Memory Bugs Classes in Bugs Framework
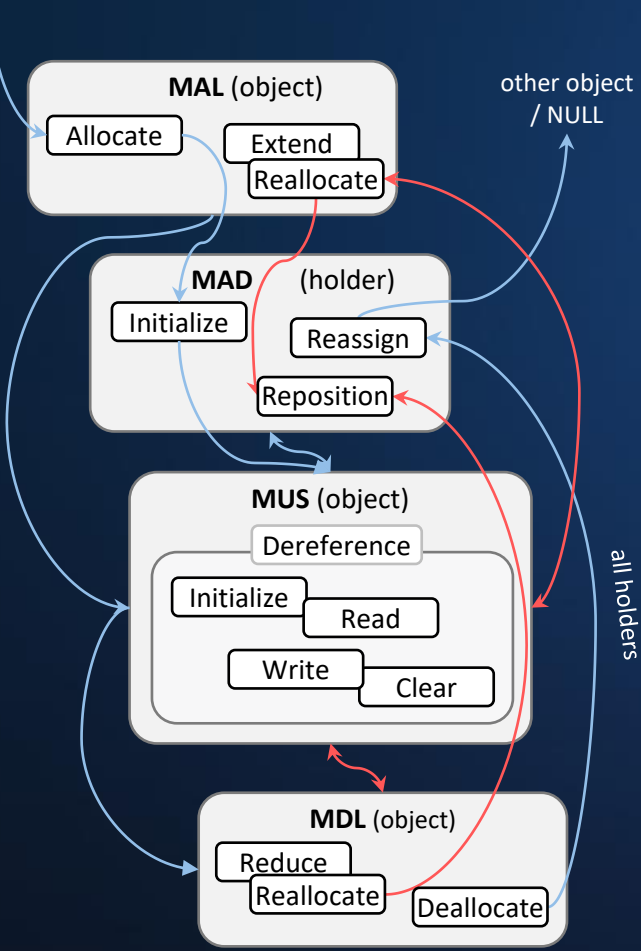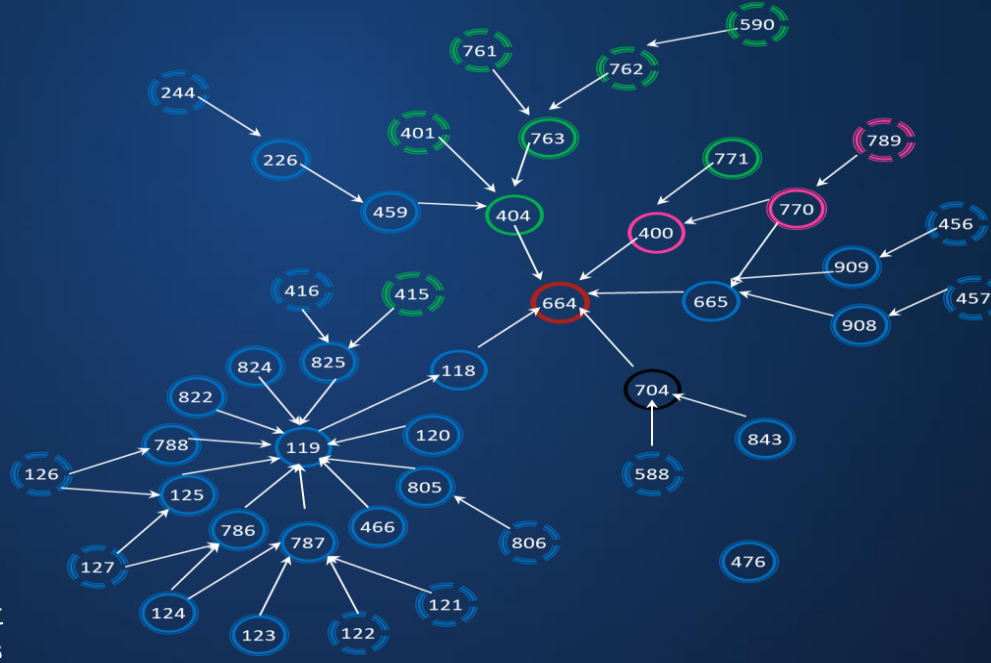
National Institute of Standards and Technology
U.S. Department of Commerce

The Bugs Framework (BF) allows precise descriptions of software bugs and vulnerabilities.

Memory Bugs Model

MAL (object)
- Allocate
- Extend
- Reallocate

MAD (holder)
- Initialize
- Reassign
- Reposition

other object / NULL

all holders

MUS (object)
- Dereference
- Initialize
- Read
- Write
- Clear

MDL (object)
- Reduce
- Reallocate
- Deallocate

Memory bugs happen at allocation, addressing, use, and deallocation.
BF classes: MAL, MAD, MUS, and MDL.

