EXAM Network Security (265400)

6 November 2009, 13:45–17:15

- This is an open-book exam: you are allowed to use the book ("Network Security Essentials" by Stallings), the papers that were distributed through Blackboard, and copies of the lecture slides. Furthermore, you are allowed to use a (paper) dictionary. Use of calculators, laptops, notebook computers, PDAs, mobile phones, etc. is not allowed. ***Please remove any such material and equipment from your desk, now!***
- Although the questions are only written in English, you are allowed to answer in either English or Dutch.
- This exam consists of 6 problems on 4 pages.
- Besides the exam, you are also given a questionnaire about the course. Please do fill out that form, and hand it in when leaving the room. Of course, you may fill out the questionnaire after handing in the exam answers, so the questionnaire doesn't cost you time that would be better spent on the exam itself.
- Because each of the three lecturers will grade the problems about their parts of the course, you should use three separate sheets of paper. Label these sheets with an 'A', 'B' and 'C', and **write the answer to each problem on the right sheet**.
- The **Kerckhoff** master students should skip part 'B', i.e., problems 2 and 3.

Continued on next page...

1. WLAN, authentication, etc.

A

Consider a Wireless Local Access Network that uses Wired Equivalence Privacy (WEP). Assume that the WEP specification is modified in the following way: the new WEP specification mandates that each implementation must use an Initialization Vector (IV) value that must be different for every frame/message transmitted.

(a) Give and explain at least three security vulnerabilities that are solved by this modification in the WEP specification!

Consider an IEEE 802.11g WLAN and assume the following:
i) Each sending wireless node (wireless station or Access Point) can transmit a maximum transmission rate.
ii) The length of each transmitted packet is 1500 bytes.
iii) Each sender uses an 24 bit Initial Vector (IV) pseudorandom generator.

(b) Why must the IV be transmitted in the clear (not encrypted)? Motivate/explain your answer.

(c) In how much time (seconds) could a receiving wireless node detect an IV collision?

(d) Describe a solution that when used, the time calculated in the answer of Question (c), which is required by a receiving wireless node to detect an IV collision is doubled. Motivate the answer!
Hint: You are not allowed to change the maximum transmission rate, but you are allowed to change any other parameter in order to answer this question.

(e) Explain how the Mobile IP solution can be used to solve the IEEE 802.11i issues associated with users (and their devices) that are roaming.

Consider an Authentication, Authorization and Accounting (AAA) architecture.

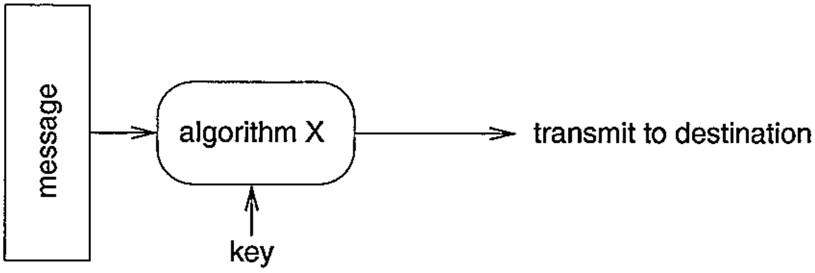
(f) Give and explain at least four advantages of using the DIAMETER protocol instead of the RADIUS protocol.

(g) Give and explain at least two advantages of using the RADIUS protocol instead of the DIAMETER protocol.

Continued on next page...

2. Goals of cryptography

Use sheet B now!



Consider a cryptographic system of which the sending side is sketched above; the receiving side is left to your imagination. The contents of 'algorithm X' are still to be chosen, and this choice determines what kind of security properties the resulting system has. Assume that keys are not compromised.

(a) Copy this table to your answer sheet and write 'yes' or 'no' in each of the nine empty cells:

what is X	**system provides confidentiality**	**system provides data-origin authentication**	**system provides (origin) non-repudiation**
AES			
RSA using sender's key			
RSA using receiver's key			

Note 1: The two RSA entries differ in which side generates the key pair and thus has the secret key. In the first case, the sender generates the pair and uses its private key in X while publishing the public key for use at the receiver. In the second case, the receiver generates the pair, and gives the public key to the sender for use in X.

Note 2: The message is short enough to fit in the blocksize of the algorithms used.

(b) Would it make sense to use a MAC for X ? Explain.

(c) Design a system that provides all three of the properties from (a).

3. Can we simplify DES?

B

Let us consider some aspects of DES encryption.

(a) Suppose we would omit the S-boxes, and replace them by a direct connection of the four outputs to the four center inputs, what problem would be introduced?

(b) Suppose we would omit the "XOR with key" operation, what problem would be introduced?

(c) Suppose we would forget about the Feistel structure, with its splitting of the data in left and right halves and XOR'ing; instead, we would use only the F-block in each round. (In other words: we take 32 bits of plaintext, send them through an F-block, send its output into the next F-block, and so on 16 times, and thus obtain a ciphertext.)
What problem would be introduced?

4. Protocols for security

C

Don't forget to write on sheet **C** now!

(a) Explain the mechanism IPSec is using to detect replay attempts.

(b) The SSL Handshake Protocol is based on public key encryption, whereas the SSL Record Protocol is based on symmetric encryption. Wouldn't it be better to use for both protocols the same encryption mechanism? If yes, which mechanism?

(c) What is the difference between a TLS session and a TLS connection?

5. Intrusion detection, Honeypots and Firewalls

C

(a) Network-based Intrusion Detection Systems can use different approaches to detect attacks. One common approach is to capture complete packets and analyse the contents of each packet. What other approach(es) exist? Give a short explanation of these approach(es).

(b) Once a system within your own network is infected (for example, since a USB stick with a virus was connected to that system), that system needs to be isolated (put into quarantine). What methods exist to isolate that system? What are the advantages and disadvantages of each method?

(c) Assume a company has as policy to forbid its employees to use the Internet, except for browsing the website of the UT (130.89.1.50). How should the network manager configure the companys firewall? Assume the firewall is a stateless, Packet-Filtering type of firewall, and connected to the company's Internet access line. Your rules should look like those of table 11.1D and E (see book of Stallings - Network Security Essentials).

(d) What is the difference between a high and a low interaction honeypot?

6. Attacks

C

(a) Your neighbor is using his/her computer for some extensive P2P data exchange. Unluckily, he forgot to protect his computer by a firewall. Would his computer be a good zombie for an idle scan? Why (not)? (Assume that it has a static IP address).

(b) The DNS cache poisoning attack based on ID-guessing requires some brute-force effort in order to be successful. In the past, two weaknesses (or bugs) in many DNS servers allowed the attacker to reduce the amount of forged DNS responses that he had to generate. Describe the two weaknesses and how to remove them.

End of this exam.