## Removing the Kitchen Sink from Software

Jason Landsborough Stephen Harding Sunny Fugate



#### Motivation

- Large feature-rich programs
- Kitchen sink



Used with permission from Rich Diesslin, <u>www.the-cartoonist.com</u>

## Why Thin

Pros:

 Security: Thinned programs do not contain the vulnerabilities present in code which was removed.

• Size: Thinned programs might be smaller and have performance gains over non-thinned code.

• Validity: Thinned programs are likely to be simpler and easier to validate, requiring fewer test cases.

• Optimality: Thinned programs can be better optimized for the specific machine, removing code for cross- compatibility.

Cons:

• Security: Thinned programs might not contain various security checks not normally raised in execution.

- Size: Thinned programs will fail or require additional time to load removed code segments.
- Validity: Thinned programs might require the same number of tests to validate that unwanted features are indeed removed.
- Optimality: Thinned programs may not run at all on other machines.

### What to Remove

Two basic classes:

- 1. Undesirable features
  - Ex: Heartbeat in OpenSSL
- 2. Unused features
  - Cold code



#### Manually Remove Features

- Identify feature
  - 1. Overwrite with NOPs

80484d7: c3 ret	080484c4 <fun3 80484c4: 80484c5: 80484c7: 80484c7: 80484ca: 80484d1: 80484d1: 80484d6: 80484d7:</fun3 	>: 55 89 e 83 e c7 0 e8 9 c9 c3	95 ∋c 18 94 24 9a fe	06 86 ff f1	6 04 G	push mov sub 08 movl call leave ret	%ebp %esp,%ebp \$0x18,%esp \$0x8048606,(%es 8048370 <puts@p< th=""></puts@p<>
-----------------	--	--	-------------------------------	----------------	--------	---	---

2. Redirect function call

00004a0:	ec18	c704	24e0	8504	68e8	c2fe	ffff	c9c3	\$	
00004b0:	5589	e583	ec18	c704	24f3	8504	08e8	aefe	U\$	
00004c0:	ffff	c9c3	5589	e583	ec18	c704	2406	8604	U	.\$
00004d0:	08e8	9afe	ffff	c9c3	5589	e583	ec18	c704	U	
									77,19	15%

 Issue: Very time consuming

00004a0:	ec18	c704	24e0	8504	08e8	c2fe	ffff	c9c3	\$
00004b0:	5589	e583	ec18	c704	24f3	8504	08e8	aefe	U\$
00004c0:	ffff	c9c3	9090	9690	9090	9090	9090	9090	
00004d0:	9090	9090	9090	90c3	5589	e583	ec18	c704	UU
00004e0:	2419	8604	08e8	86fe	ffff	c9c3	5589	e583	\$U

## Trace-based Thinning

- Dynamic trace of program execution
- diStorm Trace tool
  - DIFT by Jeff Knockel and Antonio Espinoza at University of New Mexico

## Prototype Overview

Trace and remove unused



- Only keeps used instructions
- May remove too much Riskier

## Prototype Overview

Trace and remove unused



- Only keeps used instructions
- May remove too much Riskier

Trace and remove unwanted



- Only removes unwanted instructions
- May not remove enough "Safer"

#### Unused

	1//////////////////////////////////////									1111	237	80484ce:	90							nop	
60	80484cf:	ff	do						call	*8003	238	80484cf:	90							nop	
	777777777777									11/1	239	80484d0:	90							nop	
61	80484d1:	c9							leave	1111	240	80484d1:	90							nop	
62	80484d2 :	69	79	11	11	ff			imp	80484	241	80484d2:	90							non	
1	7//////////////////////////////////////	77	77	17	17	77			11/1/1		242	8048443:	90							nop	
										11/1	243	8048444	90							nop	
										7777	244	POARAdE.	00							nop	
										////	244	0040403:	90							nop	
4		14	44	14	4	14			/////		295	8048405:	90	-						nop	-
13	8048407:	e9	74	II	II	II			Jmp	80484	246	8048407:	e9	74	II	II	II			Jub	804
54											247										
65	080484dc <funl>:</funl>										248	080484dc <fun1< td=""><td>1&gt;1</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></fun1<>	1>1								
66	80484dc:	55							push	%ebp	249	80484dc:	55							push	8e
67	80484dd:	89	e5						mov	Sesp,	250	80484dd:	89	e5						mov	%e
68	80484df:	83	ec	18					sub	\$0x18	251	80484df:	83	ec	18					sub	\$0
69	80484e2:	c7	04	24	50	86	04	08	movl	\$0x80	252	80484e2:	c7	04	24	50	86	04	08	movl	\$0
70	80484e9:	eß	b2	fe	ff	ff			call	80483	253	80484e9:	eß	b2	fe	ff	ff			call	80
71	8048400	0.9							leave		254	8048400:	69							leave	
22	80484of.								rot		255	80484of.	03							rot	
72	ourover:	63							Ter		255	onanaer:	63							Ter	
13	00040460 (60022)										200	00040460									
19	00040410 <iunz></iunz>								much	0.cha	237	00040410 1012								much	
75	8048410:	22							push	sepp	258	8048410:	22							push	se
76	8048411:	89	e5						mov	sesp,	259	8048411:	89	e5						mov	SC.
77	80484f3:	83	ec	18					sub	\$0x18	260	8048413:	83	ec	18					sub	\$0
78	80484f6:	c7	04	24	63	86	04	08	movl	\$0x8C	261	80484f6:	c7	04	24	63	86	04	08	movl	\$0
79	80484fd:	e8	9e	fe	ff	ff			call	80483	262	80484fd:	e8	9e	fe	ff	ff			call	80
80	8048502:	<b>c</b> 9							leave		263	8048502:	C9							leave	
81	8048503:	c3							ret		264	8048503:	c3							ret	
82											265										
83	08048504 <fun3></fun3>										266	08048504 <fun3< td=""><td>&gt;:</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></fun3<>	>:								
84	8048504	55							nuch	Sahn	267	8048504 -	90							0.00	
1	00103011								Publi	occp	268	8048505+	90							nop	
	17/////////////////////////////////////									////	260	8048506.	00							nop	
40	0040505	-	4						11/11		209	80485061	90							nop	
85	8048505:	83	65						mov	sesp,	270	8048507:	90							nop	
1	11/1/1/1/1/	44		14					11111	111	2/1	8048508:	90							nop	
86	8048507:	83	ec	18					sub	\$0x18	272	8048509:	90							nop	
87	804850a:	c7	04	24	76	86	04	08	movl	\$0x8C	273	804850a:	90							nop	
										11/1	274	804850b:	90							nop	
	2//////////////////////////////////////									/////	275	804850c:	90							nop	
	7//////////////////////////////////////									11/1	276	804850d:	90							nop	
	1//////////////////////////////////////									1111	277	804850e:	90							nop	
										11/1	278	804850f:	90							nop	
										7777	279	8048510:	90							nop	
00	9049511.	- 9		60	**				0011	90491	200	8048511.	00							nop	
.00	00403111	60	oa	10					Call	00402	200	00405111	90							nop	
	7//////////////////////////////////////									11/1	281	8048512:	90							nop	
12	1911111111111	44							11/1/	1111	282	8048513:	90							nop	
89	8048516:	C9							leave		283	8048514:	90							nop	
	0.0.00000000000									1111	284	8048515:	90							nop	
90	8048517:	c3							ret		285	8048516:	90							nop	
	7//////////////////////////////////////									1111	286	8048517:	90							nop	
91											287										
92	08048518 <funder< td=""><td>22</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>288</td><td>08048518 <fund< td=""><td>lef&gt;:</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></fund<></td></funder<>	22									288	08048518 <fund< td=""><td>lef&gt;:</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></fund<>	lef>:								
03	8048518-	55							nuch	Sahn	289	8048518-	55							nuch	80
0.4	8048510-	23							push	Sepp	203	8048510	90							Push	80
99	80485191	83	es						mov	sesp,	290	80485191	89	60	10					mov	50
95	804851D:	83	ec	18					sub	SUX18	291	804851b:	83	ec	18					sub	\$0
96	804851e:	c7	04	24	89	86	04	08	movl	\$0x8C	292	804851e:	c7	04	24	89	86	04	08	movl	\$0
97	8048525:	e8	76	fe	ff	ff			call	80483	293	8048525:	e8	76	fe	ff	ff			call	80
		-							3		204	004053	-0							10000	

