Secure Software Development – SSD

Handout Defenselets 1 & 2

Kogler, Grogger, Maar

15.10.2021

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

Agenda

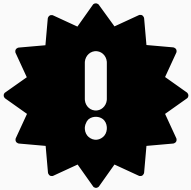
- Handout of Defenselets 1 & 2
- Interactive Demos
- Q & A

Agenda

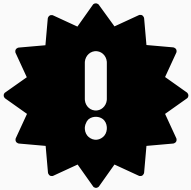
- Handout of Defenselets 1 & 2
- Interactive Demos
- Q & A

Agenda

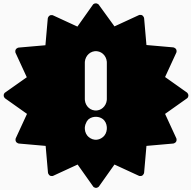
- Handout of Defenselets 1 & 2
- Interactive Demos
- Q & A



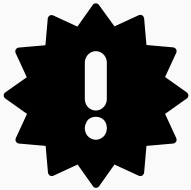
- Warmup:
  - Deadline: 22nd of October 23:59 (22.10.2021)
  - Tag: `warmup`
- Defenselets1:
  - Deadline: 12th of November 23:59 (12.11.2021)
  - Tag: `defenselets1`
- Defenselets2:
  - Deadline: 19th of November 23:59 (19.11.2021)
  - Tag: `defenselets2`



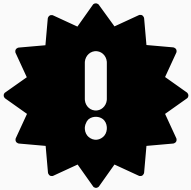
- Warmup:
  - **Deadline:** 22nd of October 23:59 (22.10.2021)
  - Tag: `warmup`
- Defenselets1:
  - **Deadline:** 12th of November 23:59 (12.11.2021)
  - Tag: `defenselets1`
- Defenselets2:
  - **Deadline:** 19th of November 23:59 (19.11.2021)
  - Tag: `defenselets2`



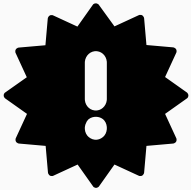
- Warmup:
  - **Deadline:** 22nd of October 23:59 (22.10.2021)
  - **Tag:** `warmup`
- Defenselets1:
  - **Deadline:** 12th of November 23:59 (12.11.2021)
  - **Tag:** `defenselets1`
- Defenselets2:
  - **Deadline:** 19th of November 23:59 (19.11.2021)
  - **Tag:** `defenselets2`



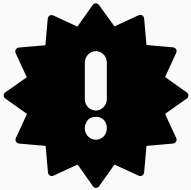
- Warmup:
  - **Deadline:** 22nd of October 23:59 (22.10.2021)
  - **Tag:** `warmup`
- Defenselets1:
  - **Deadline:** 12th of November 23:59 (12.11.2021)
  - **Tag:** `defenselets1`
- Defenselets2:
  - **Deadline:** 19th of November 23:59 (19.11.2021)
  - **Tag:** `defenselets2`



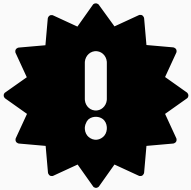
- Warmup:
  - **Deadline:** 22nd of October 23:59 (22.10.2021)
  - **Tag:** `warmup`
- Defenselets1:
  - **Deadline:** 12th of November 23:59 (12.11.2021)
  - **Tag:** `defenselets1`
- Defenselets2:
  - **Deadline:** 19th of November 23:59 (19.11.2021)
  - **Tag:** `defenselets2`



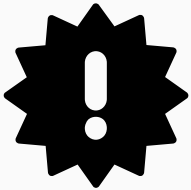
- Warmup:
  - **Deadline:** 22nd of October 23:59 (22.10.2021)
  - **Tag:** `warmup`
- Defenselets1:
  - **Deadline:** 12th of November 23:59 (12.11.2021)
  - **Tag:** `defenselets1`
- Defenselets2:
  - **Deadline:** 19th of November 23:59 (19.11.2021)
  - **Tag:** `defenselets2`



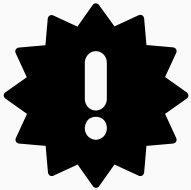
- Warmup:
  - **Deadline:** 22nd of October 23:59 (22.10.2021)
  - **Tag:** `warmup`
- Defenselets1:
  - **Deadline:** 12th of November 23:59 (12.11.2021)
  - **Tag:** `defenselets1`
- Defenselets2:
  - **Deadline:** 19th of November 23:59 (19.11.2021)
  - **Tag:** `defenselets2`



