Computer Security 1, COMPGA01 and COMPM062, 2012-13

Answer ALL questions. 2.5 hours.

Correct answers should be short, straightforward and clear, rather than long and obscure.

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

Calculators are NOT permitted

Question 1. Questions about theory and mathematical models.

1. Given a poset $A, \leq$ give an exact **mathematical** definition of GLB (defined as a certain element of a certain set satisfying certain properties). Explain the acronym GLB.

   [5 marks]

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

   $$Cat = \{Management(M), HR/Admin(H), Auditors(A), Traders(T), ITPersonnel(I)\}.$$

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

   [5 marks]

3. In the 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. What can we say about the information flow in the strict Biba model? Can information flow between two unrelated levels in the lattice?

   [5 marks]

4. Let $\mathbb{N}, |$ be a poset where $|$ is the division relation. Is it a lattice? Please justify your answer. Compute $LUB(18, 16)$ and $GLB(18, 16)$ if they are defined.

   [5 marks]

5. Which relations are NOT transitive? Any number between 0 and all solutions can be selected.

   (a) Having a shared factor for integers

   (b) Each number n is $\geq$ itself and 1 and no other number.

   (c) The relation ”dominated by” in a BLP lattice

   (d) Relation on sets commonly known as $\subset$: being subset of another set or equal.

   (e) We say that computer1$\Rightarrow$computer2 IF computer1 knows the MAC address of computer2 and stores it in a local ARP cache.

   (f) Relation $a|b$ or a divides b for natural integers.

   (g) Equality of fractions like $3/6 = 1/2$ is they are equal as real numbers.

[7 marks]

6. Which tasks can be performed by a Turing machine in constant time? Select zero, one or several answers.

   (a) Deciding whether a 10000-bit long string of 0s and 1s is generated with by pseudo-random number generator with some (unknown) 64-bits seed.

   (b) Deciding whether a given program in Java halts within 2^{64} steps

   (c) Factoring a 1024-bit SSL/TLS RSA public key

   (d) Finding a collision for MD5 hash function as implemented in Unix or other OS in order to forge a security update: produce two updates with the same signature.

   (e) Deciding whether a program contains a buffer overflow exploit.

   (f) Blocking all viruses in such a way that they are always prevented from doing any harm.

[6 marks]

[Total 33 marks]

Question 2. Questions about OS and computer security.

1. Why should the current directory ”.” not be added to UNIX PATH? Give one reason why this would be a bad idea.

   [3 marks]

2. Explain and/or draw a picture to show how a compiled C program will call a sub-routine, what is the relative position of the return address and how this can be exploited to run arbitrary code. Is it a good idea to wipe the stack to remove the local variables and data (which would remain in RAM), just before leaving the routine?

   [10 marks]

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

   [5 marks]

4. Give one example of one special privilege of the OS Kernel under Linux or Windows.

   [2 marks]

5. In Windows many objects will have a ”security descriptor”. How does it work for files? Explain what is ACL and ACE. What kind of data does one ACE contain?

   Are these objects stored in the object’s directory of the hard drive, in system directories, user data files, in RAM, or in the registry?

   What mechanisms prevent the user from reading some of sensitive administrative and system-level rights?

   [6 marks]

[Total 26 marks]

Question 3. Questions about network security and SSL/TLS.

1. An IP datagram (one IP packet) has always the following security features: Select zero, one or several answers:
   (a) it is digitally signed

   (b) it is protected against accidental modification or transmission error

   (c) it is encrypted

   (d) it cannot be decrypted if we do not have the chaining value from the previous packet

   (e) it is protected against modification of source/destination IP address

   [5 marks]

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

   [3 marks]

3. Name two protocols which use SSL/TLS, and which are extensions of earlier insecure protocols. Explain very briefly what they do.

   [2 marks]

4. Assume that we want to consult our email via IMAPS. What is the necessary **trusted setup** condition which should not be forgotten at the moment of installing or configuring our client email system? Why and when this setup would in many cases not be needed?

   [4 marks]

5. Explain the Man-In-the-Middle attack on the Diffie-Hellman key exchange. How does SSL/TLS solve or tries to solve this problem?

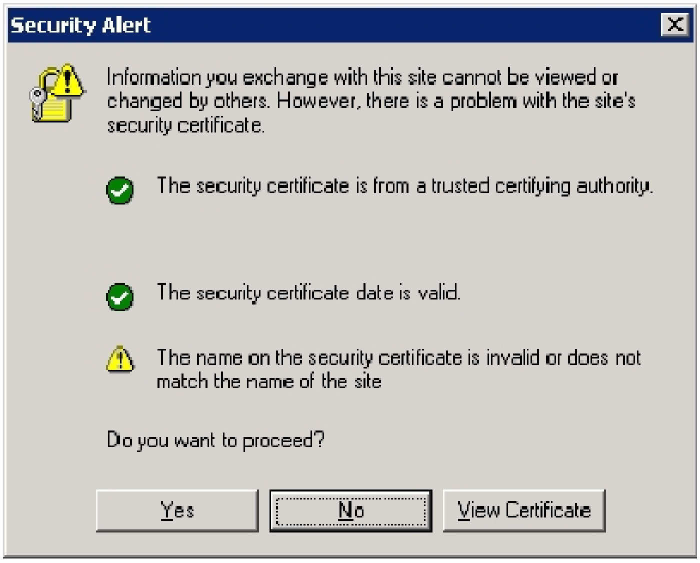
   [12 marks]

6. Explain the two main stages in TLS: TLS Handshake and Secure Communication stage. What happens at each stage? How the authenticity of public keys is guaranteed?