#### Unwanted

154	80484be-	85	00						***	Seav	154	80484be-	85	00						1001	Seav
155	8048460.	24	15						ie	80484	155	8048400.	24	15						test	9049
155	8048463		10						Je	Sebe	166	90494021								Je	Sebo.
100	80484021	22							push	sepp	150	80484021	22							push	sepp
15/	8048403:	89	62						mov	sesp,	15/	8048403:	89	62						mov	sesp.
58	8048405:	83	ec	18	10	~			sub	SUXIE	158	8048405:	83	ec	18	10	~			sub	SUXIN
59	80484C8:	C7	04	24	<b>d</b> 8	97	04	08	movl	\$0x8C	159	80484c8:	C7	04	24	<b>d</b> 8	97	04	08	movi	\$0x80
60	80484cf:	11	_d0						call	*%ea>	160	80484c1:	11	d0						call	*%ea1
61	80484d1:	C9							leave		161	80484d1:	c9							leave	
62	80484d2:	e9	79	ff	11	11			jmp	80484	162	80484d2:	e9	79	11	ff	11			jmp	80484
63	80484d7:	e9	74	ff	ff	ff			jmp	80484	163	80484d7:	e9	74	ff	ff	ff			jmp	80484
164											164										
165	080484dc <fun1></fun1>										165	080484dc <fun1< td=""><td>&gt;:</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></fun1<>	>:								
66	80484dc:	55							push	8ebp	166	80484dc:	55							push	\$ebp
67	80484dd:	89	65						mov	Sesp.	167	80484dd:	89	65						mov	Sesp.
68	80484df -	83	00	18					sub	\$0x18	168	80484df -	83	00	18					sub	S0y1
69	8048402.	07	04	24	50	86	0.4	0.8	moul	50280	169	8048402.	07	04	24	50	86	0.4	0.8	moul	\$0v8
20	8048469	0.9	b2	10		**	04	00	0011	80485	170	8048409	0.9	b2	10		**	04	00	0211	8048
24	80484691	00	52	TG		11			leave	00401	1 1 7 0	80484691	00	52	Te					leave	0040.
11	BU484ee:	69							reave		1/1	BU4B4EEI	09							reave	
12	SUGSGET:	C3							ret		172	SUGSGETI	C3							ret	
73											173		10.0								
74	080484f0 <fun2></fun2>										174	08048410 <fun2< td=""><td>&gt;:</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></fun2<>	>:								
75	8048410:	55							push	sebp	175	8048410:	55							push	sepp
76	8048411:	89	e5						mov	sesp,	176	8048411:	89	e5						mov	sesp.
77	8048413:	83	ec	18					sub	\$0x18	177	8048413:	83	ec	18					sub	\$0x18
78	8048416:	c7	04	24	63	86	04	08	movl	\$0x8C	178	8048416:	c7	04	24	63	86	04	08	movl	\$0x80
79	80484fd:	e8	9e	fe	ff	ff			call	80483	179	80484fd:	e8	9e	fe	ff	ff			call	80481
80	8048502:	c9							leave		180	8048502:	c9							leave	
81	8048503:	c3							ret		181	8048503:	c3							ret	
82											182										
83	08048504 <fun3></fun3>										183	08048504 <fun3< td=""><td>3&gt;:</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></fun3<>	3>:								
84	8048504:	55							push	8ebp	184	8048504:	90							nop	
11	11111111111	77							1/1/77	175	185	8048505:	90							non	
	1777777777777									/////	186	8048506 :	90							non	
85	8048505+	89	-						mour	Reen	187	8048507:	90							nop	
1	0040303.	100	77						11/1/1	acab,	100	8048508	00							nop	
ac	0049507.	0.2		10					anh	0.0-16	100	9049509	00							nop	
00	0040507:	03	0.4	24	20	06	0.4	0.0	sub	60m90	100	0040509:	90							nop	
01	0040304:	C/	04	24	10	00	04	00	IIIOV A	SUXOU	101	0040504:	90							nop	
										11/1/	191	804850D:	90							nop	
	~//////////////////////////////////////									///A	192	804850C:	90							nop	
										7774	193	8048504:	90							nop	
										////	194	804850e:	90							nop	
										/////	195	804850f:	90							nop	
	7//////////////////////////////////////									11/1	196	8048510:	90							nop	
188	8048511:	e8	8a	fe	ff	ff			call	80483	197	8048511:	90							nop	
	11711111111									1////	198	8048512:	90							nop	
										9774	199	8048513:	90							nop	
189	8048516:	09							leave		200	8048514:	90							nop	
111	1//////////////////////////////////////	77							7/1/7/	7777	201	8048515:	90							non	
190	8048517+	03							PAT		202	8048516	90							nop	
20	0040317.								rec	1777	202	8048517	00							nop	
ni.										22220	203	00403171	90							nop	
191	analogia desid	6.									209	00040510 -6									
192	08048518 <funde< td=""><td>1221</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>205</td><td>08048518 <rund< td=""><td>lei&gt;:</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></rund<></td></funde<>	1221									205	08048518 <rund< td=""><td>lei&gt;:</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></rund<>	lei>:								
193	8048518:	55							push	sebp	206	8048518:	55							push	sebp
194	8048519:	89	e5						mov	sesp,	207	8048519:	89	e5						mov	sesp.
195	804851b:	83	ec	18					sub	\$0x18	208	804851b:	83	ec	18					sub	\$0x18
196	804851e:	c7	04	24	89	86	04	08	movl	\$0x8C	209	804851e:	c7	04	24	89	86	04	08	movl	\$0x80
220			-			40			0011	80485	210	9049535.	- 9	26	10		**			0011	80481
197	8048525:	e8	76	fe	11	II			CHII	00402	210	00403231	00	10	16					Call	0040.

