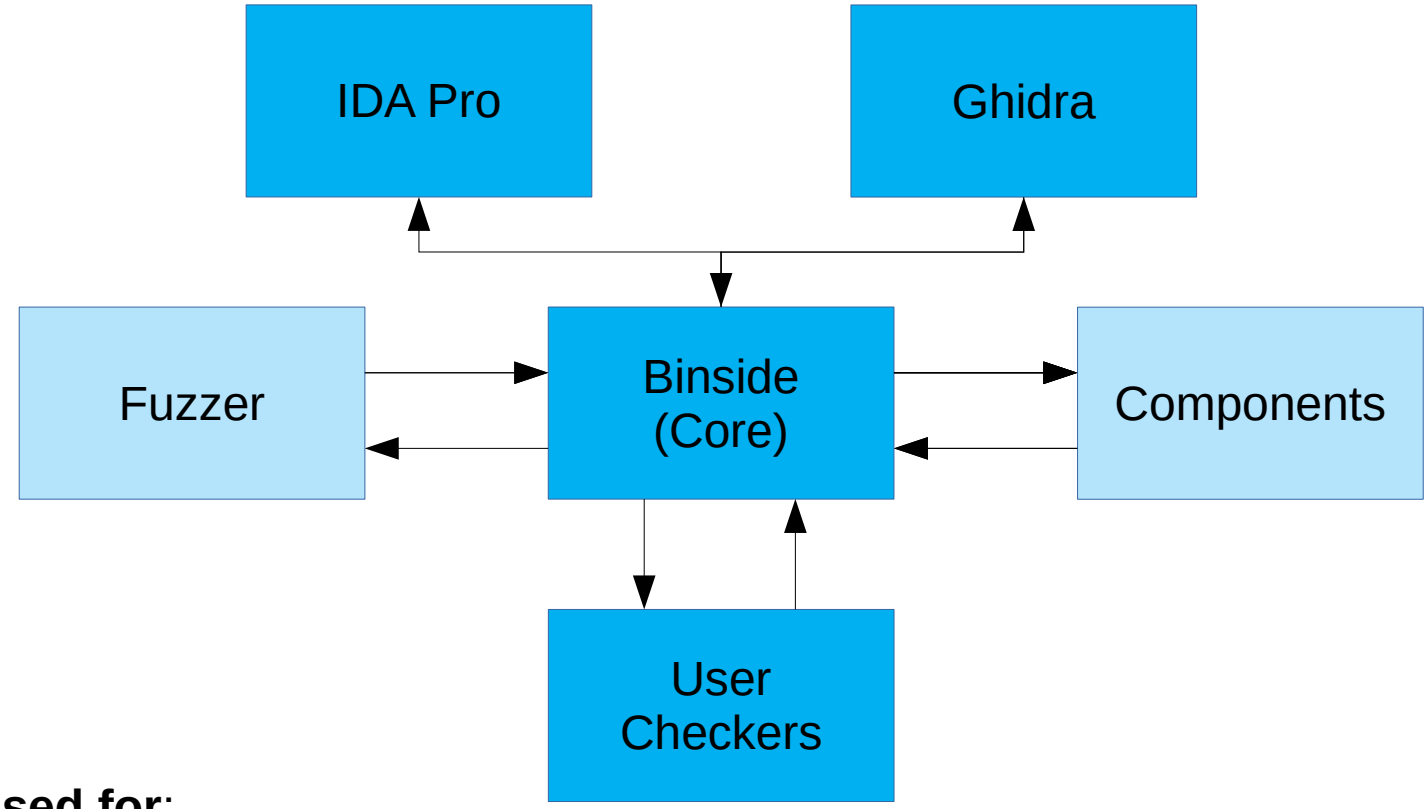
BinSide:
Binary static analysis framework

