EXAM Network Security (265400)

31 October 2007, 13:30–17:00

- This is an open-book exam: you are allowed to use the book ("Network Security Essentials" by Stallings), the papers that were distributed through Teletop, 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.

1. Secure WLAN and RADIUS/DIAMETER

A

(a) Consider a WLAN that uses the IEEE 802.11i Robust Security Network (RSN) mode.
i) Explain in your own words how the IEEE 802.11i RSN mode uses RADIUS? Which main IETF standards are needed in order to support the interoperation between the IEEE 802.11i RSN mode and RADIUS?
ii) Explain in your own words how the IEEE 802.11i RSN mode uses DIAMETER? Which main IETF standards are needed in order to support the interoperation between the IEEE 802.11i RSN mode and DIAMETER?
iii) Give and explain at least three advantages of using RADIUS in the IEEE 802.11i RSN mode instead of using DIAMETER!

(b) Consider a IEEE 802.11a WLAN and assume the following:
i) Each sending wireless node (wireless station or Access Point) can transmit at maximum transmission rate.
ii) The length of each transmitted packet is 1500 bytes.
iii) Each sender uses a 24 bit Initial Vector (IV) pseudorandom generator.
In how many seconds could a receiving wireless node detect a IV collision?

(c) Consider a weakened IEEE 802.11 system where the Integrity Check Vector (ICV) is still appended to plaintexts, but where WEP (Wired Equivalence Privacy) encryption is turned off.
Show and explain that an attacker can produce traffic for which ICV is valid!

(d) Consider a streamcipher-based encryption system in which plaintext is encrypted by XORing it bit by bit with a pseudo-random keystream.
Show and explain that an attacker who can alter bits in ciphertexts transmitted over a wireless link using this system can modify the plaintexts obtained by the receiving station.

(e) Consider that an attacker can modify arbitrary bits in WEP-encrypted traffic.
Show and explain how the attacker can modify the bits in the WEP-encrypted traffic in such a way as to defeat any integrity provided by the WEP ICV!

2. Comparing DES and RSA **B**

Did you notice that you should now use sheet **B**?

For symmetric encryption like DES, we concluded that keys of about 100 bits are quite safe, taking many times the age of the universe to be broken. However, for RSA typically keys are used that are about 10 times larger than that.

(a) Does this mean that typical RSA users want their secrets to be protected so much better, or is there another reason why RSA keys need to be longer? Explain!

In the lectures, we discussed strengthening DES by applying it twice ("double DES") or three times ("triple DES").

(b) It was found that "double DES" is hardly more secure than single DES, due to the so-called "meet-in-the-middle" attack. Explain in your own words why this is different for triple DES.

Now consider strenghtening RSA by applying it twice ("double RSA") or three times ("triple RSA") (with different keys for each time it is applied, of course).

(c) Is the meet-in-the-middle attack a risk for "double RSA"? Why, or why not?

(d) Consider "triple RSA": is this indeed very much more secure than standard (i.e., single) RSA? Why, or why not?
(Note that the fact that this question asks about "triple RSA" should not be taken as a statement about possible weaknesses in "double RSA"; in particular, it does not imply an answer to question (c).)

Continued on next page...

3. Secure communication B

Suppose that Alice and Bob have a system consisting of two boxes, one in Alice's office and one in Bob's office, connected by a long cable. Each of the boxes has a switch which can be set to 0 or 1, and a lamp which indicates the position of the switch of the *other* box. Thus, Alice and Bob can use these boxes to exchange bits, and thus messages.

The cable is not secure: an eavesdropper, say Eve, might connect measurement equipment to the cable to observe what is happening. Interestingly, the boxes work such that from these measurements, Eve can only find the *sum* of Alice's and Bob's switch settings. So Eve measures 0 if both switches are set to 0, she measures 2 if both switches are set to 1, and she measures 1 if one switch is at 0 and the other is at 1; in the latter case, Eve *cannot* measure *which* switch is at 0 and which is at 1.

Note: these boxes are not fantasy; a system with (approximately) these properties was invented a few years ago.

Unfortunately, besides these boxes, Alice and Bob do not have any method for (secure) communication, and cannot use public-key cryptography either.

(a) Suppose Alice and Bob simply use the boxes to simultaneously transfer un-encrypted messages to each other, by simply moving their switches such that one bit of the message is transmitted each second; you may assume that Alice and Bob (and Eve) have accurate clocks so synchronization is not a problem.
How many of the bits in these messages can Eve find out, on average? Explain your answer.
Would this be acceptable in practical situations?

(b) Design a method to use these boxes to construct a stream of *random* bits that both Alice and Bob know, but that Eve cannot know.

(c) Assuming Alice and Bob have an unlimited stream of random bits that only they know (e.g., as found in the previous question), what is the best way to use this for encrypting their real data? Can this encryption be broken by Eve?

---

4. IPSec C

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

(a) Assume that the traffic between different branches of company X is transferred over the Internet. To protect this traffic, company X considers encrypting all such traffic using IPSec. Would this have as consequence that all computers within company X that communicate with other branches need to have IPSec software installed? Explain!

(b) What is in IPSec-AH the disadvantage of including the source and destination addresses in the computation of the Integrity Check Value?

(c) What is in IPSec-AH the advantage of including the source and destination addresses in the computation of the Integrity Check Value?

Continued on next page...

5. Scans

C

(a) A new computer, with a previously unused IP address, has just been connected to the Internet. The computer has not yet started any communications with other computers but, to the surprise of the owner, it already receives a very large number TCP Reset messages. Do you believe these messages could come from someone who is scanning this computer? Explain!

(b) Are there other explanations for this traffic? Explain!

(c) Since the owner doesn't like these TCP Reset messages, he considers buying a firewall to block such messages. However, before buying such firewall, he asks you (since you've followed a course on network security) for advice. What would be your advice (give as much information as needed)?

6. System security

C

(a) What is a root-kit?

(b) Would a host-based Intrusion Detection System (IDS) be able to detect root-kits? Explain!

(c) Would a network-based IDS, which gets flow information as input, be able to detect viruses?

(d) What are the weaknesses of anomaly-based IDS?

End of this exam.