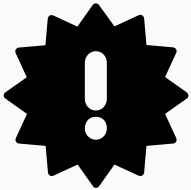
- Warmup:
  - **Deadline:** 22nd of October 23:59 (22.10.2021)
  - **Tag:** `warmup`
- Defenselets1:
  - **Deadline:** 12th of November 23:59 (12.11.2021)
  - **Tag:** `defenselets1`
- Defenselets2:
  - **Deadline:** 19th of November 23:59 (19.11.2021)
  - **Tag:** `defenselets2`



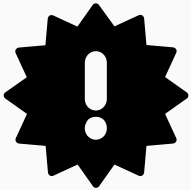
- Warmup:
  - **Deadline:** 22nd of October 23:59 (22.10.2021)
  - **Tag:** `warmup`
- Defenselets1:
  - **Deadline:** 12th of November 23:59 (12.11.2021)
  - **Tag:** `defenselets1`
- Defenselets2:
  - **Deadline:** 19th of November 23:59 (19.11.2021)
  - **Tag:** `defenselets2`



- Test System:
  `https://sase.student.iaik.tugraz.at/`
- Practicals: `https://www.iaik.tugraz.at/teaching/materials/ssd/practicals/`
- Defenselets: `https://www.iaik.tugraz.at/teaching/materials/ssd/defenselets/`

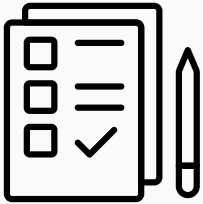


- Test System: `https://sase.student.iaik.tugraz.at/`
- Practicals: `https://www.iaik.tugraz.at/teaching/materials/ssd/practicals/`
- Defenselets: `https://www.iaik.tugraz.at/teaching/materials/ssd/defenselets/`

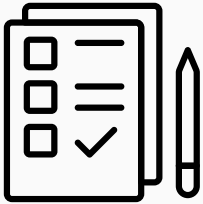


- Test System: `https://sase.student.iaik.tugraz.at/`
- Practicals: `https://www.iaik.tugraz.at/teaching/materials/ssd/practicals/`
- Defenselets: `https://www.iaik.tugraz.at/teaching/materials/ssd/defenselets/`

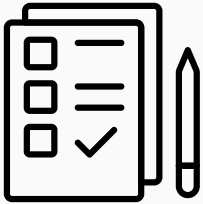
Defenselets 1



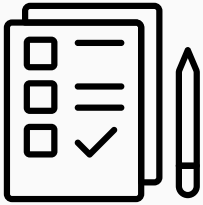
- File Handler (6 Points)
- Stack Encryption (7 Points)
- Tic Tac Toe (7 Points)
- Tiny File (7 Points)
- Points overall: 27



- File Handler (6 Points)
- Stack Encryption (7 Points)
- Tic Tac Toe (7 Points)
- Tiny File (7 Points)
- Points overall: 27

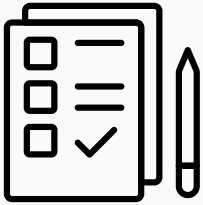


- File Handler (6 Points)
- Stack Encryption (7 Points)
- Tic Tac Toe (7 Points)
- Tiny File (7 Points)
- Points overall: 27



- File Handler (6 Points)
- Stack Encryption (7 Points)
- Tic Tac Toe (7 Points)
- Tiny File (7 Points)
- Points overall: 27

Defenselets 1



- File Handler (6 Points)
- Stack Encryption (7 Points)
- Tic Tac Toe (7 Points)
- Tiny File (7 Points)
- Points overall: 27

- Small program to read arbitrary file
- Only if password is known
- Problem:
  - leaks addresses

- Small program to read arbitrary file
- Only if password is known
- Problem:
  - leaks addresses

- Small program to read arbitrary file
- Only if password is known
- Problem:
  - leaks addresses

- Small program to read arbitrary file
- Only if password is known
- Problem:
  - leaks addresses

File Handler

- Points: 6
- Deliverables:
  - 50%: Input to leak an address of the program
  - 50%: Fixed `file_handler.c` file

- Points: 6
- Deliverables:
  - 50%: Input to leak an address of the program
  - 50%: Fixed `file_handler.c` file.

- Points: 6
- Deliverables:
  - 50%: Input to leak an address of the program
  - 50%: Fixed `file_handler.c` file.

- Points: 6
- Deliverables:
  - 50%: Input to leak an address of the program
  - 50%: Fixed `file_handler.c` file.

