Memory Bugs Classes in NIST Bugs Framework (BF)

Handouts

Irena Bojanova, NIST

Carlos Galhardo, INMETRO

National Institute of Standards and Technology
U.S. Department of Commerce

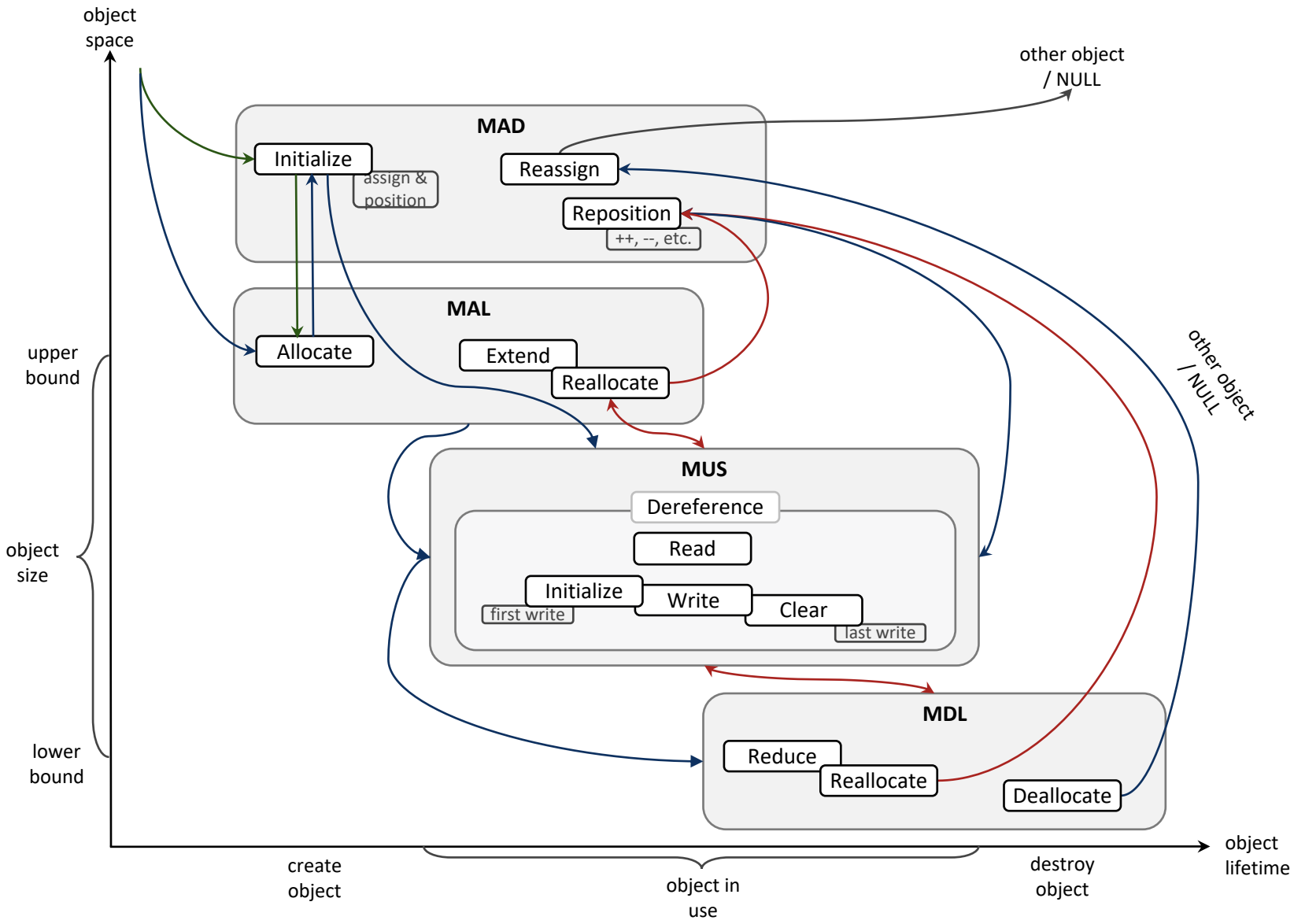
