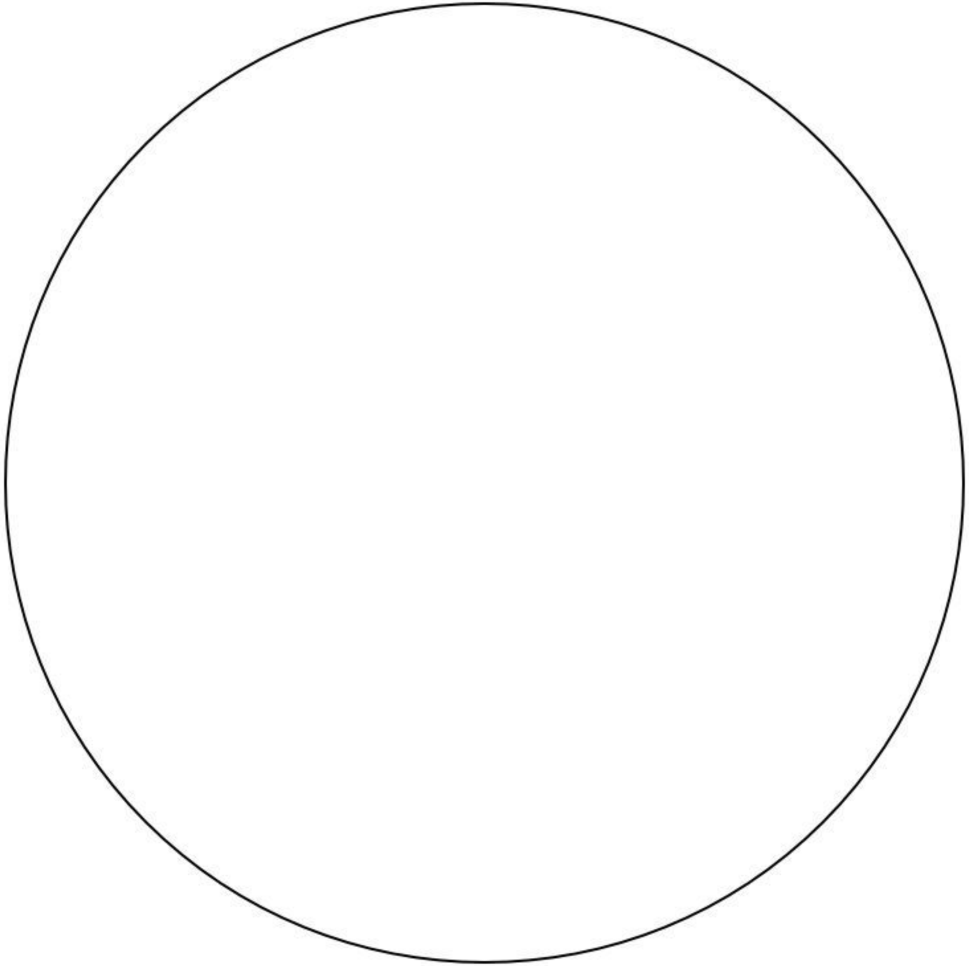
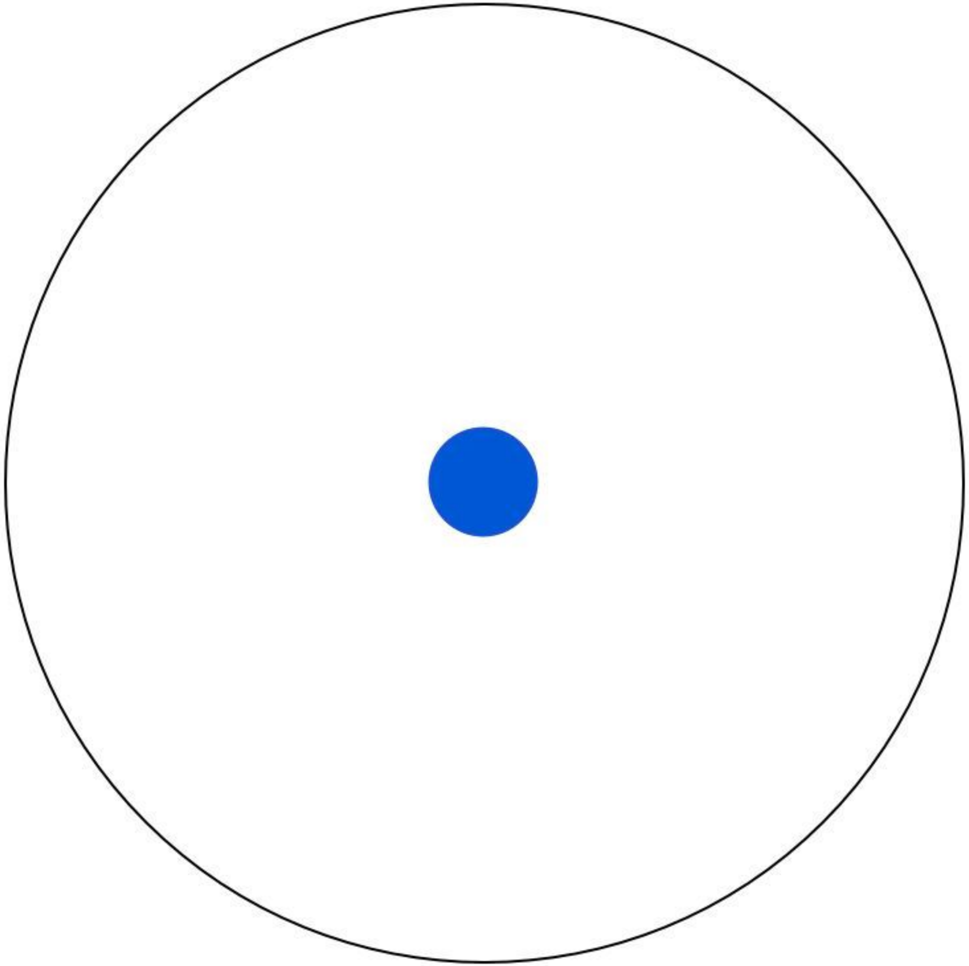
Sailing the Seas of the Science of Security

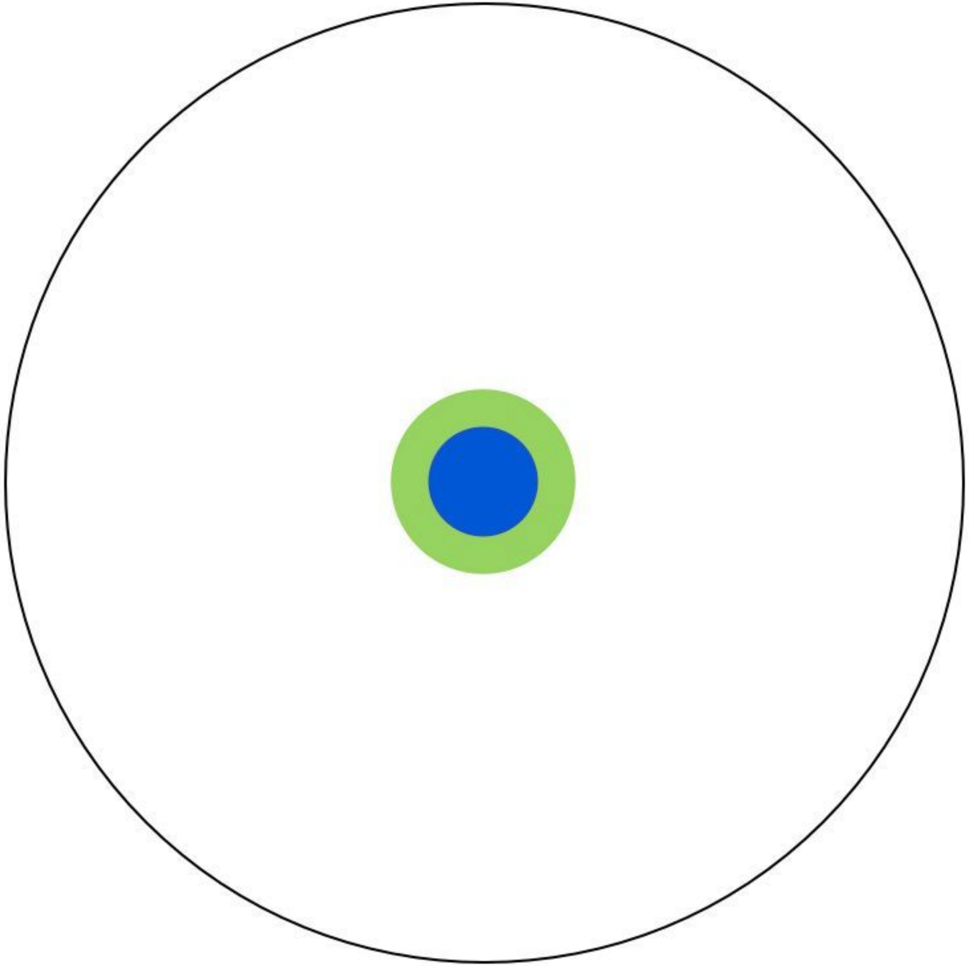
Yan Shoshitaishvili
Arizona State University

Science!