- Encryption code from a larger project
- Generates secret key
- Problem:
  - the secret key can be leaked

- Encryption code from a larger project
- Generates secret key
- Problem:
  - the secret key can be leaked

- Encryption code from a larger project
- Generates secret key
- Problem:
  - the secret key can be leaked

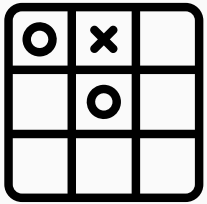
- Encryption code from a larger project
- Generates secret key
- Problem:
  - the secret key can be leaked

- Points: 7
- Deliverables:
  - 50%: Input to leak the secret key
  - 50%: Fixed `stack_encryption.c` file

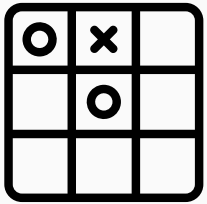
- Points: 7
- Deliverables:
  - 50%: Input to leak the secret key
  - 50%: Fixed `stack_encryption.c` file.

- Points: 7
- Deliverables:
  - 50%: Input to leak the secret key
  - 50%: Fixed `stack_encryption.c` file.

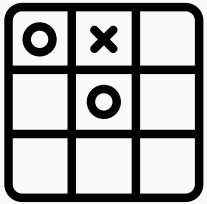
- Points: 7
- Deliverables:
  - 50%: Input to leak the secret key
  - 50%: Fixed `stack_encryption.c` file.



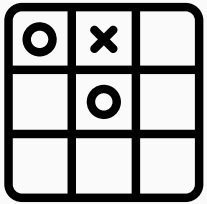
- Classic game of tic tac toe
- Problem:
  - the game can be hacked



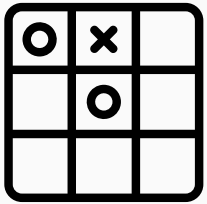
- Classic game of tic tac toe
- Problem:
  - the game can be hacked



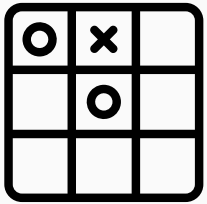
- Classic game of tic tac toe
- Problem:
  - the game can be hacked



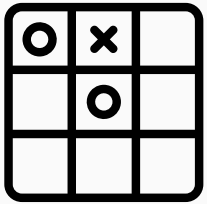
- Points: 7
- Deliverables:
  - 50%: Input to win the game without *winning*
  - 50%: Fixed `tic_tac_toe.c` file.



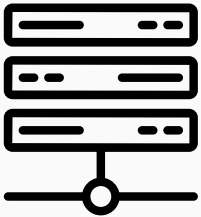
- Points: 7
- Deliverables:
  - 50%: Input to win the game without *winning*
  - 50%: Fixed `tic_tac_toe.c` file.



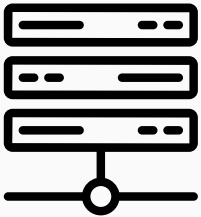
- Points: 7
- Deliverables:
  - 50%: Input to win the game without *winning*
  - 50%: Fixed `tic_tac_toe.c` file.



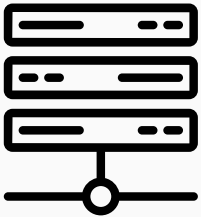
- Points: 7
- Deliverables:
  - 50%: Input to win the game without *winning*
  - 50%: Fixed `tic_tac_toe.c` file.



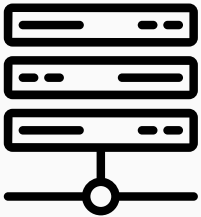
- File Server to receive files from the **current** folder
- or **subdirectories** of the current folder
- Problem:
  - you can also request arbitrary files outside *above* the current folder



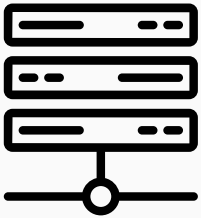
- File Server to receive files from the **current** folder
- or **subdirectories** of the current folder
- Problem:
  - you can also request arbitrary files outside *above* the current folder



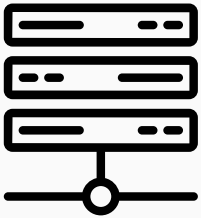
- File Server to receive files from the **current** folder
- or **subdirectories** of the current folder
- Problem:
  - you can also request arbitrary files outside *above* the current folder



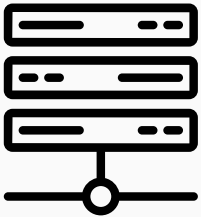
- File Server to receive files from the **current** folder
- or **subdirectories** of the current folder
- Problem:
  - you can also request arbitrary files outside *above* the current folder



- Points: 7
- Deliverables:
  - 100%: Fixed `clean_input` function in `tiny_file.c` file.

