

# BF: Bug, Fault, Error, Weakness, or Vulnerability

Irena Bojanova, NIST

## Motivation

- Software security vulnerabilities are leveraged to attack cyberspace and critical infrastructure, leading to security failures. When communicating about them, however, even security experts might conflate essential related software concepts.

## Objective

- Define the Bugs Framework (BF) critical research concepts of software security bug, exploitable error, weakness, and vulnerability; software fault and error; and failure in the context of cybersecurity, and elucidate their causation and propagation.

## BF Software Security Concepts Definitions

Software security **bug/fault types** relate to distinct phases of software execution with specific **operations**, the input **operands** to the operations, and the output **results** from the operations.

- A **software security bug** is a code or specification defect (an operation defect) – proper operands over an improper operation.
  - A **software fault** is a name, data, type, address, or size error (an operand error) – improper operands over a proper operation.
- ‘Name’ is about a resolved or bound object, function, data type, or namespace; ‘data’, ‘type’, ‘address’, and ‘size’ are about an object.
- A **software error** is a result from an operation with a bug or an operation with a faulty operand that can propagate to a new fault.
  - A **software security exploitable error** is an undefined system behavior that results from an operation with a faulty operand.
  - A **software security weakness** is a (bug, operation, error), (fault, operation, error), or a (fault, operation, exploitable error) triple; i.e., it is of a bug type – a bug causes an error, or of a fault type – a fault causes an error or an exploitable error.

The bug must be fixed to **resolve** the vulnerability; fixing a fault will **mitigate** the vulnerability.

- A **security failure** is a violation of a system security requirement caused by an adversary attack leveraging an exploitable error.

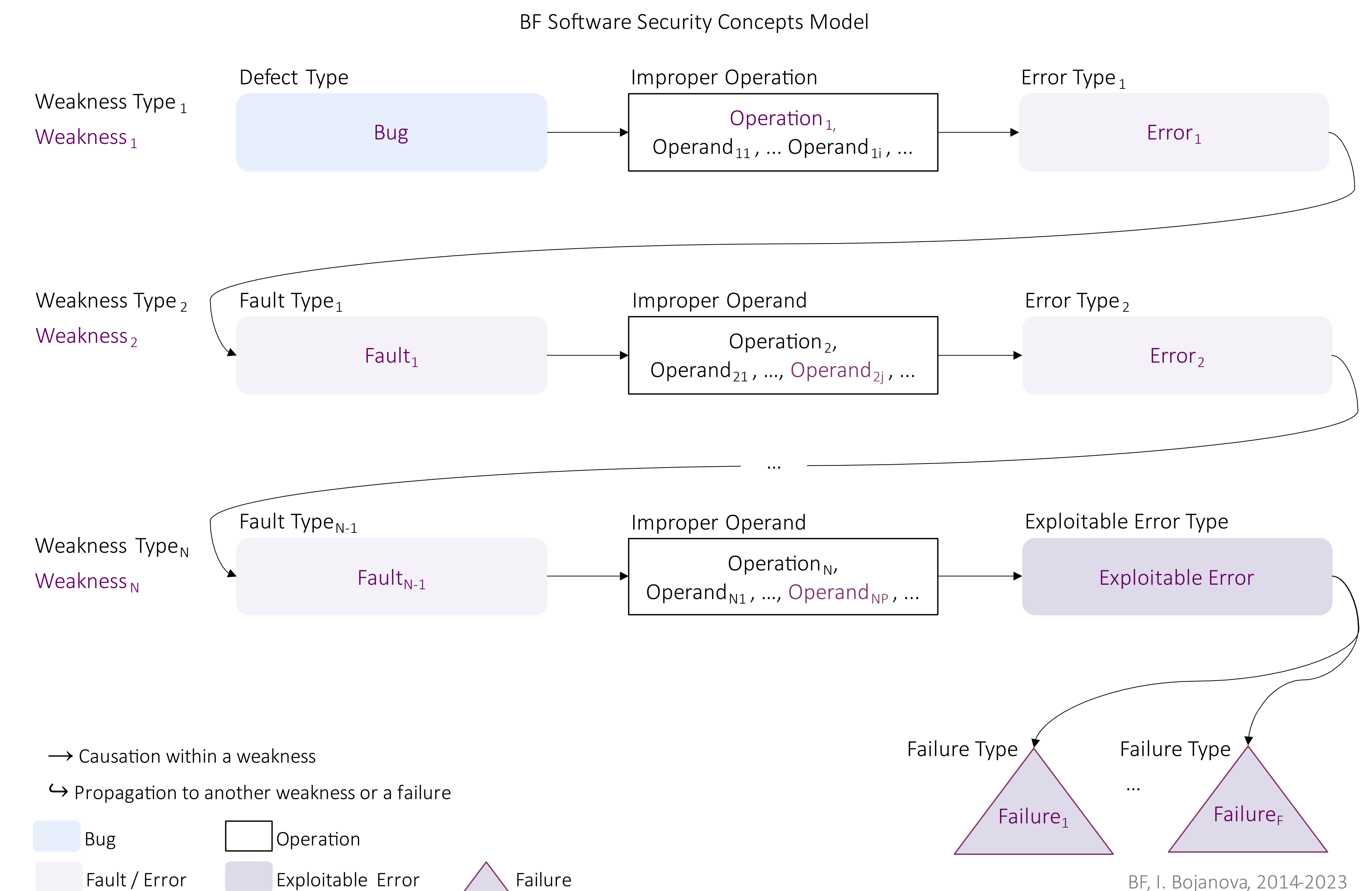
A failure may result in a fault, causing a new vulnerability of only fault type weaknesses. Fixing the bug in the first vulnerability will resolve the **chain** of vulnerabilities.

