PRINCIPLES FOR GOOD SECURITY DESIGN

Everything you need to know about designing for security can be shown with an example from Star Wars

Dr. A-M Horcher, Central Michigan University  horcheram@gmail.com
SIMPLE

Also known as Economy of Mechanism

Simple means less points of failure
FAIL-SAFE

All Systems fail

Fail in a manner to not compromise security
Complete Mediation

- Controls must check for all possible situations
- User is never left hanging wondering what to do
LEAST PRIVILEGE

- Need to know
- Remove choices the user should not make
- Reduce cognitive load
LEAST SHARED

Same commands used differently

Shared Controls are maintenance problems
SEPARATE PRIVILEGE

- No all powerful IDs
- Checks and Balances
OPEN DESIGN

No Security through Obscurity

Changeable Information secures, not Design
LEAST SURPRISE

Works the way the user expects

Follows a well known model
There’s an app
For that
“Shall we play a game?”

You may play the game that reviews the design principles and tours the Star Wars universe. The game will contain the option to view the concept explanation.