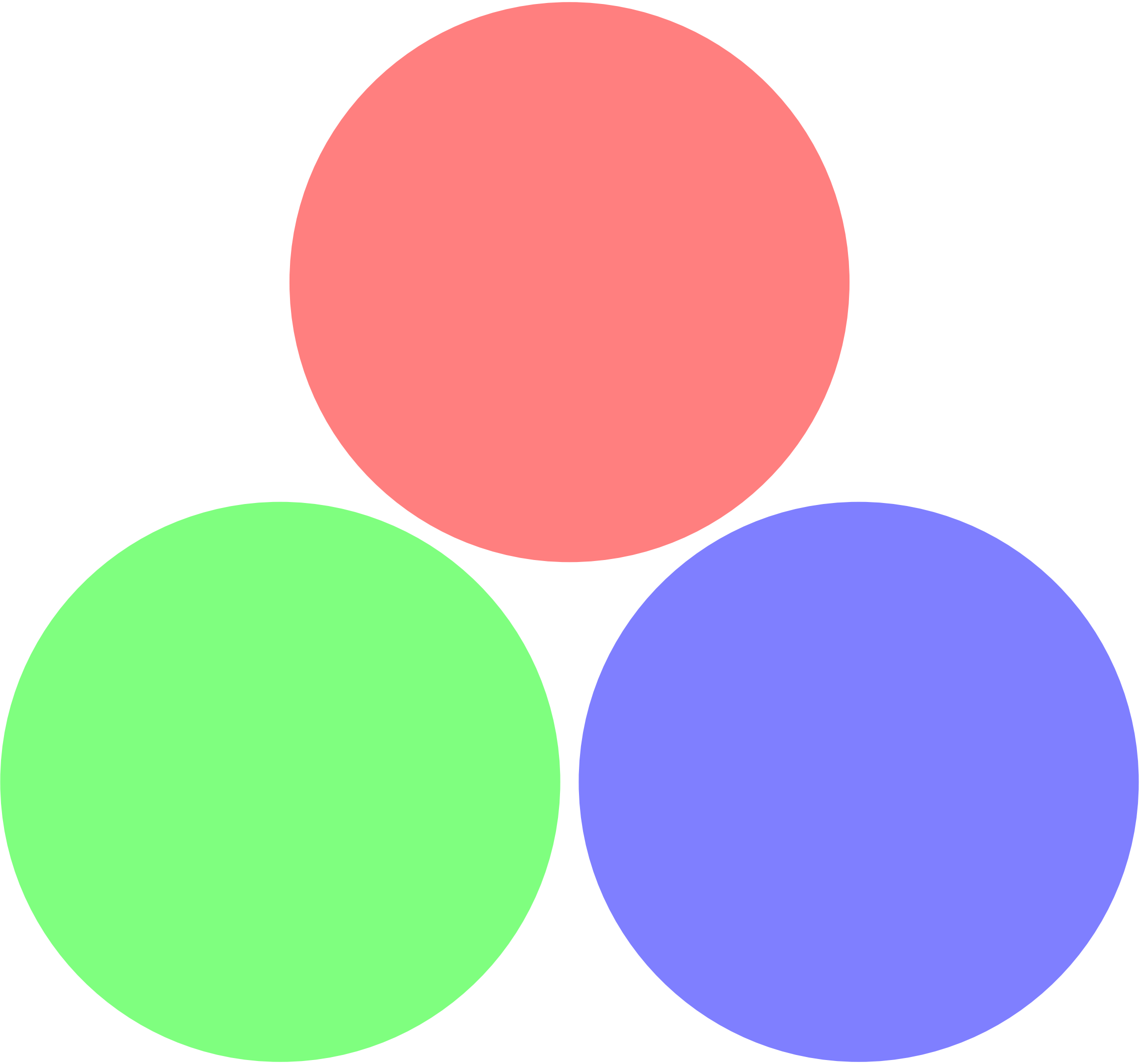
All Our Powers Combined

Connecting Academics, Engineers, and Hackers

Security



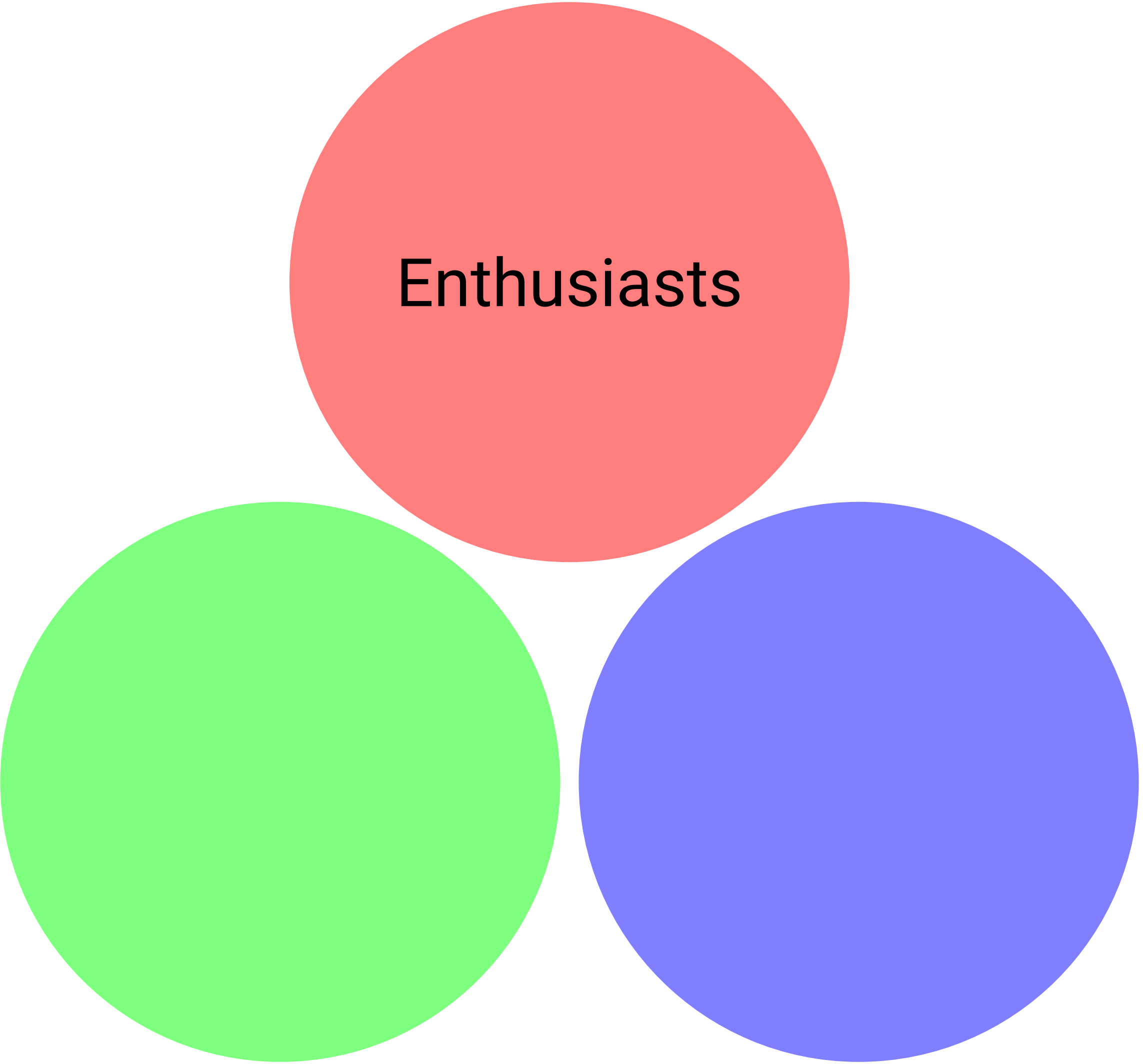
Enthusiast Community

Centered around conferences (DEFCON, HITCON, etc), CTF, and open-source projects.

Full of students, hackers, etc.

Labor of love.

Striving for fulfillment.