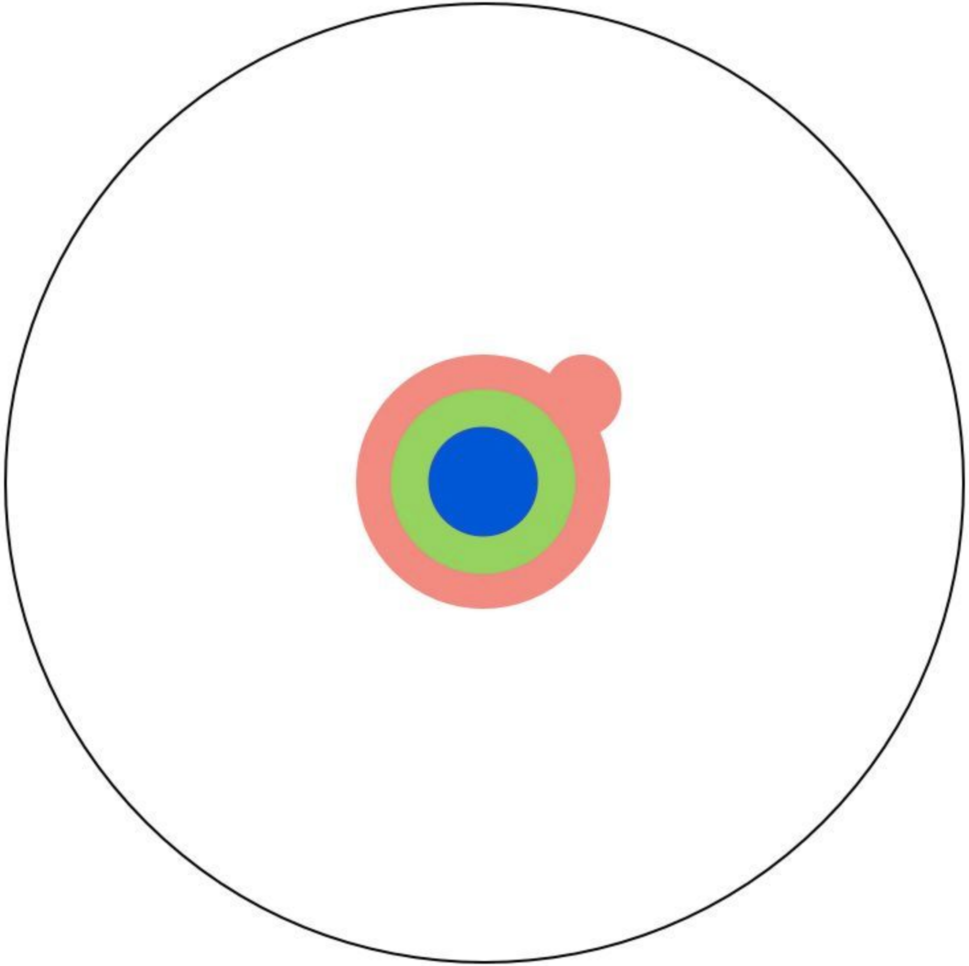


https://matt.might.net/articles/phd-school-in-pictures

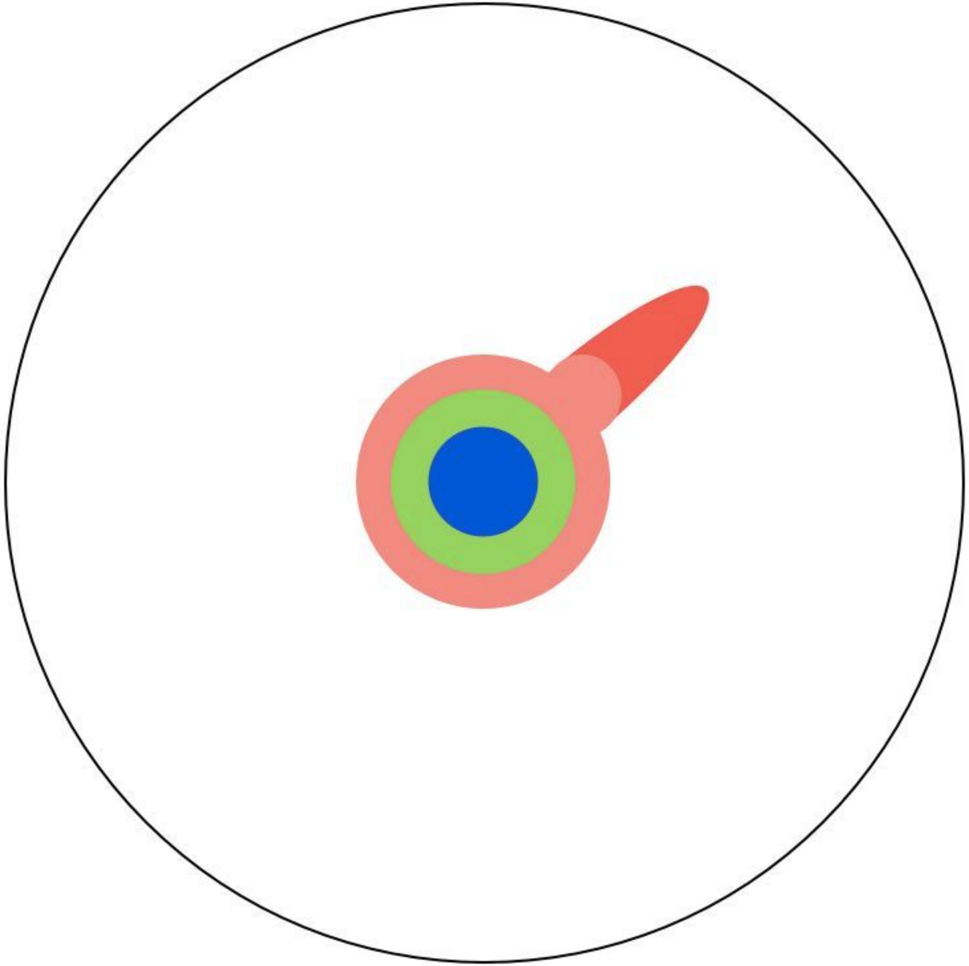




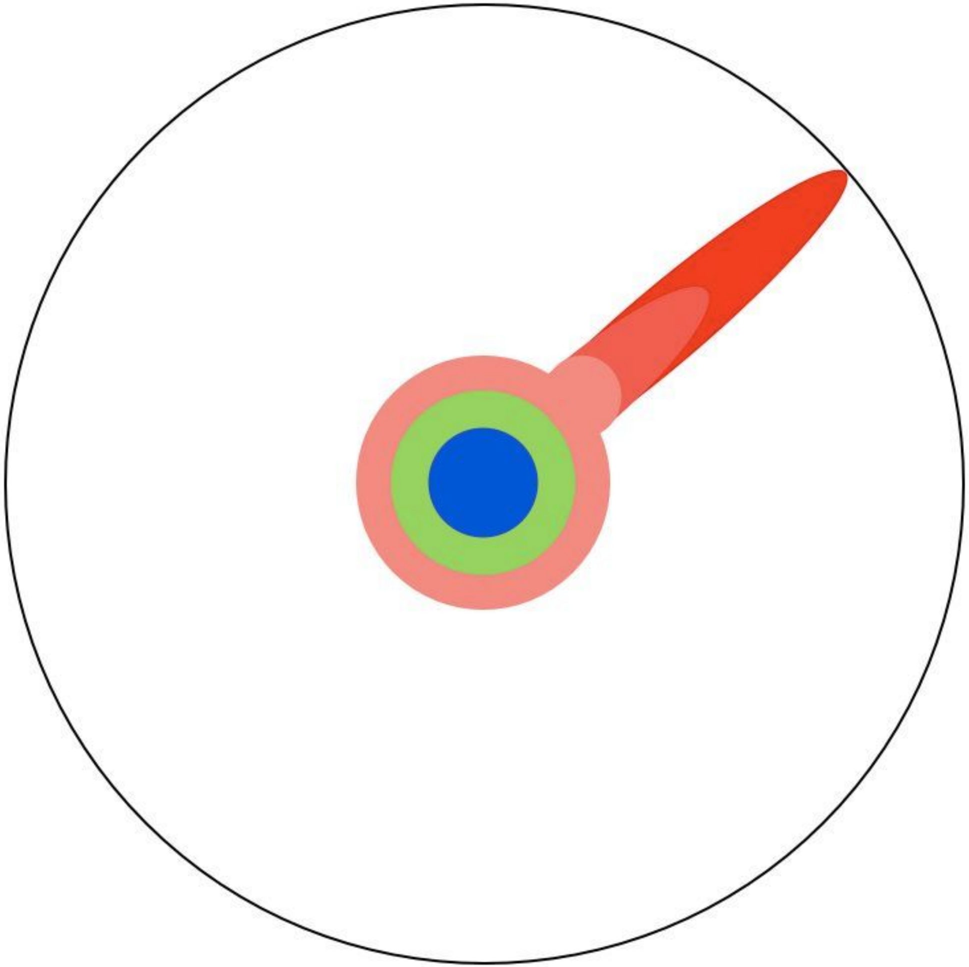
https://matt.might.net/articles/phd-school-in-pictures



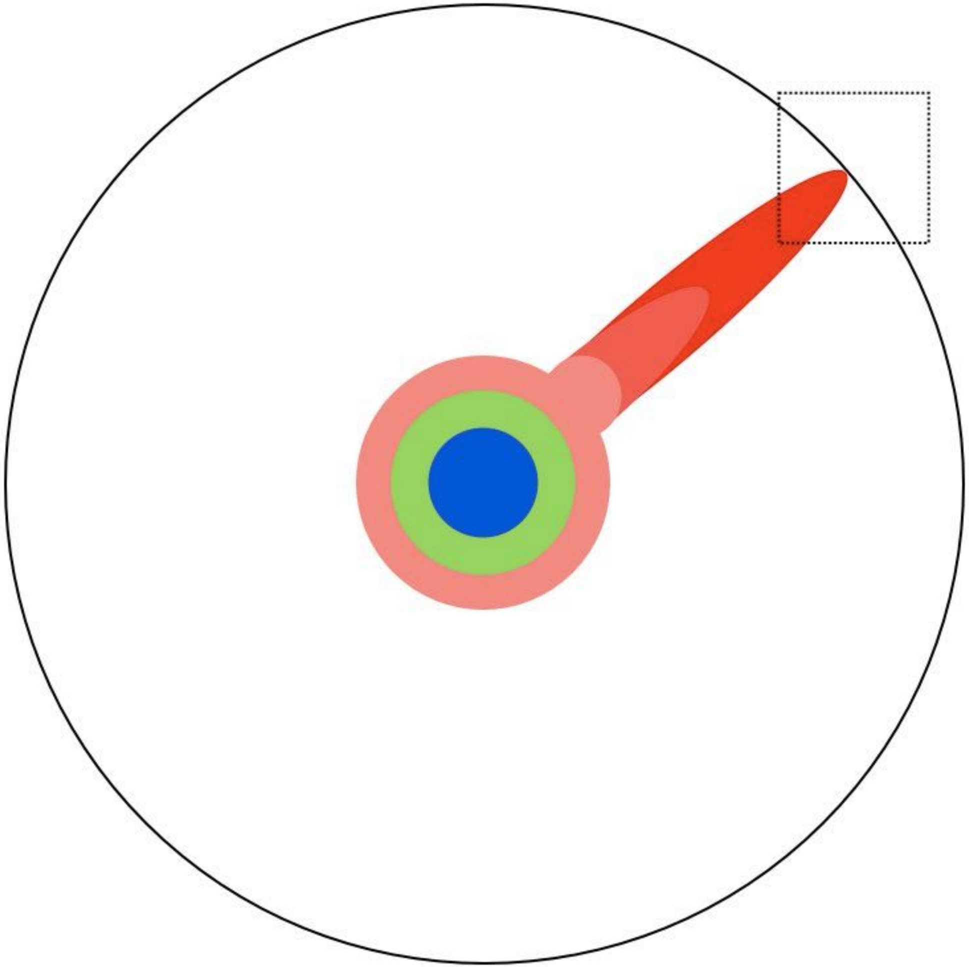
https://matt.might.net/articles/phd-school-in-pictures



