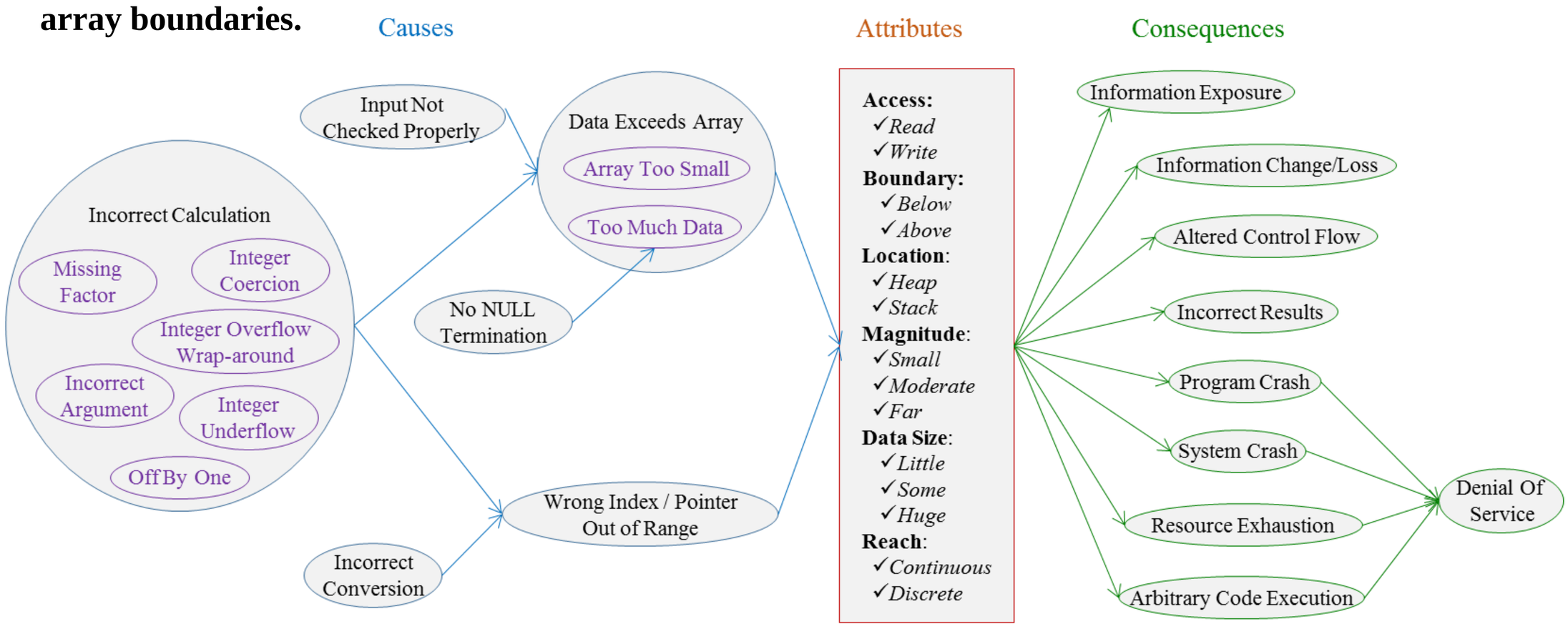
The Bugs Framework (BF): A Structured, Integrated Framework to Express Software Bugs

Irena Bojanova, NIST; Paul E. Black, NIST; Yaacov Yesha, NIST, UMBC; Yan Wu, BGSU
{irena.bojanova, paul.black, yaacov.yesha}@nist.gov, yayesha@cs.umbc.edu, yanwu@bgsu.edu

