

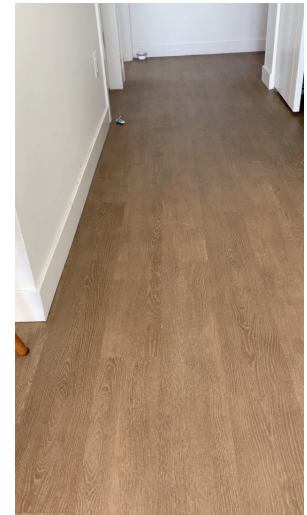
Specifying Ourselves out of a Job



SYSTOPIA



Margo Seltzer
Canada 150 Research Chair in Computer Systems
University of British Columbia



The Long Road to Program Synthesis

An Architecture A Day Keeps The Hacker Away

David A. Holland, Ada T. Lin, and Margo I. Seltzer
Harvard University
{d holland, ada, margo}@eecs.harvard.edu
September 15, 2004

Abstract

Abstract patch machines individually or in small groups, at a huge disadvantage.

System security as it is practiced today is a living battle. In this paper, we explore a possible counter-heuristic approach for binary-based attacks, using virtual machines, machine descriptions, and randomization to achieve load homogeneity at the machine level. This heterogeneity increases the "cost" of focused-based binary attacks to a significantly higher level than that of generic attacks. The current state-of-the-art in binary-based attacks is the emergence of focused recent technology approaches to make our approach achievable at a reasonable cost, still only moderate run time overhead.