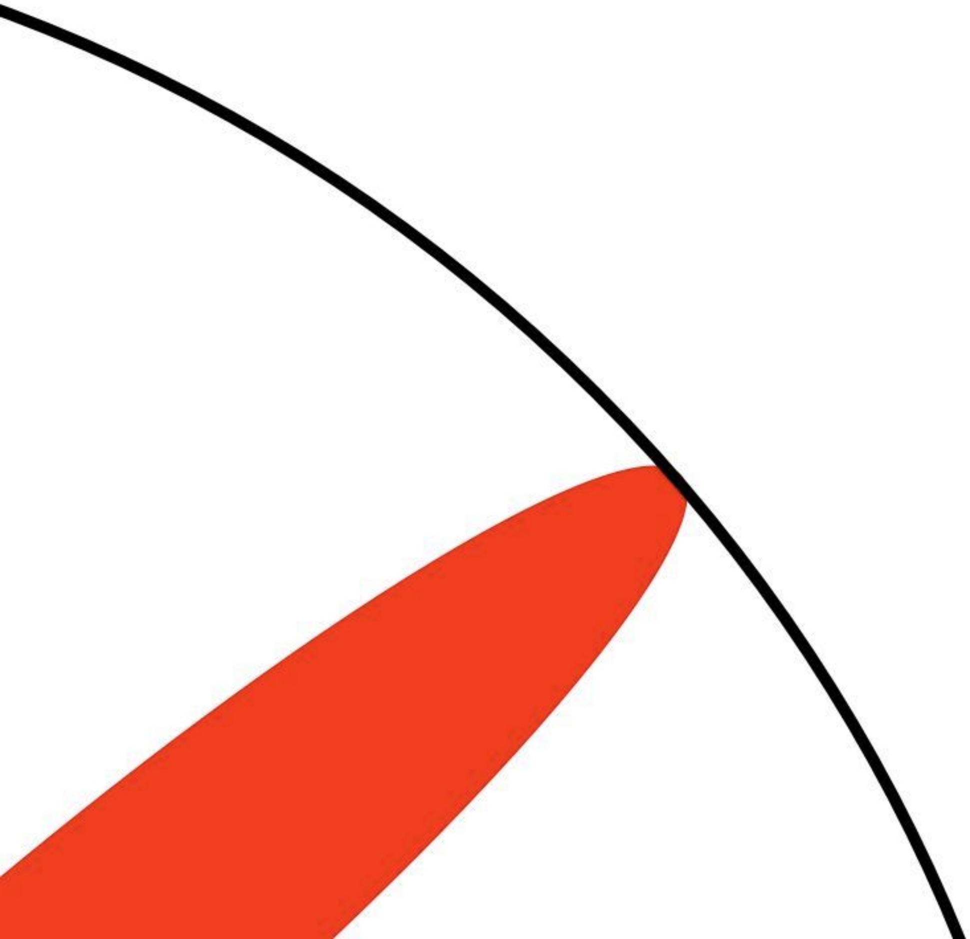
https://matt.might.net/articles/phd-school-in-pictures



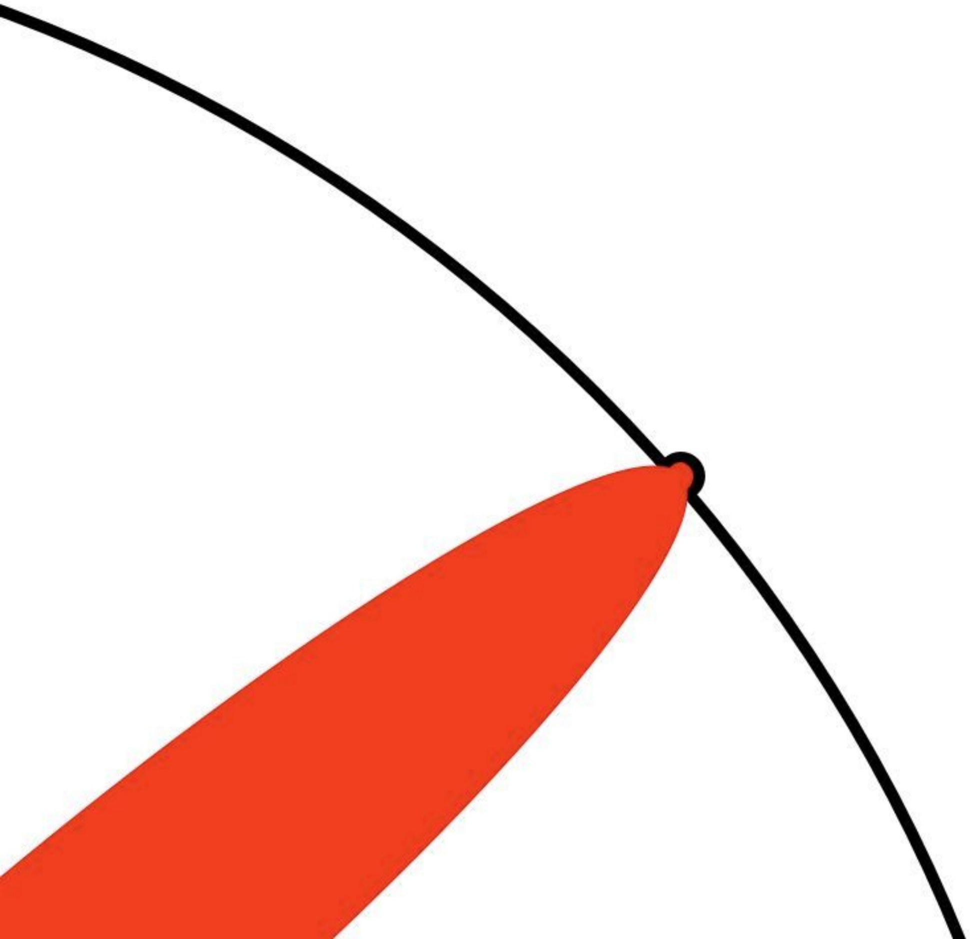
https://matt.might.net/articles/phd-school-in-pictures



https://matt.might.net/articles/phd-school-in-pictures



https://matt.might.net/articles/phd-school-in-pictures



https://matt.might.net/articles/phd-school-in-pictures

DON’T PANIC

angr.io
docs.angr.io
github.com/angr/angr

Program Transformation

Automatic Exploitation

Vulnerability Detection

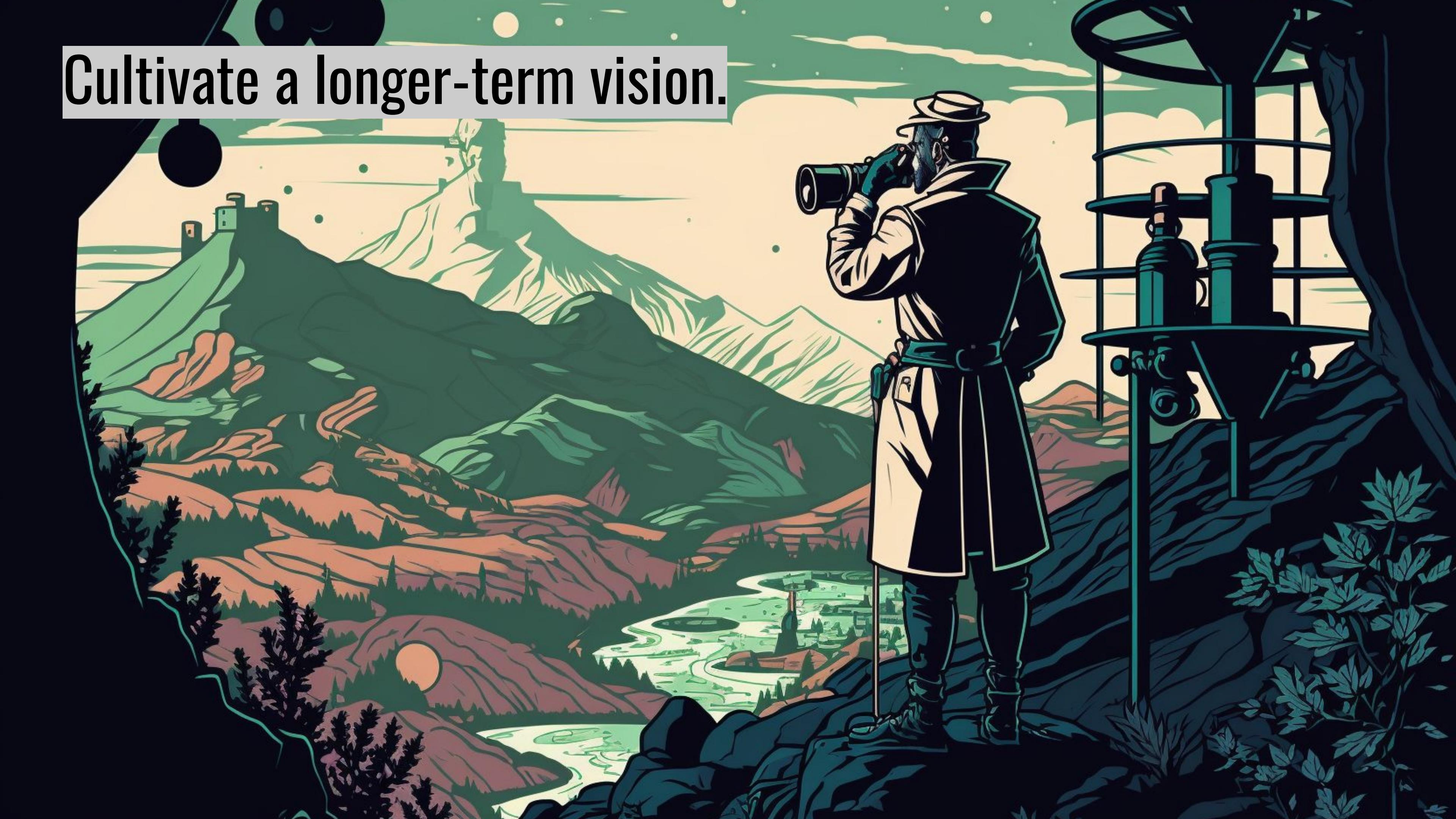
Decompilation

Symbolic Execution

CFG Recovery

X86	AMD64	MSP430
AVR	ARM	ARM64
PPC	PPC64	MIPS
Java/Dalvik		MIPS64
SP:ARC	RISC-V	*

Cultivate a longer-term vision.