Enthusiasts

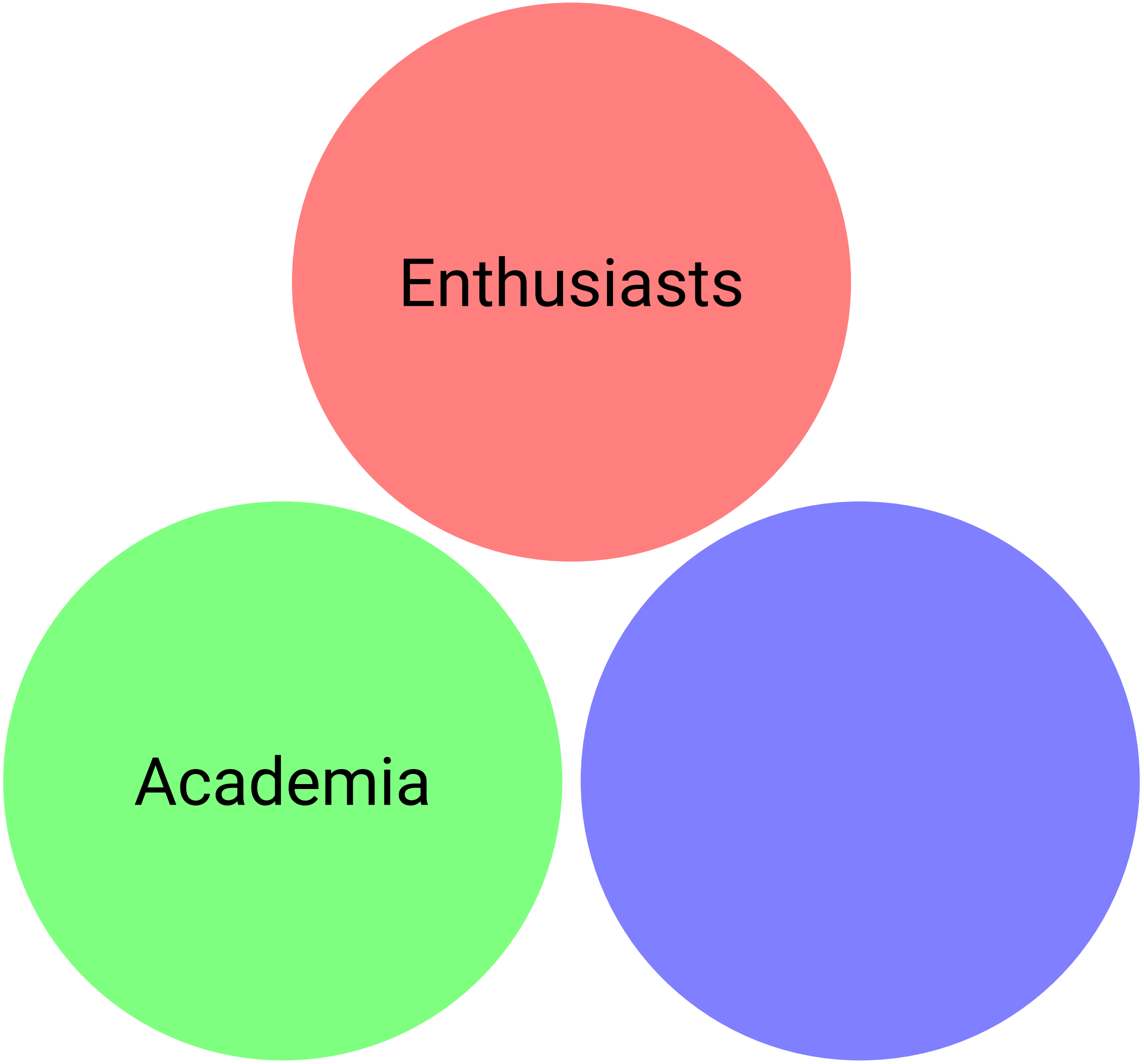
Academic Community

Operates primarily out of university research labs.

Full of professors, postdocs, PhD researchers.

Labor of love + overhead.

Striving for innovation.