   [5 marks]

7. For each of the following **four** security alerts, provide a plausible explanation as to why these messages are displayed, and what are the risks if we accept.

Q3.7.a.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

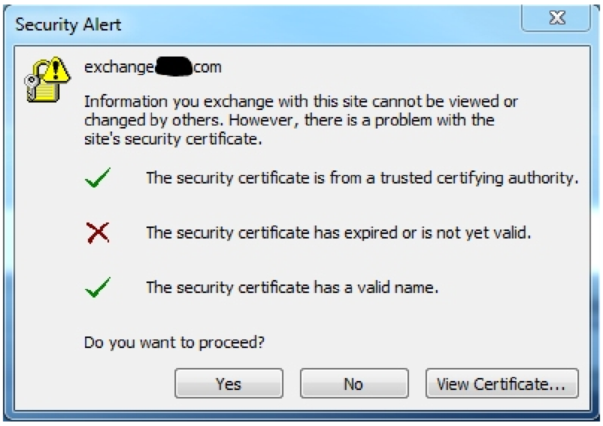
✓ The security certificate is from a trusted certifying authority.

✓ The security certificate date is valid.

⚠ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

Q3.7.b.



Security Alert

exchange[redacted]com

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

✓ The security certificate is from a trusted certifying authority.

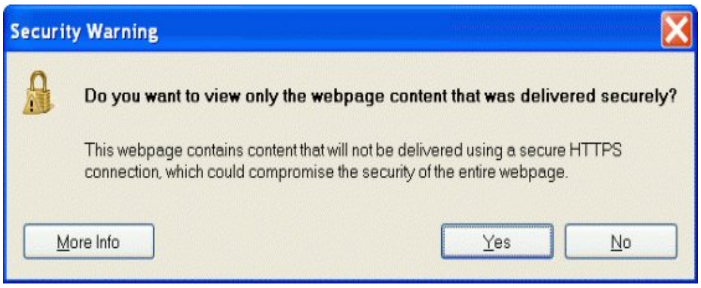
✗ The security certificate has expired or is not yet valid.

✓ The security certificate has a valid name.

Do you want to proceed?

[Question 3.7 continues on the next page]

Q3.7.c.

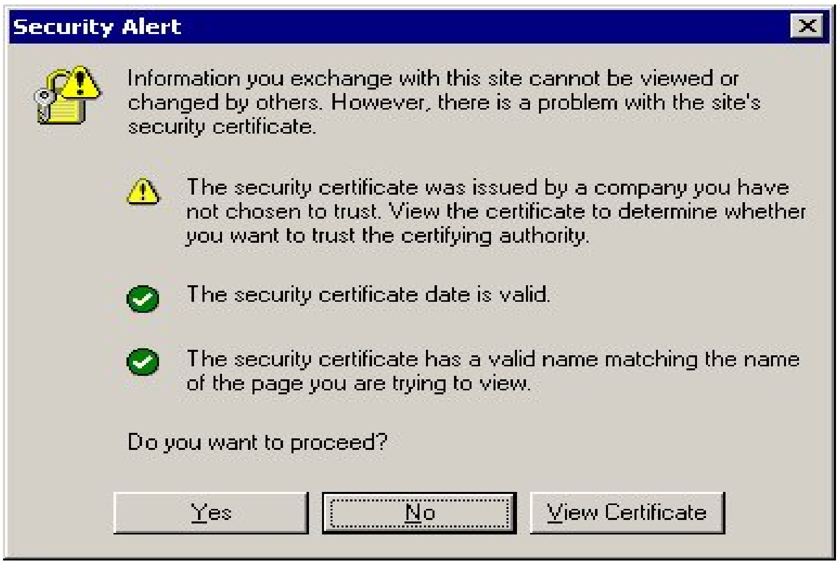


Security Warning

Do you want to view only the webpage content that was delivered securely?

This webpage contains content that will not be delivered using a secure HTTPS connection, which could compromise the security of the entire webpage.

Q3.7.d.



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.

✓ The security certificate date is valid.

✓ The security certificate has a valid name matching the name of the page you are trying to view.

Do you want to proceed?

[10 marks]

[Total 41 marks]

[Total For The Whole Exam 100 marks]

END OF PAPER