OS Verification by Abstract Interpretation

Hochschule **RheinMain**
University of Applied Sciences
Wiesbaden Rüsselsheim

- Goals:
  1. Learn, understand *Abstract Interpretation* methodology
  2. Analyse an understand BINSEC, a FOSS binary code analysis tool (written in OCaml)
  3. Apply it to (simple) Operating Systems
  4. Formally prove absence of runtime errors (ARTE) and absence of privilege escalation (APE)

Abstract Interpretation Basics

Abstract each numeric variable by an interval

```
int i = 100;
int x = 0;
while(i > 1) {
 i–;
}
int x = 42 / i;
```

- Abstract interpretation can prove properties (Here: no division by zero)
- No specification required for this property (implicit)

Abstract Interpretation Basics

Abstract each numeric variable by an interval

```
int i = 100;
int x = 0;
while(i > 1) {
 i-;
}
int x = 42 / i;
```

$\longleftrightarrow \quad i \in \{100\}$

- Abstract interpretation can prove properties (Here: no division by zero)
- No specification required for this property (implicit)

Abstract Interpretation Basics

Abstract each numeric variable by an interval

```
int i = 100;      ⟷   i ∈ {100}
int x = 0;        ⟷   i ∈ {100}, x ∈ {0}
while(i > 1) {
 i-;
}
int x = 42 / i;
```

- Abstract interpretation can prove properties (Here: no division by zero)
- No specification required for this property (implicit)

Abstract Interpretation Basics

Abstract each numeric variable by an interval

`int i = 100;`	$\longleftrightarrow$	$i \in \{100\}$
`int x = 0;`	$\longleftrightarrow$	$i \in \{100\}, x \in \{0\}$
`while(i > 1) {`	$\longleftrightarrow$	$i \in \{100\}, x \in \{0\}$
`  i-;`		
`}`		
`int x = 42 / i;`		

- Abstract interpretation can prove properties (Here: no division by zero)
- No specification required for this property (implicit)

Abstract Interpretation Basics

Abstract each numeric variable by an interval

`int i = 100;`	$\longleftrightarrow$	$i \in \{100\}$
`int x = 0;`	$\longleftrightarrow$	$i \in \{100\}, x \in \{0\}$
`while(i > 1) {`	$\longleftrightarrow$	$i \in \{100\}, x \in \{0\}$
` i-;`	$\longleftrightarrow$	$i \in \{99\}, x \in \{0\}$
`}`		
`int x = 42 / i;`		

- Abstract interpretation can prove properties (Here: no division by zero)
- No specification required for this property (implicit)

Abstract Interpretation Basics

Abstract each numeric variable by an interval

`int i = 100;`	$\longleftrightarrow$	$i \in \{100\}$
`int x = 0;`	$\longleftrightarrow$	$i \in \{100\}, x \in \{0\}$
`while(i > 1) {`	$\longleftrightarrow$	$i \in [99, 100], x \in \{0\}$
`  i-;`	$\longleftrightarrow$	$i \in \{99\}, x \in \{0\}$
`}`		
`int x = 42 / i;`		

- Abstract interpretation can prove properties (Here: no division by zero)
- No specification required for this property (implicit)

Abstract Interpretation Basics

Abstract each numeric variable by an interval

`int i = 100;`	$\longleftrightarrow$	$i \in \{100\}$
`int x = 0;`	$\longleftrightarrow$	$i \in \{100\}, x \in \{0\}$
`while(i > 1) {`	$\longleftrightarrow$	$i \in [99, 100], x \in \{0\}$
` i-;`	$\longleftrightarrow$	$i \in [98, 99], x \in \{0\}$
`}`		
`int x = 42 / i;`		

- Abstract interpretation can prove properties
  (Here: no division by zero)
- No specification required for this property (implicit)

Abstract Interpretation Basics

Abstract each numeric variable by an interval

`int i = 100;`	$\longleftrightarrow$	$i \in \{100\}$
`int x = 0;`	$\longleftrightarrow$	$i \in \{100\}, x \in \{0\}$
`while(i > 1) {`	$\longleftrightarrow$	$i \in [98, 100], x \in \{0\}$
`  i-;`	$\longleftrightarrow$	$i \in [98, 99], x \in \{0\}$
`}`		
`int x = 42 / i;`		

- Abstract interpretation can prove properties
  (Here: no division by zero)
- No specification required for this property (implicit)

Abstract Interpretation Basics

Abstract each numeric variable by an interval

`int i = 100;`	$\longleftrightarrow$	$i \in \{100\}$
`int x = 0;`	$\longleftrightarrow$	$i \in \{100\}, x \in \{0\}$
`while(i > 1) {`	$\longleftrightarrow$	$i \in [98, 100], x \in \{0\}$
`  i-;`	$\longleftrightarrow$	$i \in [97, 99], x \in \{0\}$
`}`		
`int x = 42 / i;`		

