

Methodology

- Open design and abstraction
 - o The way we build things should not be kept secret
- Layering
 - o Defense in depth
 - Organize software in layers so that modules at a given layer interact only with modules in the layers immediately above and below it
- Modularity
 - o Design and implement the software as a collection of co – operating components (module): each module interface is an abstraction
 - o You can change a single module without modifying the whole system
- Complete linkage
 - o Tie software security design and implementation to the security specification for that software
 - o Security should not be an after thought
- Design for iteration (Continual Improvement)
 - o Plan the design in such a way that it can be changed
- Security focal points
 - o One of the several models to help frame your thinking
 - CIA
 - Defensible network architecture
 - Zero – trust
- CIA (Confidentiality, Integrity, Availability)