CSCI 445 - Homework 5 [*]

Assigned April 26th; Due May 3rd, 11:59 PM {50 points}

Prof. Adwait Nadkarni

1 RSA

1. {10 points} Prof. Pedantic gives you (securely) his RSA public key:

   $$K^+ = \langle e = 13, n = 77 \rangle$$

   What is the corresponding ciphertext for the plaintext message $M = 2$, encrypted with Prof. Pedantic's public key? Show your work.

2. {5 points} Given his public key $\langle e = 13, n = 77 \rangle$, what is Prof. Pedantic's private key?

3. {5 points} Why were you able to answer the previous question? That is, is RSA broken? If it isn't broken, then why were you able to derive his private key from his public key?

2 Intrusion Detection

(a) {15 points} This problem considers the base rate fallacy discussed in class. Let $Pr(M)$ be the probability that a given packet is malware (i.e., ground truth). Let Pr(A) be the probability that there is an alarm raised by the IDS. Your IDS is 99.9% accurate at detecting intrusions [i.e., $Pr(A|M) = 0.999$] and it is 99.9% accurate at detecting when an event is not an intrusion [i.e., $Pr(!A|!M) = 0.999$]. An intrusion occurs once every one million events (i.e., the base rate of incidence is 1 / 1,000,000). What is the "true alarm" rate [i.e., determine $Pr(M|A)$]? Show your work.

(b) {15 points} This problem considers the creating of ROC curves discussed in class. Assume the same trivial detection algorithm as the slides. $D(k, T) \rightarrow [0, 1]$, takes a package of length k and a threshold T. If the packet length $k \leq T$, then an alarm is raised. Produce a table similar to that in the lecture slides showing the TP% and FP%. From this table, draw an ROC curve. Use the following traffic classifications:

- Attack packet lengths: 1, 2, 2, 3, 3, 6, 6, 10
- Non-attack packet lengths: 3, 3, 5, 6, 7, 7, 8, 8, 8, 9

[*] Last revised on April 26, 2024.

Submission Instructions

Submit your solution as a single PDF using Blackboard. To upload your assignment, navigate to the “Mobile App Security (Spring 2024)” course. Use the “Homework 5” assignment.

Writeups submitted in Word, ASCII, PowerPoint, Corel, RTF, Pages, and other non-PDF formats will not be accepted. Consider using LaTeX to format your homework solutions. (For a good primer on LaTeX, see the Not So Short Introduction to LATEX.)

Note that you may submit a PDF scan of hand a hand written solution; however, you will receive **0 points** if the instructor cannot read your hand writing. If the instructor has any difficulty reading your hand writing, you may not submit hand written solutions for future assignments.

Please post questions (especially requests for clarification) about this homework to Piazza.