- Abstract interpretation can prove properties (Here: no division by zero)
- No specification required for this property (implicit)

Abstract Interpretation Basics

Abstract each numeric variable by an interval

`int i = 100;`	$\longleftrightarrow$	$i \in \{100\}$
`int x = 0;`	$\longleftrightarrow$	$i \in \{100\}, x \in \{0\}$
`while(i > 1) {`	$\longleftrightarrow$	$i \in [2, 100], x \in \{0\}$
` i-;`	$\longleftrightarrow$	$i \in [1, 99], x \in \{0\}$
`}`		
`int x = 42 / i;`		

- Abstract interpretation can prove properties
  (Here: no division by zero)
- No specification required for this property (implicit)

Abstract Interpretation Basics

Abstract each numeric variable by an interval

`int i = 100;`	$\longleftrightarrow$	$i \in \{100\}$
`int x = 0;`	$\longleftrightarrow$	$i \in \{100\}, x \in \{0\}$
`while(i > 1) {`	$\longleftrightarrow$	$i \in [2, 100], x \in \{0\}$
`  i-;`	$\longleftrightarrow$	$i \in [1, 99], x \in \{0\}$
`}`	$\longleftrightarrow$	$i \in \{1\}, x \in \{0\}$
`int x = 42 / i;`		

- Abstract interpretation can prove properties
(Here: no division by zero)
- No specification required for this property (implicit)

Abstract Interpretation Basics

Abstract each numeric variable by an interval

`int i = 100;`	$\longleftrightarrow$	$i \in \{100\}$
`int x = 0;`	$\longleftrightarrow$	$i \in \{100\}, x \in \{0\}$
`while(i > 1) {`	$\longleftrightarrow$	$i \in [2, 100], x \in \{0\}$
`  i-;`	$\longleftrightarrow$	$i \in [1, 99], x \in \{0\}$
`}`	$\longleftrightarrow$	$i \in \{1\}, x \in \{0\}$
`int x = 42 / i;`	$\longleftrightarrow$	$i \in \{1\}, x \in \{42\}$

- Abstract interpretation can prove properties (Here: no division by zero)
- No specification required for this property (implicit)

Abstract Interpretation Basics

Abstract each numeric variable by an interval

`int i = 100;`	$\longleftrightarrow$	$i \in \{100\}$
`int x = 0;`	$\longleftrightarrow$	$i \in \{100\}, x \in \{0\}$
`while(i > 1) {`	$\longleftrightarrow$	$i \in [2, 100], x \in \{0\}$
` i-;`	$\longleftrightarrow$	$i \in [1, 99], x \in \{0\}$
`}`	$\longleftrightarrow$	$i \in \{1\}, x \in \{0\}$
`int x = 42 / i;`	$\longleftrightarrow$	$i \in \{1\}, x \in \{42\}$

- Abstract interpretation can prove properties
  (Here: no division by zero)
- No specification required for this property (implicit)

Abstract Interpretation Basics

Abstract each numeric variable by an interval

`int i = 100;`	$\longleftrightarrow$	$i \in \{100\}$
`int x = 0;`	$\longleftrightarrow$	$i \in \{100\}, x \in \{0\}$
`while(i > 1) {`	$\longleftrightarrow$	$i \in [2, 100], x \in \{0\}$
` i-;`	$\longleftrightarrow$	$i \in [1, 99], x \in \{0\}$
`}`	$\longleftrightarrow$	$i \in \{1\}, x \in \{0\}$
`int x = 42 / i;`	$\longleftrightarrow$	$i \in \{1\}, x \in \{42\}$

- Abstract interpretation can prove properties (Here: no division by zero)
- No specification required for this property (implicit)

Absence of runtime errors (ARTE) is an implicit property

Possible Occupations

- Article “No Crash, No Exploit: Automated Verification of Embedded Kernels“ by Nicole et al, submitted to RTAS 2020.
- Shows ARTE and APE for a simple real-time OS (EducRTOS)
- Based on analysis tool BINSEC (binsec.github.io)
  1. Analyse artifact provided for evaluation of soundness
  2. Analyse and BINSEC inner workings
  3. Apply to other architectures (RISC-V, ARM)
  4. ...

Formalities ...

- Practical work and technical discussion
  ("Praktische Tätigkeit und Fachgespräch") → register now
  Also need signed form "Antritt zur Prüfung in einer Lehrveranstaltung" ASAP
- Time slot: Thursday 10:00 - 13:15
- First session: 28.10.2021
- Place: ZAPP or D17