

## Discussion Section

*Date:* October 11, 2013

---

### Principles of secure design

1. Principle of least privilege
2. Principle of fail-safe defaults
3. Principle of economy of mechanism
4. Principle of complete mediation
5. Principle of open design
6. Principle of separation of privilege
7. Principle of least common mechanism
8. Principle of least astonishment

### Scenarios

Which principle(s) do(es) each of the following implement? Which do they violate?

1. A movie company sells movies on DVDs. When you play the DVD, it tries to load a small program onto the player. If that succeeds, it tries to create a special module for the operating system of the player. This module sends a message to the movie company's web site noting that you are playing it on a computer (giving only the IP address of the computer).

The movie company wants to allow you to make one single copy of the movie on a disk as backup. If you try to copy the movie to the disk, the module asks the web site to see if you have already made a copy. If so, it blocks the copy operation. If not, it allows you to copy the movie, but notifies the web site you have done so. Then, if you try to make a second copy, the web site will say this is the second copy.

None of these details are made public; all the movie company says is that you can make a single copy on a hard drive for backup purposes.

2. In early Rome, the laws were kept secret from the plebeians but available to the patricians and the priests.
3. Hotels in some Eastern European countries have a clerk on each floor. Whenever you leave the floor, you must give the clerk your room key. When you return, the clerk will give the key back to you.
4. I recently called my telephone service provider. Like so many others, it had a phone menu that read you a series of options, and asked you to push the corresponding button. Once you did, it repeated the number you pushed, and asked you to press "1" if that was correct and "2" if it was not correct.

In fact, at one point, it asked me a question, and the exchange went like this:

"Press 1 if your answer is yes and press 2 if your answer is no."

*I pressed 1.*

"You pressed 1. Press 1 if this is correct and press 2 if this is not correct."

5. According to the U. S. Constitution, both the House of Representatives and the Senate must agree on a law, and the President must sign it.
6. Kai-Ping Yee has defined the "Principle of Expected Ability", which says that the system must not lead the user to believe it is possible to do something that cannot be done.