1 Insecurity



1999

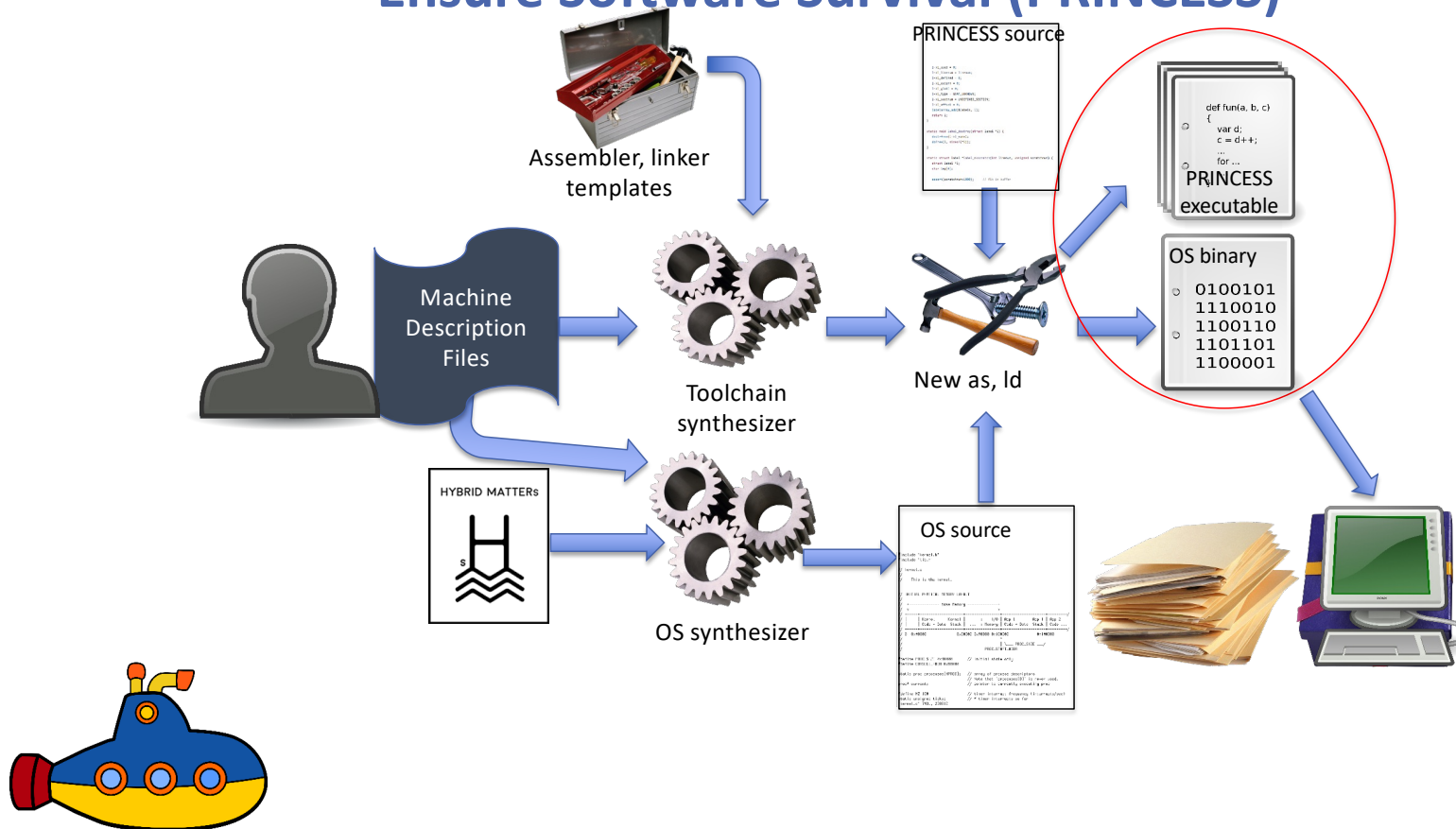


2004

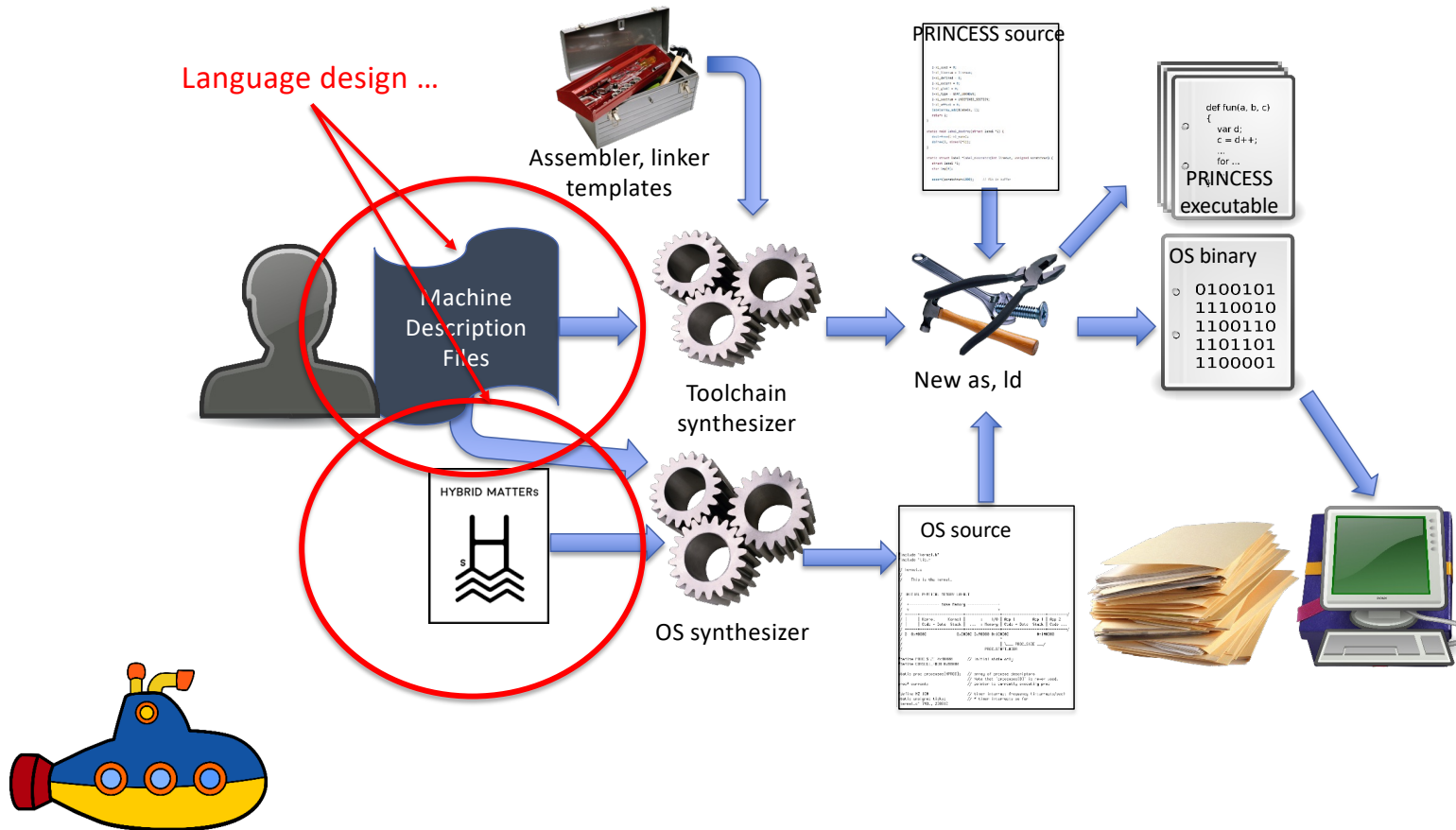
2005



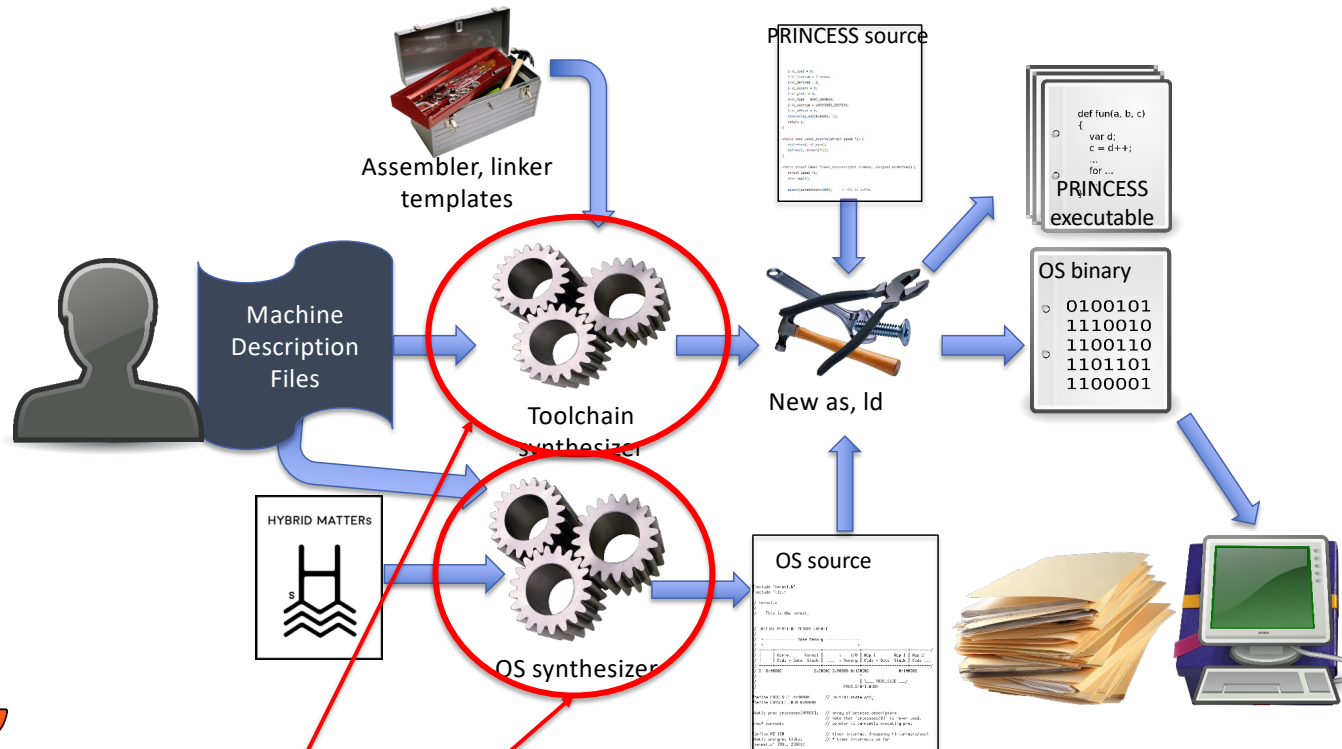
Probabilistic Representation of Intent Commitments to Ensure Software Survival (PRINCESS)