## GA-based Thinning

- Genetic Algorithm feature removal
- Software Evolution
  - Developed by Eric Schulte from University of New Mexico



#### Genetic Algorithm Overview



## Binary Mutation

#### **Mutation Operations:**



#### Two Point Crossover



Source: modified from Post-compiler software optimization for reducing energy by Schulte, Dorn, Harding, Forrest, and Weimer

## Fitness Script

- Script with test cases run by GA
- Basic overview:
- 1. Variant passed in as script argument
- 2. Generate many test cases for feature(s) to keep
- 3. Run each test case on original and variant binaries
- 4. If output differs, exit with bad fitness, otherwise continue until test cases finish
- 5. Calculate fitness value

### Fitness Calculation

Program size - number of nops, adjusted with largest return value

- PROG\_SIZE = length(program\_variant)
- PROG\_NOPS = count\_nops(program\_variant)
- FN = PROG\_SIZE PROG\_NOPS
- FITNESS = FN + RETVAL \* 5

## Fitness Script For echo

- Choose 0-5 options from: {-e, -E}
- Choose 0-1000 random characters for string
- Remove special characters
- Test variant and compare with original
  - Same -> continue
  - Diff -> fail, print bad fitness and terminate
- Repeat 1000 times
- Calculate fitness and terminate

### Results For echo

Goal: remove -n feature

- Before: [jason]\$ echo -n "test" test[jason]\$
  - Non-NOP instructions: 2,609
- After: [jason]\$ ./thinned\_300000 -n "test" test [jason]\$
  - Non-NOP instructions: 2,173
  - 436 fewer instructions ~17%

#### Fitness Script For sha1sum

#### Test case 1:

- Choose random number of random characters for string
- Test string hash of variant and compare with original
  - Same -> continue
  - Diff -> fail, print bad fitness and terminate
- Repeat 50 times

#### Test case 2:

- Make random file filled with random number of random bytes
- Test file hash of variant and compare with original
  - Same -> continue
  - Diff -> fail, print bad fitness and terminate
- Repeat 50 times
- Calculate fitness and terminate

### Results For sha1sum

Goal: Remove unused features — keep string/file hashing

- Before: [jason]\$ sha1sum test\_file eba19174a7bf59dfe65a805563d3cb27d9ed673d test\_file
  - Non-NOP instructions: 5,049
- After: [jason]\$ ./thinned\_300000 test\_file eba19174a7bf59dfe65a805563d3cb27d9ed673d test\_file
  - Non-NOP instructions: 4,764
  - 285 fewer instructions  $\sim 6\%$

## Minimized Changes

- Terminate as soon as feature is removed
  - fitness script gives perfect fitness (zero)
  - -n removed from echo 706 fitness evaluations

- Delta debugging
  - Undo changes that do not contribute to fitness

## Delta Debugging

- Feature removed: Fitness == 0
- Echo result: 1 instruction

[Jas 2c2 < eo	son]\$ diff cho: fi	echo.s le form	thinnedDDB.s at elf64-x86	-64	
5 61	inthinned D		file format	a1f64_v86_64	
CEO.		00.	TILE TUTILAL	el104-X00-04	
6500	2650,653				
<	401700:	40 80	fe 6e	cmp	\$0x6e,%sil
>	401700:	90		nop	
>	401701:	90		nop	
>	401702:	90		nop	
>	401703:	90		nop	
[Jas	son]\$				

#### Current Issues and Limitations

- Machine-dependent
- No GUI programs
- Large programs
- Remove error handling
  - Unintentional program failure

