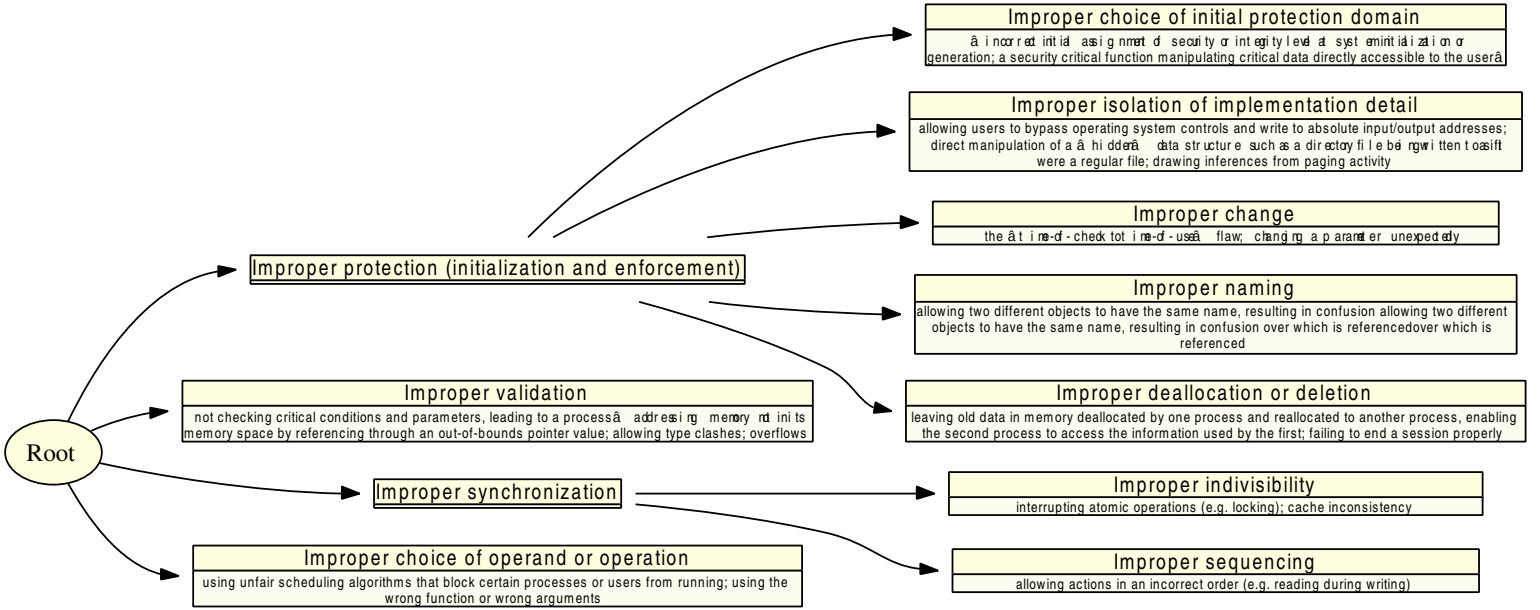
Root
Improper protection (initialization and enforcement)
Improper validation
not checking critical conditions and parameters, leading to a processâ addressing memory nd inits memory space by referencing through an out-of-bounds pointer value; allowing type clashes; overflows
Improper synchronization
Improper choice of operand or operation
using unfair scheduling algorithms that block certain processes or users from running; using the wrong function or wrong arguments
Improper choice of initial protection domain
â incorrect initial assignment of security or integrity level at system emintialization or generation; a security critical function manipulating critical data directly accessible to the userâ
Improper isolation of implementation detail
allowing users to bypass operating system controls and write to absolute input/output addresses; direct manipulation of a â hiddenâ data structure such as a directory file being written to asift were a regular file; drawing inferences from paging activity
Improper change
the â time-of-check to time-of-useâ flaw; changing a parameter unexpectedly
Improper naming
allowing two different objects to have the same name, resulting in confusion allowing two different objects to have the same name, resulting in confusion over which is referencedover which is referenced
Improper deallocation or deletion
leaving old data in memory deallocated by one process and reallocated to another process, enabling the second process to access the information used by the first; failing to end a session properly
Improper indivisibility
interrupting atomic operations (e.g. locking); cache inconsistency
Improper sequencing
allowing actions in an incorrect order (e.g. reading during writing)