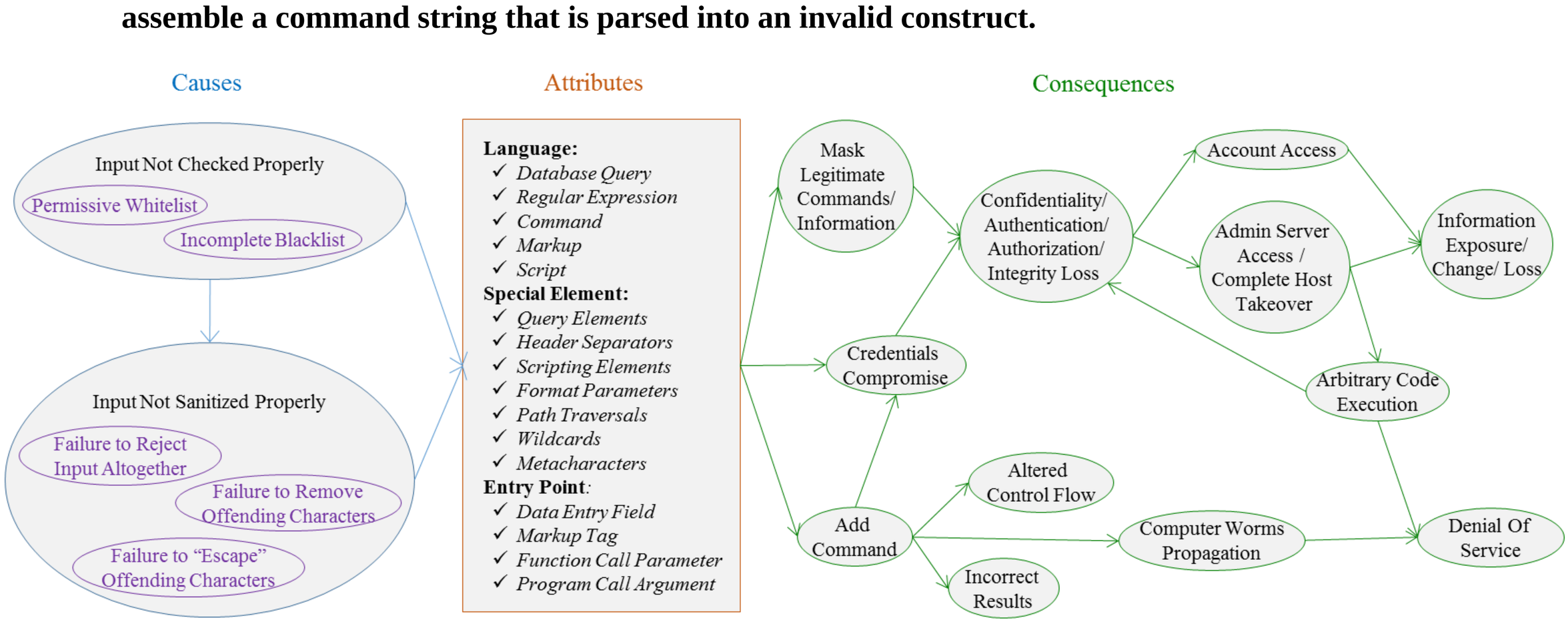
To achieve higher levels of assurance for digital systems, we need to answer questions such as does this software have bugs of these critical classes? Do two software assurance tools find the same set of bugs or different, complimentary sets? Can we guarantee that a new technique discovers all problems of this type? To answer such questions, we need a vastly improved way to describe classes of vulnerabilities and chains of failures. We present a descriptive Bugs Framework (BF) that will raise the current realm of best efforts and useful heuristics. We provide definitions of three weakness classes. We have available examples of applying our BF taxonomy to describe particular vulnerabilities.

Our Definitions and BF Taxonomy

Buffer Overflow (BOF): The software can access through an array a memory location that is outside the array boundaries.



Injection (INJ): Due to malicious input with a language-specific special element, the software can assemble a command string that is parsed into an invalid construct.



Control of Interaction Frequency (CIF): The software does not properly limit the number of repeating interactions per specified unit.