

# CS253 HW2

## a. Explain the security flaw in this program

This code allow anyone to access to the resource unless he/she trigger ERROR\_ACCESS\_DENIED. However, the Principle of Fail-Safe Defaults states that, unless a subject is given explicit access to an object, it should be denied access to that object. Thus, if an attacker can avoid the ERROR\_ACCESS\_DENIED(e.g., try to trigger other error), the resource can be stolen, which genertes a security flaw.

## b. Rewrite the code to avoid the flaw

```
DWORD dwRet = IsAccessAllowed(...);  
if (dwRet == ACCESS_ALLOWED) {  
    // Security check OK.  
} else {  
    // Security check failed.  
    // Inform user that access denied.  
}
```