Sway in the wind.

"My" angr projects

Each of my angr-based research projects pushed the underlying system forward!

A subset:

Firmalice: initial angr development, static analysis and symbolic execution
Driller: symbolic execution improvements
State of the Art of War: full-framework polishing, path merging
Ramblr: *proper* static analysis
Your Exploit is Mine: symbolic execution introspection
BootStomp: flexible symbolic taint tracking
BinTrimmer: signedness-agnostic abstract static variables, Value-Set Analysis
BootKeeper: solidifying Value-Set Analysis
Karonte: large-scale static analysis reliability
Arbiter: static/symbolic analysis integration

Flexing angr's base to support each new project left us with permanent improvements to the framework!

Mentored mentoring.

Impact of Mentoring

From angr's inception to my PhD defense...
... there were 42 contributors to angr (https://github.com/angr/angr/graphs/contributors?from=2013-08-08&to=2017-08-01&type=c)
... and I mentored 15 of them!

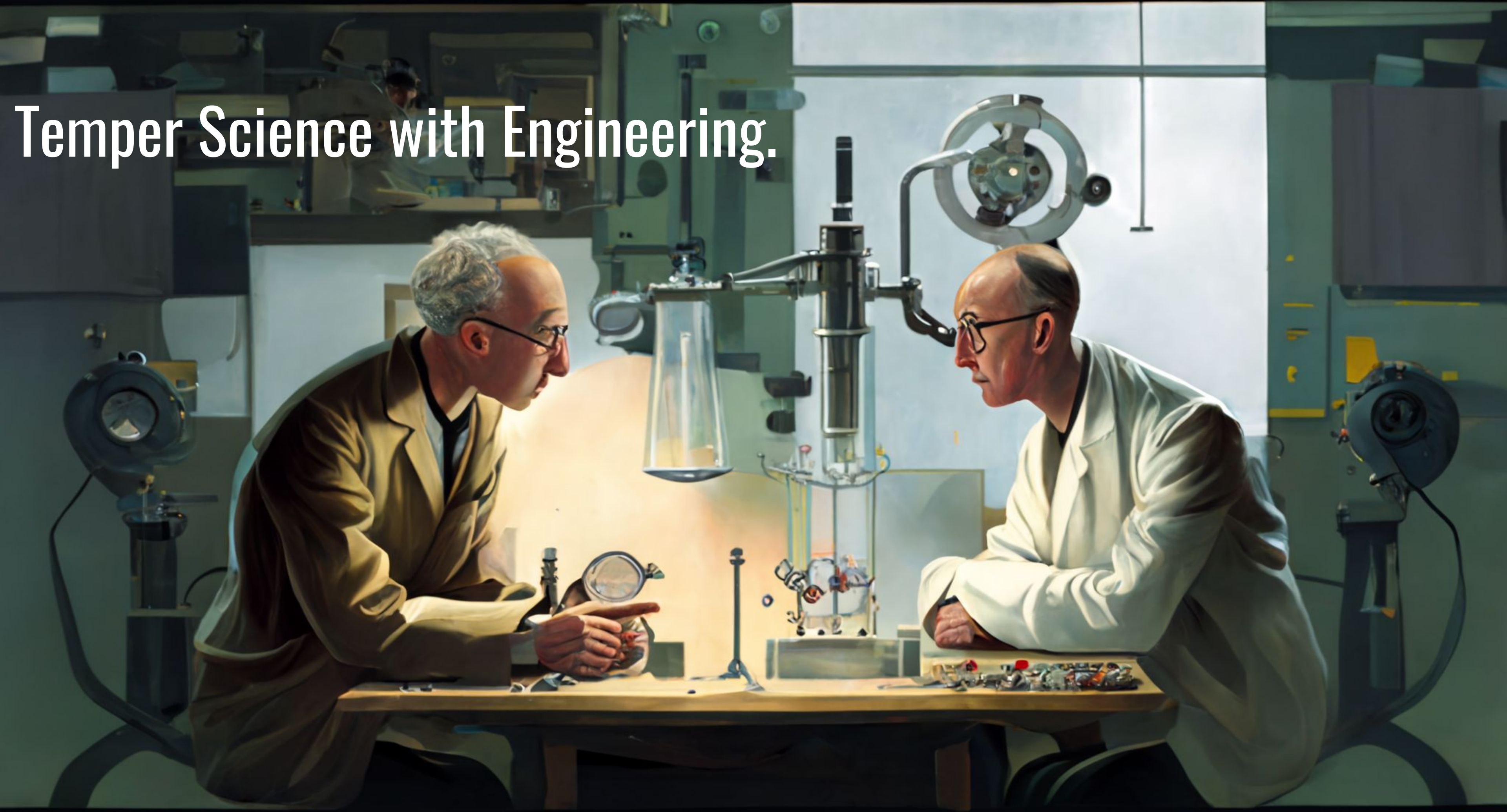
Critical for system growth.

Great for publication and impact!

Very rewarding.

Impossible without excellent support from professors.

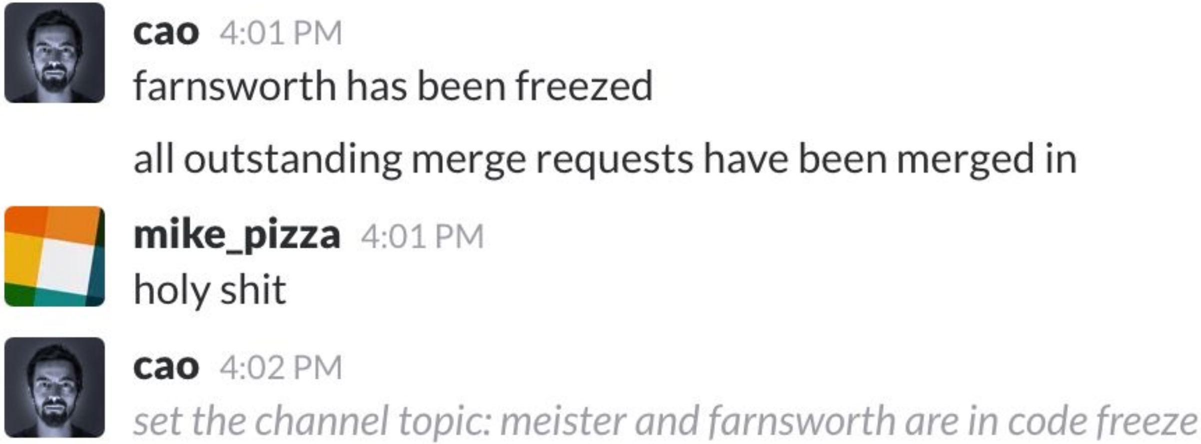
Temper Science with Engineering.



CYBER
CYBER

CGC
CYBER
GRAND CHALLENGE
DARPA
MECHANICAL PHISH
SHELLPHISH
MAYHEM
SECURE
SCORING
CYBER
DARPA

# Code Freeze?

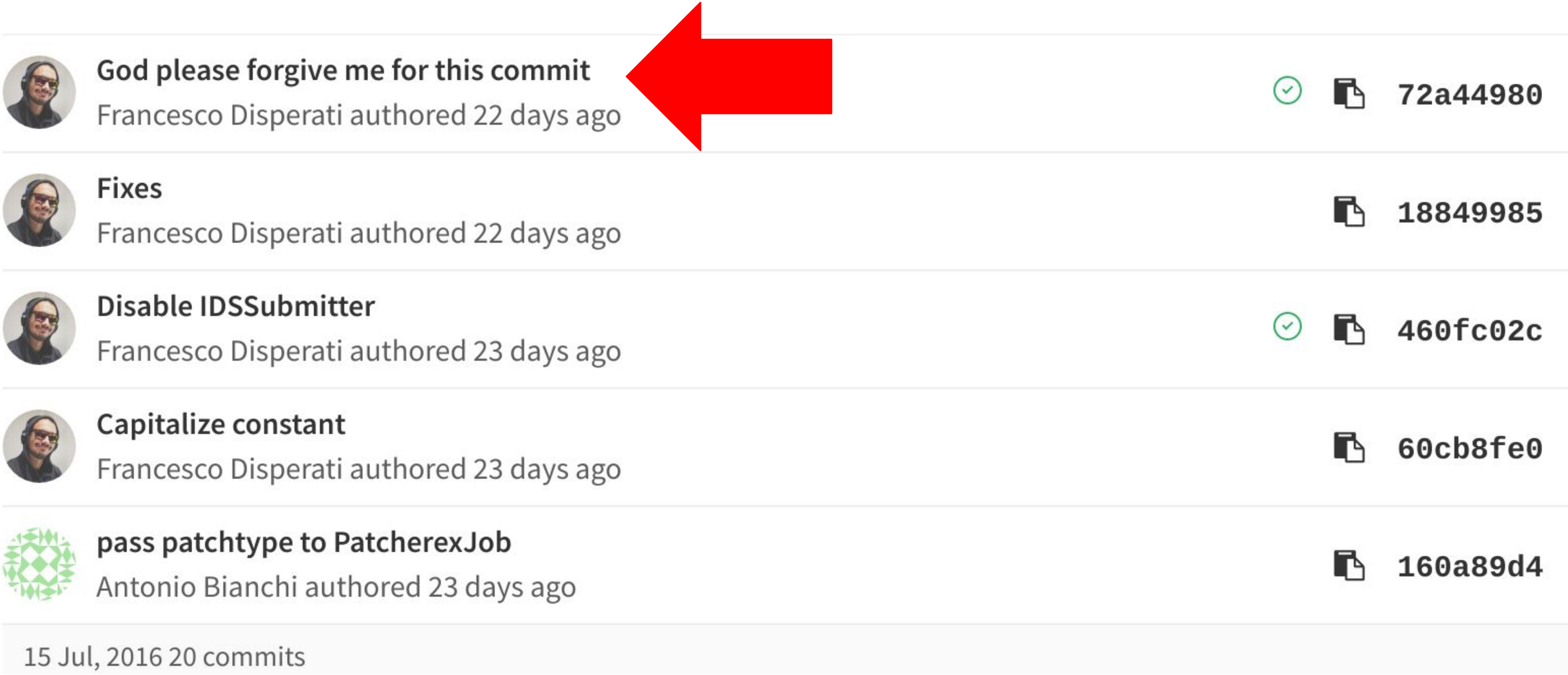


cao 4:01 PM
farnsworth has been freezed

all outstanding merge requests have been merged in

mike_pizza 4:01 PM
holy shit

cao 4:02 PM
set the channel topic: meister and farnsworth are in code freeze



God please forgive me for this commit
Francesco Disperati authored 22 days ago ✓ 72a44980