SAMATE

INMETRO

HCSS 2020

09/15/2020

The BF Memory Bugs Model



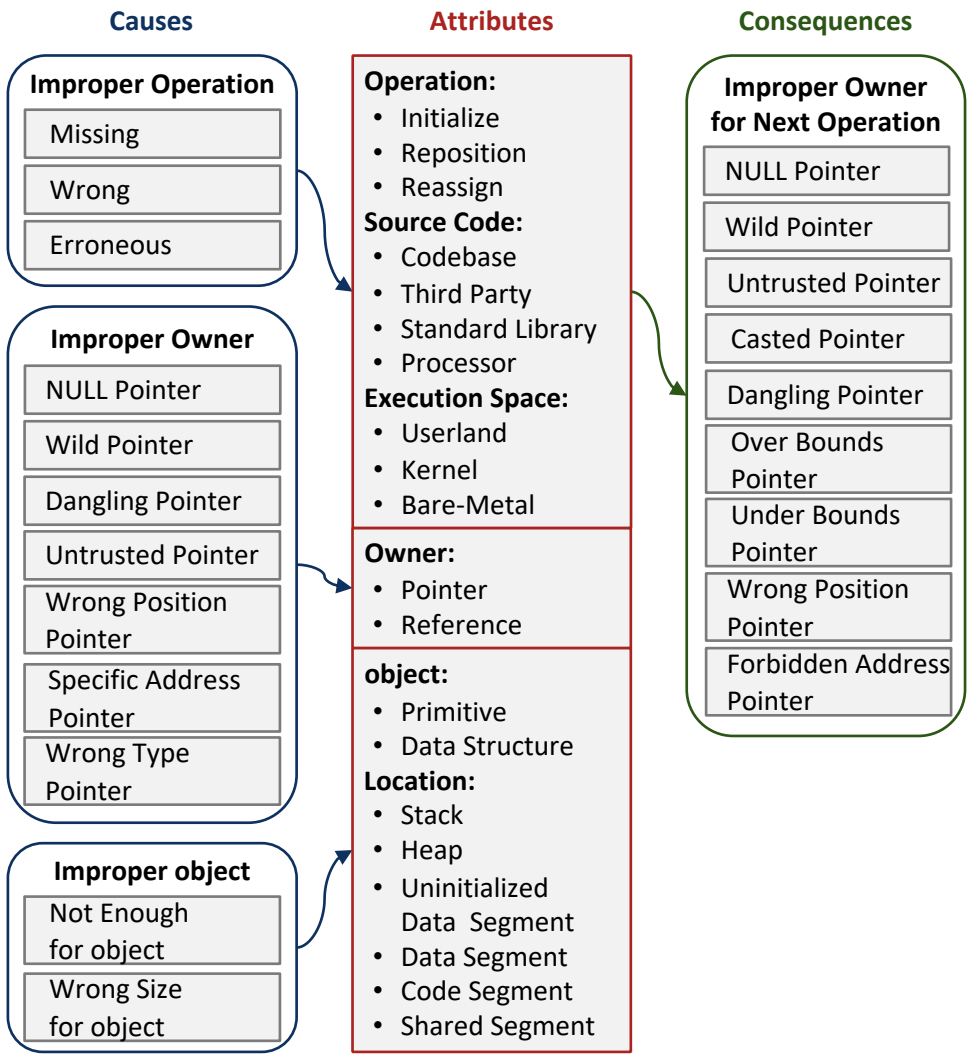
MAD – Memory Addressing Bugs

MAL – Memory Allocation Bugs

