# Input/Output Check Bugs & Injection

Irena Bojanova, Carlos Galhardo, Sara Moshtari

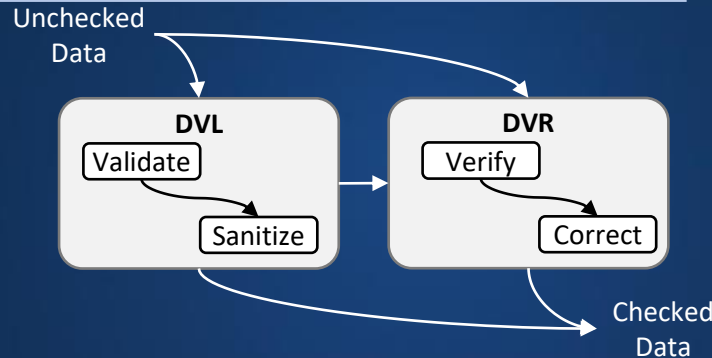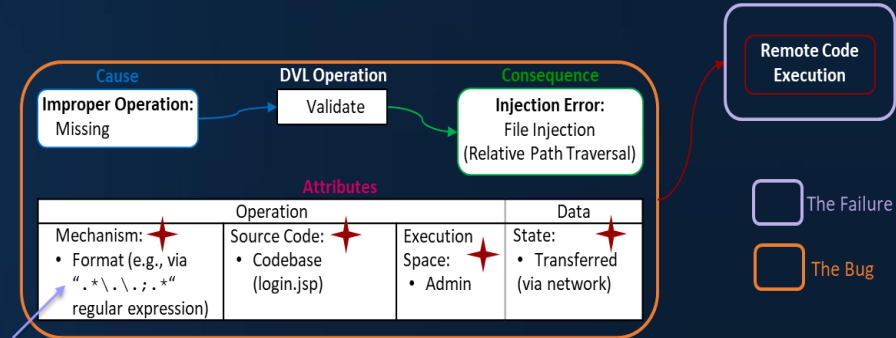National Institute of Standards and Technology, U.S. Department of Commerce

The Bugs Framework (BF): We are classifying software bugs to allow precise descriptions of vulnerability that exploit them.

## Model

The data check bugs model helped us identify two BF classes:

- Data Validation Bugs (DVL)
- Data Verification Bugs (DVR)

Unchecked Data

**DVL**
Validate
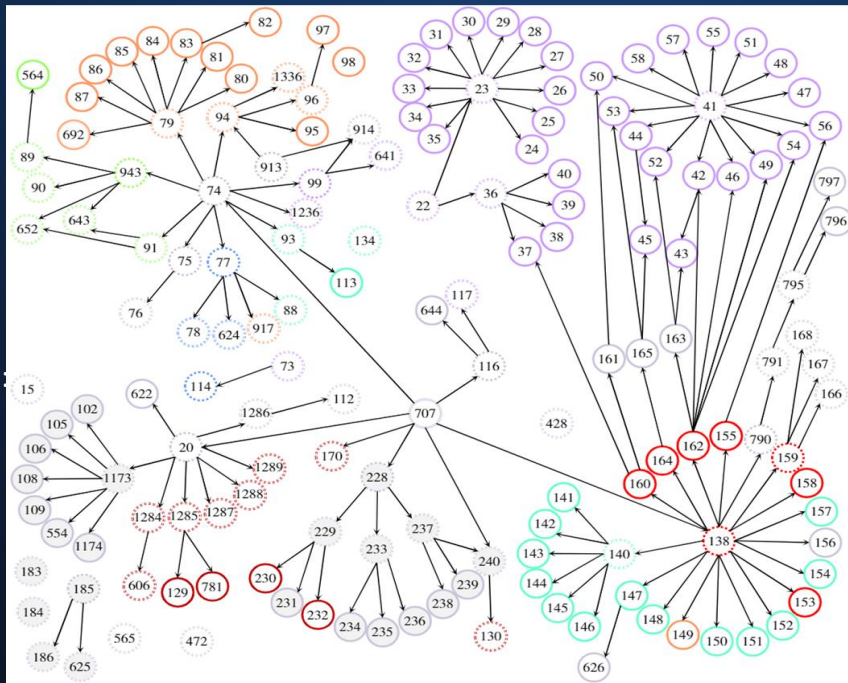Sanitize

**DVR**
Verify
Correct

Checked Data

## Input/Output and Injection related CWEs mapped to BF DVL & DVR

CWEs by DVL Injection Error:
- Query Injection
- Command Injection
- Source Code Injection
- Parameter Injection
- File Injection

CWEs by other consequences:
- DVL Invalid Data
- DVR Wrong Value, Inconsistent Value, and Wrong Type
- No consequence



## Example: CVE-2020-5902- BIG IP TMEU RCE

BIG-IP TMUI, also referred to as the Configuration utility, has a RCE vulnerability in undisclosed pages.

| Cause | DVL Operation | Consequence |
|---|---|---|
| **Improper Operation:** Missing | Validate | **Injection Error:** File Injection (Relative Path Traversal) |

Attributes

| Operation | | | Data |
|---|---|---|---|
| Mechanism:<br>• Format (e.g., via ".*\.\.;.*" regular expression) | Source Code:<br>• Codebase (login.jsp) | Execution Space:<br>• Admin | State:<br>• Transferred (via network) |

Remote Code Execution

The Failure

The Bug

## Example: CVE-2014-0160 – Heartbleed (Updated)

| Cause | DVR Operation | Consequence |
|---|---|---|
| **Improper Operation:** Missing | Verify | **Improper Data:** Inconsistent Value (for payload size) |

Attributes

| Operation | | | Data |
|---|---|---|---|
| Mechanism:<br>• Quantity | Source Code:<br>• Codebase (d1_both.c and tl_lib.c) | Execution Space:<br>• Userland | State:<br>• Transferred (via network) |

| Cause | MUS Operation | Consequence |
|---|---|---|
| **Improper Operation:** Missing | Clear | **Memory Error:** Not Cleared Object |

Attributes

| Operation | | Pointer | Object |
|---|---|---|---|
| Mechanism:<br>• Sequential | Source Code:<br>• Codebase | Execution Space:<br>• Userland | Span:<br>• Huge | Location:<br>• Heap |

| Cause | MAD Operation | Consequence |
|---|---|---|
| **Improper Size:** Inconsistent Value (for size of s→s3→rrec.data[0]) | Reposition | **Improper Pointer:** Over Bounds |

Attributes

| Operation | | | Object |
|---|---|---|---|
| Mechanism:<br>• Sequential | Source Code:<br>• Codebase (d1_both.c and tl_lib.c) | Execution Space:<br>• Userland | Location:<br>• Heap |

| Cause | MUS Operation | Consequence |
|---|---|---|
| **Improper Pointer:** Over Bounds (for s→s3→rrec.data[0]) | Read | **Memory Error:** Buffer Overflow |

Attributes

| Operation | | | Pointer | Object |
|---|---|---|---|---|
| Mechanism:<br>• Sequential | Source Code:<br>• Codebase (d1_both.c and tl_lib.c) | Execution Space:<br>• Userland | Span:<br>• Huge | Location:<br>• Heap |

A Bug

A Weakness

The Failure

Information Exposure