Resit Advanced Network Security

Jaap-Henk Hoepman, Joeri de Ruiter

August 20, 2018

Name: _____

Student number: S _____

Please answer your questions using the space provided on the exam sheet. Write legibly, and use proper sentences; an unreadable answer is a wrong answer. . . Answer questions concisely, but with sufficient detail and precision. Always explain your answers. Please leave space in the margin for correction marks. Use a separate piece of scratch paper for draft answers, private computations or remarks.

Write your name and student number on every page.

You are not allowed to use books, notes, tablets, PC's and (smart)phones during the exam.

The total number of points that can be scored is 60, as specified alongside the questions. The final grade equals $1 + 9 * \frac{points}{60}$, rounded to the nearest half grade (except for grades between 5 and 6 which are rounded to nearest full grade).

Good luck!

Question 1 (12 points): Wi-Fi

a. *(3 points)* Consider the following scenario. A company sets up a wireless network that is protected using WPA2-Enterprise, where authentication is performed using PEAP-TTLS and the employees' company-wide username and password are used as credentials. What is the main risk involved when considering the configuration on the client side (e.g. an employee's laptop)?

b. *(3 points)* What is the main advantage and disadvantage of using PEAP-TLS compared to PEAP-TTLS?
Advantage:
Disadvantage:

c. *(3 points)* To authenticate when connecting to a WiFi network we can distinguish between WPA(2)-Personal and WPA(2)-Enterprise. What is the difference between the two?

d. *(3 points)* Assume a credential to access a network would be compromised. What would be the consequence with regard to passive eavesdropping for WPA(2)-Personal and for WPA(2)-Enterprise? Explain your answer.

Answer:

a. When a client is wrongly configured (for example when all certificates are accepted), the client can connect to a rogue network and, depending on the authentication method, provide credentials to a malicious party. These credentials might then also be used to access other resources of the company (i.e. the breach is not contained to only the Wi-Fi network).

b. The advantage is that credentials cannot just leak when connected to malicious network. The disadvantage is that it introduces the need for key management, which is hard to get right, as everyone needs a public key pair and corresponding certificate.

c. WPA(2)-Personal uses a shared key for authentication, whereas WPA(2)-Enterprise uses per-user authentication (e.g. using a username/password or certificate).

d. When intercepting the 4-way handshake, the only unknown input in the derivation of the session keys is the PMK (pairwise master key). With WPA(2)-Personal the PMK is derived from the shared key that is used to connect to the network. Therefore, if this shared key leads, it is possible to passively eavesdrop if the 4-way handshake is intercepted. With WPA(2)-Enterprise the PMK (used in the 4-way handshake) is not directly derived from the credentials, but is provided in the authentication step. This makes it harder to passively eavesdrop on WPA(2)-Enterprise sessions, even if the user's credentials are known.

Question 2 (6 points): Netflows

a. *(4 points)* Network flows can be used to detect suspicious activities on a network (e.g. botnet traffic or hacking attempts). What are the main differences when comparing this approach to traditional deep packet inspection (in an intrusion prevention system) with regard to performance and detection?
Performance:
Detection:

b. *(2 points)* An organisation experiences a DDoS attack by a very large botnet. What effect will this have on the flow metering and export phase of the flow monitoring process?

Answer:

a. Performance: the flow monitoring process introduce delays in the analysis, therefore a traditional IPS might be able to respond faster. However, with netflow is possible to handle more data than a traditional IPS that uses DPI.
Detection: with netflows we can only see metadata, whereas with DPI we have access to all data and are able to detect more attacks.

b. The large number of bots that take part in the attack results in a large number of flows. Therefore flow caches will fill up quickly and emergency expiration is triggered to flush the caches.

Question 3 (6 points): BGP

a. *(3 points)* One of the important aspects of SCION is isolation. Explain what this means with regard to end-entity authentication and how this compares to the current TLS infrastructure with respect to compromise of a Certificate Authority (CA).

b. *(3 points)* In the route discovery in SCION, the entities get short-lived certificates. What is the rationale behind the choice to make these certificates short-lived?

Answer:

a. CAs can only distribute certificates for their own isolation domain (ISD), so a compromise is kept local (i.e. it is not possible to create certificates for hosts in other ISDs). With the current TLS infrastructure. every CA can hand out certificates for any domain.

b. Revocation becomes easier. There is no need for additional infrastructure to revoke certificates. Certificates are simply revoked by not renewing them once they expired.