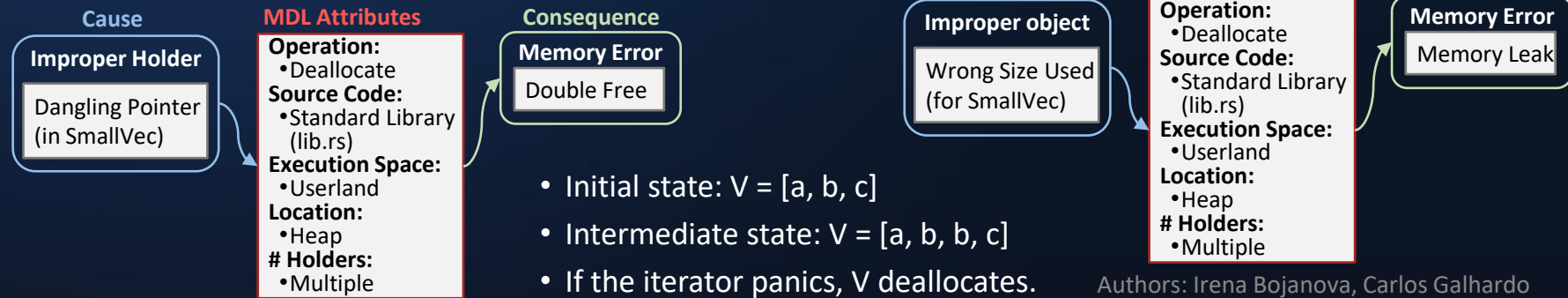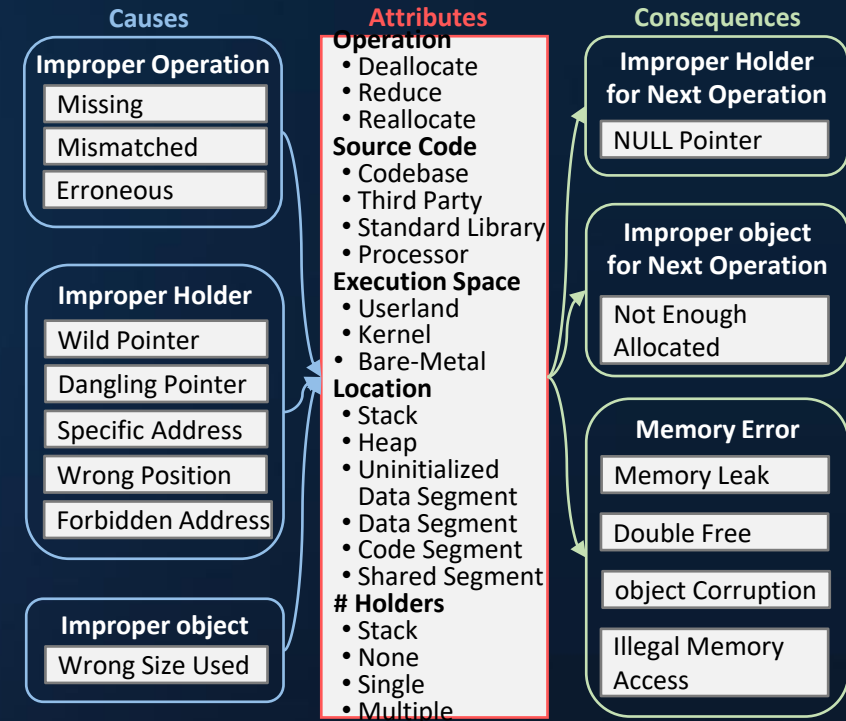## Validation: Covers all memory related CWEs and more.

Example: CVE-2018-20991: An issue was discovered in the smallvec crate before 0.6.3 for Rust. The Iterator implementation mishandles destructors, leading to a double free.

Cause

Improper Holder

Dangling Pointer (in SmallVec)

MDL Attributes

Operation:
- Deallocate

Source Code:
- Standard Library (lib.rs)

Execution Space:
- Userland

Location:
- Heap

 # Holders:
- Multiple

Consequence

Memory Error

Double Free

- Initial state: V = [a, b, c]
- Intermediate state: V = [a, b, b, c]
- If the iterator panics, V deallocates.

Memory Deallocation Bugs (MDL) Class

Causes

Improper Operation
- Missing
- Mismatched
- Erroneous

Improper Holder
- Wild Pointer
- Dangling Pointer
- Specific Address
- Wrong Position
- Forbidden Address

Improper object
- Wrong Size Used

Attributes

Operation
- Deallocate
- Reduce
- Reallocate

Source Code
- Codebase
- Third Party
- Standard Library
- Processor

Execution Space
- Userland
- Kernel
- Bare-Metal

Location
- Stack
- Heap
- Uninitialized Data Segment
- Data Segment
- Code Segment
- Shared Segment

 # Holders
- Stack
- None
- Single
- Multiple

Consequences

Improper Holder for Next Operation

NULL Pointer

Improper object for Next Operation

Not Enough Allocated

Memory Error

Memory Leak

Double Free

object Corruption

Illegal Memory Access

Cause

Improper object

Wrong Size Used (for SmallVec)

MDL Attributes

Operation:
- Deallocate

Source Code:
- Standard Library (lib.rs)

Execution Space:
- Userland

Location:
- Heap

 # Holders:
- Multiple

Consequence

Memory Error

Memory Leak

Authors: Irena Bojanova, Carlos Galhardo