#### Future Work

#### I hope you are excited about the future - and ready to transform!



"Future of Technology and Impact on HR and Management" by Gerd Leonhard is licensed under CC BY-SA 2.0

#### Larger Open Source Software

- Try thinning approaches on [slightly] larger open source software
- Will need to develop better ways of randomly generating test cases for much larger programs
  - Currently requires knowledge of program usage and arguments (manpage learnin')

### GA-Based Diversification

- Why diversification?
  - Change program structure
  - Code-reuse exploits rely on specific program
     structure

#### GA-Based Diversification





#### GA-Based Diversification



#### Semantic Preserving Binary Transformations

- Learn transformations based on GA results
  - Transformations to minimize instructions
  - Transformations to increase diversity

#### GA-Assisted Malware Reversing

• Use GA to mutate malware



Change in Machine-State

#### Other Ideas

- Use tracing to influence GA
- Performance
- Failing gracefully

#### Questions?



### Backup slides

#### Manual Binary Modification

Showing removal of function from simple program

#### void fun1()

printf("This is function 1\n");

#### }

void fun2()

printf("This is function 2\n"); }

#### void fun3()

3

#### printf("This is function 3\n");

void fundef()

printf("Unsupported function\n");

#### }

int main()

int option; printf("Enter option: "); scanf("%d", &option); switch(option)

case 1:

fun1(); break;

case 2:

fun2(); break;

case 3:

fun3(); break;

#### default:

fundef();

#### break;

return 0;

}

		chsim1: ~	_ 0 X	ľ			sjf@so	:hsim1:	~		_ = ×
File Edit View	Search Terminal	Help		File E	dit Vie	v Search	Terminal	Help			
080484c4 <fun3 80484c4: 80484c5: 80484c7: 80484ca: 80484d1: 80484d1:</fun3 	<ul> <li>55</li> <li>89 e5</li> <li>83 ec 18</li> <li>c7 04 24 06 8</li> <li>e8 9a fe ff f</li> <li>c9</li> </ul>	push mov sub 6 04 08 movl f call leave	%ebp %esp,%ebp \$0x18,%esp \$0x8048606,(%esp) 8048370 <puts@plt></puts@plt>	000032 000033 000034 000035 000036 000037 000038	0: 070 0: 5b8 0: 05e 0: ff3 0: ff2 0: ff2 0: ff2	0000 5 c32c 1 3a00 0 6098 0 6898 0 6c98 0 6c98 0 7098 0	589 e553 500 008b 000 585b 408 ff25 408 6800 408 6808 408 6810	83ec ( 93fc 1 c9c3 ( 6498 ( 0000 ( 0000 (	04e8 0000 ffff ff85 0000 0000 0408 0000 00e9 e0ff 00e9 d0ff 00e9 c0ff	0000 d274 0000 0000 ffff ffff	USt [t :X[ .5`%d .%hh .%lh .%ph
80484d7: 080484d8 <fund< td=""><td>c3 lef&gt;;</td><td>ret</td><td>Sebo</td><td>000039 00003a 00003b</td><td>0: ff2 0: ff2 0: 31e</td><td>5 7498 0 5 7898 0 1 5e89 e</td><td>408 6818 408 6820 183 e4f0 851 5668</td><td>0000 ( 0000 ( 5054 5</td><td>00e9 b0ff 00e9 a0ff 5268 5085</td><td>ffff ffff 0408</td><td>.%th .%xh 1.^PTRhP</td></fund<>	c3 lef>;	ret	Sebo	000039 00003a 00003b	0: ff2 0: ff2 0: 31e	5 7498 0 5 7898 0 1 5e89 e	408 6818 408 6820 183 e4f0 851 5668	0000 ( 0000 ( 5054 5	00e9 b0ff 00e9 a0ff 5268 5085	ffff ffff 0408	.%th .%xh 1.^PTRhP
80484d9: 80484db: 80484de: 80484e5: 80484e5:	89 e5 83 ec 18 c7 04 24 19 8 e8 86 fe ff f	f call	%esp,%ebp \$0x18,%esp \$0x8048619,(%esp) 8048370 <puts@plt></puts@plt>	00003d 00003e 00003f 000040	0: 688 0: 688 0: 688 0: c36 0: c70	9090 9 9804 0 9000 0 9000 0	090 9090 82d 8498 000 85c0 804 08ff	9090 9 0408 8 74f5 5 d0c9 0	9090 9090 83f8 0677 5589 e583 c390 8d74	9090 02f3 ec18 2600	
80484eb: 080484ec <main< td=""><td>c3</td><td>ret</td><td>Richa</td><td>000042</td><td>0: eal 0: d27 0: 8490</td><td>f 01d0 d f f555 8 8 0408 f</td><td>1f8 7502 9e5 83ec fd2 c9c3</td><td>f3c3 b 1889 4 908d b</td><td>ba00 0000 4424 04c7 b426 0000</td><td>0085 0424 0000</td><td>u</td></main<>	c3	ret	Richa	000042	0: eal 0: d27 0: 8490	f 01d0 d f f555 8 8 0408 f	1f8 7502 9e5 83ec fd2 c9c3	f3c3 b 1889 4 908d b	ba00 0000 4424 04c7 b426 0000	0085 0424 0000	u
80484ed: 80484ed: 80484ef: 80484f2:	55 89 e5 83 e4 f0 83 ec 20	pusn mov and sub	%eop %esp,%ebp \$0xffffff0,%esp \$0x20,%esp	000046	0: 7cf 0: a16 0: 741	6498 0 ffff c 9704 0 5589 e	408 0075 605 8498 885 c074 583 ec18	1355 0 0408 ( 1eb8 ( c704 2	9965 8360 0109 f303 0000 0000 2464 9704	6690 85c0 08ff	lf. .dtf. t.U\$d
80484fc: 8048501: 8048505: 8048509:	e8 5f fe ff f 8d 44 24 1c 89 44 24 04 c7 04 24 3d 8	f call f call lea mov 6 04 08 movl	\$0x804862e,(%esp) 8048360 <printf@plt> 0xlc(%esp),%eax %eax,0x4(%esp) \$0x804863d,(%esp)</printf@plt>	00004a 00004b 00004c 00004d	0: 000 0: 558 0: 558 0: fff 0: 08e	6979 1 3 c704 2 9 e583 e 6 c9c3 5 3 9afe f	4e0 8504 c18 c704 589 e583 fff c9c3	08e8 ( 24f3 8 ec18 ( 5589 (	c2fe ffff 8504 08e8 c704 2406 e583 ec18	e503 c9c3 aefe 8604 c704	U\$ U\$ U\$ U

