EXAM Security of Telematics Systems (265400)

29 June 2007, 9:00–12:30

- 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 8 problems on 3 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**.

---

1. RADIUS/DIAMETER [A]

Consider that you will have to apply the AAA concept in a network scenario that has the following characteristics:

- the network consists of a high number of entities, i.e., routers, etc., and it is spread on a very large geographical area (e.g., one or two countries)
- AAA clients are used at the border of the network, while the AAA servers can be located anywhere in the network
- one or more AAA intermediate entities, i.e., proxies, etc., should be able to be used
- the Authentication/Authorization server(s) are located in another physical location than the Accounting server(s)

Which protocol will you use in this network scenario in order to provide the required AAA support? Motivate your answer!

---

2. WLAN security [A]

(a) Consider a Wireless Local Area Network that uses the Wired Equivalence Privacy (WEP) for shared key authentication.

Show and motivate/explain how a security attacker who observes a single run of the WEP shared key authentication protocol can impersonate (pretend to be) a wireless station in any subsequent protocol run.

(b) Explain to what extent does the success of the security attack in question (a) depends on the keyless nature of the integrity mechanism in IEEE 802.11(b).

(c) A WLAN-attacker can receive the ciphertexts of many packets. Assuming WEP is used, explain in detail how the attacker can calculate the XOR of the plaintexts of two of these packets, using the received ciphertexts.

(d) What do you need to assume about the nature of the plaintexts in order to extract each of the plaintexts P1 and P2 given the string P1 XOR P2?

---

3. Symmetric encryption, MAC and hash functions **B**

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

(a) Consider the CBC mode for using block ciphers. The block diagram of this mode contains an 'encryption' operation. Could we replace this operation by a MAC calculation, without making the system useless or unsafe? Why?

(b) Same question as (a) but for the OFB mode.

(c) Suppose that you are very paranoid, and the only "heavy" cryptographic algorithm that you trust, is a secure hash function. You don't trust any of the well-known MACs, block ciphers, etc.
Can you still, using only the secure hash function (and possibly light operations like the XOR), provide confidential communications? How, or why not?
(Hint: take a look at e.g. the OFB mode.)

---

4. Diffie-Hellman **B**

(a) Describe in your own words briefly what the Diffie-Hellman algorithm can be used for.

Suppose we have 3 parties, A, B, and C, who want to communicate confidentially bilaterally (i.e., C should not be able to decrypt communication between A and B, etc.). The Diffie-Hellman algorithm requires each party to generate a pair of numbers; these are denoted as (X_A, α^{X_A}) for party A, etc. We now have a choice between two ways of doing this:

[i] each party generates just *one* such pair of numbers and uses this for communication with *both* of the other parties.

[ii] each party generates *two* pairs, i.e. a *separate* pair for communication with each of the other parties.

Suppose we choose option [i].

(b) What would happen if party B and party C accidentally choose the *same* (secret) value, i.e., $X_B = X_C$; in particular, could confidentiality of the communication still be assured?

(c) Could A know that B and C have chosen the same secret value? How, or why not?

(d) Is it likely that B and C would choose the same secret value? Why?

(e) Which option, [i] or [ii], do you think is used in practice? Why?

Continued on next page...

5. IPSec **C**

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

(a) An interesting difference between IPSec-AH and IPSec-ESP is that for IPSec-AH the Message Authentication Code (MAC) algorithm includes the source and destination IP addresses, whereas the MAC algorithm for IPSec-ESP does not cover both IP addresses. Still IPSec-AH as well as IPSec-ESP claim to ensure authentication. How is this possible?

(b) One of the problems with IPSec is that it allows for many variants and options. Which variants and options are in your opinion superfluous and should be removed? And which variant(s) / option(s) should stay? Motivate your answer!

---

6. Firewalls **C**

(a) Someone claims that SSH does not require the use of a Public Key Infrastructure (PKI) and, as a consequence, partners who want to communicate must have pre-configured shared keys. Is this claim correct? Explain!

(b) The same person claims that SSL/TLS requires the use of a Public Key Infrastructure (PKI). Therefore the data transferred between a SSL/TLS client and a SSL/TLS server will be encrypted using a public key encryption algorithm. Is this claim correct? Explain!

---

7. Network Address Translators (NATs) **C**

Assume you have a PC directly connected to the Internet. All applications work without problems. A few days ago, however, you discovered that there are other computers scanning some ports on your PC. Since you do not like this, you decided to take measures and you bought a (full-cone) NAT.

(a) Will the full-cone NAT be able to prevent that future scan attempts reach your computer? Explain.

(b) Someone tells you that, as opposed to NATs, firewalls were designed to block unwanted traffic. To block scans to your computer, it would therefore be better to buy a firewall. Is that correct? If yes, what kind of firewall. If no, why not.

---

8. Detecting Scans **C**

Assume your next job will be a network manager at a large Internet provider. Your first task is to set-up a measurement infrastructure to detect scans.

(a) How would this measurement infrastructure look like? Explain.

(b) What kind of protocols do you expect the scans will be based on; do you expect these protocols to be TCP, UDP or another protocol? Explain why you expect this.

End of this exam