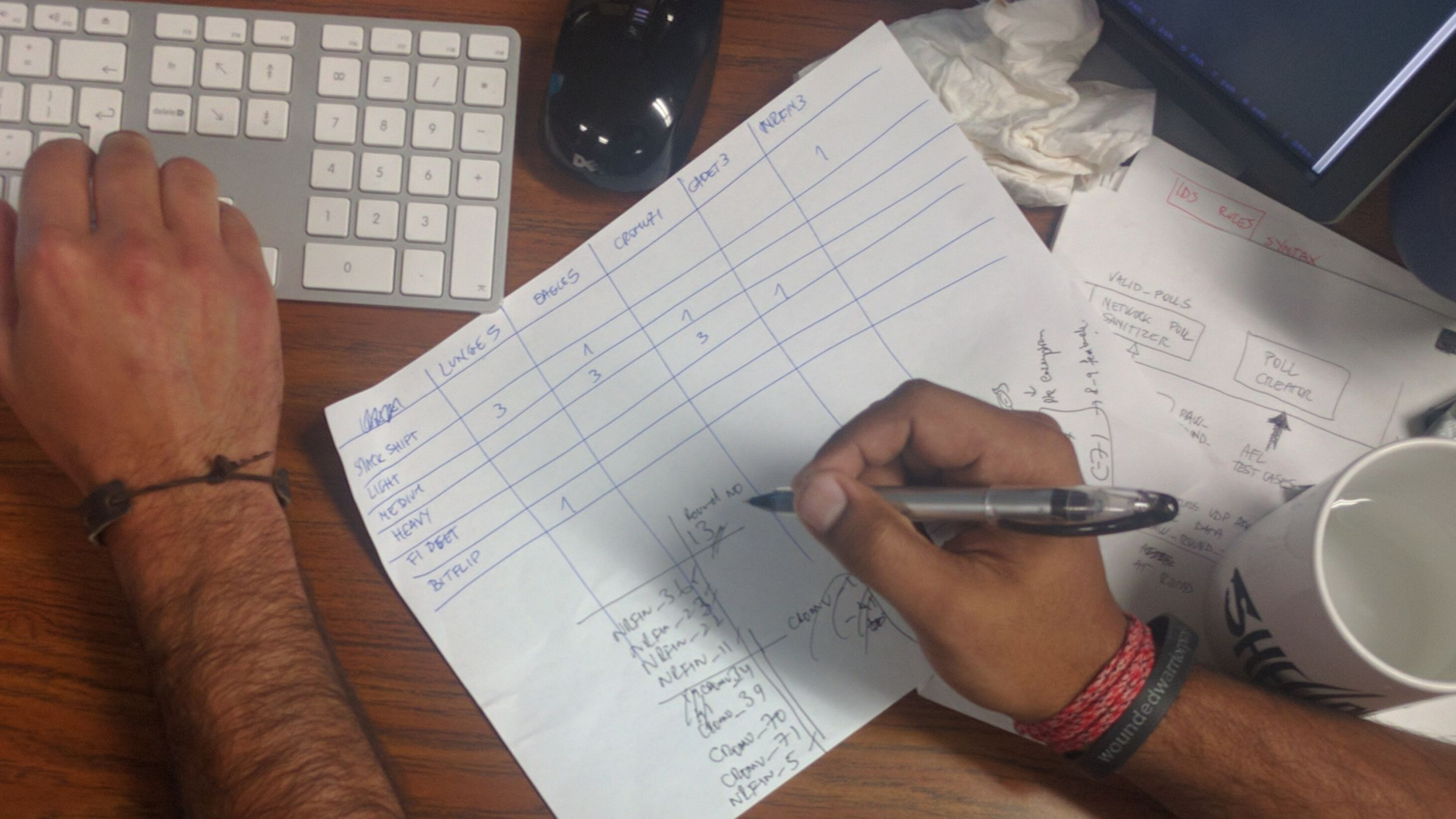
Fixes
Francesco Disperati authored 22 days ago 18849985

