAdmin(H), MarketTraders(T), ITEngineers(E)\}.$$

   Compute the exact number of security classes in the product lattice.

   [3 marks]

6. Compute the bottom element $\bot$ in the product lattice.

   [2 marks]

7. Name and compute the following bound in the product lattice:

   $$(admin, \{E\}) \vee (kernel, \{H\}).$$

   [2 marks]

8. Name and compute the following bound in the product lattice:

$$(low, \{E\}) \wedge (kernel, \{T, E\}).$$

[2 marks]

9. List all the security classes that a subject with classification $(admin, \{E\})$ can write.

[3 marks]

10. A security software package with anti-virus functionality was installed by a person with clearance $(kernel, \{H, T, E\})$ and all its key components have level $(kernel, \{H, T, E\})$. Explain how the Low-Water-Mark Policy for Subjects could allow a sub-process spawned, potentially running at a different integrity level than the father process, to access any file in the system and check them for viruses.

[4 marks]

11. Explain how the Biba's optional Controlled Invocation (Ring Invocation) policy could potentially be used to prevent a trader who logs at level $(admin, \{T\})$ from injecting an exploit into his trading console program running as $(kernel, \{T\})$ which would allow him to override the limit of 5 millions dollars per day which is the maximum amount of money he is allowed to spend in one day on purchasing some trading options on an external automated market exchange system.

[4 marks]

[Total 30 marks]

[Total For The Whole Exam 100 marks]

END OF PAPER