Ivanov G.S. gregory@ispras.ru
Kurmangaleev S.F. kursh@ispras.ru

ИСП РАН

BinSide: Architecture

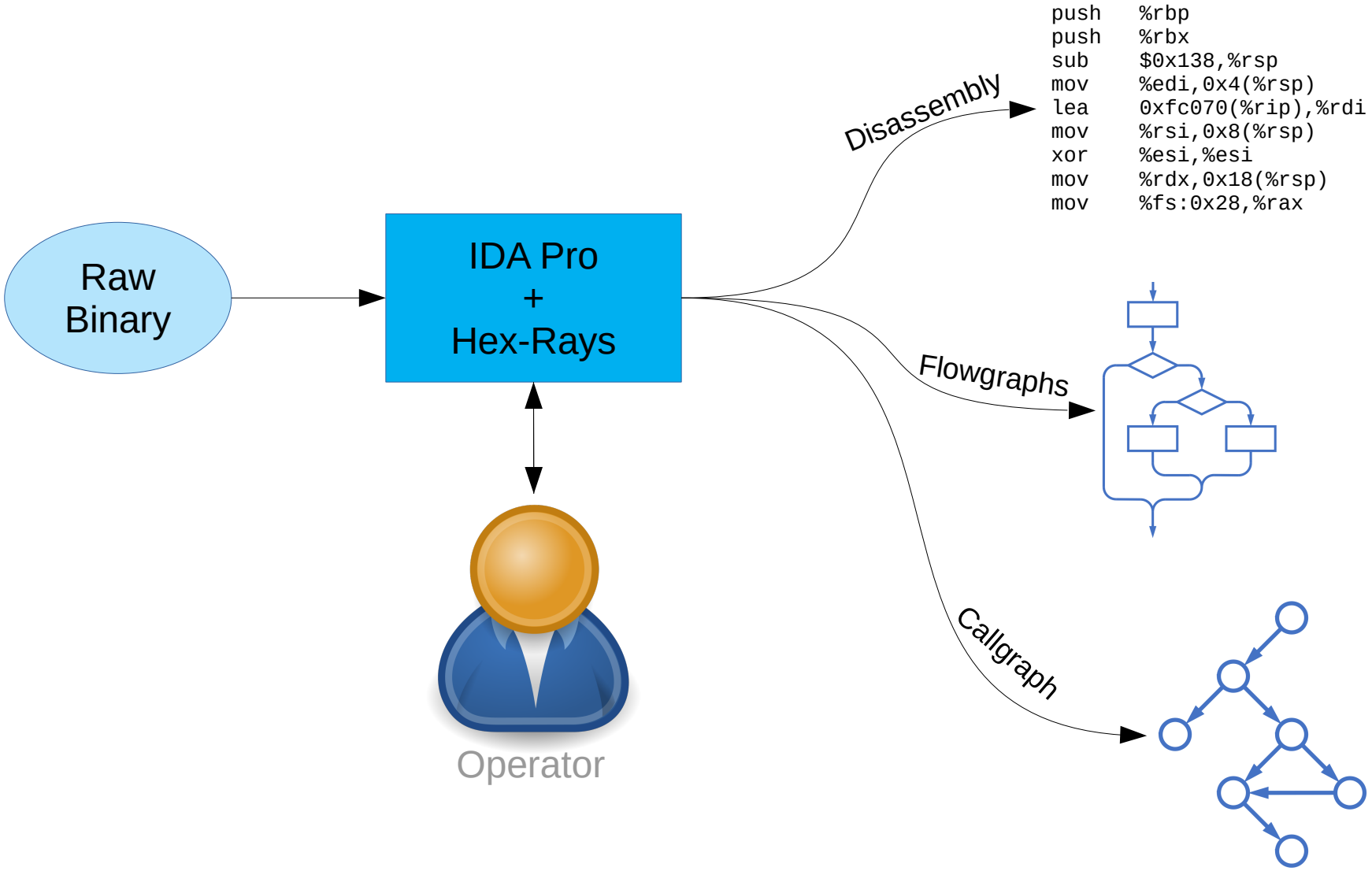


Can be used for:

- Interprocedural defects search
- Binary code analysis acceleration
- Dynamic analysis assistance

ИСП РАН

BinSide: IDA Pro



ИСП РАН

BinSide: Intermediate represintation REIL*

*REIL - Reverse Engineering Intermediate Language

```
push   %rbp
push   %rbx
sub    $0x138,%rsp
mov    %edi,0x4(%rsp)
lea    0xfc070(%rip),%rdi
mov    %rsi,0x8(%rsp)
xor    %esi,%esi
mov    %rdx,0x18(%rsp)
mov    %fs:0x28,%rax
```

Disassembly

Binside
(REIL tranlators)

REIL

```
# mov    %edi,0x4(%rsp)
and   rdi,          0xffffffff,              t1
add   4,            rsp,                     t4
and   t4,           0xffffffffffffffff,      t5
add   t5,           ssbase,                  t7
stm   t1,           EMPTY,                   t7
# lea    0xfc070(%rip),%rdi
str   1223776,      EMPTY,                   rdi
# mov    %rsi,0x8(%rsp)
str   rsi,          EMPTY,                   t0
add   8,            rsp,                     t3
and   t3,           0xffffffffffffffff,      t4
add   t4,           ssbase,                  t6
stm   t0,           EMPTY,                   t6
```