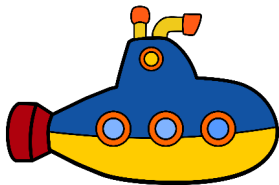
OS and Tool Synthesis: It's all PL



OS and Tool Synthesis: It's **all** PL

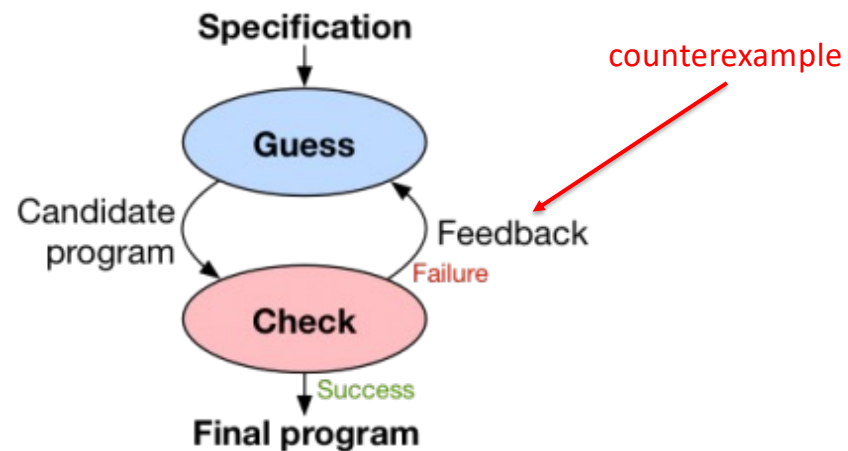


A funny thing about synthesis...

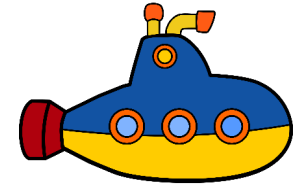


What is CEGIS?

- Counterexample-Guided Inductive Synthesis
- AKA: Guess and Check



I'm doing what ???



DEFENSE ADVANCED
RESEARCH PROJECTS AGENCY

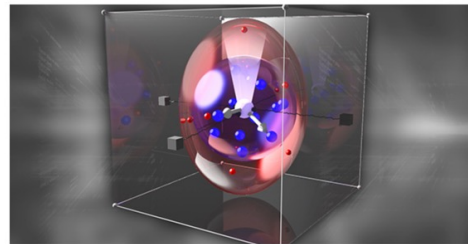
ABOUT US / OUR RESEARCH / NEWS / EVENTS / WORK WITH US /

EXPLORE BY TAG

Defense Advanced Research Projects Agency > Program Information

Building Resource Adaptive Software Systems (BRASS)

Dr. Raymond Richards

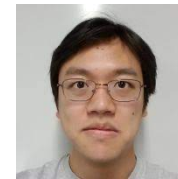
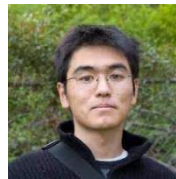