	im1: ~/Develop	ment/SCHSIM/M	13-BinaryTransfo	orms/experiment _ 🗆	×				,	sjf@sc	hsim1:	~				- 0	×
File Edit	View Search	Terminal Hel	р		File	Edit	View	Searc	ch Te	erminal	Help						
File Edit 80484b6: 80484b2: 80484c2: 80484c3: 80484c4: 80484c4: 80484c5: 80484c6: 80484c6: 80484c8: 80484c8: 80484c8: 80484c2: 80484	View Search c7 04 e8 ac c9 c3 <fun3>: 90 90 90 90 90 90 90 90 90 90</fun3>	Terminal Hel 4 24 f3 85 04 e fe ff ff	p 08 movl call leave ret nop nop nop nop nop nop nop nop nop nop	\$0x80485f3,(%esp) 8048370 <puts@plt></puts@plt>	File 0000 0000 0000 0000 0000 0000 0000 0	Edit 330: 340: 350: 350: 370: 380: 390: 390: 390: 300: 300: 3400: 3400: 3400: 4400: 4400: 4400: 4400: 4400: 4400: 4400:	View 5b81 05e8 ff35 ff25 ff25 ff25 ff25 ff25 d6860 fff4 b887 c3b8 c704 b884 ealf d274 8498 803d 7cff a164	Seard c32c 3a00 6098 6898 6c98 7098 7498 7898 5e89 8504 9090 9804 0000 2484 9804 0000 2484 9804 01d0 f555 0408 8498 ffff 9704	ch T 1500 0000 0408	erminal 008b 585b ff25 6800 6808 6810 6818 6820 e4f0 5668 9090 8498 85c0 08ff 8498 7502 83ec c9c3 0075 8498 c074	Help 93fc c9c3 6498 0000 0000 0000 0000 5054 ec84 9090 0408 74f5 d0c9 0408 f3c3 1889 908d 1355 0408 1255	ffff 0000 0408 00e9 00e9 00e9 00e9 5268 0408 9690 83f8 5589 c390 c1f8 ba00 4424 b426 89e5 01c9 0000	ff85 0000 e0ff d0ff c0ff b0ff 5085 e8bf 9090 0677 e583 8d74 0289 0000 83ec f3c3 0000	d274 0000 ffff ffff ffff ffff 0408 ffff 9090 02f3 ec18 2600 c2c1 0085 0424 0000 08e8 6690 85c0	[X[. .5`X[. .%hh. .%lh. .%ph. .%th. .%xh 1.^P h`QVh. t. t. t. t. t. t. t.	TRhP.	.t
80484d3: 80484d4: 80484d5: 80484d6: 80484d6: 80484d7:	90 90 90 c3		nop nop nop ret			480: 490: 4a0: 4b0: 4c0:	7415 d0c9 ec18 5589 ffff	5589 e979 c704 e583 c9c3	e583 ffff 24e0 ec18 9090	ec18 ffe9 8504 c704 9690 98c2	c704 74ff 08e8 24f3 9090	2464 ffff c2fe 8504 9090	9704 5589 ffff 08e8 9090	08ff e583 c9c3 aefe 9090	t.Ut \$ U\$	.\$d	
080484d8 80484d8:	<fundef>: 55</fundef>		push	%ebp	0000	4e0:	2419	8604	08e8	86fe	ffff	c9c3	5589	e583	\$	U 15	 5%