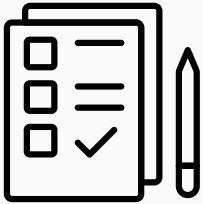


- Points: 7
- Deliverables:
  - 100%: Fixed `clean_input` function in `tiny_file.c` file.

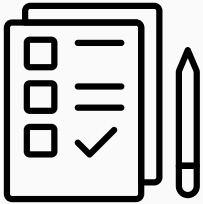


- Points: 7
- Deliverables:
  - 100%: Fixed `clean_input` function in `tiny_file.c` file.

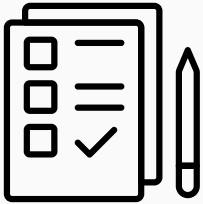
Defenselets 2



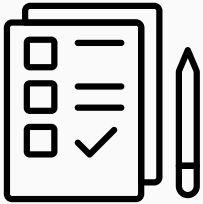
- Airport (7 Points)
- Binary Hotfix (7 Points)
- Reverse Polish Notation (7 Points)
- Stack Machine (7 Points)
- Points overall: 28



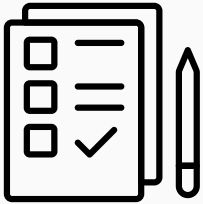
- Airport (7 Points)
- Binary Hotfix (7 Points)
- Reverse Polish Notation (7 Points)
- Stack Machine (7 Points)
- Points overall: 28



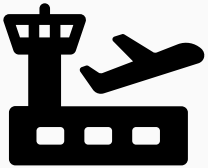
- Airport (7 Points)
- Binary Hotfix (7 Points)
- Reverse Polish Notation (7 Points)
- Stack Machine (7 Points)
- Points overall: 28



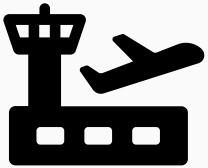
- Airport (7 Points)
- Binary Hotfix (7 Points)
- Reverse Polish Notation (7 Points)
- Stack Machine (7 Points)
- Points overall: 28



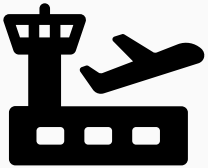
- Airport (7 Points)
- Binary Hotfix (7 Points)
- Reverse Polish Notation (7 Points)
- Stack Machine (7 Points)
- Points overall: 28



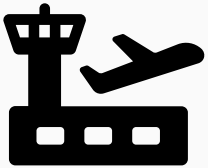
- Simulation of an airport
- Problem:
  - Sometime the simulation stops working



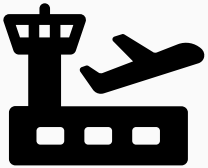
- Simulation of an airport
- Problem:
  - Sometime the simulation stops working



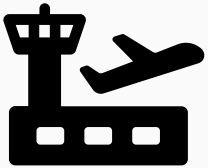
- Simulation of an airport
- Problem:
  - Sometime the simulation stops working



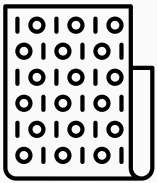
- Points: 7
- Deliverables:
  - 100%: Fixed source files (*.h *.c).



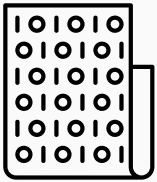
- Points: 7
- Deliverables:
  - 100%: Fixed **source** files (*.h *.c).



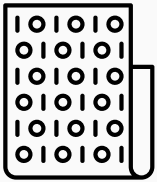
- Points: 7
- Deliverables:
  - 100%: Fixed **source** files (*.h *.c).



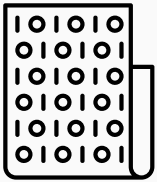
- University Management System
- Binary only
- Problem:
  - With the given input the program crashes



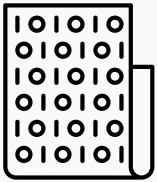
- University Management System
- Binary only
- Problem:
  - With the given input the program crashes



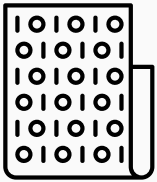
- University Management System
- Binary only
- Problem:
  - With the given input the program crashes



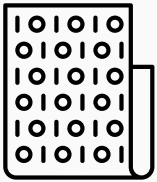
- University Management System
- Binary only
- Problem:
  - With the given input the program crashes



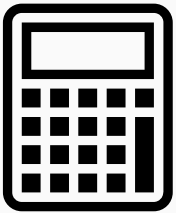
- Points: 7
- Deliverables:
  - 100%: Provide a fixed binary. Change only one byte!



