

Homework #1

Due: April 10, 2026

Points: 100

Questions

To receive full credit, you must justify your answers! Also, please check your writing to ensure you use good grammar, spelling, and that the reader can understand your answers.

1. (14 points) Classify each of the following as a violation of confidentiality, of integrity, of availability, or of some combination thereof.
 - (a) John copies Mary's homework.
 - (b) Paul crashes Linda's system.
 - (c) Carol changes the amount of Angelo's check from \$100 to \$1,000.
 - (d) Gina forges Roger's signature on a deed.
 - (e) Rhonda registers the domain name "Pearson.com" and refuses to let the publishing house buy or use that domain name.
 - (f) Jonah obtains Peter's credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number.
 - (g) Henry spoofs Julie's IP address to gain access to her computer.
2. (16 points) The aphorism "security through obscurity" suggests that hiding information provides some level of security. Give an example of a situation in which hiding information does not add appreciably to the security of a system. Then give an example of a situation in which it does.
3. (20 points) The PostScript language describes page layout for printers. Among its features is the ability to request that the interpreter execute commands on the host system.
 - (a) Describe a danger that this feature presents when the language interpreter is running with administrative or root privileges.
 - (b) Explain how the principle of least privilege could be used to ameliorate this danger.
4. (30 points) Compare the principles of secure design with the principles of privacy by design. Where do they overlap, and how do they differ?
5. (20 points) The story "Diabologic" by Eric Frank Russell presents an explorer making first contact with an alien race. That race thinks very logically. He proceeds to confound them.
 - (a) Why can the newly-contacted race not cope with the explorer's tactics?
 - (b) What key theme of this story relates to attacking or defending a computer system, and how does it do so?

Extra Credit

- E1. (20 points) In response to a serious intrusion, the university system president directed that an intrusion detection system be installed on each campus to monitor the network traffic campus network. The goal was to allow the system information security officers (SSOs) to detect and co-ordinate response to attacks that spanned multiple campuses. The intrusion detection system was placed outside the campus gateway, so it could only record traffic crossing the gateway. It did not try to block any traffic, nor was it able to decrypt any encrypted traffic. The campus information security officers (CSOs) were told of the installation, and were also told not to reveal it for legal reasons. No-one else on campus was told of the additional monitoring.

What was the effect of the failure to inform the campus community of the existence of this monitoring system? How do you think it impacted the security of the campus?