## GA-Thinning

#### Echo thinned

/Users/I	andsbor/Deskt	op/GECCO slide materials/o	rig_echo_dis						/Users/landsbor/Deskto	p/GECCO slide materials/echo_300k_di
591 592 593 594 595 596	401937: 40193e: 401943: 401946: 401948: 401948:	48 8d 3d 4c 2a 00 00 b9 07 00 00 00 48 89 c6 £3 a6 74 6a 48 8d 3d 40 2a 00 00	<pre>lea 0x2a4c(%rip),%rdi mov 50x7,%ecx mov %rax,%rsi repz cmpsb %es:(%rdi),%ds:(%r je 4019b4 <iswprint@plt+0: lea 0x2a40(%rip),%rdi</iswprint@plt+0: </pre>	# 40438a <close_stdout+0x211a> #i) #9cc&gt; # 404391 <close_stdout+0x2121></close_stdout+0x2121></close_stdout+0x211a>	938 939 940 941 942 943	401937: 40193e: 401943: 401946: 401948: 401948:	48 8d 3d 4c 2a 00 00 b9 07 00 00 00 48 89 c6 f3 a6 74 6a 90	lea nov nov repz je nop	0x2a4c(%rip),%rdi # 4 \$0x7,%ecx %rax,%rsi cmpsb %es:(%rdi),%ds:(%rsi) 4019b4 <iswprint@plt+0x9cc></iswprint@plt+0x9cc>	0438a <close_stdout+0x211a></close_stdout+0x211a>
					944 945 946 947 948 949	40194b: 40194c: 40194c: 40194e: 40194f: 40194f:	90 90 90 90 90	nop nop nop nop		
597 598 599 600 601	401951: 401956: 401959: 401959: 401956:	b9 0a 00 00 00 48 89 c6 bb 01 00 00 00 f3 a6 0f 97 c1	<pre>mov \$0xa,%ecx mov %rax,%rai mov \$0x1,%ebx repz cmpab %es:(%rdi),%ds:(%ra seta %cl</pre>	si)	950 951 952 953 954	401951: 401956: 401959: 401959: 401950:	b9 0a 00 00 00 48 89 c6 bb 01 00 00 00 f3 a6 90	nov nov repa nop	<pre>\$0xa,%ecx %rax,%rsi \$0x1,%ebx cmpsb %es:(%rdi),%ds:(%rsi)</pre>	
602	401963-	05 92 02	sath MI		956	401962:	90 90 05 92 c2	nop	241	
603	401966:	38 d1	emp %dl,%el		958	4019661	90	nop	101	
604	401968:	0f 85 56 fc ff ff	jne 4015c4 <iswprint#plt+0;< td=""><td>c5de&gt;</td><td>960</td><td>401968:</td><td>0f 85 56 fc ff ff</td><td>jne</td><td>4015c4 <iswprint@plt+0x5dc></iswprint@plt+0x5dc></td><td></td></iswprint#plt+0;<>	c5de>	960	401968:	0f 85 56 fc ff ff	jne	4015c4 <iswprint@plt+0x5dc></iswprint@plt+0x5dc>	
605	401950:	48 85 05 05 35 20 00	mov 0x203b0b(%rip),%rax	# 605680 «version_etc_copyright+0x200	961 962 963 964 965 966	401966: 401965: 401970: 401971: 401972: 401973:	90 90 90 90 90	nop nop nop nop nop		
606	401975:	48 c7 04 24 00 00 00	movg \$0x0,(%rsp)		967 968	401974: 401975:	90	nop		
					969 970 971 972 973	401976: 401977: 401978: 401979: 401978:	90 90 90 90	nop nop nop		
607 608	40197c: 40197d:	00 4c 8d 0d 17 2a 00 00	les 0x2al7(%rip),%r9	# 40439b <close_stdout+0x212b></close_stdout+0x212b>	974 975	40197b: 40197c:	90 00 4c 8d 0d	nop add	%cl,0xd(%rbp,%rcx,4)	
609	401984:	4c 8d 05 1b 2a 00 00	lea 0x2alb(%rip),%r8	# 4043a6 <close_stdout+0x2136></close_stdout+0x2136>	976 977 978 979	401980: 401981: 401983: 401987:	2a 00 00 4c 8d 05 1b 2a	add sbb	(%rax),%al %cl,0x5(%rbp,%rcx,4) (%rdx),%ebp	
610 611 612 613 614 615	40198bs 401992: 401999: 401990: 401990: 401983: 401986:	48 8d 15 c1 29 00 00 48 8d 35 88 29 00 00 48 8b 08 48 8b 05 e5 3a 20 00 48 8b 38 31 c0	<pre>lea 0x29cl(%rip),%rdx lea 0x2988(%rip),%rsi mov (%rax),%rcx mov 0x203ae5(%rip),%rax mov (%rax),%rdi xor %eax,%eax</pre>	<pre># 404353 <close_stdout+0x20e3> # 404321 <close_stdout+0x20b1> # 605488 <version_etc_copyright+0x200< pre=""></version_etc_copyright+0x200<></close_stdout+0x20b1></close_stdout+0x20e3></pre>	980 981 982 983 984 985 985	401989: 40198b: 401992: 401999: 401990: 401983: 401986:	00 00 48 8d 15 c1 29 00 00 48 8d 35 88 29 00 00 48 8b 08 48 8b 05 e5 3a 20 00 48 8b 38 31 c0	add lea mov mov mov	<pre>%al,(%rax) 0x2901(%rip),%rdx # 4 0x2988(%rip),%rsi # 44 (%rax),%rcx 0x203ae5(%rip),%rax # (%rax),%rdi %eax,%eax</pre>	04353 <close_stdout+0x20e3> 04321 <close_stdout+0x20b1> 605488 <version_etc_copyright+0x20< td=""></version_etc_copyright+0x20<></close_stdout+0x20b1></close_stdout+0x20e3>
616	4019a81	e8 63 07 00 00	callq 402110 <iswprint@plt+0< td=""><td>(1128&gt;</td><td>987 988 989 990</td><td>4019a8: 4019a9: 4019aa: 4019ab:</td><td>90 90 90 90</td><td>nop nop nop</td><td></td><td></td></iswprint@plt+0<>	(1128>	987 988 989 990	4019a8: 4019a9: 4019aa: 4019ab:	90 90 90 90	nop nop nop		
617 618 619	4019ad: 4019af: 4019b4:	31 ff e8 84 f4 ff ff 31 ff	<pre>xor %edi,%edi callq 400e38 <exit@plt> xor %edi,%edi</exit@plt></pre>		992 993 994	4019ad: 4019af: 4019b4:	31 ff e8 84 f4 ff ff 90	xor callq	%edi,%edi 400e38 <exit€plt></exit€plt>	
620 621 622 623 624 625 626 627 628	4019b6: 4019bb: 4019c1: 4019c6: 4019c9: 4019c9: 4019d3: 4019d8: 4019d8:	e8 b5 f7 ff ff 41 bc 01 00 00 00 e9 07 fb ff ff 44 89 fe 48 89 54 24 10 e8 a5 f5 ff ff 48 8b 54 24 10 e9 7a fc ff ff be 20 00 00 00	<pre>calig 401170 <iswprint&plt+0; mov 50x1,%r12d jmpq 4014cd <iswprint&plt+0; mov %r15d,%esi mov %rdx,0x10(%rsp) calig 400f78 <overflow&plt; mov 0x10(%rsp),%rdx jmpq 401657 <iswprint&plt+0; mov 50x20,%esi</iswprint&plt+0; </overflow&plt; </iswprint&plt+0; </iswprint&plt+0; </pre>	<188> <4e5> <66f>	995 996 997 998 999 1000 1001 1002 1003 1004	4019b51 4019b6: 4019c1: 4019c1: 4019c6: 4019c9: 4019c9: 4019c8: 4019d8: 4019d8:	90 e8 b5 f7 ff ff 41 bc 01 00 00 00 e9 07 fb ff ff 44 89 fe 48 89 54 24 10 e8 a5 f5 ff ff 48 8b 54 24 10 e9 7a fc ff ff 90	nop callq mov jmpq mov callq mov jmpq nop	401170 <iswprint@plt+0x188> 50x1,%r12d 4014cd <iswprint@plt+0x4e5> %r15d,%esi %rdx,0x10(%rsp) 400f78 <overflow@plt> 0x10(%rsp),%rdx 401657 <iswprint@plt+0x66f></iswprint@plt+0x66f></overflow@plt></iswprint@plt+0x4e5></iswprint@plt+0x188>	
					1005 1006 1007 1008	4019de: 4019df: 4019e0: 4019e1:	90 90 90	nop nop nop		
629 630	4019e2: 4019e7:	48 89 54 24 10 e8 8c f5 ff ff	mov %rdx,0x10(%rsp) callq 400f78 <_overflow@plt3		1009 1010 1011	4019e2: 4019e7: 4019e8:	48 89 54 24 10 90 90	nop	%rdx,0x10(%rsp)	
111					1012 1013	4019e9: 4019ea:	90 90	nop		