RESOURCES

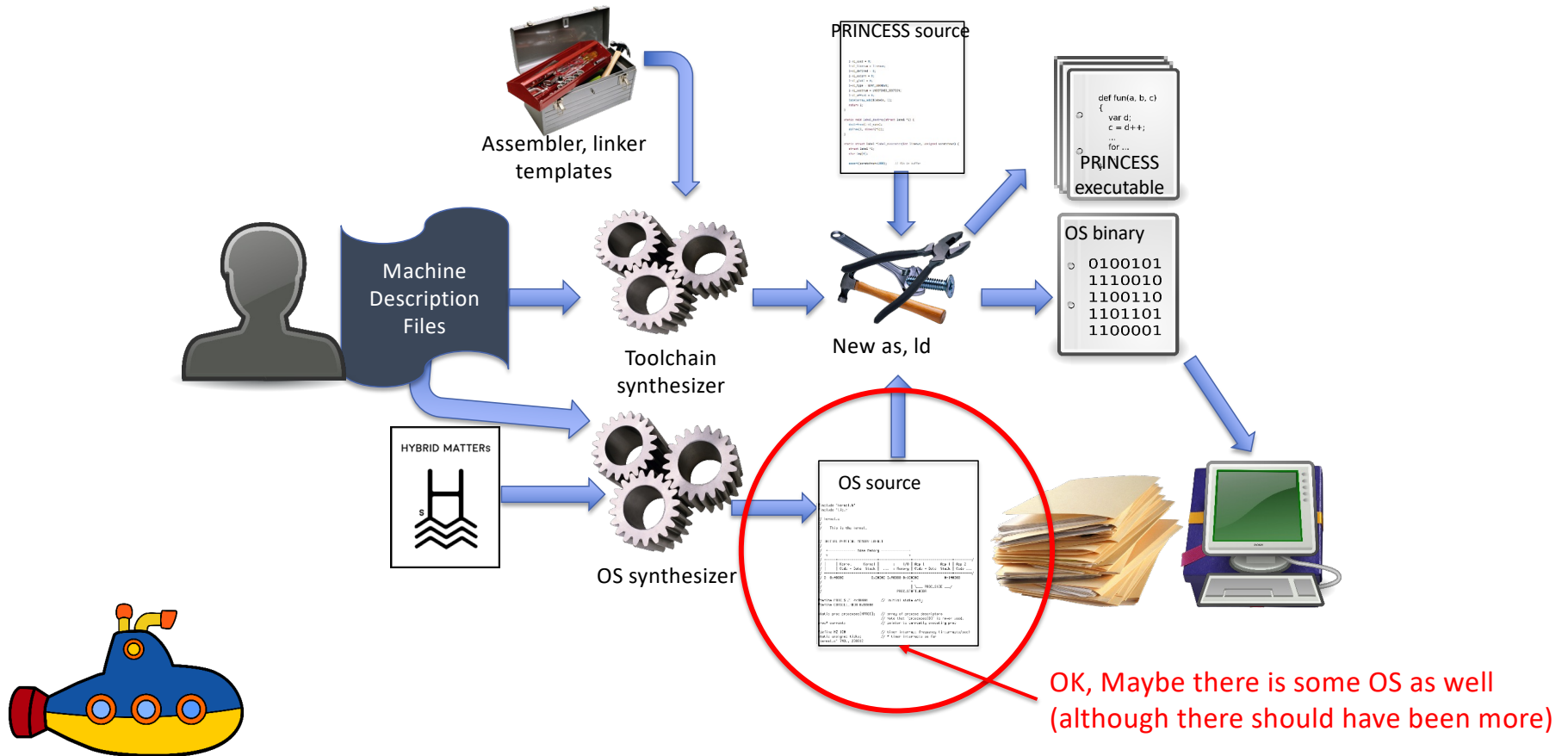
[BRASS FAQ](#)

[BRASS Proposers' Day Program Slides](#)

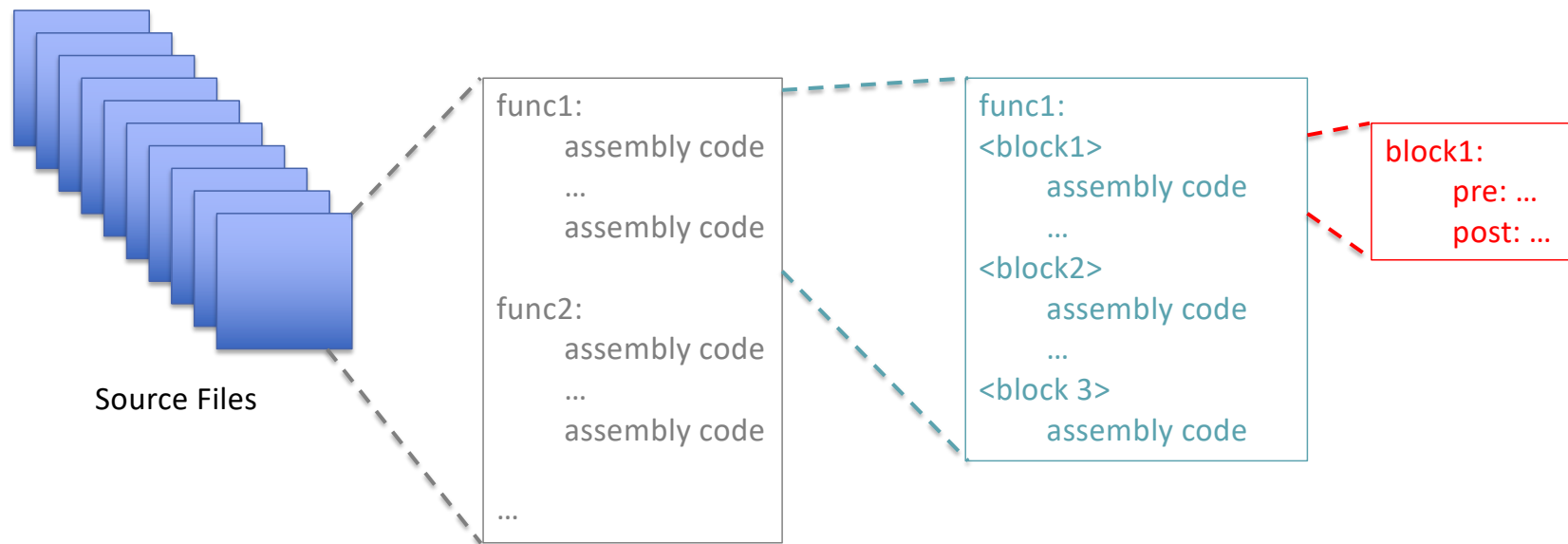
[BRASS Proposers' Day Program
Overview \(Video\)](#)



OK, Maybe it's not ALL PL ...



So, How do we Synthesize an OS?



What did we Manage to do?

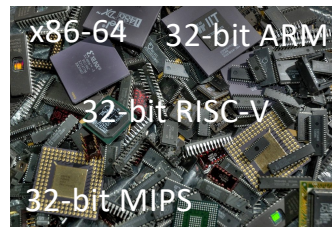
Two Operating Systems



OS/161



Four Processors



17 Use Cases

```

792415C0      55      push ebp
792415C1      89E5      mov ebp, esp
792415C3      8B45 08    mov eax, [ebp+0x08]
792415C6      DB28      fld tword [eax]
792415C8      8B4D 0C    mov ecx, [ebp+0x0C]
792415CB      DB29      fld tword [ecx]
792415CD      DEC1      faddp
792415CF      8B55 10    mov edx, [ebp+0x10]
792415D2      DB3A      fstp tword [edx]
792415D4      DB68 0A    fld tword [eax+0x0A]
792415D7      DB69 0A    fld tword [ecx+0x0A]
792415DA      DEC1      faddp
792415DC      DB7A 0A    fstp tword [edx+0x0A]
792415DF      5D        pop ebp
792415E0      C2 0C00   ret 0x000C
    
```