Disable IDSSubmitter
Francesco Disperati authored 23 days ago ✓ 460fc02c

Capitalize constant
Francesco Disperati authored 23 days ago 60cb8fe0

pass patchtype to PatcherexJob
Antonio Bianchi authored 23 days ago 160a89d4

15 Jul, 2016 20 commits



	LUNGE5	EAGLES	CROMU71	CADET3	NRFIN3
STACK SHIFT					1
LIGHT	3	1			
MEDIUM		3	1		
HEAVY			3	1	
FI DBET					
BITFLIP	1				

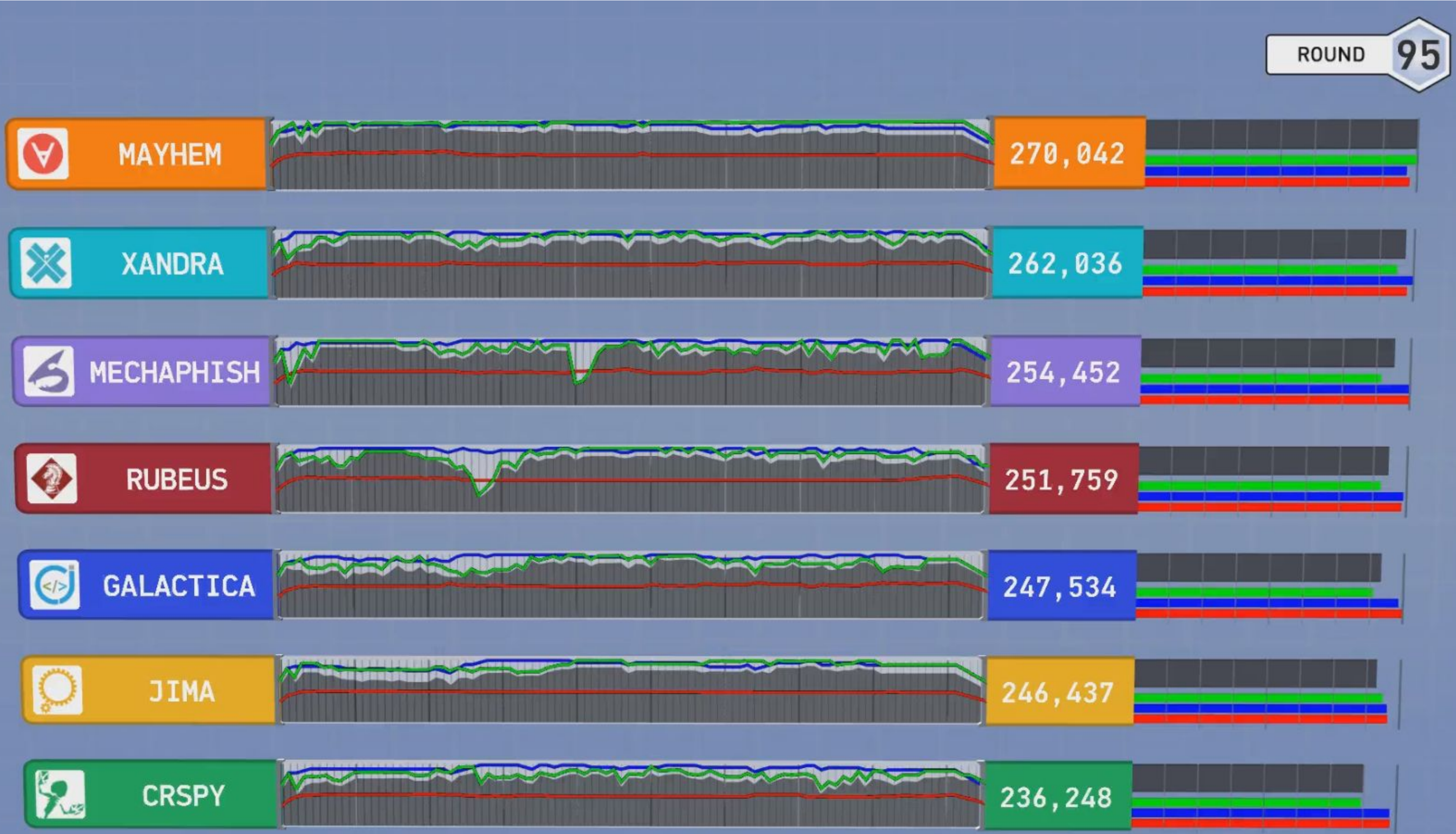
found NO

~~13~~

NRFIN_36
NRFIN_23
NRFIN_32
NRFIN_11
CROMU_14
CROMU_39
CROMU_70
CROMU_71
NRFIN_5

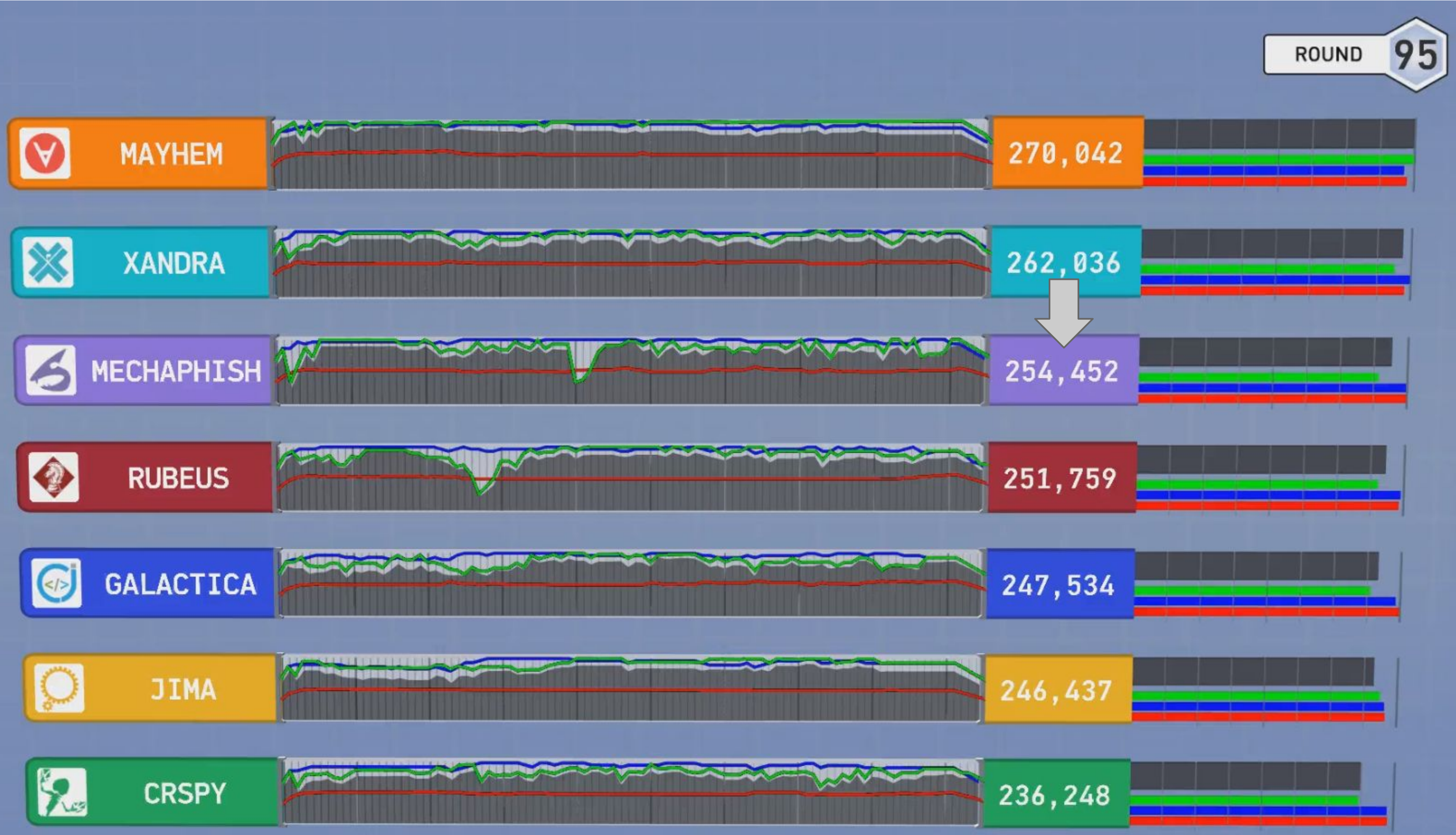
CROMU

Tue 2 Aug, 23:54
~15 hours before access shutdown



ROUND 95

MAYHEM	270,042
XANDRA	262,036
MECHAPHISH	254,452
RUBEUS	251,759
GALACTICA	247,534
JIMA	246,437
CRSPY	236,248



ROUND 95

MAYHEM	270,042
XANDRA	262,036
MECHAPHISH	254,452
RUBEUS	251,759
GALACTICA	247,534
JIMA	246,437
CRSPY	236,248

Reaping the Benefits...

The CGC, and its requisite engineering work, led to...

Test cases!
Media attention!
Mindshare!
Contributors!

Through this, angr turned from a research prototype to a *research vehicle*!

# Limiting the scope...

CGC vs "real" operating systems...

7 system calls	vs	387 system calls
no persistence	vs	persistence!
simple exploits	vs	mitigations! crazy heap, JIT, etc
well-defined test cases	vs	"broke my use-case"

Paying the price…

Engineering effort has costs:

PhD students lose research time.
Engineers require large salaries.
Undergrad/MS students burn out.

Conscious effort (and strong professor support!) needed to make this feasible.

Spread the wealth!

Closed source systems.

Version-delayed open source systems (latest version available to collaborators only).

Open source upon publication. Don't forget support!

Just develop right there on github!

Don't forget the big picture!

# To C or not to C?

DARPA CGC ran on binary code.

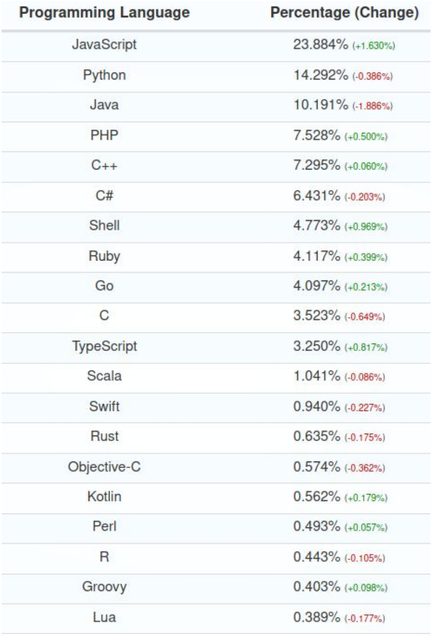
angr is quite adept at analyzing binary code...
... preferably code that is compiled from C.

C market share:
between ~3.5% and ~17% market share

All binary-compiled language market share:
between ~18% and ~30% market share

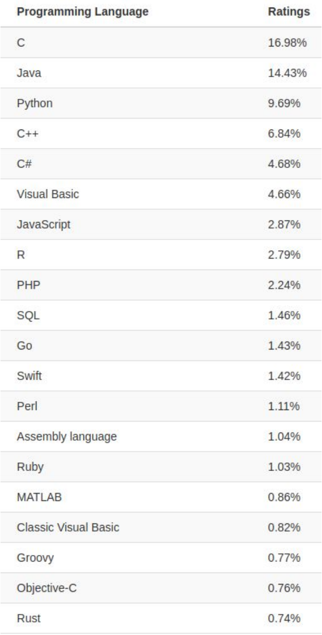
Even with our (incomplete!) Java support, we max out at 46% of analyzable code.

GitHut 2.0, Q2 2020
Market Share of Git Pushes



Programming Language	Percentage (Change)
JavaScript	23.884% (+1.630%)
Python	14.292% (-0.386%)
Java	10.191% (-1.886%)
PHP	7.528% (+0.500%)
C++	7.295% (+0.060%)
C#	6.431% (-0.203%)
Shell	4.773% (+0.969%)
Ruby	4.117% (+0.399%)
Go	4.097% (+0.213%)
C	3.523% (-0.649%)
TypeScript	3.250% (+0.817%)
Scala	1.041% (-0.086%)
Swift	0.940% (-0.227%)
Rust	0.635% (-0.175%)
Objective-C	0.574% (-0.362%)
Kotlin	0.562% (+0.179%)
Perl	0.493% (+0.057%)
R	0.443% (-0.105%)
Groovy	0.403% (+0.098%)
Lua	0.389% (-0.177%)

TIOBE Language Index, 8/2020
Market Share, Various Metrics

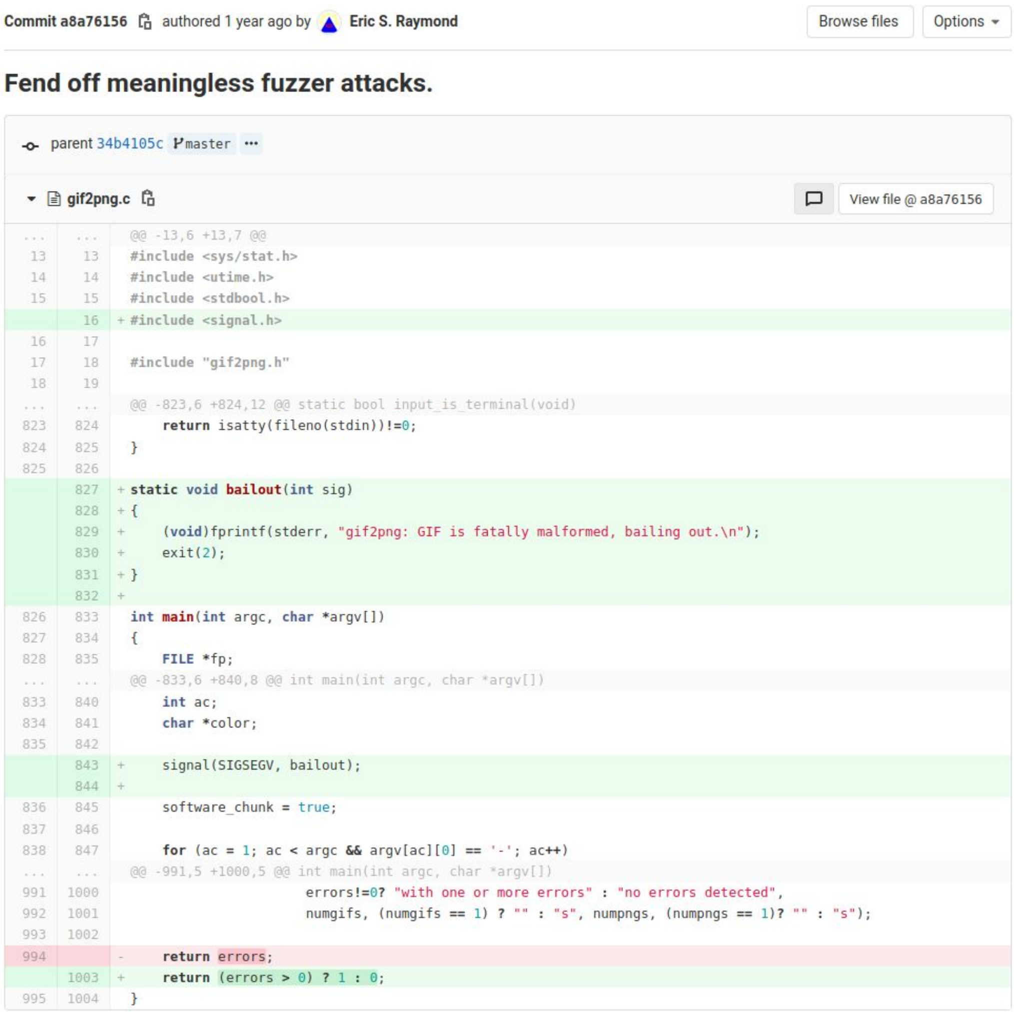


Programming Language	Ratings
C	16.98%
Java	14.43%
Python	9.69%
C++	6.84%
C#	4.68%
Visual Basic	4.66%
JavaScript	2.87%
R	2.79%
PHP	2.24%
SQL	1.46%
Go	1.43%
Swift	1.42%
Perl	1.11%
Assembly language	1.04%
Ruby	1.03%
MATLAB	0.86%
Classic Visual Basic	0.82%
Groovy	0.77%
Objective-C	0.76%
Rust	0.74%

We can only open the door...