Translators supports 4 architectures:

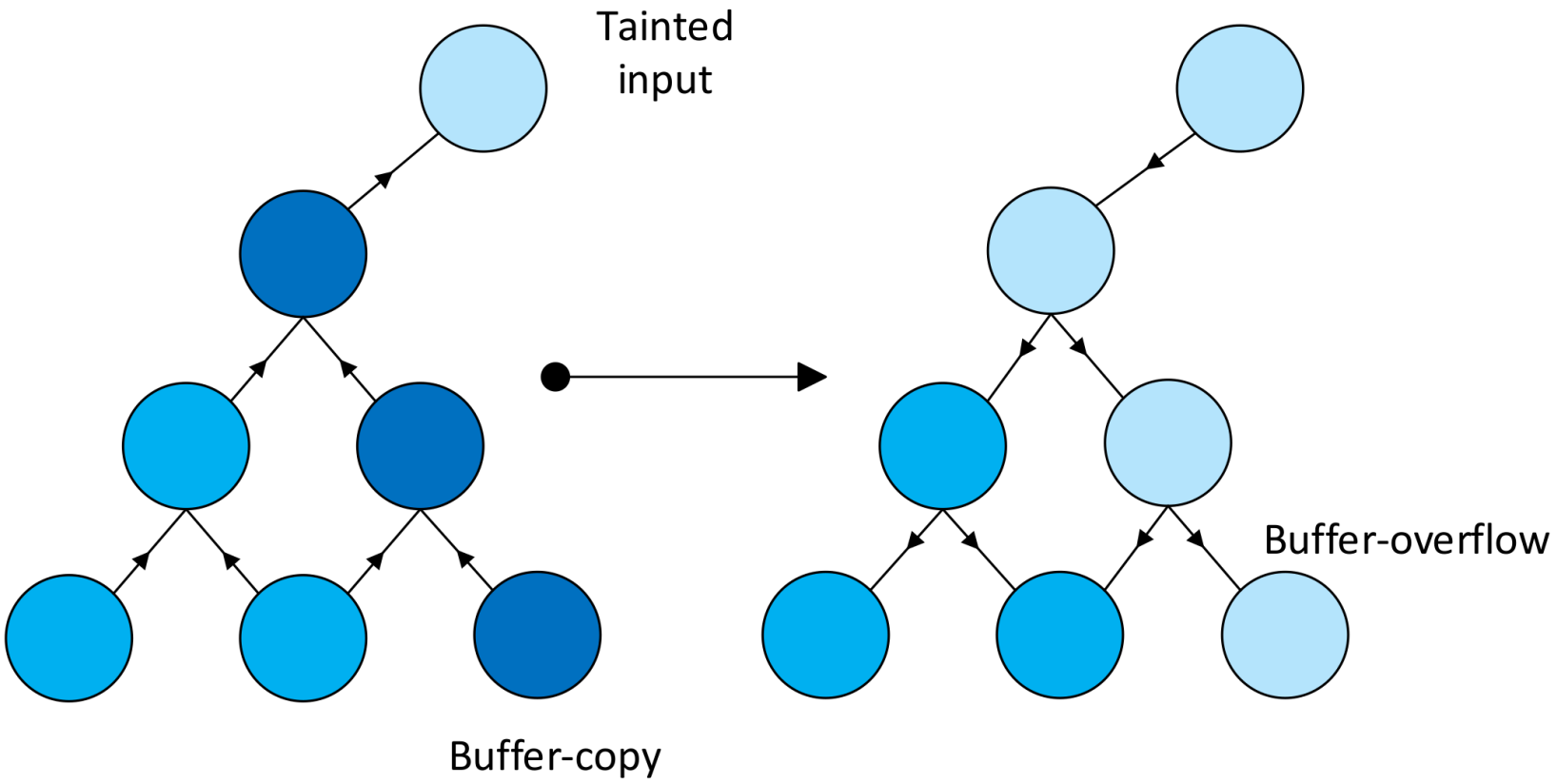
- ARM
- MISP
- x86
- x64

REIL consists of 17 non-side-effects instructions:

- 10 for math and logic operations
- 1 for conditional jump
- 3 for data transfer operations
- 3 for service instructions

