Alternative assessment:

Computer Security 1, COMP0054

Main Summer Examination period, 2019/20

There are FOUR questions.

Answer ALL questions.

Word limit / page limit:
10 pages maximum and
3000 words maximum.

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.

Question 1. Questions about network and communications security which require longer answers and some research.

1.1. What is the purpose of TCP protocol? Explain the TCP handshake and the SYN flooding attack. What are the assumptions about the attackers? How can we defend against this attack? The answer is expected to be 1 page maximum.

[8 marks]

1.2. Based on paper and slides by Degabriele and Paterson posted as two PDF links inside our Moodle section 6, and also our TLS slides explain on one page maximum, how IPv6 encrypts data of packets in ESP mode. What is the ESP mode for and how does it compare to AH? Which of the two does encryption and confidentiality? Is a MAC used inside ESP with encryption only in mind?

What is the maximum size of payload allowed in IPv6? What is the maximum data block size in TLS? We want to know exactly how an ESP trailer works, please provide two examples of valid padding and trailer, assuming cipher block size of 128 bits. Please also provide one example which is not valid due to padding being invalid. Can a padding be empty? Can a trailer be empty?

[8 marks]

1.3. Here we will study our TLS slides with MAC-then-encrypt and padding oracles, and also and again slides and paper by Degabriele and Paterson. Explain in detail in TWO pages maximum, the concept of breaking CBC MAC encryption with a series of spoofed messages. Explain the concept of ESP Trailer oracles. How does it compare to Vaudenay padding oracles and to attack when the padding WAS checked [e.g. timing difference attacks] on TLS studied in class and in our slides? What are arguments in favour or against using MAC-then-encrypt? Is MAC-then-encrypt provably secure? What is CPA? What is CCA? Please include one drawing showing CBC mode decryption (not encryption) process. The notations used in figures and inside the text must be consistent and all abbreviations should be intelligible. What is the order 3 operations: decrypt, verify MAC, verify ESP trailer in typical basic encrypted IPv6 operation? How ESP trailer oracle can be made due to how fragmentation is handled and what is the text of the error message exploited?

[14 marks]

[Total 30 marks]

Question 2. Multiple choice questions about communications security. For each question please indicate an answer Y or N. A third answer “I don’t know” is not allowed.

2.1. Which statements about cryptographic engineering, CBC mode and attacks in TLS are correct?

(a) the dominant philosophy in TLS until 2017 was MEE = Mac then Encode and Encrypt. This means that the message authenticity could only be checked after decryption.

(b) In 2018 TLS switched to key transport.

(c) In 2018 TLS switched to AE.

(d) CBC mode requires a random or unique IV which is chosen by the sender and required for decryption.

(e) CBC is secure against known plaintext attacks.

(f) CBC is secure against chosen plaintext attacks.

(g) TLS in 2008 was secure against padding attacks because implementations checked the padding.

(h) Padding in TLS has variable size and must be non-empty therefore padding verification can always potentially fail producing an (encrypted) error message.

(i) A padding oracle is an oracle to which we send a message and it appends valid padding added to this message.

(j) We call a padding oracle any method to tell apart if padding bytes were correct or not and leaking some information about their correctness to the attacker.

(k) Padding oracles are just distinguishers and do not allow to perform decryption of any data inside TLS secure sessions.

(l) Padding oracle attacks are chosen ciphertext attacks with modification of original ciphertexts.

(m) CBC is vulnerable to padding oracle attacks.

[12 marks]

2.2. Which statements about cryptography in TLS are correct?

(a) Public key encryption in TLS ensures the authenticity of messages.

(b) Public key encryption schemes become insecure once the adversary learns the encryption key.

(c) There exist public key encryption schemes that are secure (in practice) against *active* adversaries ('IND-CCA attackers').

(d) Signature schemes ensure the confidentiality of messages.

(e) Digital signatures ensure the authenticity of messages.

(f) Digital signatures prevent message replay and re-ordering attacks.

(g) TLS is insecure once the adversary learns the signature verification key.

(h) Key Transport (KT) schemes or hybrid encryption KEM+DEM schemes offer Forward Security and session independence.

(i) AE security ensures that an attack where ciphertexts are modified to extract meaningful information cannot work.

(j) TLS contains data which are authenticated but not encrypted.

(k) AE protects against real-time truncation attacks where information is leaked about parts of messages being or not correctly decrypted before the full message in several blocks is processed.

(l) AES-GCM is a type of AE used in TLS since 2015.

[12 marks]

[Total 24 marks]

Question 3.

3.1. In Unix, when an ordinary process is run by a user, does it have the access rights of the user, or the rights of its owner? Explain the meaning of EUID and RUID. Explain the concept of a setgid program.

[4 marks]

3.2. Give four examples of privileges that a process owned by the Kernel (for example a system process) will have under Linux.

[4 marks]

3.3. 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 would prevent the user from reading some of sensitive administrative and system-level rights?

[7 marks]

3.4. What is a reference monitor? State the three main properties it should satisfy.

[3 marks]

[Total 18 marks]

Question 4. Questions about theory and mathematical models.

4.1. What is an order relation? Is a relation defined over integers by “each element is related to every other element” an order relation? Is it also a lattice?

[4 marks]

4.2. Explain briefly the Chinese wall model. Imagine a law firm working for several large corporate clients. Propose a contrived example where a Write operation (W) would be denied, and explain why.

[6 marks]

4.3. Consider a set which contains $1, a, b, ab$ and their linear combinations with coefficients being 0 or 1, such as say $ab + a + 1$ and with 0 being an empty linear combination. This set is sometimes known as Zhegalkin polynomials in 2 variables, Algebraic Normal Form (ANF) with 2 variables, or the ring of Boolean polynomials B_2. It corresponds to usual polynomials in two variables a, b where all the coefficients are reduced modulo 2 and with $x^2 = x$ for any variable x. In this ring we have $+$ and $*$ are operations for modulo 2 of polynomials which have all the desired properties we expect (such as distributivity $x(y+z) = xy + xz$. This set is also a lattice for the order relation being a division of polynomials in our ring. Questions to answer:

(a) How many elements has this set?

(b) How many elements in this set are divisors of 0 (tricky, think twice)?

(c) What is the BOTTOM element ($\perp$, the min or the GLB of all)?

(d) What is the TOP element ($\top$, the max or LUB of all)?

(e) What is $LUB(a, ab + b)$?

[10 marks]

4.4. Given a lattice of type $C = P(Cat)$, and a totally ordered set of classifications H write a definition of the Bell-LaPadula product lattice.

[4 marks]

4.5. 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? What if we had a total order?

[4 marks]

[Total 28 marks]

[Total for assessment: 100 marks]

END OF PAPER