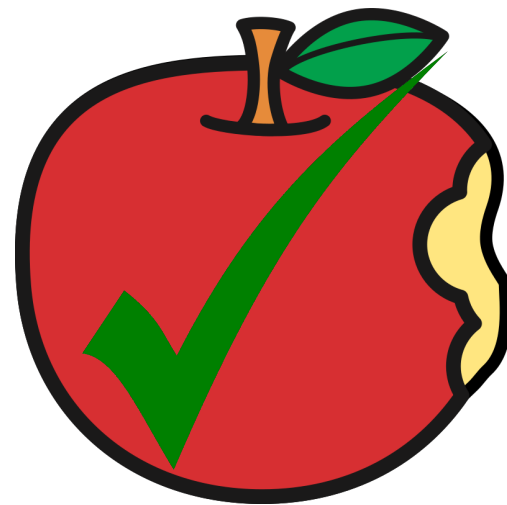
Use Case	Eagle (lines)	Verification Time (ms)				Synthesis Time (s)				Assembly (lines)			
		ARM	MIPS	RISC-V	x86-64	ARM	MIPS	RISC-V	x86-64	ARM	MIPS	RISC-V	x86-64
SJ	9	150	260	—	130	43	140	—	13	12	12	15	9
LJ	11	180	320	—	150	—	—	—	—	(14)	(13)	(16)	(12)
CRT-i	10	46	73	55	48	0.08	2.9	1.1	0.08	0	1	1	0
CRT-s	10	53	78	60	53	6.2	9.0	11	0.50	4	2	4	2
SYS	6	12	15	13	9	0.69	2.7	1.1	0.09	1	1	1	1
IRQ	4	12	19	—	9	0.47	33	—	0.09	1	3	1	1
TS	23	1300	2600	—	1900	—	—	—	—	(23)	(26)	(30)	(20)
TS-e	7	12	15	13	9	0.90	3.1	1.3	0.10	1	1	1	1
TS-s	8	48	74	55	50	0.62	2.9	1.1	0.15	1	1	1	1
TS-l	8	48	74	55	49	1.1	2.9	1.1	0.16	1	1	1	1
TS-c	7	12	14	13	9	0.87	3.1	1.1	0.10	1	1	1	1
IS	12	130	170	140	63	4.7	14	5.8	0.18	2	2	2	1
GD	14	260	340	270	150	19	52	23	0.84	3	3	4	2
CD	12	52	77	58	53	2.9	9.7	3.9	0.23	2	2	2	1
CL	16	51	76	59	55	190	210	440	0.24	3	3	4	1
CH	16	52	76	57	54	—	13	5.1	0.24	(4)	2	2	1
SA	13	14	16	38	11	46	120	140	12	3	3	3	4

Lessons Learned (1)

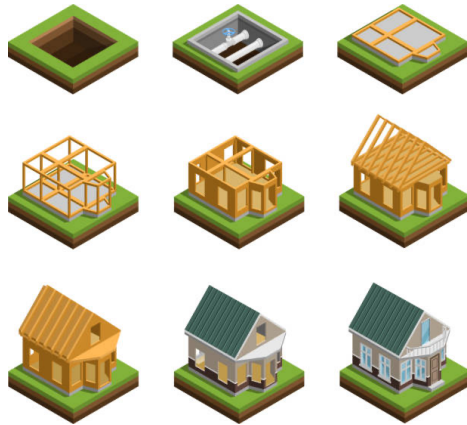
- Synthesis is a spectrum



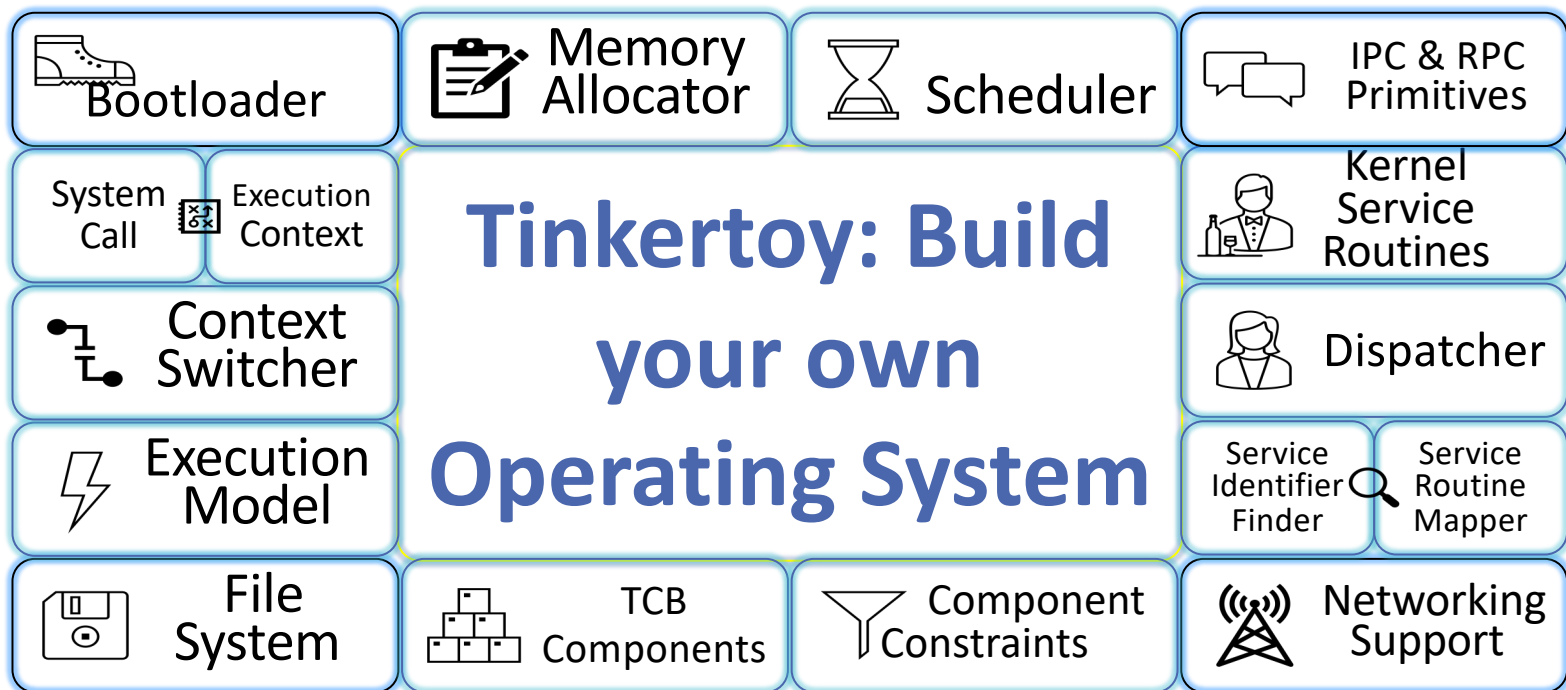
Lessons Learned (2)