Enthusiasts

Academia

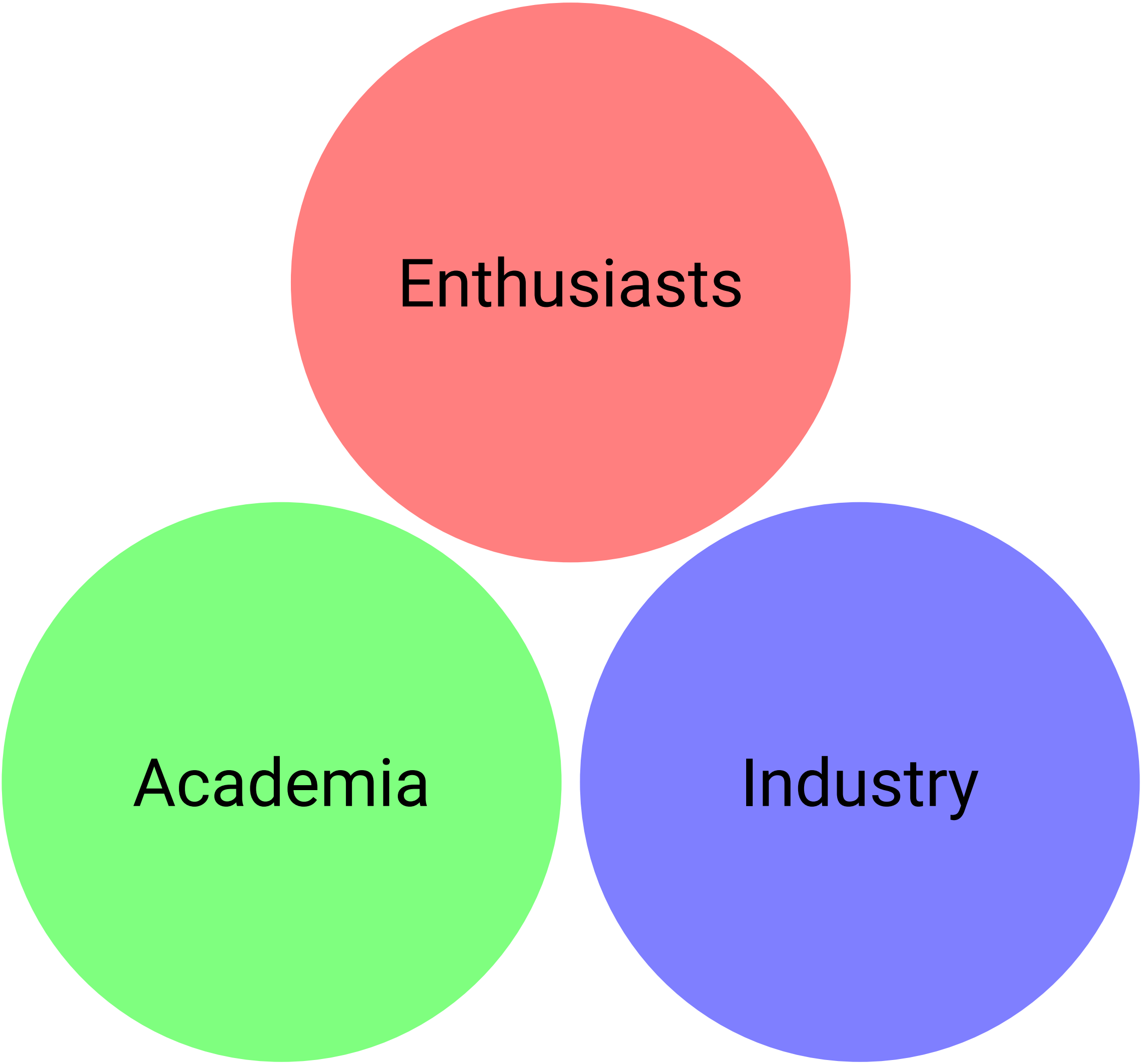
Industry Community

Operates primarily out of for-profit companies.

Full of brilliant engineers, hackers, etc.

Labor of love + profit.

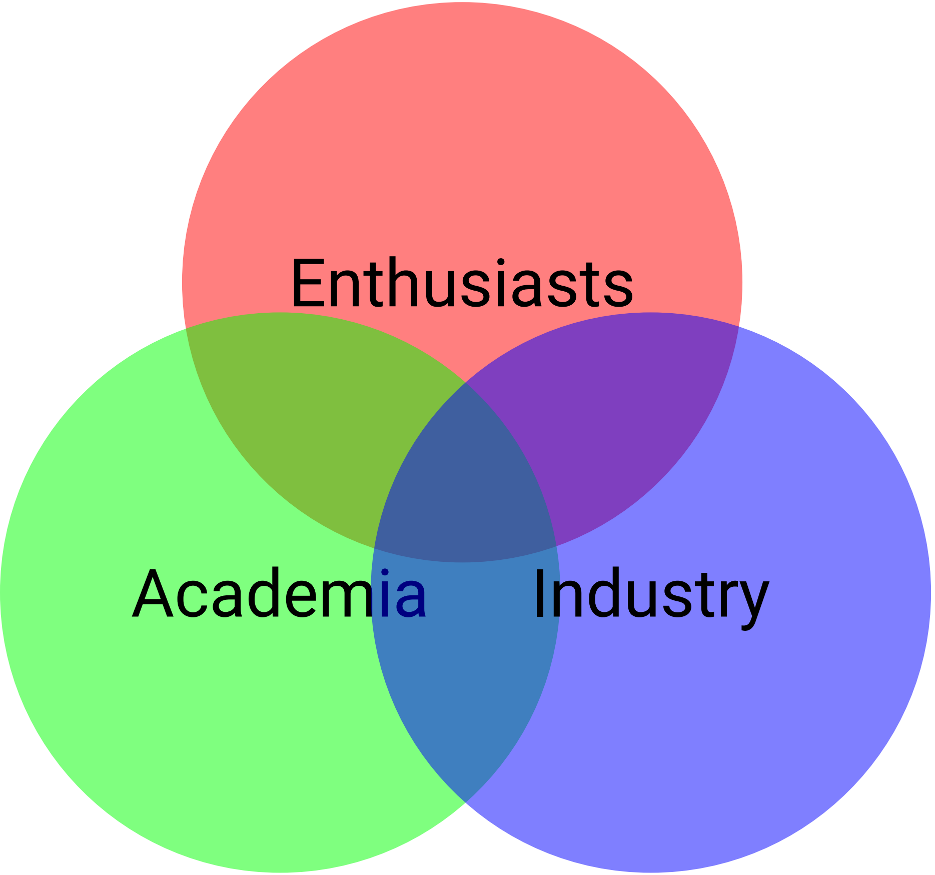
Striving for usefulness.

