BF Vulnerability Model

Bug_1

$Error_1 \rightarrow$ Faulty $Operand_{2j}$

$Error_2 \rightarrow$ Faulty $Operand_{3j}$

$Error_n \rightarrow$ Faulty $Operand_{np}$

Exploitable $Error_1$

$Weakness_1$
($operation_1$,
$operand_{11}$, ...
$operand_{1i}$, ...)

$Weakness_2$
($operation_2$, ...,
$operand_{2j}$, ...)

...

$Weakness_n$
($operation_n$, ...,
$operand_{np}$, ...)

$\oplus$

... Bug_2

$Error_1 \rightarrow$ Faulty $Operand_{2k}$

$Error_m \rightarrow$ Faulty $Operand_{mq}$

Exploitable $Error_2$

$Weakness_1$
($operation_1$,
$operand_{11}$, ...
$operand_{1i}$, ...)

...

$Weakness_m$
($operation_m$, ...,
$operand_{mq}$, ...)

$Failure_1$
($exploit_1$)

...

Faulty $Operand_1$

$Error_1 \rightarrow$ Faulty $Operand_{2j}$

$Error_l \rightarrow$ Faulty $Operand_{lr}$

Exploitable $Error_k$

$Weakness_1$
($operation_1$,
$operand_{1i}$, ...)

...

$Weakness_l$
($operation_l$, ...
$operand_{lr}$, ...)

$Failure_k$
($exploit_k$)

BF, I. Bojanova , 2014-2023

Weakness: An improper state (operation, $operand_1$, ..., $operand_n$) tuple with at least one improper element (depicted in purple).

First Weakness – caused by a Bug in the Operation, resulting in an Error

Propagation Weakness – caused by a Fault of an Operand, resulting in an Error

Final Weakness – caused by a Fault in an Operand, resulting in an Exploitable Error

Failure – a violation of a security requirement caused by an exploit may result in a Fault starting a new faults-only vulnerability

Chaining weaknesses underlying a vulnerability

Converging vulnerabilities

Chaining vulnerabilities