Occasionally, for an exploit to be harmful, several vulnerabilities must **converge** at their exploitable errors. The bug in at least one of the chains must be fixed to avoid the failure.

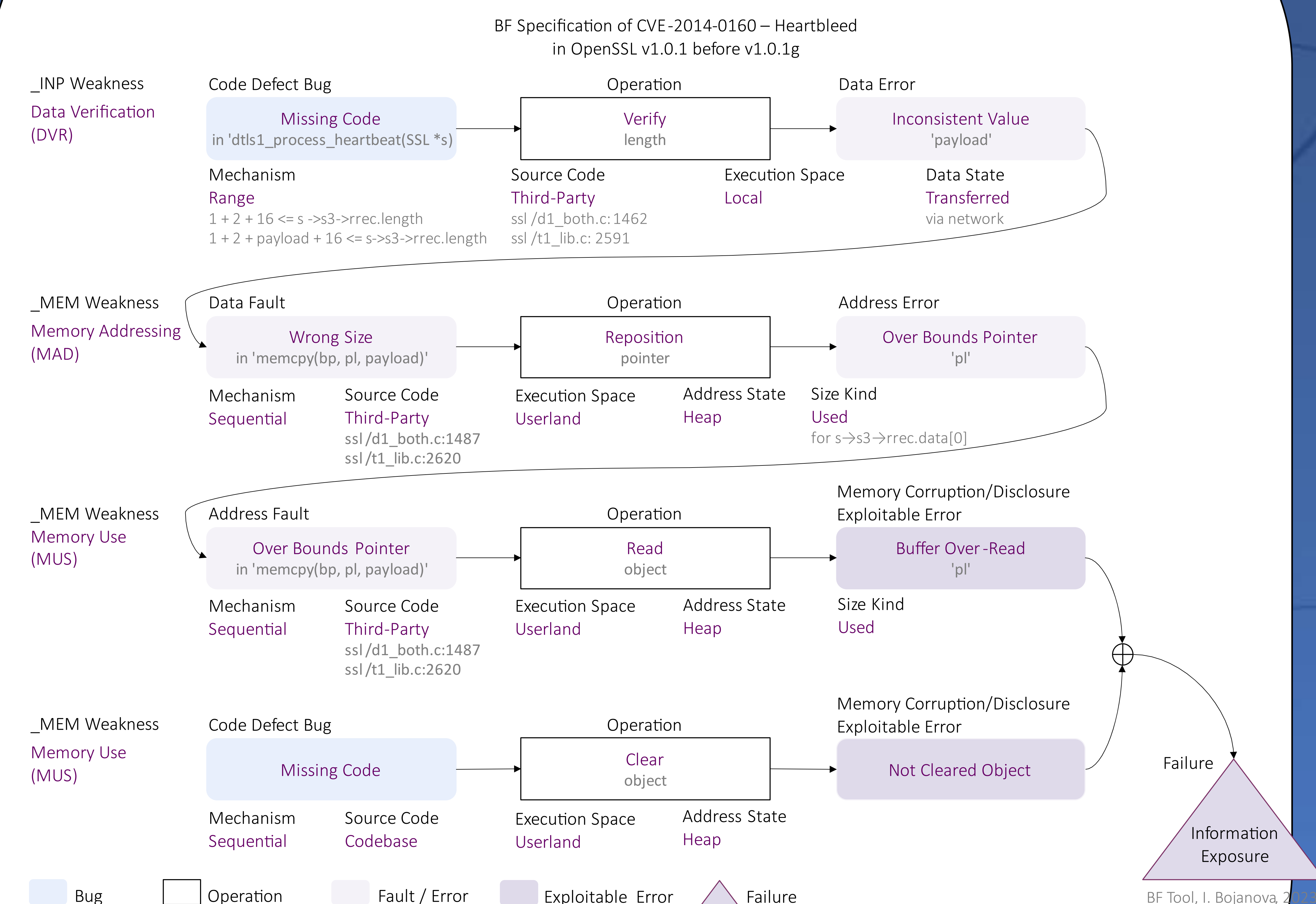
## Potential Impact

- Clear communication between professionals and executives about cyber security bugs, weaknesses, exploitable errors, vulnerabilities, and failures; and software faults and errors.
- Unambiguous context for cybersecurity AI model training.

## BF Software Security Concepts Model



## BF Specification of CVE-2014-0160 – Heartbleed



Missing verification of payload length towards an upper limit leads to use of an inconsistent size for an object, allowing a pointer reposition over its bounds, which, when used in `memcpy()` leads to a heap buffer over-read. If exploited, this can lead to exposure of sensitive information – confidentiality loss.