CS 490: Cryptography and Computer Security

Homework #02

Assigned Date : Thursday, March 26, 2015
Due Date : Thursday, April 09, 2015 @ 09:29:59 a.m.

Instructions

- This is an individual assignment. **Do your own work**. Acts of academic misconduct (plagiarism, use of illicit solutions manuals, etc.) are subjected to university code of conduct.
- Produce your answers using an appropriate word processing application.
- Submit your solutions through Moodle. A dropbox will be available with 24 hours in advance of the deadline. Late policy is enforced per syllabus late policy. Your digital submission must be in PDF format. Grades and specific feedback will be communicated through Moodle.
  - You may, **in addition** to the digital submission, handover a printed, stapled copy of your answers to the instructor at the beginning of class, **if** you prefer to have explicit written feedback of your answers. This, however, is not required neither is considered the primary submission option.
- **DO NOT** email your solutions to the instructor.
- Make proper arrangements, after consulting the instructor, to deliver your solutions **BEFORE** the due date, if you have a planned absence on the due date.
- Answer all questions
- Your solutions are due on **Thursday, April 09, 2015 @ 09:29:59 a.m.**
- Total points: **[UG: 200, MS: 350 points]**

Questions

Q1. [**50 points**] Consider the rights *{read, write, execute, append, list, modify, own}*.

Q1.a [**10 points**] Using the primitive commands discussed in the class, write a command *delete_all_rights (p,q,s)*. This command causes p to delete all rights the subject q has over object s.

Q1.b [**10 points**] Modify your command so that the deletion can occur only if p has *modify* rights over s.

Q1.c [**30 points**] Modify your command so that the deletion can occur only if p has *modify* rights over s and q does not have *own* rights over s.

Q2. [**10 points**] Explain the consequences of not applying the principle of attenuation of privileges. In particular, what is the maximal set of rights that subjects within the system can acquire?.

Q3. [**25 points**] Given the security levels **TOP SECRET, SECRET, CONFIDENTIAL**, and **UNCLASSIFIED** and categories **A**, **B**, and **C**, specify what type of access (*read*, *write*, both, or neither) is allowed in each of the following situations. Assume that discretionary access control allow anyone access unless otherwise specified.

Q3.a [**5 points**] Paul, cleared for (**TOP SECRET, {A,C}**), wants to access a document classified (**SECRET, {B,C}**).

Q3.b [**5 points**] Anna, cleared for (**CONFIDENTIAL, {C}**), wants to access a document classified (**CONFIDENTIAL, {B}**).

Q3.c [**5 points**] Jesse, cleared for (**SECRET, {C}**), wants to access a document classified (**CONFIDENTIAL, {C}**).

Q3.d [**5 points**] Sammi, cleared for (**TOP SECRET, {A,C}**), wants to access a document classified (**CONFIDENTIAL, {C}**).

Q3.e [**5 points**] Robin, who has no clearances, i.e., at (**UNCLASSIFIED**) level, wants to access a document classified (**CONFIDENTIAL, {B}**).

Q4. [**15 points**] If one-time pads are provably secure, why are they so rarely used in practice?

Q5. [**10 points**] Prove that two users who perform a Diffie-Hellman key exchange will have the same shared key

Q6. [**10 points**] Let the two primes $p = 41$ and $q = 17$ be given as setup parameters for RSA. Which of the parameters $e_1 = 32$, $e_2 = 49$ is a valid RSA exponent? Justify your choice.

Q7. [**40 points**] Compute the following exponentiations $x^e \ mod \ m$ applying the *square-and-multiply* algorithm:

Q7.a [**20 points**] $x = 2, e = 79, m = 101$

Q7.b [**20 points**] $x = 3, e = 197, m = 101$

Q8. [**20 points**] Assume yourself to be Eve who just obtained the ciphertext $c = 1141$ by eavesdropping on a certain channel. The corresponding public key $K_{pub} = (n, e) = (2623, 2111)$.

Q8.a [**10 points**] Consider the encryption formula. All variables except the plaintext m is known. Why can't you simply solve the equation for c?

Q8.b [**10 points**] To determine d you have to calculate $d \equiv e^{-1} \ mod \ \phi(n)$. There is an efficient formula to calculate $\phi(n)$. Can we use it here?

Q9. [**20 points**] Compute the two public keys and the common key for the Diffie-Hellman key exchange (DHKE) scheme with parameters $p = 467, \alpha = 2$, and

Q9.a [**10 points**] $a = 3, b = 5$

Q9.b [**10 points**] $a = 400, b = 134$

Extra Credit

Q10. [**25 points**] Research and Explain the *extended euclidean algorithm*

Q11. [**15 points**] Use the extended euclidean algorithm and compute the corresponding private key d for Q6. above.

MS Requirements

Q12. [**150 points**] Prepare a summary critique (between 3/4 - 1 page, single space, PDF format) for each of the graduate readings assigned to you on 03/17/2014. Formulate each critique based on your answers for the following questions.

(a) Title, author(s), date of publication, and venue
(b) What is the primary contribution(s) (according to the authors) of this paper?
(c) What are the critical assumptions (if any) of this paper?
(d) Justify the applicability (or inapplicability) and the validity (or invalidity) of the original contributions to present day networking. *You must logically justify your arguments*.
(e) Propose at least 2 additional, preferably recent, (*within the last 8-10 years*) publications that a would be reader of this paper must read next.
(f) What is your impression of the primary contribution of this paper?

Graduate Grading

- [**25 × 3 points**] Submit your critiques (3 individual PDFs) through the **HW01: Graduate Critique** forum in Moodle.
- [**25 × 3 points**] Select three critiques, preferably from three different colleagues, and *critique their paper critiques*. Post your comments as replies.