Life After PRINCESS



Tinkertoy: An OS for Synthesis





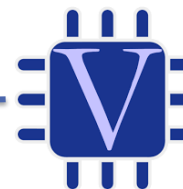
COMET



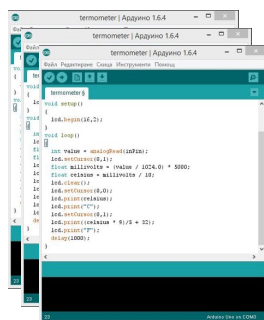
Specification



Language
description



Language
description



Arduino C Program



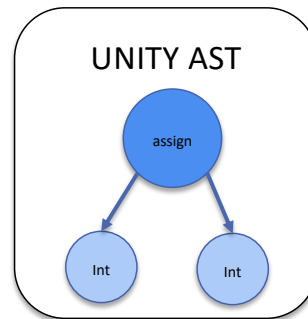
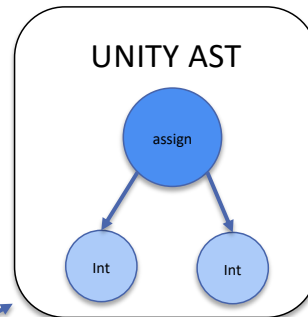
```
1 module MISR(dat_in,reset,clock,dat_out);
2   [module MISR(dat_in,reset,clock,dat_out);
3   1 input 3:0 dat_in;
4   1 module MISR(dat_in,reset,clock,dat_out);
5   2 input 3:0 dat_in;
6   3 input reset,clock;
7   4 output 3:0 dat_out;
8   5 reg 3:0 dat_out;
9   6 reg 3:0 misr_tempreg;
10  7
11  8 always@(posedge clock or posedge reset)
12  9 begin
13  10   if(reset == 1)
14  11     dat_out <- 4'b0000;
15  12   else
16  13     begin
17  14       misr_tempreg = dat_out;
18  15       dat_out[0] = misr_tempreg[3] ^ dat_in[0];
19  16       dat_out[1] = misr_tempreg[3] ^ misr_tempreg[0] ^ dat_in[1];
20  17       dat_out[2] = misr_tempreg[1] ^ dat_in[2];
21  18       dat_out[3] = misr_tempreg[2] ^ dat_in[3];
22  19     end
23  20 end
24 21 endmodule
```

Verilog Program

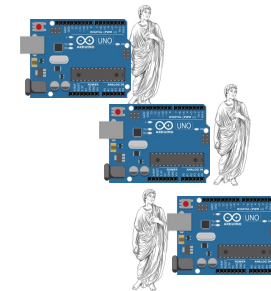
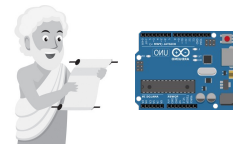
COMET: Reusing Synthesis

Specification

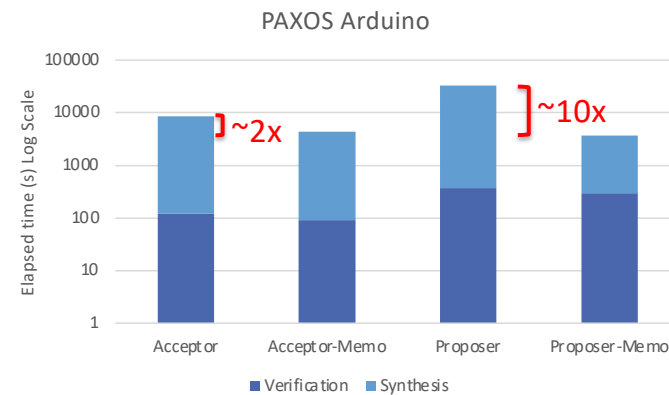
declare:
 in1, in2, out: integer
 cntrl: bool
 initially
 out = 0
 assign
 out = in1 if (cntrl)
 out = in2 if (not(cntrl))