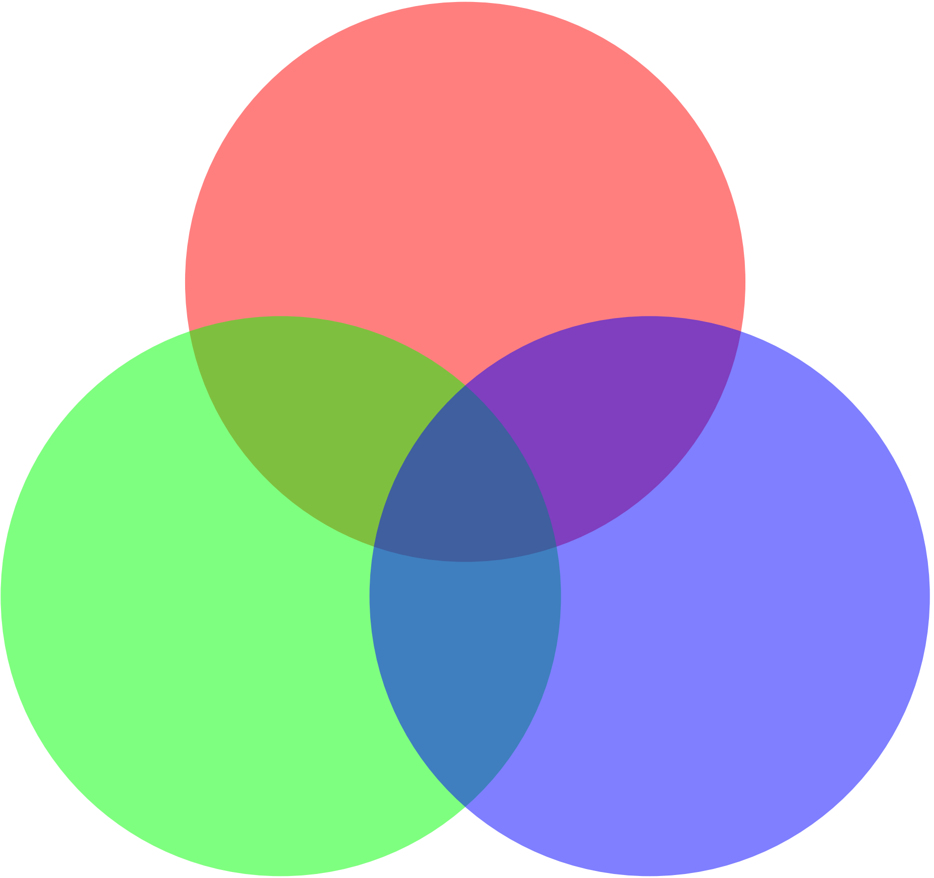


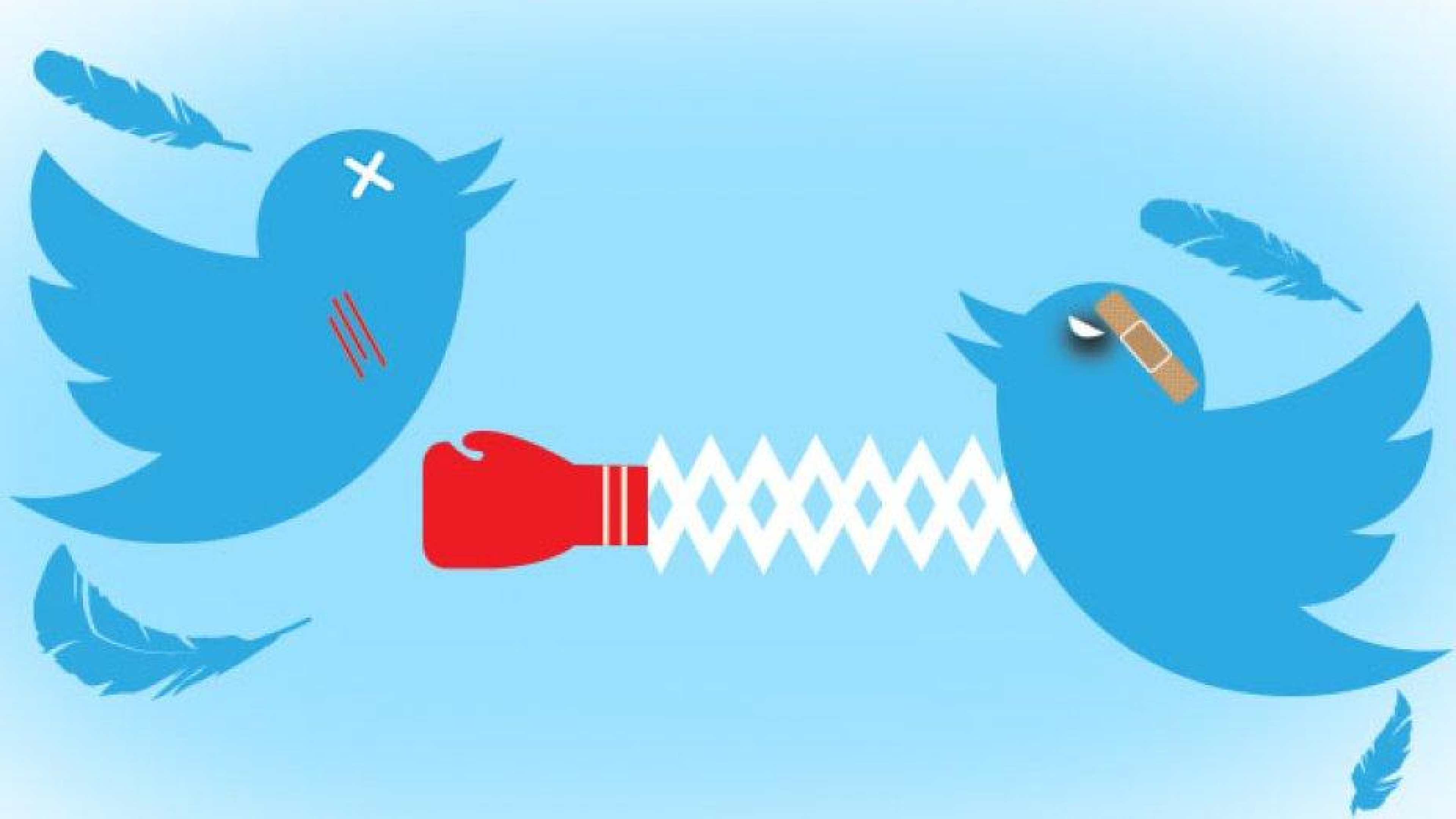
Enthusiasts

Academia

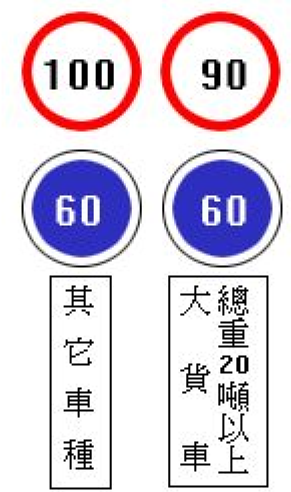
Industry


Enthusiasts
Academia
Industry





Why?



Why me?