Finding bugs is angr's most-used application...

... but do developers even want that?



Commit a8a76156 authored 1 year ago by Eric S. Raymond

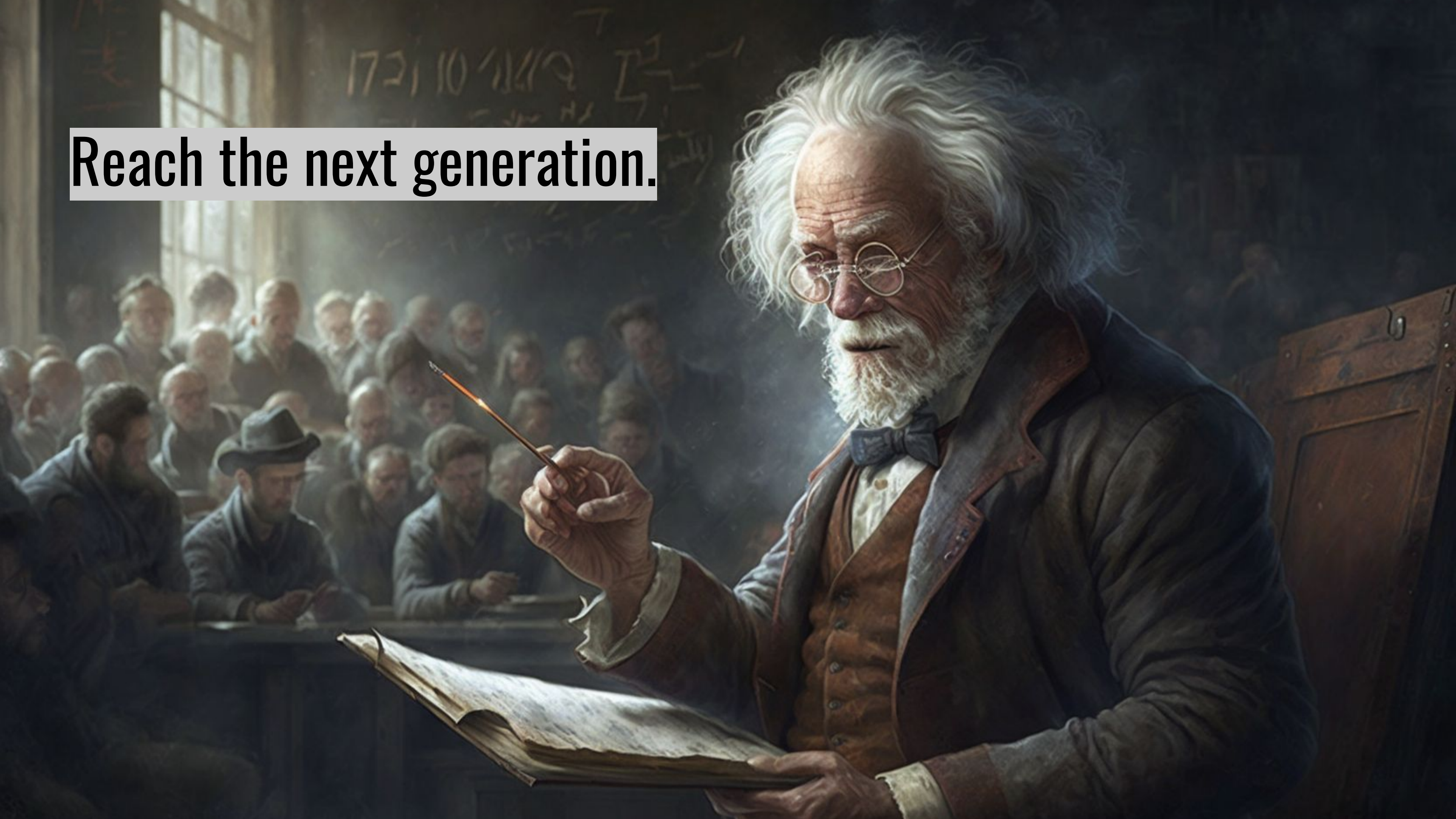
Fend off meaningless fuzzer attacks.

parent 34b4105c master

gif2png.c

```
@@ -13,6 +13,7 @@
 #include <sys/stat.h>
 #include <utime.h>
 #include <stdbool.h>
+#include <signal.h>
 
 #include "gif2png.h"
 
@@ -823,6 +824,12 @@ static bool input_is_terminal(void)
     return isatty(fileno(stdin))!=0;
 }
 
+static void bailout(int sig)
+{
+    (void)fprintf(stderr, "gif2png: GIF is fatally malformed, bailing out.\n");
+    exit(2);
+}
+
 int main(int argc, char *argv[])
 {
     FILE *fp;
@@ -833,6 +840,8 @@ int main(int argc, char *argv[])
     int ac;
     char *color;
 
+    signal(SIGSEGV, bailout);
+
     software_chunk = true;
 
     for (ac = 1; ac < argc && argv[ac][0] == '-'; ac++)
@@ -991,5 +1000,5 @@ int main(int argc, char *argv[])
                 errors!=0? "with one or more errors" : "no errors detected",
                 numgifs, (numgifs == 1) ? "" : "s", numpngs, (numpngs == 1)? "" : "s");
 
-    return errors;
+    return (errors > 0) ? 1 : 0;
 }
```

Reach the next generation.



ASU Charter

ASU is a comprehensive **public research university**, measured not by
whom it excludes, but by **whom it includes** and how they **succeed**;
advancing **research and discovery** of public value;
and assuming **fundamental responsibility**
for the economic, social, cultural and overall
health of the **communities** it serves.

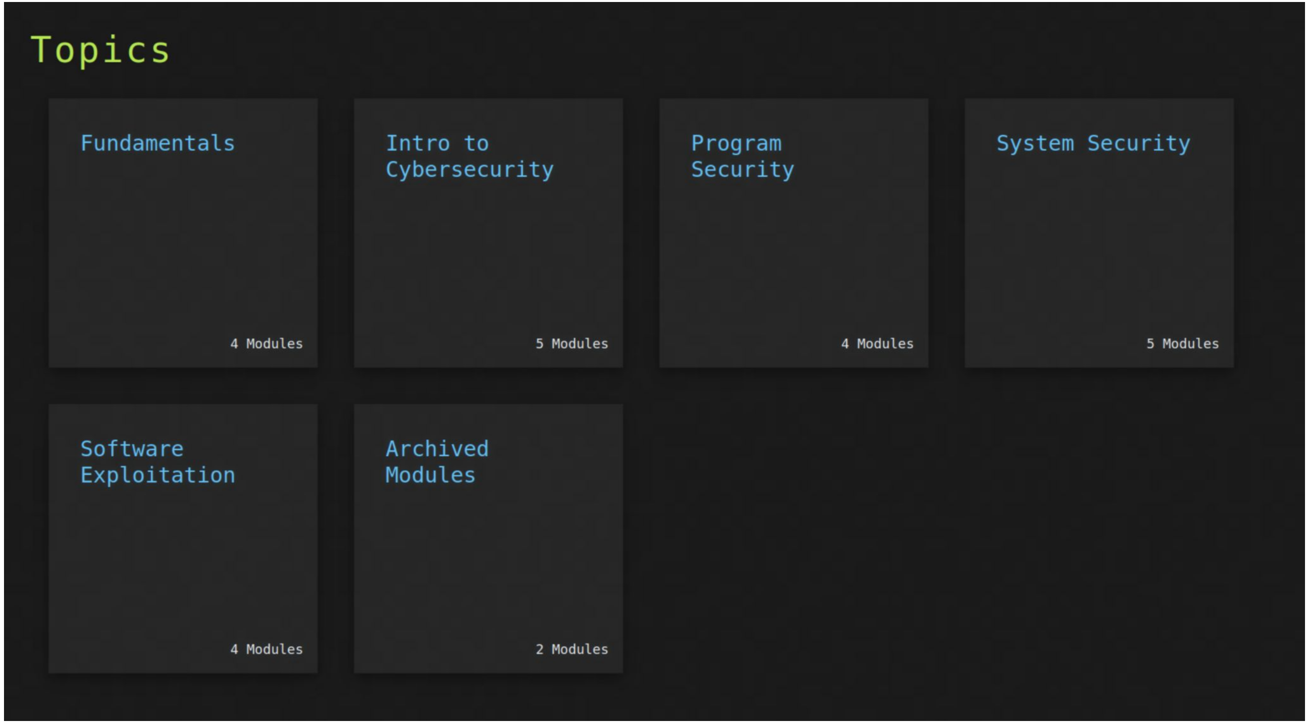
# A critical look on education…

Binary analysis lacked a flexible, truly open-source framework.

Security education lacked a comprehensive, accessible, *turnkey* platform.

So we made one!