Proposer

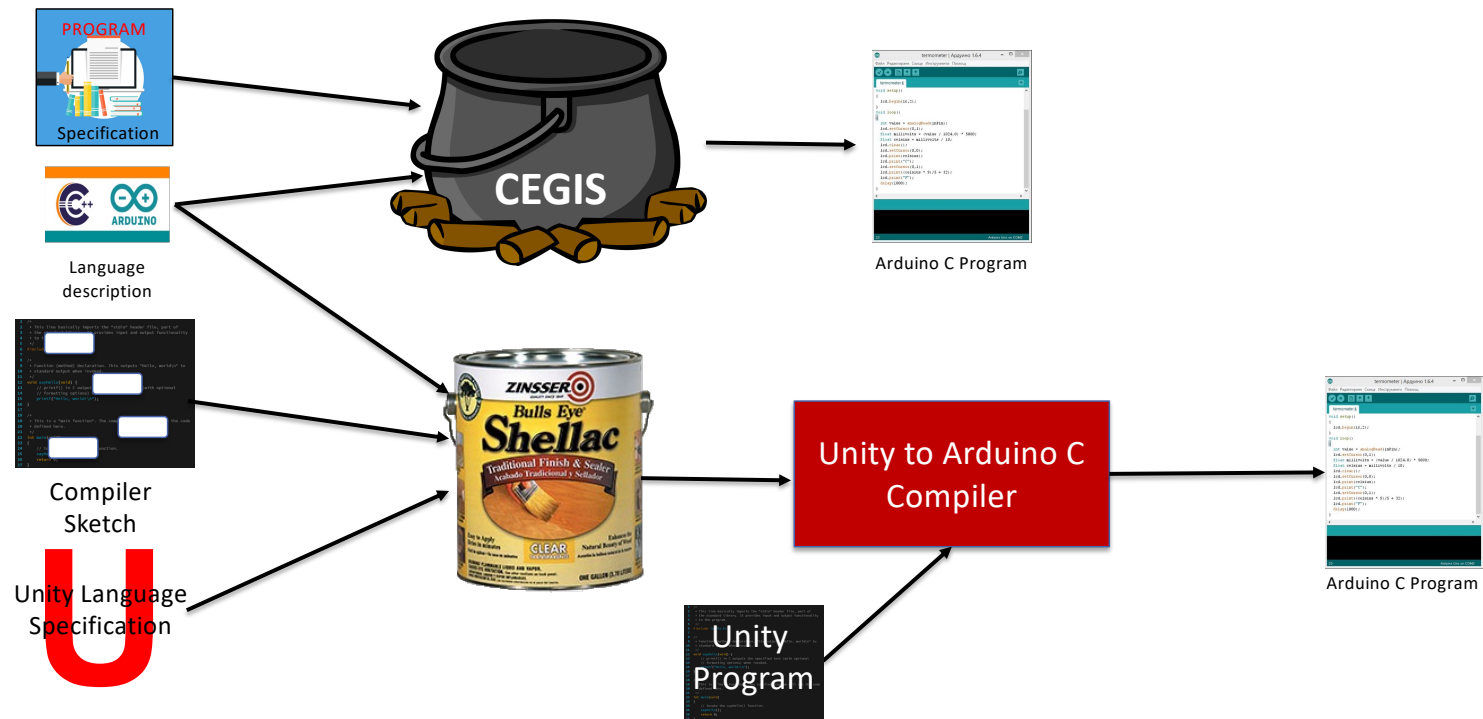


Acceptors



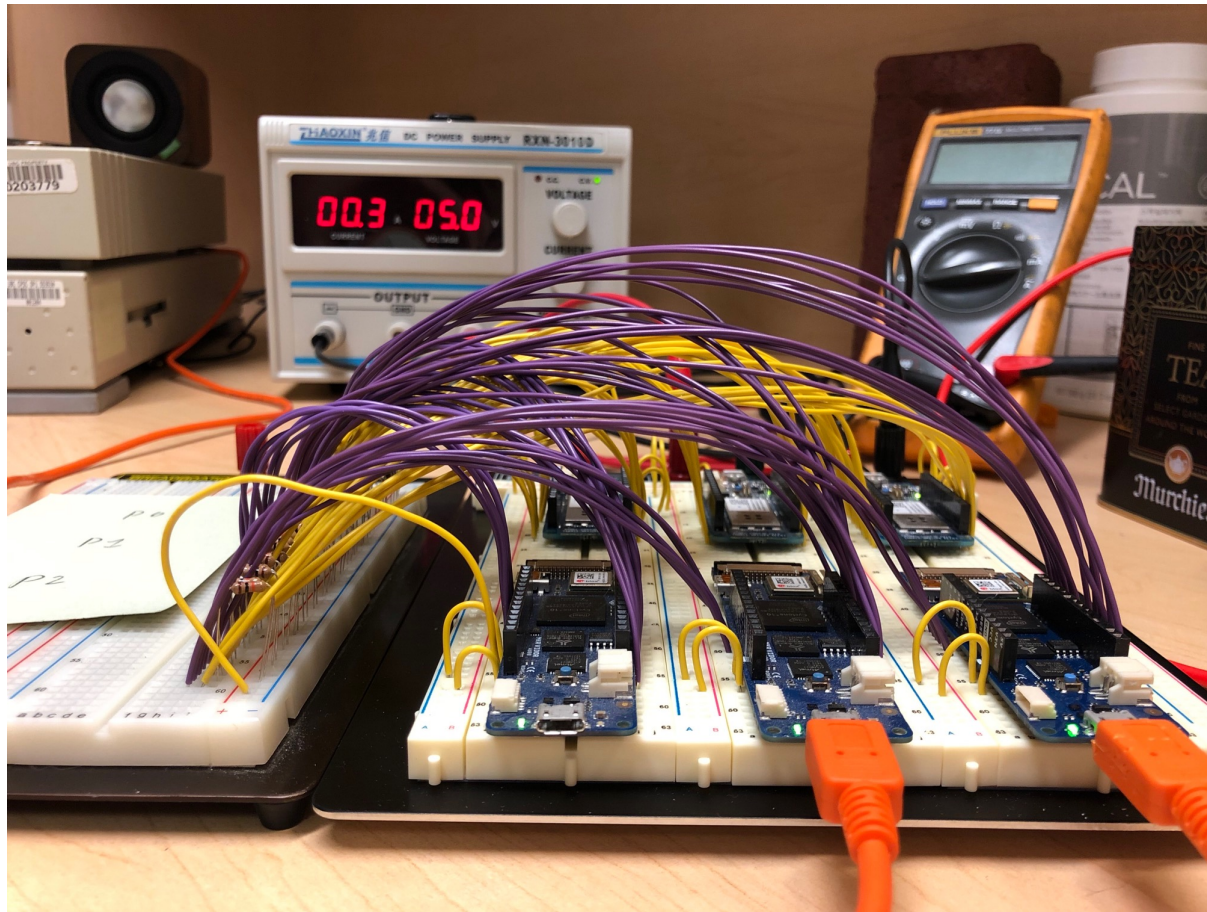


SHELLAC



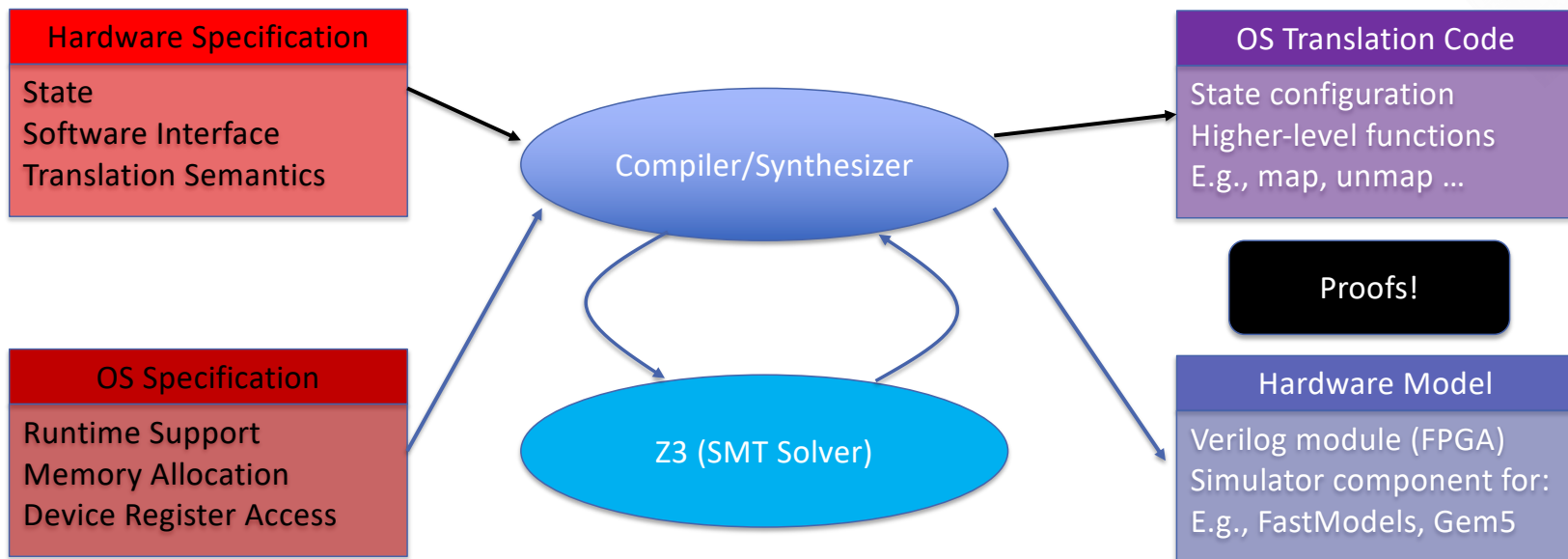
October 2022

Chen, C., Seltzer, M., Greenstreet, M., Shellac: Synthesis of a Multi-Pass Compiler (VSTTE 2022)



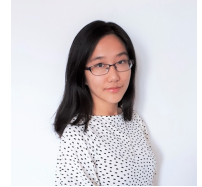


Velociraptor: Generating Hardware Translations





GhostWriter



Specification Vendor

Device Manufacturer

Protocol Designer

OS Vendor

Specification Types

Device Specification

Registers, Shared Memory, Interrupts

Device Class Specification

Protocol-level Interfaces

OS Specification

Kernel APIs and Programming Model

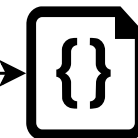
Goal Conditions

Synthesizer

Find the combination of available abstract micro-operations that satisfy the goal conditions

Code Generator

