COMP 4384: Assignment #1

Revision 2

Due on September 29, 2020 at 1:00 PM

30 Points (10% Overall)

Problem 1

(11 points)

A. (*2 points*) What is *non-repudiation* in terms of computer security, and how does it relate to the C-I-A triad?

B. (*2 points*) *Provide* an example of a vulnerability in your home computer system and *what harm* might come if the vulnerability described above is exploited?

C. (*2 points*) Describe **two** examples of control mechanisms that might exist for an IoT device.

D. (*3 points*) *Find* one recent (2019 or 2020) computer security attacks that have been reported in the media and *discuss* the vulnerabilities that were the root cause of the attacks, and *how* we can prevent those attacks in the future.

E. (*2 points*) Abu Mahmoud runs a very successful Zarb restaurant, and wants to keep his secret spice marination recipe secret at all costs. He demands his assistants to report any contact with his competition to him, even if it is only social contact. Will this have the desired effect? Why or why not?

Problem 2

(9 points)

A. (*5 points*) Classify each of the following as a violation of C-I-A, or of some combination thereof. Explain your answers in one to two sentences.

   (a) A student looks over the shoulder of another student during an exam.

   (b) Your pet dog pulls out the power cord to your computer.

   (c) Two students conspire to give each other better grades in a peer-graded assignment.

   (d) A user mistypes the recipient's email address and their sent email is bounced back to them.

   (e) A newspaper prints information obtained from a leak at the White House but attribute it to the wrong source.

B. (*4 points*) Classify each of the following as a prevention, detection, or recovery mechanism:

   (a) A firewall is placed between a server-machine and it's connection to the Internet.

   (b) Anti-virus running on a person's home computer/laptop.

   (c) A backup job scheduled daily at night to backup all data on your computer/laptop.

   (d) A honeybot[1] is placed at the same network as the the database server.

[1] `https://en.wikipedia.org/wiki/Honeypot_(computing)`

Problem 3

(10 points)

In 1983, Ken Thompson and Dennis Ritchie jointly received the Turing Award "for their development of generic operating systems theory and specifically for the implementation of the UNIX operating system". His acceptance speech, "Reflections on Trusting Trust" [1], presented the backdoor attack now known as the *Thompson hack* or *trusting trust attack*, and is widely considered a seminal computer security work in its own right. Read Ken Thompson's paper titled *Reflections of trusting trust* [1] and answer the following questions:

A. (*2 points*) In your own words, summarize the attack described by Ken Thompson in STAGE III.

B. (*2 points*) Why is the described attack difficult to detect?

C. (*2 points*) Do you believe the attack described is plausible? What would be the challenges involved in implementing the attack? *Explain* your answer.

D. (*2 points*) In your own words, describe how would you alter the C compiler to include the sequence '\v' to represent the vertical tab character knowing that the current C compiler does not support the sequence '\v'.

E. (*2 points*) What is the output of running the program at `https://gist.github.com/benjholla/9dd76ca9269e8c9af99a` and what is the term used to describe such programs?

References

[1] K. Thompson, "Reflections on trusting trust," *Communications of the ACM*, vol. 27, no. 8, pp. 761–763, 1984.