EXAM Network Security (265400)

7 November 2008, 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; each problem has the same weight for the final grade.
- 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 'A', i.e., problems 1 and 2.

Continued on next page...

1. RSA encryption [A]

In RSA, the plaintext and ciphertext are represented by numbers.

(a) What is the valid range of these numbers, in terms of the RSA key parameters n, e, d?

(b) Why can e not be an even number?
(In other words, which rule about choosing e would be violated if e is even?)

(c) In the homework, we saw that small plaintexts (numbers) such as 0 and 1 are not well-encrypted by RSA. There's another plaintext that is not well-encrypted, namely $n-1$. Show this.
(Hint: start by calculating $(n-1)^2 \bmod n$).

Suppose RSA is used to encrypt (with the public key) secure messages that can only be "yes" or "no". Since RSA can only encrypt numbers, these messages are represented by the numbers 1000 (for "yes") and 2000 (for "no"). If an adversary who does not have the private key, intercepts a ciphertext, (s)he can very easily find out whether the plaintext was "yes" or "no", by simply encrypting the numbers 1000 and 2000 (using the public key!) and comparing the outcomes to the intercepted ciphertext.
(You may assume that e and n are such that $1000^e \gg n$, so the small-plaintext problem does not play a role here. Furthermore, you may assume that the adversary knows that 1000 means yes and 2000 means no.)

(d) Propose a simple way to improve the system such that the adversary can no longer find out whether the message was "yes" or "no".
You should assume that the adversary knows how your improvement works, has access to the public key, but not to the private key. And of course the intended recipient, who does have the private key, should still be able to find out whether "yes" or "no" was sent.

---

2. Symmetric block encryption [A]

(a) When one changes a symmetric block cipher such that its key becomes twice as long, why does the time needed for brute-force cracking by an adversary become more than twice as long?

(b) For a good symmetric cipher, is it acceptable that there are two *different* plaintexts which, for the *same* key, give the *same* ciphertext? Explain.

(c) For a good symmetric cipher, is it acceptable that there are two *different* plaintexts P_1 and P_2, and two *different* keys K_1 and K_2, such that encrypting P_1 with K_1 gives the *same* ciphertext as encrypting P_2 with K_2? Explain.

Suppose AES is used to encrypt secure messages that are either "yes" or "no". To be precise: each such message is padded with space characters to fill one block of 128 bits, and this block is then encrypted with AES. We assume that an adversary intercepting the ciphertexts does not have the key; thus the risk discussed in the previous problem for RSA does not exist.

(d) Still, using AES this way is risky; what is the risk?

Continued on next page...

3. Secure WLAN and RADIUS/DIAMETER

B

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

Assume that you are working as a network architect for a telecommunication operator company. Assume also that you have to specify and design an AAA (Authentication, Authorization and Accounting) solution that could be applied within a very large Internet based communication network, which should be able to support AAA services to fixed and wireless & mobile users. In order to get access to the Internet, the wireless & mobile users are using the IEEE 802.11 wireless technology.

The possible AAA solutions that you are allowed to use are:

- RADIUS in combination with IEEE 802.1x
- DIAMETER in combination with IEEE 802.1x

Questions:

(a) List and describe at least four security vulnerabilities associated *only* with the situation that wireless & mobile users need to get access and use the Internet based communication network (i.e., vulnerabilities that do *not* play a role with fixed users).

(b) List and describe at least four advantages of selecting the DIAMETER and IEEE 802.1x combination instead of the RADIUS and IEEE 802.1x combination.

(c) List and describe at least four security safeguards that you could propose in order to increase the security of the communication network for the situation that wireless & mobile users are willing to access and use the communication network.

Consider an IEEE 802.11a WLAN (Wireless LAN) and assume the following:

1. Each sending wireless node (wireless station or Access Point) transmits at maximum rate.
2. The length of each transmitted packet is 1500 bytes.
3. Each sender uses a 20 bit (instead of 24 bit) Initial Vector (IV) pseudorandom generator.
4. Consider also that:

$\ln(0.1) = -2.3025$;	$\ln(0.2) = -1.60943$;	$\ln(0.3) = -1.203$;
$\ln(0.4) = -0.69314$;	$\ln(0.5) = -0.69314$;	$\ln(0.6) = -0.51082$;
$\ln(0.7) = -0.35667$;	$\ln(0.8) = -0.22314$;	$\ln(0.9) = -0.10536$;
$\sqrt{4.605170} = 2.14$;	$\sqrt{3.21887} = 1.79$;	$\sqrt{2.40794} = 1.55$;
$\sqrt{1.83258} = 1.35$;	$\sqrt{1.38629} = 1.17$;	$\sqrt{1.02165} = 1.01$;
$\sqrt{0.71334} = 0.84$;	$\sqrt{0.44628} = 0.66$;	$\sqrt{0.21072} = 0.45$.

1,02164.

Questions:

(d) How many seconds should a receiving wireless node observe the traffic such that it can be 40 % certain that it observes a collision? Explain your answer.

(e) If the receiving node observes 2.5 times longer than calculated in (d), can this receiver be 100 % certain that it observes a collision? Explain your answer.

Continued on next page...

4. Protocols for security

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

(a) IPSec supports two modes: transport mode and tunnel mode. Are there any advantages of using tunnel mode above transport mode? If yes, what are these advantages?

(b) Someone claims that a difference between IPSec-AH and IPSec-ESP is that IPSec-ESP requires the use of a Public Key Infrastructure (PKI), whereas IPSec-AH does not require a PKI. Is this claim correct? Explain!

(c) TLS allows the establishment of sessions as well as connections. Why do you need both? Explain, and give one or more examples of possible usage.

(d) The SSH transport protocol includes a key re-exchange mechanism. Why did they include such mechanism? Explain!

---

5. Port scans

C

(a) Consider:
(i) a UDP scanner that relies on ICMP messages (as explained in the course), and
(ii) a TCP SYN scanner.
What will these two scanners report if a firewall filters the traffic between them and the target machine?

(b) There is a fundamental reason why the web server of UT would likely not be a good zombie for an idle scan. What is it?

---

6. Firewalls and NATs

C

Rule Number	Action	Source IP	Source Port	Destination IP	Destination Port	Flags	Remarks
1	Allow	*	>1023	our FTP	21	*	FTP: Active open - connect
2	Allow	our FTP	21	*	*	ACK	FTP: Active open - data
3	Allow	our FTP	20	*	*	*	FTP: Active open - connect
4	Allow	*	>1023	our FTP	20	ACK	FTP: Active open - data
5	Allow	*	>1023	our FTP	21	*	FTP: Passive open - connect
6	Allow	our FTP	21	*	*	ACK	FTP: Passive open - data
7	Allow	*	>1023	our FTP	*	*	FTP: Passive open - connect
8	Allow	our FTP	>1023	*	*	ACK	FTP: Passive open - data
9	Allow	*	>1023	our WWW	80	*	Web: incoming traffic
10	Allow	our WWW	80	*	*	ACK	Web: outgoing traffic
11	Block	*	>1023	*	*	*	Block all other traffic

See the above table with firewall rules.

(a) Which firewall rule(s) is/are redundant (and can therefore be removed, without loss of functionality)?

(b) Which firewall rule(s) is/are not correct (do not deliver the required result)? How should it/they be changed to be correct?

(c) Assume a PC on the Internet is behind a Network Address Translator (NAT). That PC wants to use our FTP and Web server. Would that be possible with our firewall rules? Explain!