SHELLPHISH

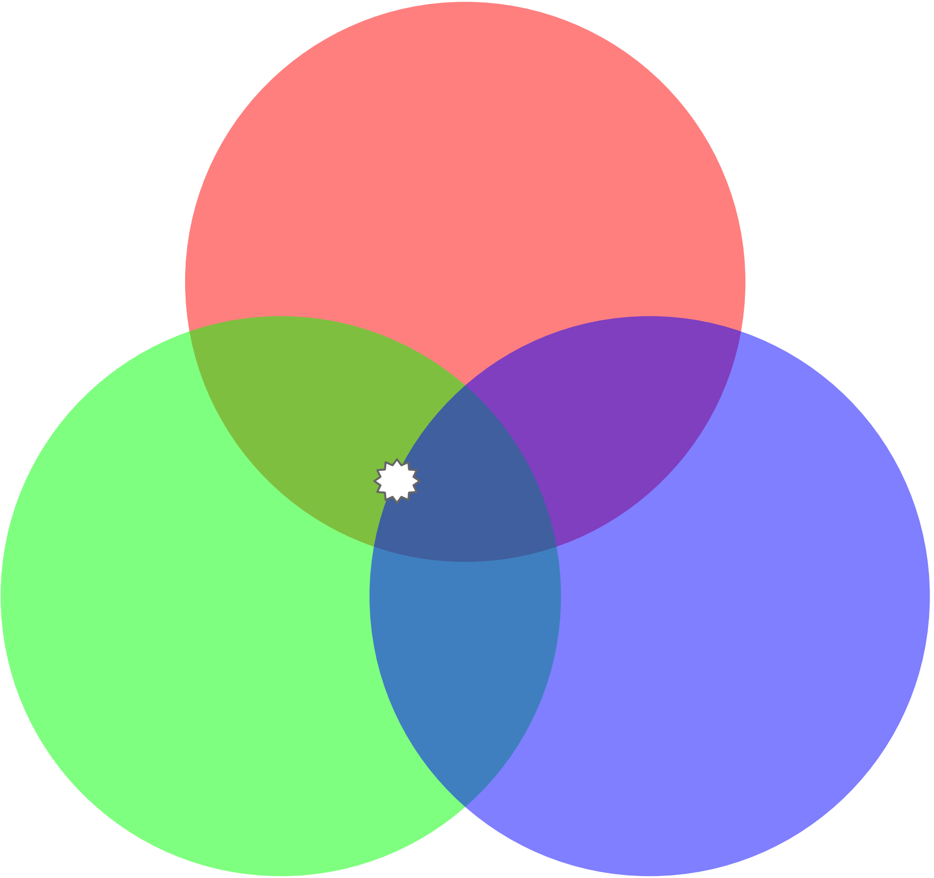
DEFCON

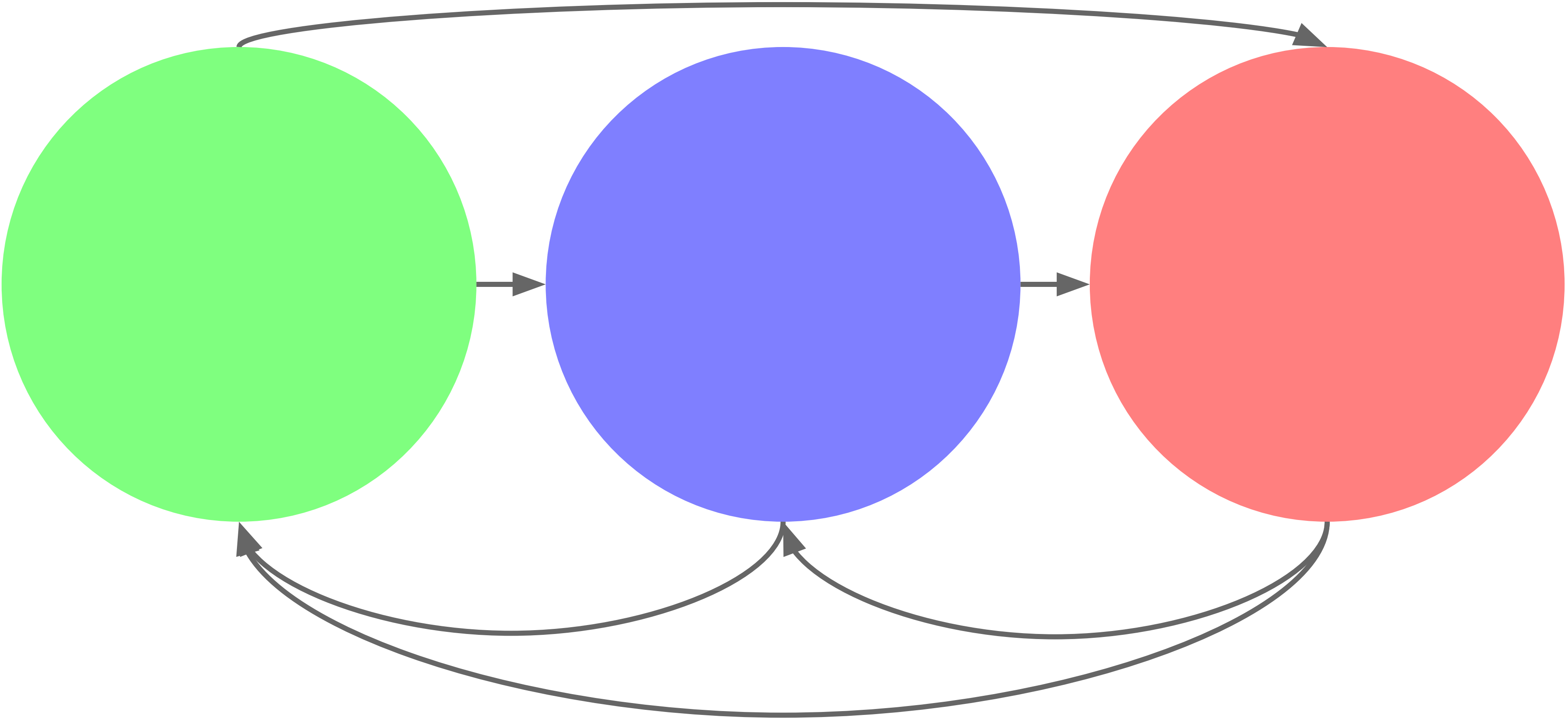
ARIZONA STATE UNIVERSITY • 1885 •

GREAT SEAL OF THE STATE OF ARIZONA ★ 1912 ★

DITAT DEUS

CGC





Example: LLVM

🟢 Created at UIUC in 2000.

🟢 Open-sourced in 2003.

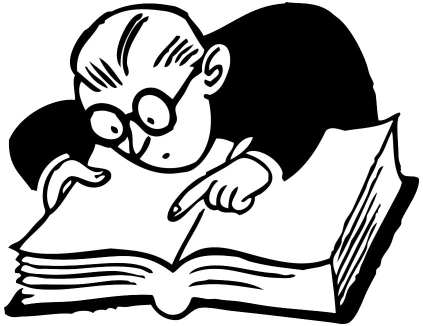
🔵 Adopted by Apple in 2005.

🔵 🟢 Continued use by academia and industry.

🔴 🔵 🟢 Nested success stories in spin-off projects!

- libfuzzer, KLEE, etc

Complications Arise



Research?

Academic meaning: invention, innovation, or understanding *(novel research)*.

Industry meaning: finding bugs in software *(vulnerability research)*.

Industry research...

- finding a new bug
- developing a new technique
- developing a new tool

- actionable results

Academic research...

- finding a new *class* of bug
- developing a new technique
- applying a technique in a new way

- demonstrating potential

Terminology differences — Effects

Academics *must* present at academic conferences to survive.

- constant need for novelty => short attention span
- papers become very hard to approach

Different goals of “research” limit interactions.

- little cross-attendance between academic conferences, industry conferences, and enthusiast conferences

This causes friction.

- Tweet wars (printf turing-completeness, Cloak&Dagger, symbolic execution)
- Duplicated effort.

Terminology differences — Solutions?

Better int

- USE
- USE
- CSA
- NDS

More cro

- inter

Assume

- Example: Cloak & Dagger

Come to the BAR!

Paper deadline: Dec 15, 2017
Workshop: Feb 18, 2018

Audience:

- Academics
- Industry
- Enthusiasts (CTFers and tool builders)

Explicitly includes a disucssion session!
www.ndss-symposium.org/ndss2018/cfp-ndss2018-bar

Industry prototypes...

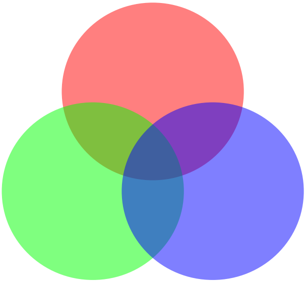
- written by professionals
- well-designed
- well-documented
- decently supported

Academic prototypes...