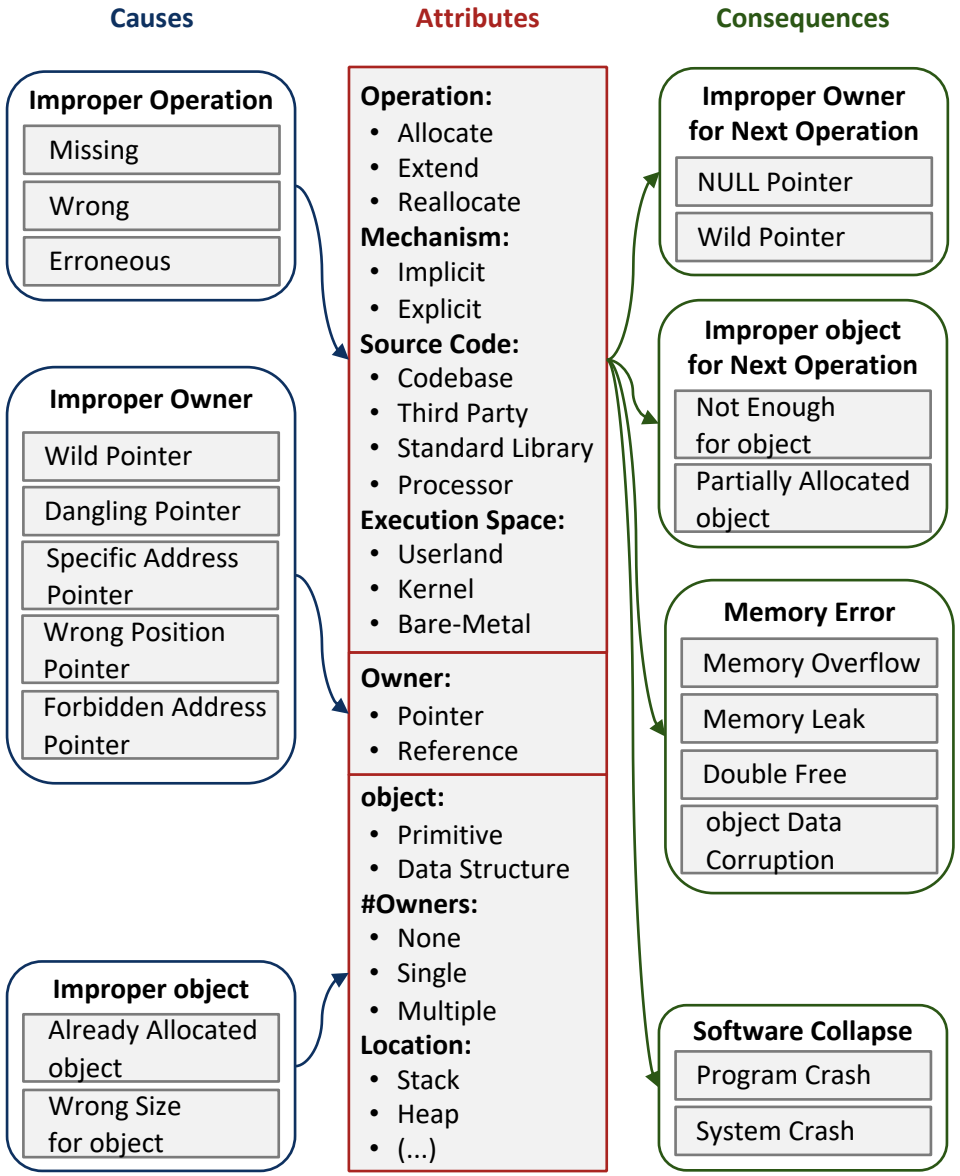
MUS – Memory Use Bugs

MDL – Memory Deallocation Bugs

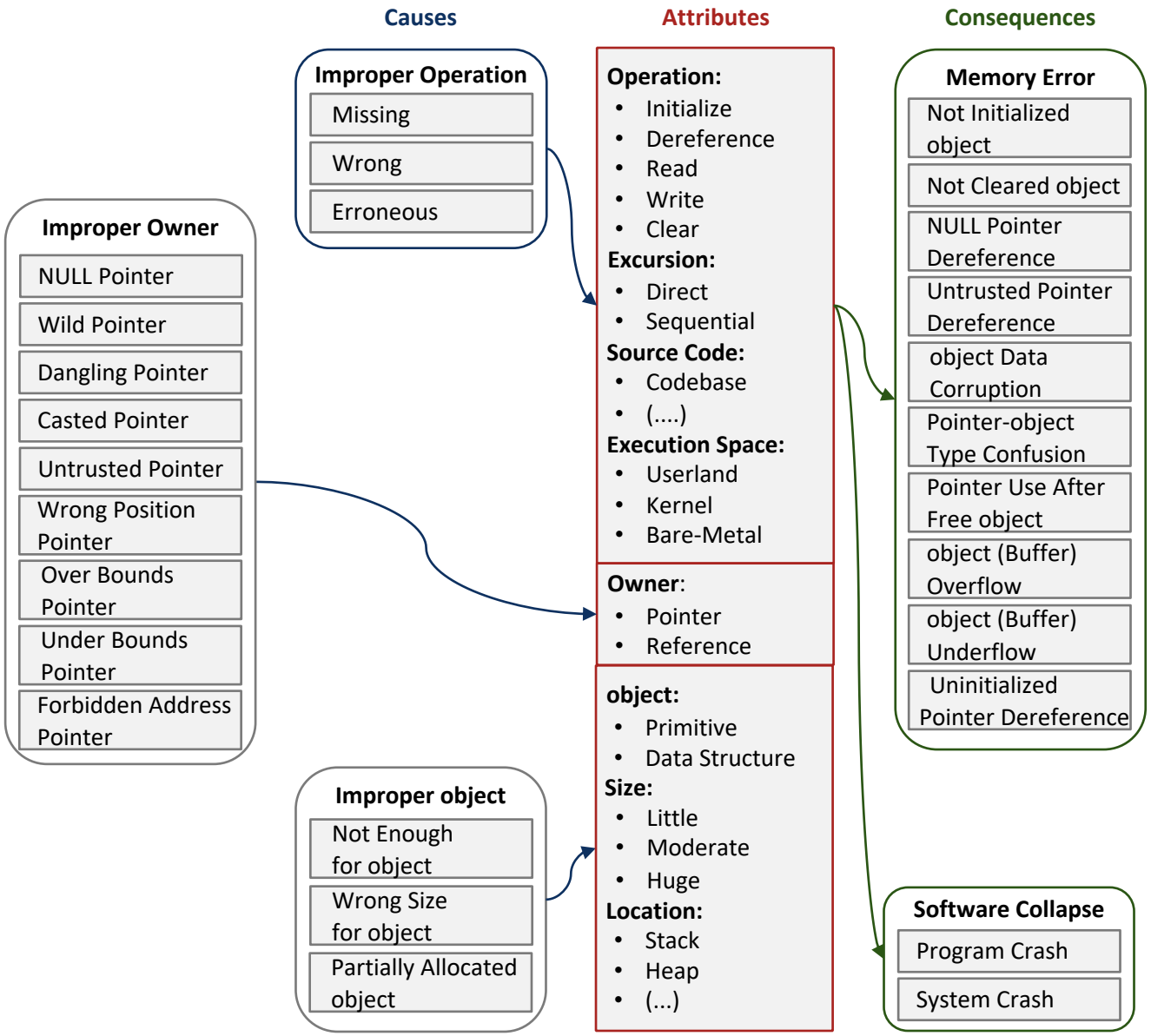
MAD – Memory Addressing Bugs



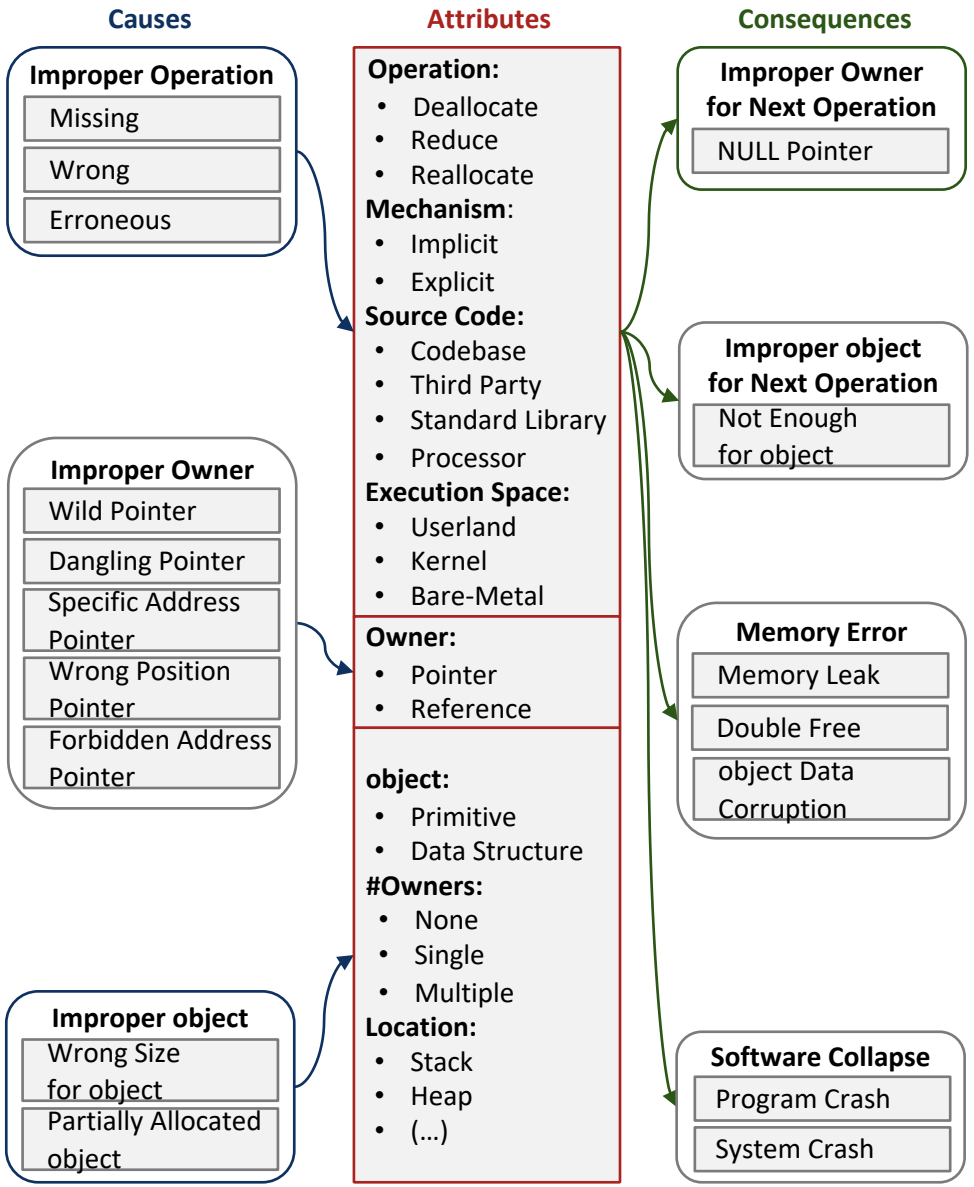
MAL – Memory Allocation Bugs



