# Review of Security Foundations and Design Principals

## Background

The list below shows learning objectives that are defined as foundational knowledge in Information Assurance and Security for computer science majors in the latest curriculum guidelines. Le Moyne’s CS curriculum disperses these topics into several different classes. The senior capstone course provides us with an opportunity to review our understanding of these fundamental concepts.

1. Describe the principle of least privilege and isolation as applied to system design.
2. Summarize the principle of fail-safe and deny-by-default.
3. Discuss the implications of relying on open design or the secrecy of design for security.
4. Explain the goals of end-to-end data security.
5. Discuss the benefits of having multiple layers of defenses.
6. For each stage in the lifecycle of a product, describe what security considerations should be evaluated.
7. Describe the cost and tradeoffs associated with designing security into a product.
8. Describe the concept of mediation and the principle of complete mediation.
9. Be aware of standard components for security operations, instead of re-inventing fundamentals operations.
10. Explain the concept of trusted computing including trusted computing base and attack surface and the principle of minimizing trusted computing base.
11. Discuss the importance of usability in security mechanism design.
12. Describe security issues that arise at boundaries between multiple components.
13. Identify the different roles of prevention mechanisms and detection/deterrence mechanisms.
14. Understand tradeoffs of balancing key security properties (Confidentiality, Integrity, Availability).
15. Explain the concepts of risk, threats, vulnerabilities and attack vectors (including the fact that there is no such thing as perfect security).
16. Explain the concepts of authentication, authorization, access control.
17. Explain the concept of trust and trustworthiness.
18. Recognize that there are important ethical issues to consider in computer security, including ethical issues associated with fixing or not fixing vulnerabilities and disclosing or not disclosing vulnerabilities.

## Tasks and Due Dates

1. Read articles listed below and formulate your answers to all problems. Due: 9/8

Meet with your group to discuss and present solutions to the class. Due: 9/8

1. Write up solutions based on in-class discussion. Due: 9/15

## Readings

* Introductory chapter of Computer Security by Goodrich and Tomassia: pages 2 – 24 and 39-40.
* Article by Schneier on Security by Obscurity: <https://www.schneier.com/crypto-gram/archives/2002/0515.html>
* Article by Daud on incorporating security into the software development lifecycle: http://www.iaeng.org/publication/IMECS2010/IMECS2010\_pp724-728.pdf

### Problem 1

In this problem you will analyze the security of a password reset system that works as follows:

*If a user has forgotten their password, they can reset it by answering three preselected personal questions correctly. Typical questions include birthday, zip-code, where one met their spouse, name of first car, name of first child, etc.*

1. Explain how the password reset system upholds *or* compromises each of the following security concepts:
   1. confidentiality
   2. integrity
   3. availability
2. In the 2008 elections hackers gained access to vice presidential candidate Sarah Palin’s email by tricking the password reset system above. The attackers changed Palin’s password by answering all her personal questions correctly. This was easy to do as her answers were easily found online.

Briefly describe how authentication and authorization were compromised in this attack.

Consider a new password reset system:

*When the user tries to reset their password the system sends a code to the user’s phone or to another email account. The user needs to enter the code to verify their identity before being able to reset their password.*

1. Who are the trusted parties in the original password reset system? Who are the trusted parties in the new system?
2. Does the new system minimize the reliance on trusted parities? Explain briefly.
3. Which security design principles does the new system uphold better than the older system? The security design principles are:

* principle of least privilege and isolation as applied to system design
* fail-safe and deny-by-default
* having multiple layers of defenses
* principle of complete mediation
* usability of the system.

1. List two vulnerabilities of the new system.
2. Describe the risk of the two vulnerabilities you listed above.
3. Describe an attack vector which can be used to take advantage of one of the vulnerabilities you listed above.

### Problem 2

Provide a brief explanation of your answers. Note the security design principles are listed in 1e.

1. Which is the primary security design principal that is upheld by the following mechanism?

*A mail server accepts mail from the Internet and copies the messages into a spool directory; a local server will complete delivery. The mail server surrenders the right to access the file as soon as it has finished writing it into the spool directory.*

1. Does the following mechanism uphold or violate the fail safe/deny-by default design principle?

*If the mail server is unable to create a file in the spool directory, it closes the network connection, issues an error message, and stops. It does not try to store the message elsewhere or to expand its privileges to save the message in another location, because an attacker could use that ability to overwrite other files or fill up other disks (a denial of service attack).*

1. Which is the primary security design principal that is **not** upheld by the following mechanism?

*When a process tries to open a file for read access, the operating system determines if the process is allowed to read the file. If so, the process receives a file descriptor encoding the allowed access. Whenever the process wants to read the file, it presents the file descriptor and the OS then allows the access. If the owner of the file removes permission for the process to read the file* ***after*** *the file descriptor is issued, the OS will still allow access.*

### Problem 3

1. Describe how security can be incorporated into each of the following traditional phases of software development:
   1. Requirement gathering
   2. Design
   3. Implementation
   4. Testing and Deployment.
2. Once a product that implements all security requirements has been deployed, what additional actions should be taken to ensure that the security requirements are being maintained?
3. Describe how designing security into a product is a tradeoff by giving one reason for it and one against it.
4. Give one argument for keeping security critical code proprietary and one argument for making it publically available.
5. Suppose your company has just identified a security hole in your product. List one reason to disclose the known vulnerability to the public and one reason this would be a bad idea.

### Problem 4

1. List 3 standard/common security mechanisms and a brief description of its usage.
2. Describe a scenario where a system was hard to use leading it to be less secure.
3. A prevention mechanism prevents attacks from being able to be carried out while a detection/deterrence mechanism deters attackers from wanting to carry out the attack.

Alice loves her bike and wants to make sure it is not stolen.

* 1. Describe a prevention mechanism Alice can use to protect her bike.
  2. Describe a detection/deterrence mechanism Alice could use.