П

#### Sha1sum thinned

///	sers/la	andsbor/Deskt	top/GECCO slide materials/or	rig_sha1a	sum_dis					/Users/landsbor/Desktop/GECCO slide materials/sha1sum_300k_d
2	699	403e851	44 0f b6 a4 24 c6 00	novzbl	0xc6(%rsp),%r12d	4025	403e841	00 44 0f b6	add	%al,-0x4a(%rdi,%rcx,1)
. 12	263					4026	403e881	a4	movsb	%ds:(%rsi),%es:(%rdi)
- 14	700	403e8c1	00 00			4028	403e8b;	29 CB 00 41 ba	and	\$010x46(\$rcx)
112	11/1	11111111				4029	403e8e:	01 00	add	teax, (trax)
	11.					4030	403e90:	00 00	add	%al,(%rax)
2	701	4036861	4c 8b bc 24 b0 00 00	nov	0xb0(%rsp),%r15	4031	403e92:	4c 8b bc 24 b0 00 00	mov	0xb0(%rsp),%r15
2	703	403e961	44 Of b6 ac 24 c7 00	novzbl	0xc7(%rsp),%r13d	4033	403e9a1	44 Of b6 ac 24 c7 00	movzb)	1 0xc7(%rsp),%r13d
2	704	403e9d:	00 00			4034	403ea1:	00 00		
2	705	403e9f:	76 b2	jbe	403e53 <close_stdout+0xf53></close_stdout+0xf53>	4035	403ea3:	76 b2	jbe	403e57 <close_stdout+0xf57></close_stdout+0xf57>
2	707	403ea4:	74 ad	1e	403e53 <close stdout+0xf53=""></close>	4036	403ea8:	74 ad	1e	403e57 <close stdout+0xf57=""></close>
2	708	403ea6:	48 8b 54 24 58	nov	0x58(%rsp),%rdx	4038	403eaa:	48 8b 54 24 58	nov	0x58(%rsp),%rdx
2	709	403eab:	48 8d 44 15 01	lea	0x1(%rbp,%rdx,1),%rax	4039	403eaf :	48 8d 44 15 01	lea	Ox1(%rbp,%rdx,1),%rax
2	711	403eb21	66 0f 1f 44 00 00	nopy	0x0(krax,krax,1)	4040	403eb61	66 Of 1f 44 00 00	nopw	0300 (Star, Star, 1)
2	712	403eb8:	41 Of b6 Oc 06	movzbl	(%r14,%rax,1),%ecx	4042	403ebc:	41 Of b6 Oc 06	movzb)	1 (%r14,%rax,1),%ecx
2	713	403ebd:	48 83 c0 01	add	SOx1, %rax	4043	403ec1:	48 83 c0 01	add	\$0x1,%rax
	714	403ec1:	86 C7 74 09	test	ADJama sciosa stdout+Oxfor	4044	403ec5:	74 09	test	403ed2 colose stdout+0xfd2>
2	716	403ec5:	48 83 c2 01	add	\$0x1, %rdx	1111	1//////////////////////////////////////		11111	
2	717	403ec91	4c 39 d8	cnp	srll, srax	4046	403ec91	4c 39 d8	cnp	\$r11, \$rax
2	718	4036001	48 89 54 24 58	30	<pre>%viets <close_stdout+vxite> %rdx.0x58(%rep)</close_stdout+vxite></pre>	4047	4036001	48 89 54 24 58	xchg	andx, 0x58(Arep)
2	720	403ed3:	e9 7b ff ff ff	japq	403e53 <close_stdout=0xf53></close_stdout=0xf53>	4049	403ed3:	e9 7b ff ff ff	japq	403e53 <close_stdout+0xf53></close_stdout+0xf53>
2	721	403ed8:	48 8d 05 87 31 00 00	lea	0x3187(%rip),%rax # 407066 <version_etc_copyright+0x46></version_etc_copyright+0x46>	4050	403ed8:	48 8d 05 87 31 00 00	lea	0x3187(%rip),%rax # 407066 <version_etc_copyright+0x46></version_etc_copyright+0x46>
2	122	403edf:	e5 31 ed	xor	arijd, arijd	4051	403edf:	90 75 eb	inop	403end colose stdout+0xfod>
2	723	403ee21	41 b9 01 00 00 00	nov	\$0x1,%r9d	4053	403ee21	41 b9 01 00 00 00	BOV	\$0x1, %r9d
2	724	403ee81	31 db	NOT	Sebx, Sebx	4054	403ee81	31 db	NOT	%ebx,%ebx
2	725	403eea:	48 89 84 24 88 00 00	nov	<pre>%rax,0x88(%rsp)</pre>	4055	403eea:	90	nop	
2	727	403ef2:	e9 49 14 11 11	inpg	403340 <close stdout+0x440=""></close>	4057	403eec:	90	nop	
2	728	403ef7:	48 8d 35 64 31 00 00	lea	0x3164(%rip),%rsi # 407062 <version_etc_copyright+0x42></version_etc_copyright+0x42>	4058	403eed:	90	nop	
2	729	403efe:	41 bd 01 00 00 00	nov	SOX1, %r13d	4059	403eee:	90	nop	