MUS – Memory Use Bugs



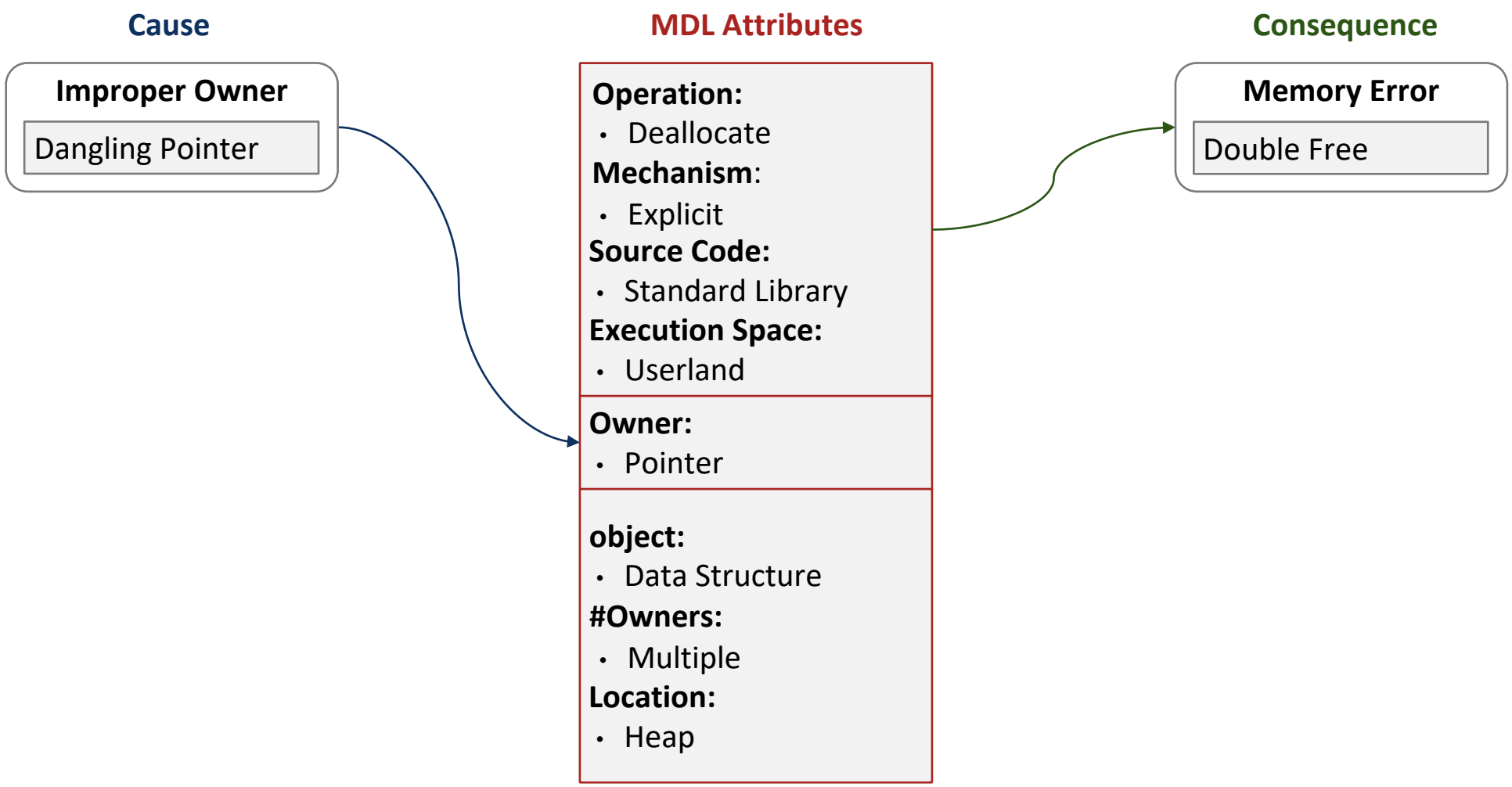
MDL – Memory Deallocation Bugs



Example 1: CVE-2018-20991

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

