BF Vulnerability Model

Bug$_1$

Error$_1 \longrightarrow$ Faulty Operand$_{2j}$

Error$_2 \longrightarrow$ Faulty Operand$_{3j}$

Error$_n \longrightarrow$ Faulty Operand$_{np}$

Exploitable Error$_1$

Improper State$_1$
(operation$_1$,
operand$_{11}$, ...
operand$_{1i}$, ...)

Improper State$_2$
(operation$_2$, ...,
operand$_{2j}$, ...)

...

Improper State$_n$
(operation$_n$, ...,
operand$_{np}$, ...)

$\oplus$

... Bug$_2$

Error$_1 \longrightarrow$ Faulty Operand$_{2k}$

Error$_m \longrightarrow$ Faulty Operand$_{mq}$

Exploitable Error$_2$

Improper State$_1$
(operation$_1$,
operand$_{11}$, ...
operand$_{1i}$, ...)

...

Improper State$_m$
(operation$_m$, ...,
operand$_{mq}$, ...)

Failure$_1$
(exploit$_1$)

...

Faulty Operand$_1$

Error$_1 \longrightarrow$ Faulty Operand$_{2j}$

Error$_l \longrightarrow$ Faulty Operand$_{lr}$

Exploitable Error$_k$

Improper State$_1$
(operation$_1$,
operand$_{1i}$, ...)

...

Improper State$_l$
(operation$_l$, ...
operand$_{lr}$, ...)

Failure$_k$
(exploit$_k$)

BF, I. Bojanova , 2014-2024

Improper State: An operation, operand$_1$, ..., operand$_n$) tuple with at least one improper element (depicted in purple)

Initial State – a weakness caused by a Bug in the Operation, resulting in an Error

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

Final State – a 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

$\oplus$ Converging vulnerabilities

$\hookrightarrow$ Chaining vulnerabilities