Generate the source code (C/C++/Rust) from the given combination of abstract micro-operations



C/C++/Rust Code



Fun things to do in Program Synthesis

1. If we synthesize software, do we have to pay a price in performance? [We think not.]
2. Synthesizing Evaluation Platforms, e.g., microservices
3. Synthesizing Security Exploits.
4. Synthesis as a way to verify existing code.
5. The Data Calculator is kind of a form of synthesis, where does that fall on my spectrum?
6. Many more: Come talk to me and let's brainstorm and start a collaboration!

Thank You!



NSERC
CRSNG

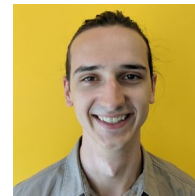
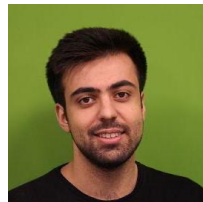
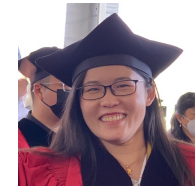
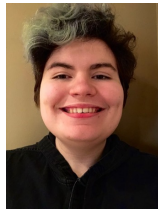
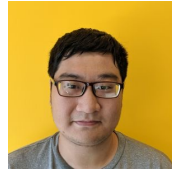
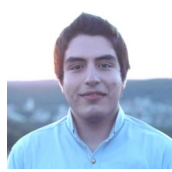


HUAWEI

ORACLE®
Labs

ARM

My Team



... and many, many undergraduates!