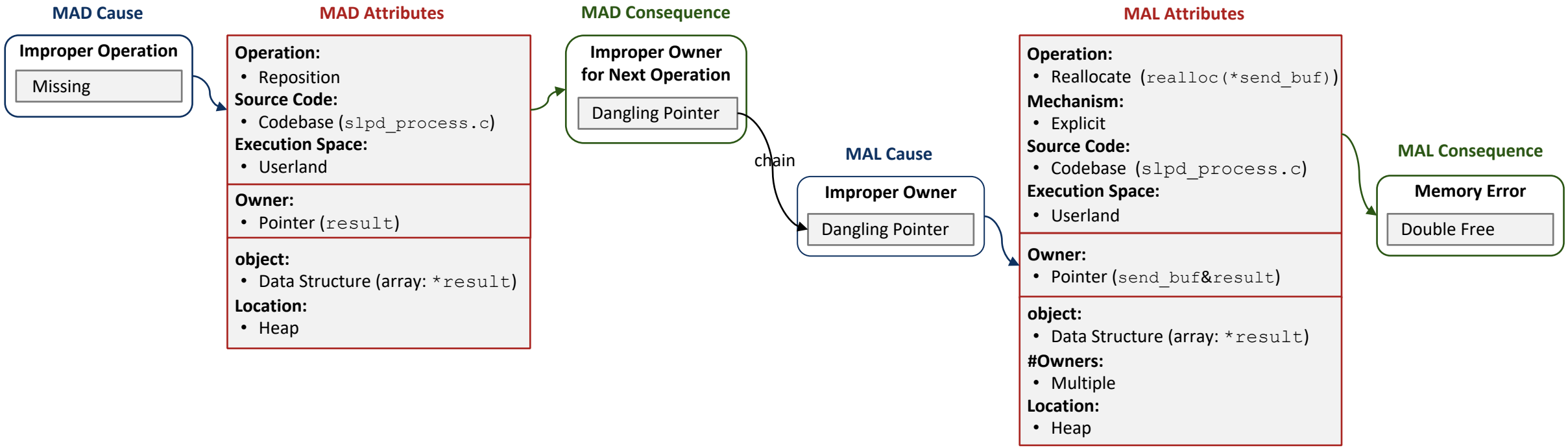
BF MDL Description of CVE-2018-20991



Example 2: CVE-2017-17833

- CVE description: OpenSLP releases in the 1.0.2 and 1.1.0 code streams have a heap-related memory corruption