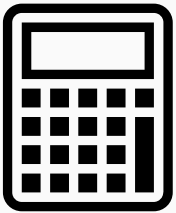
- Points: 7
- Deliverables:
  - 100%: Provide a fixed binary. Change only **one** byte!



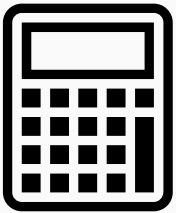
- Points: 7
- Deliverables:
  - 100%: Provide a fixed binary. Change only **one** byte!



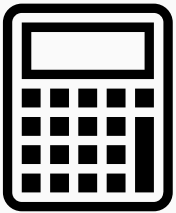
- RPN Calculator
- Problem:
  - Sometime the program crashes.



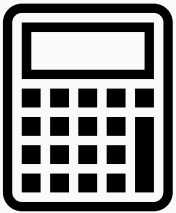
- RPN Calculator
- Problem:
  - Sometime the program crashes.



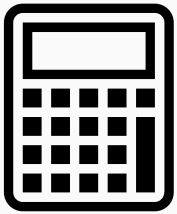
- RPN Calculator
- Problem:
  - Sometime the program crashes.



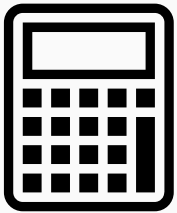
- Points: 7
- Deliverables:
  - 50%: Input to crash the calculator
  - 50%: Fixed source files (*.h *.c).



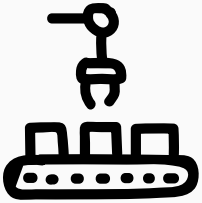
- Points: 7
- Deliverables:
  - 50%: Input to crash the calculator
  - 50%: Fixed source files (*.h *.c).



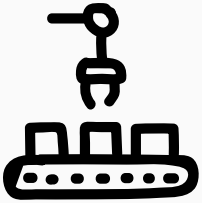
- Points: 7
- Deliverables:
  - 50%: Input to crash the calculator
  - 50%: Fixed source files (*.h *.c).



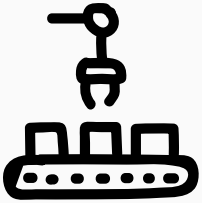
- Points: 7
- Deliverables:
  - 50%: Input to crash the calculator
  - 50%: Fixed **source** files (*.h *.c).



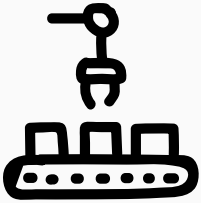
- Simple Stack Machine
- Problem:
  - User reported a heap overflow.



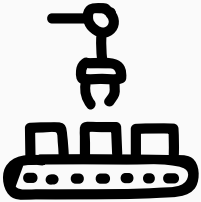
- Simple Stack Machine
- Problem:
  - User reported a heap overflow.



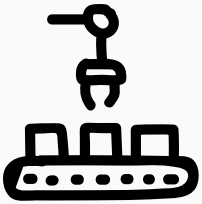
- Simple Stack Machine
- Problem:
  - User reported a heap overflow.



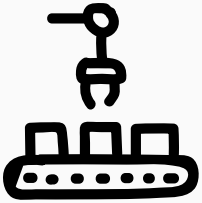
- Points: 7
- Deliverables:
  - 50%: Reproduce the address sanitizer bug with `main.c`.
  - 50%: Fixed stack machine `stack_machine.h` and `stack_machine.c`.



- Points: 7
- Deliverables:
  - 50%: Reproduce the address sanitizer bug with `main.c`.
  - 50%: Fixed stack machine `stack_machine.h` and `stack_machine.c`.



- Points: 7
- Deliverables:
  - 50%: Reproduce the address sanitizer bug with `main.c`.
  - 50%: Fixed stack machine `stack_machine.h` and `stack_machine.c`.



- Points: 7
- Deliverables:
  - 50%: Reproduce the address sanitizer bug with `main.c`.
  - 50%: Fixed stack machine `stack_machine.h` and `stack_machine.c`.

Demo

Questions?