Comprehensive Curriculum



Topics

Fundamentals
4 Modules

Intro to Cybersecurity
5 Modules

Program Security
4 Modules

System Security
5 Modules

Software Exploitation
4 Modules

Archived Modules
2 Modules

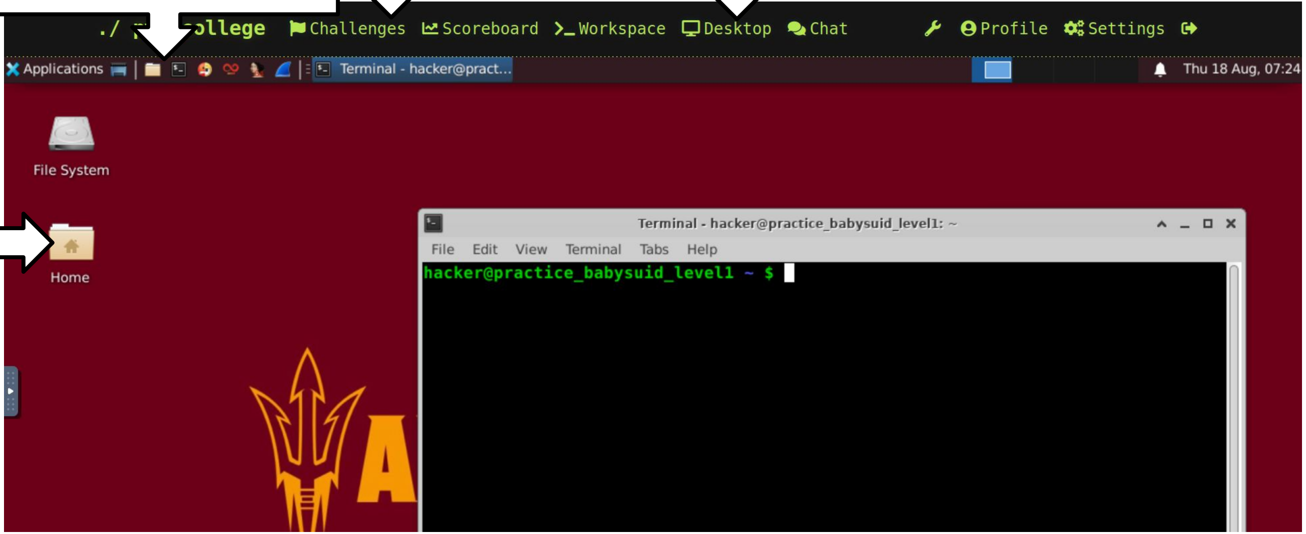
Turnkey Education

Challenges to learn security skills!

A full learning/practice desktop in the cloud!

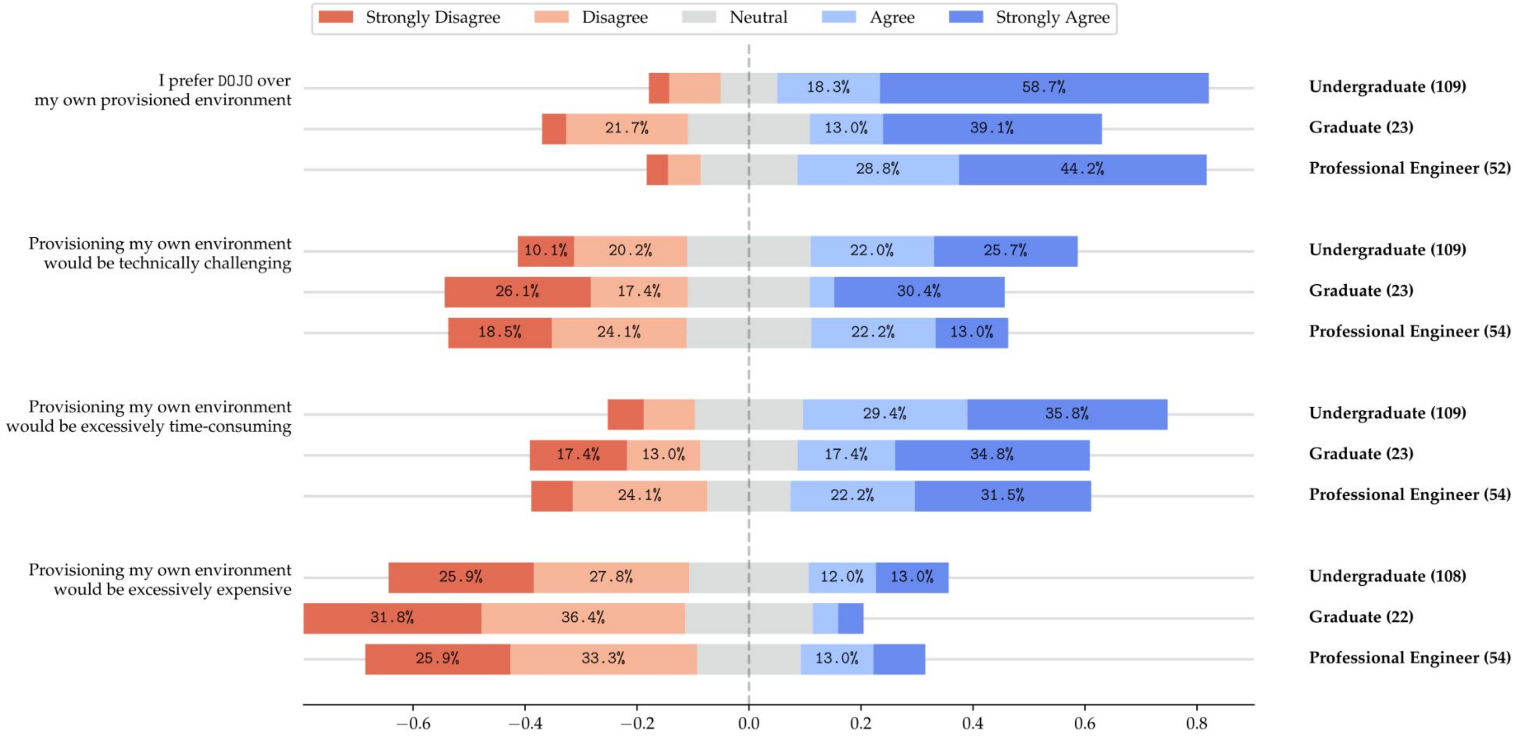
Preinstalled tools for learning to hack!

A persistent home directory for user data!

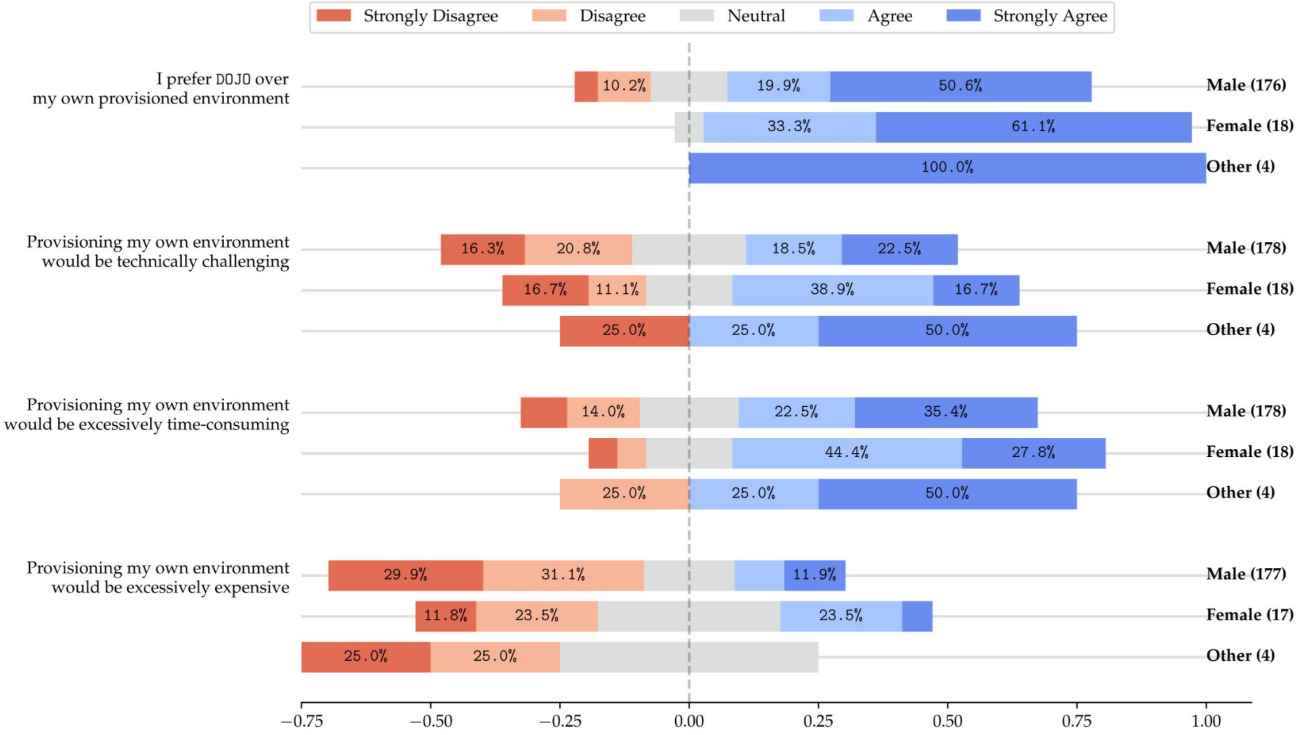


```
hacker@practice_babysuid_level1 ~ $
```

Democratizing Security Education



# Path to Inclusivity?



Join us in educating!

pwn.college isn't just a revolution for students, but for teachers as well!

Become a Sensei:

Found your own dojo.

Import our challenges or upload your own.

Reward students with emoji "badges".

Educate the world to...

Hack the Planet! (or prevent that from happening!)

Learn more at https://pwn.college

What about the researchers?

pwn.college does great at teaching security skills, but not research skills...

No replacement for painstaking, 1-on-1 mentorship...
... but definitely smoothes the onboarding process!

Thank you!

Yan Shoshitaishvili
yans@asu.edu
@Zardus@defcon.social

Want to visit? sefcom.asu.edu/apprenticeship.html
Want to learn? pwn.college