issue which may manifest itself as a denial-of-service or a remote code-execution vulnerability.

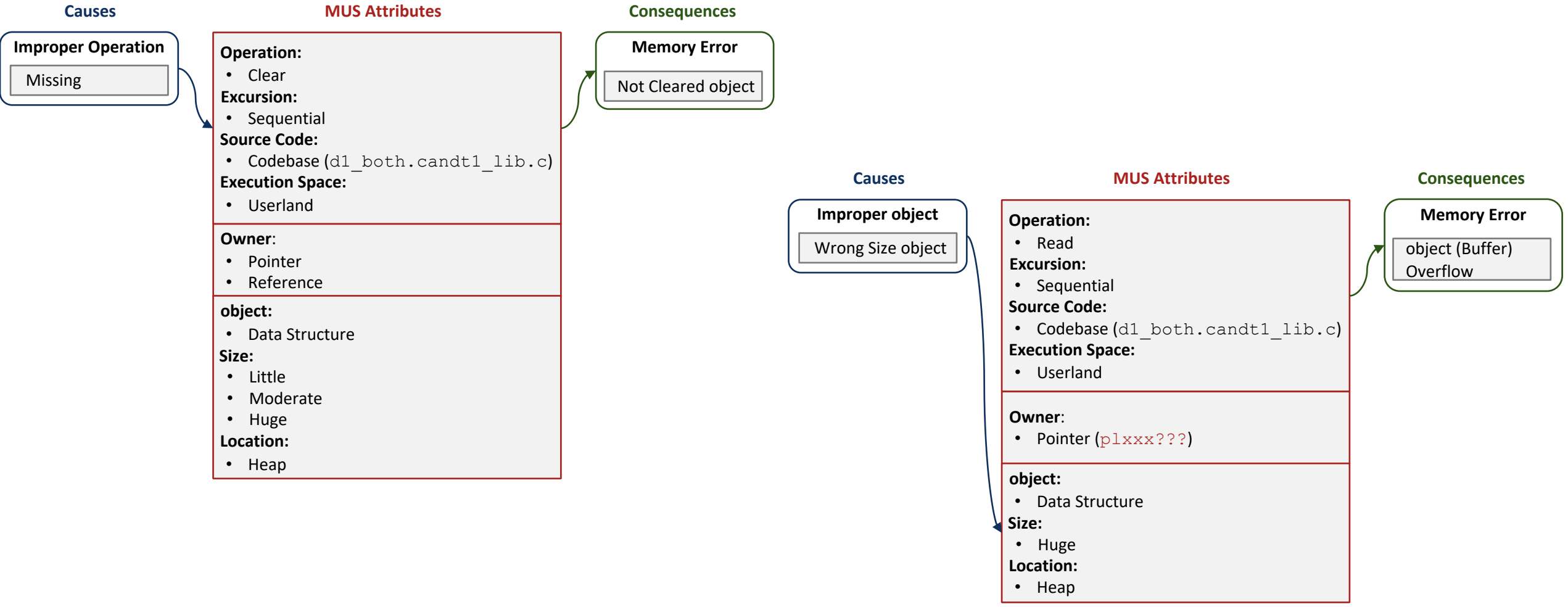
CVE-2017-17833



Example 3: CVE-2014-0160 – Heartbleed

- CVE description: The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

CVE-2014-0160 – Heartbleed



Contact Us

irena.bojanova@nist.gov and cegalhardo@inmetro.gov.br

BF Web Site: https://samate.nist.gov/BF/