- written by graduate students under extreme deadlines
- minimalistic demonstration of concept
- completely unsupported or undocumented

Enthusiast prototypes...

- written by some random hacker
- often better-supported than academic prototypes



angr Observations

Documentation seems...

- *very* important for enthusiasts
- *moderately* important for industry people
- *slightly* important for academics

Functionality seems...

- *very* important for industry
- *moderately* important for enthusiasts
- *slightly* important for academics

(This is a bad feedback mechanism...)

Moving Forward

There is hope for angr!

- increasingly effective community support on slack
- perseverance by enthusiast community members
- continued adoption (and adaptation) by industry

But what about the general case?

- In the US: NSF Transition To Practice grants
- Google Summer of Code, Mozilla Open Source Grants, etc
- Idea: “community service” homework, such as documentation.

DECREE OS
(read/write/select/
mmap/munmap/
get_random/exit)

VS

The Real World

CAPTURE THE FLAG

CTF means different things to different people.

- an incredible test of skill
- an awesome opportunity to stay capable and relevant
- an irrelevant game where kids play with toys
- a waste of time

CTF takes time.

- hard for industry
- either ignored or actively discouraged by many professors!

CAPTURE THE FLAG — Solutions?

It is up to us in decision-making roles to support CTF.

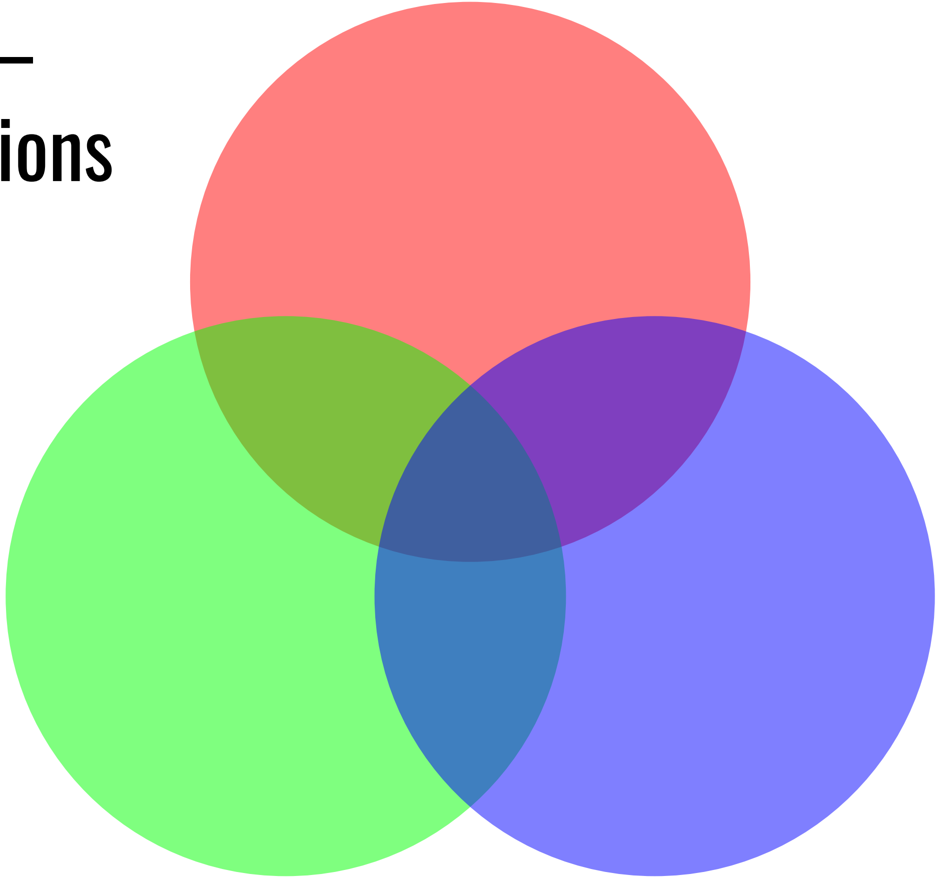
- CTF is a first-order priority at ASU.

More participants in industry and academia should strive for leadership positions in CTF.

Also, problem is resolving itself...

- academics noticed Shellphish in the CGC.
- CTFers dominating pwn2own, etc.

Conclusion — Overall Solutions



Talk with each other.

Learn from each other.

Do better with community integration.

Ask?

Yan Shoshitaishvili

yans@asu.edu

@Zardus

This presentation: https://goo.gl/jRiuAG

Join in on slack: http://angr.io/invite.html

If a grad school or visiting internship is something that interests you, let me know!

Communities have different motivations for collaboration.

- 🟢 Academics: reproducibility, impact, *but need better incentives*
- 🔵 Industry: profit motive
- 🔴 Enthusiasts: enthusiasm

Frustrations

Pull Request ghosting — deciding partway through the implementation of a pull request that your company wants to keep the modifications proprietary.

Workarounds?

- moving target (Linux kernel)
- GPL (other drawbacks)