2	731	4031041	31 db	XOT	sebx, sebx	4061	403ef01	90	nop	
2	732	403f0c:	48 89 b4 24 88 00 00	nov	<pre>%rsi,0x88(%rsp)</pre>	4062	403ef1:	00 e9	add	Sch, Scl
2	733	403113:	00	(max)	103345 caless stdeutsfer4405	4063	403ef3:	49 14	rex.W	B hit
2	735	403f19:	e8 2a d4 ff ff	calle	401348 < stack chk fail@plt>	4065	403ef6:	ff 48 8d	decl	-0x73(%rax)
2	736	403fle:	66 90	xchg	tax, tax	4066	403ef9:	35 64 31 00 00	xor	\$0x3164, teax
2	737	403120:	48 89 50 24 40	nov	<pre>%rbx,-0x30(%rsp)</pre>	4067	403efe:	90	nop	
2	739	4035281	48 89 cb	BOV	krox. krbx	4069	4032001	90	nop	
2	740	403f2d:	4c 89 6c 24 e8	nov	%r13,-0x18(%rsp)	4070	403f01:	41 b9 01 00 00 00	mov	\$0x1,%r9d
2	741	403f32:	4c 89 74 24 f0	nov	<pre>srl4,-Oxl0(%rsp)</pre>	4071	403207:	31 db	xor	tebx, tebx
2	743	4031371	4c 89 64 24 e0	nov	%r12,-0x20(%rap)	4073	403£10:	00	nov	ersi, oxob(ersp)
2	744	403f3e:	4c 89 7c 24 f8	nov	%r15,-0x8(%rap)	4074	403f11:	e9 27 14 11 11	jmpq	40333d <close_stdout+0x43d></close_stdout+0x43d>
2	745	4031431	48 83 ec 78	sub	\$0x78, trap	4075	403f161	e8 2a d4 ff ff	callq	401345 <dogettext@plt+0xd></dogettext@plt+0xd>
2	747	403140:	48 89 54 24 30	nov	krdx.0x30(krsp)	4077	403f1d:	48 89 50 24 40	nov	%rbx,-0x30(%rsp)
2	748	403151:	e8 d2 d3 ff ff	callq	401328 < errno_location@plt>	4078	403f22:	48 89 6c 24 d8	nov	%rbp,-0x28(%rsp)
2	749	403156:	49 89 C6	nov	%rax,%r14	4079	403527:	48 89 cb	nov	%rcx, %rbx
2	751	40315b1	85 ed	test	tebp, tebp	4081	403f2b1	90	nop	
2	752	40315d1	4c 8b 2d de 45 20 00	BOV	0x2045dc(%rip),%r13 # 608540 <exit_failure+0x10></exit_failure+0x10>	4082	4031201	90	nop	
2	753	4031641	89 44 24 3c	nov	Seax, 0x3c(Srsp)	4083	403f2d1	90	nop	
	755	4031681	3b 2d c0 45 20 00	CER	0x2045c0(%rip).%ebp # 608534 Kevit failure=0x45	4084	4031201	4c 89 74 24 f0	nop	%r140x10(%rsp)
2	756	403174:	72 57	5b	403fcd <close_stdout+0x10cd></close_stdout+0x10cd>	4086	403£34:	89 fd	nov	tedi, tebp
2	757	403176:	44 8d 65 01	lea	0x1(%rbp),%r12d	4087	403£36:	5a	pop	ardx
	759	4031/41	45 89 e7	Tea	srl2d, srl5d	4088	4031371	4c 89 7c 24 f8	BOV	%r15,-0x8(%rsp)
2	760	4031841	4c 89 fe	nov	sr15, srs1	4090	4031411	48 83 ec 78	sub	\$0x78, srsp
2	761	403187:	48 cl e6 04	shl	S0x4,%rsi	4091	403145:	48 89 74 24 28	nov	%rs1,0x28(%rsp)
2	762	40318b:	99 39 C5 0f 84 3c 01 00 00	cmp 1e	4040d0 sclose stdout=0x11d0>	4092	403148:	48 89 54 24 30	calle	401326 scheinitEniteOrea
2	764	403594:	4c 89 ef	nov	tr13, trdi	4094	403554:	49 89 66	nov	Tax, 1r14
2	765	403197:	e8 14 20 00 00	callq	405fb0 <close_stdout+0x30b0></close_stdout+0x30b0>	4095	403£57:	8b 00	BOV	(%rax),%eax
	766	4031901	49 89 05 98 45 20 00	BOV	trax, 0x20459a(krip) # 608540 cexit failure+0x10>	4096	4031591	40 8b 2d do 45 20 00	test	0x2045dc/krip) krll d 60853c cexit failure:0x2
2	768	4031861	8b 3d 88 45 20 00	nov	0x204588(%rip),%edi # 608534 <exit_failure+0x4></exit_failure+0x4>	4098	4031621	89 44 24 3c	nov	teax, 0x3c(trap)
and the second se	740	403fec:	4c 89 fa	nov	%r15,%rdx	4099	403166:	Of 88 8e 01 00 00	38	4040fa <close_stdout+0x11fa></close_stdout+0x11fa>

Changes: 345

# Simple program and echo plots