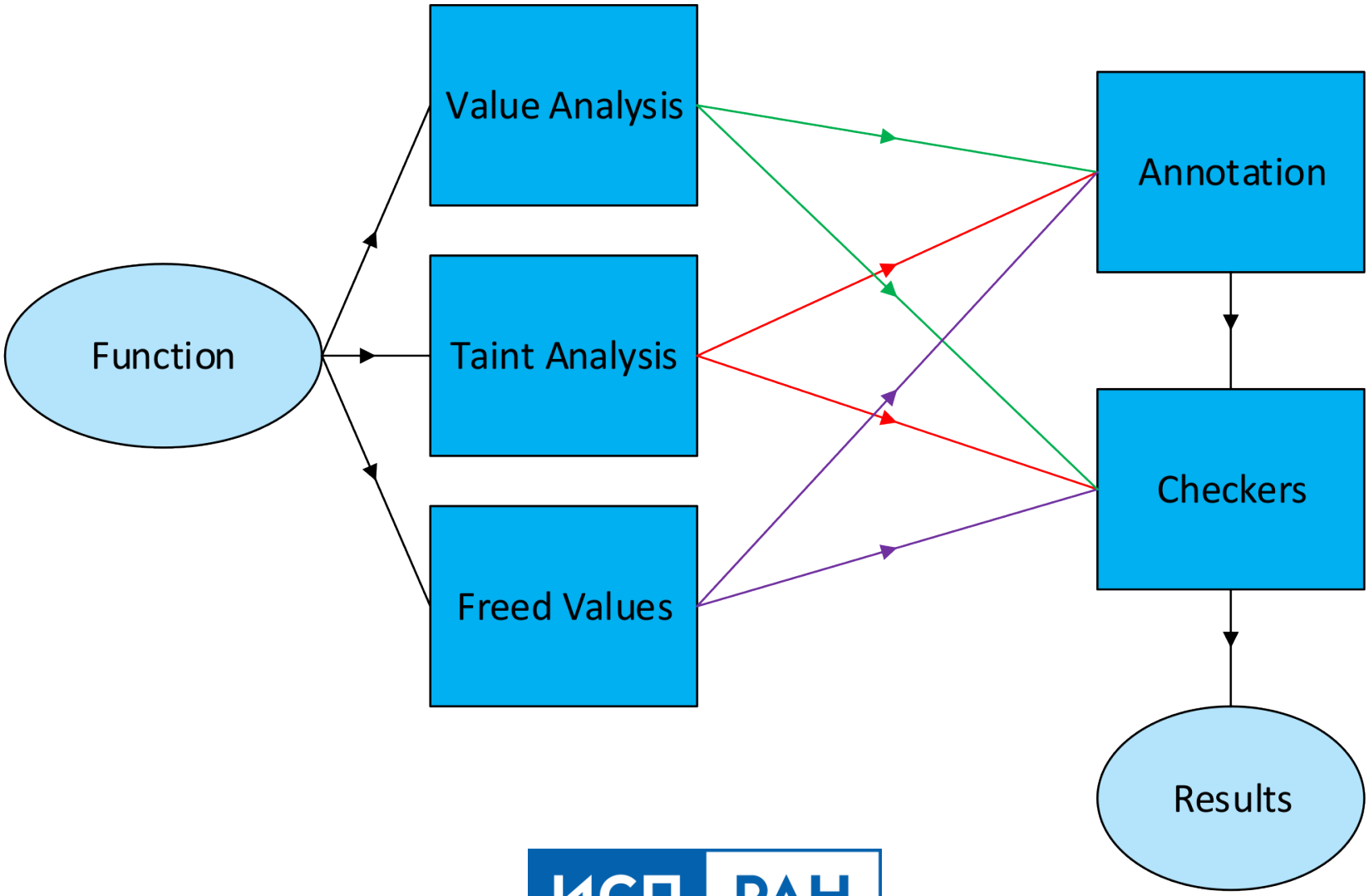
ИСП РАН

BinSide (Core): Interprocedural defects search



ИСП РАН

BinSide (Core): Intraprocedural analysis



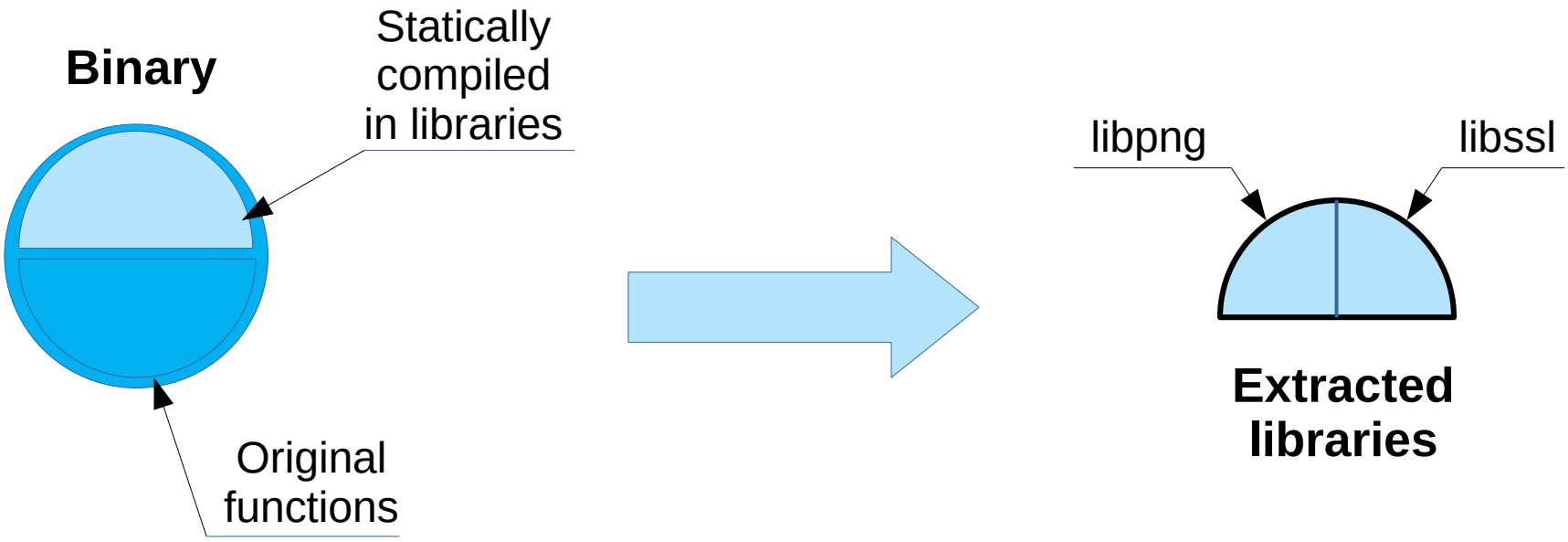
ИСП РАН

BinSide: Types of searched defects

- Heap memory allocation-deallocation issues (CWE-415, CWE-416)
- Inaccurate data copy operations (CWE-121, CWE-122)
- Use of externally-controlled format string (CWE-415)