Question 4 (6 points): Botnets

a. *(3 points)* One method that is used in botnets to evade detection is domain flux. Explain how this works and what this defends against (from the perspective of the botmaster).

b. *(3 points)* When considering offensive techniques to defend against botnets we can distinguish between indirect and direct attacks. Explain the difference between these two types of attacks and give an example for each type.

Answer:

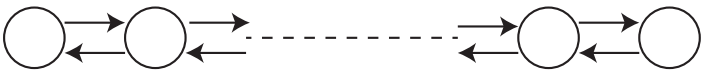
a. Many different domain names are used to refer to the same IP address. These domain names can, for example, be generated using a domain name generation algorithm. This defends against URL/domain name based detection using blacklists.

b. The aim of a direct attack is to disable the botnet by attacking one (or more) of the core components, whereas the goal of an indirect attack is to reduce the usability of the botnet. An example of a direct attack is to exploit a bug in the bot software. An example of an indirect attack is the insertion of fake information into the dropzone.

Question 5 (15 points):

a. *(5 points)* What is the difference between the leader election problem and the mutual exclusion problem?

b. *(10 points)* Consider a *line* of n processors, with the following topology:



Every processor has a left and right hand neighbour except the first in the line (that does not have a left hand neighbour) and the last in the line (that does not have a right hand neighbour). Nodes can send messages to their immediate neighbours. Nodes know which neighbour they have and can specify which direction a message should be sent to. The links are FIFO. The system is synchronous. Each node has a unique identifier in $\mathbb{N}$. Design a leader election protocol that elects a leader, and argue why it is correct.

Answer:

a. In leader election, the problem is reach a global configuration where one node is in state *elected* and all other nodes are not, after which the system terminates. In mutual exclusion, nodes continually request access to one shared critical resource, and the following properties must hold: *mutual exclusion*, *progress* and *no starvation*.

b. Actually, on a line the problem is trivial to solve. The essence of leader election is symmetry breaking, which in this case means that either the start or the end can elect themselves leader immediately. The protocol for any node i (note: node 0 is not necessarily the first node!) then becomes

$C[i].leader \leftarrow$ *has-left-neighbour* $\wedge \neg$ *has-right-neighbour*

Question 6 (15 points):

a. *(7 points)* Consider the following *agreement* protocol tolerating Byzantine failures, where nodes can sign (and verify) messages. We write $[m]_\sigma$ for the sequence of signatures of the nodes in σ on message m .

- Sender p:

  if $C[p].in = 1$ **then send** $[1]_p$ to all other nodes.
  decide $C[p].in$

- All other nodes q:

  for each $r \in \{1,\ldots,R\}$
  do if you receive a valid message $m = [1]_{p;\sigma}$
  then send $[m]_q = [1]_{p;\sigma;q}$ to all other nodes
  decide 1
  decide 0

In class we proved this algorithm reaches agreement provided $R = f + 1$, where f is the maximum number of faulty nodes. What goes wrong if $R < f + 1$?

b. *(8 points)* Show how you can use this protocol for agreement as a sub-protocol to reach consensus among n nodes as long as the number of faulty nodes f is less than half of the total number of nodes n. Prove your protocol correct.

Answer:

a. If $R < f + 1$, i.e. let $R = f$, and consider the following execution. Consider the sequence of faulty nodes p_1 to p_f, where $p_1 = p$ is the sender (i.e. faulty). p_{f+1} is a correct node. The sender p sends $[1]_p$ *only* to p_2 and then stops. Similarly, in round $i < R$, node p_{i+1} sends $[1]_{1;\ldots;i+1}$ *only* to node p_{i+2} and then stops. This means that in round $R = f$ a correct node p_{f+1} receives a message $[1]_{1;\ldots;f}$ which is valid. It therefore decides 1. It tries to send on this value, but as this is the last round all other correct nodes do not receive a valid $[1]_\sigma$ message, and hence decide 0. This means there is no agreement among the correct processors.

b. Use the agreement protocol as a subroutine used by each processor to broadcast its input value. Processors store the value received from each processor this way in a vector with n elements. Nodes decide on the majority among the values in this vector, breaking ties in a deterministic way. We need to prove validity and agreement.

   Agreement: all (correct) processors decide on the same value, because all (correct) processors receive the same value for processor i through the agreement protocol. Hence the vector of values used to base the decision on contains the same set of values.

   Validity: Let $f < n/2$ and let all (more than $n/2$) correct nodes have the same input value, say x. By use of the agreement protocol used to broadcast this value to all other processors, all processors have at least $n/2+1$ entries with the value x in the vector of received values. Then x is the majority and will be decided upon.

(end of exam)