Secure Software Development – SSD

Tutorial 1

Kogler, Grogger, Maar

20.10.2021

Winter 2021/22, www.iaik.tugraz.at/ssd

Agenda

- Tools
- Q & A

Agenda

- Tools
- Q & A

Questions?

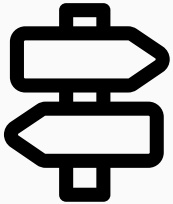
Sanitizers

- Thread Sanitizer `-fsanitize=threads`
- Demo
- How to fix?
  - locking / lock-free algorithms

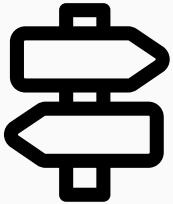
- Thread Sanitizer `-fsanitize=threads`
- Demo
- How to fix?
  - locking / lock-free algorithms

- Thread Sanitizer `-fsanitize=threads`
- Demo
- How to fix?
  - locking / lock-free algorithms

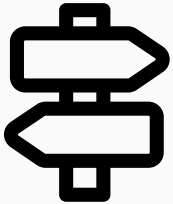
- Thread Sanitizer `-fsanitize=threads`
- Demo
- How to fix?
  - locking / lock-free algorithms



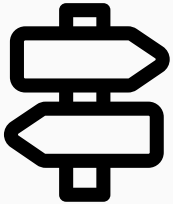
- Address Sanitizer `-fsanitize=address`
- Demo
- How to fix?
  - check for out-of-bounds accesses
  - buffer sizes
  - use-after-free



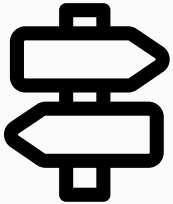
- Address Sanitizer `-fsanitize=address`
- Demo
- How to fix?
  - check for out-of-bounds accesses
  - buffer sizes
  - use-after-free



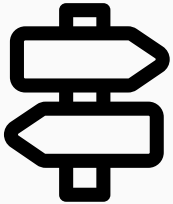
- Address Sanitizer `-fsanitize=address`
- Demo
- How to fix?
  - check for out-of-bounds accesses
  - buffer sizes
  - use-after-free



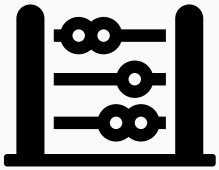
- Address Sanitizer `-fsanitize=address`
- Demo
- How to fix?
  - check for out-of-bounds accesses
  - buffer sizes
  - use-after-free



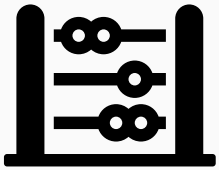
- Address Sanitizer `-fsanitize=address`
- Demo
- How to fix?
  - check for out-of-bounds accesses
  - buffer sizes
  - use-after-free



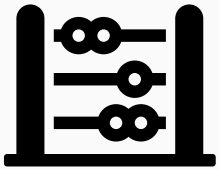
- Address Sanitizer `-fsanitize=address`
- Demo
- How to fix?
  - check for out-of-bounds accesses
  - buffer sizes
  - use-after-free



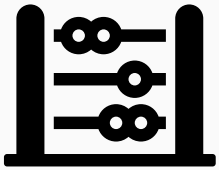
- Integer Sanitizer `-fsanitize=integer`
- Demo
- How to fix?
  - check data types
  - also verify the ranges of your data
  - overflow aware operations like `__builtin_add_overflow`



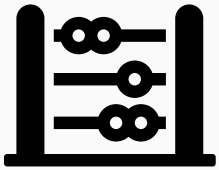
- Integer Sanitizer `-fsanitize=integer`
- Demo
- How to fix?
  - check data types
  - also verify the ranges of your data
  - overflow aware operations like `__builtin_add_overflow`



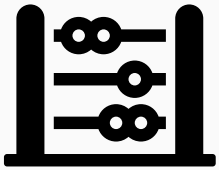
- Integer Sanitizer `-fsanitize=integer`
- Demo
- How to fix?
  - check data types
  - also verify the ranges of your data
  - overflow aware operations like `__builtin_add_overflow`



- Integer Sanitizer `-fsanitize=integer`
- Demo
- How to fix?
  - check data types
  - also verify the ranges of your data
  - overflow aware operations like `__builtin_add_overflow`

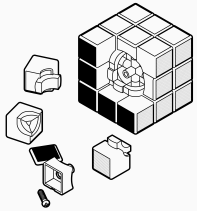


- Integer Sanitizer `-fsanitize=integer`
- Demo
- How to fix?
  - check data types
  - also verify the ranges of your data
  - overflow aware operations like `__builtin_add_overflow`

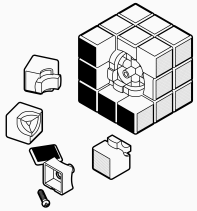


- Integer Sanitizer `-fsanitize=integer`
- Demo
- How to fix?
  - check data types
  - also verify the ranges of your data
  - overflow aware operations like `__builtin_add_overflow`

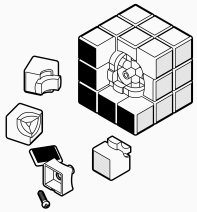
Assembly Tools



- Radare2
- Ghidra
- Cutter



- Radare2
- Ghidra
- Cutter



- Radare2
- Ghidra
- Cutter

Questions?