ИСП РАН

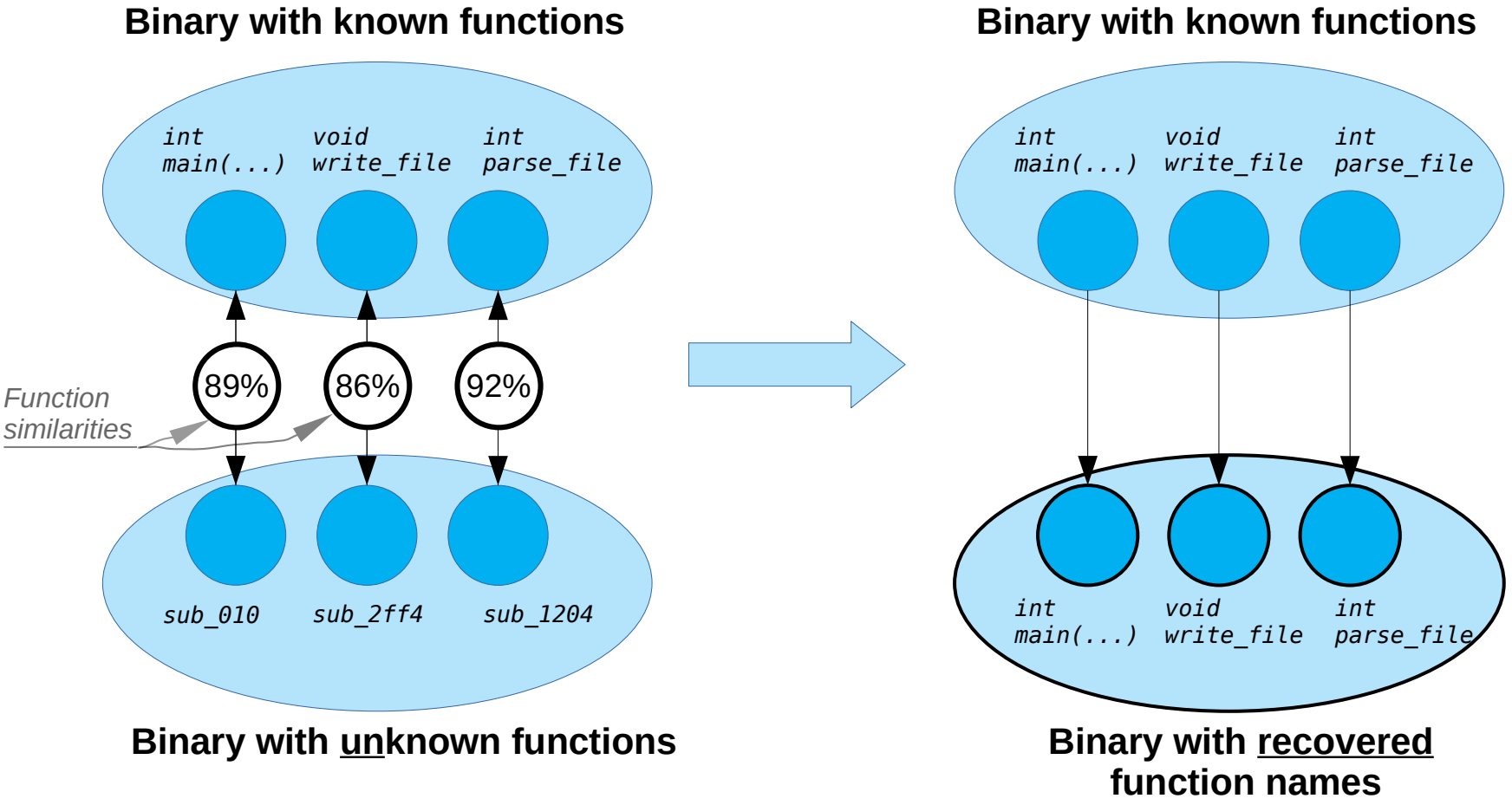
BinSide: Components (*Library Identification)



*Based on Binary Code Clone Search Tool

ИСП РАН

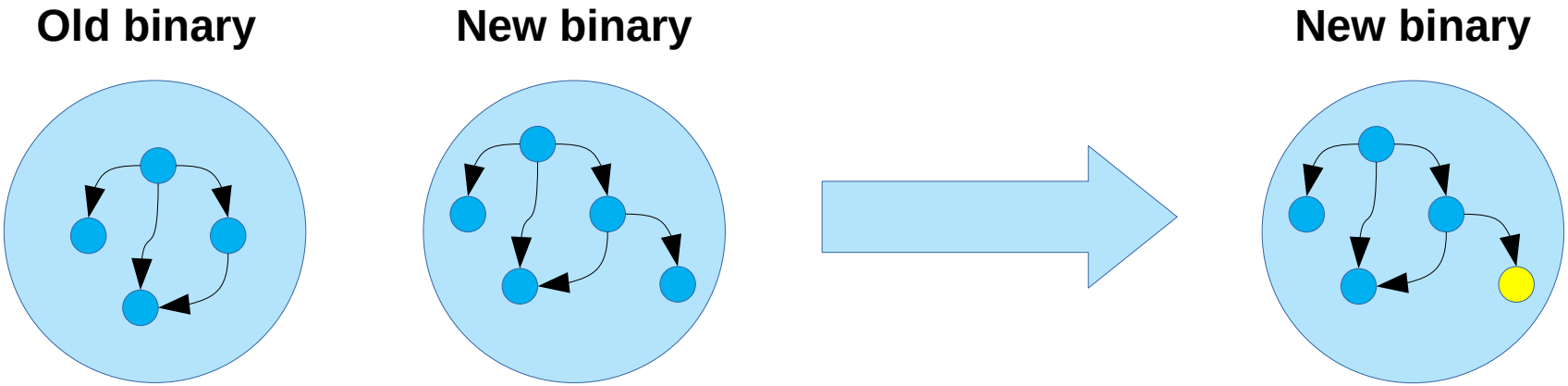
BinSide: Components (*Function Name Recovery)



*Based on Binary Code Clone Search Tool

ИСП РАН

BinSide: Components
(*Binary Differences between releases)



*Based on Binary Code Clone Search Tool

ИСП РАН

ИСП РАН

www.ispras.ru