

Industrial Research

(according to one guy)

Zak Fry

Goals for Today

- A (maybe slightly narrow) view into Industrial Research
 - Contrast with other industry jobs
 - What does the work look like generally?
 - Project overview for recent work
 - How might one get there?
 - Answer questions
-
- Try to provide info and mitigate "intimidation factor"!

Who is this talk for?

- Everyone interested in CS jobs
 - Not just CS majors! (e.g., data science, cognitive and behavioral science, physics, computer engineering, IT, technical writers, many others)
- Education levels: bachelors, masters, and PhD
- Folks interested in almost any type of job description (industrial research and development has most of them)
- Any level of familiarity with research/development/coding/languages/etc.

Me

- Undergrad BS in Computer Science (University of Delaware)
 - 3 years of undergrad research (I got lucky and fell into this – you can too!)
- PhD under Wes (University of Virginia)
 - Focus in automation in software maintenance and engineering
- Senior Scientist at GrammaTech Inc (11yrs)
 - Started on the commercial product team (mostly dev)
 - Now focus in runtime monitoring, cybersecurity, cognitive/behavioral cyber factors
 - Have done a bit of everything at this point!

What is Industrial Research/Dev?

- Creating software where commercial sales aren't the *prime* motivator
 - Solve problems key to government/industry/society
 - Tolerance for (some) failure, scientific process
- Often try to push the "wins" into commercial products
- Plenty of software development, but often different processes
- Responsibilities range:
 - Full development software engineer
 - Prototyping and building unproven systems
 - Shaping research programs, mostly "ideas"/management
- New code vs. maintenance/fixes – often the former, but depends!

GammaTech Inc



- Started 1989 out of Cornell University (Navy grant)
- Grew into half-research / half-commercial company
 - Try out ideas via government funding, transition to saleable products
- Peaked at 120 employees, many small research teams covering many topics
- Sold 6 years ago to private equity, research/commercial split into two companies, GT is currently ~30 employees
- **Things change!** This happens with all companies, but perhaps more with small/start-up companies

Industrial Research More Broadly

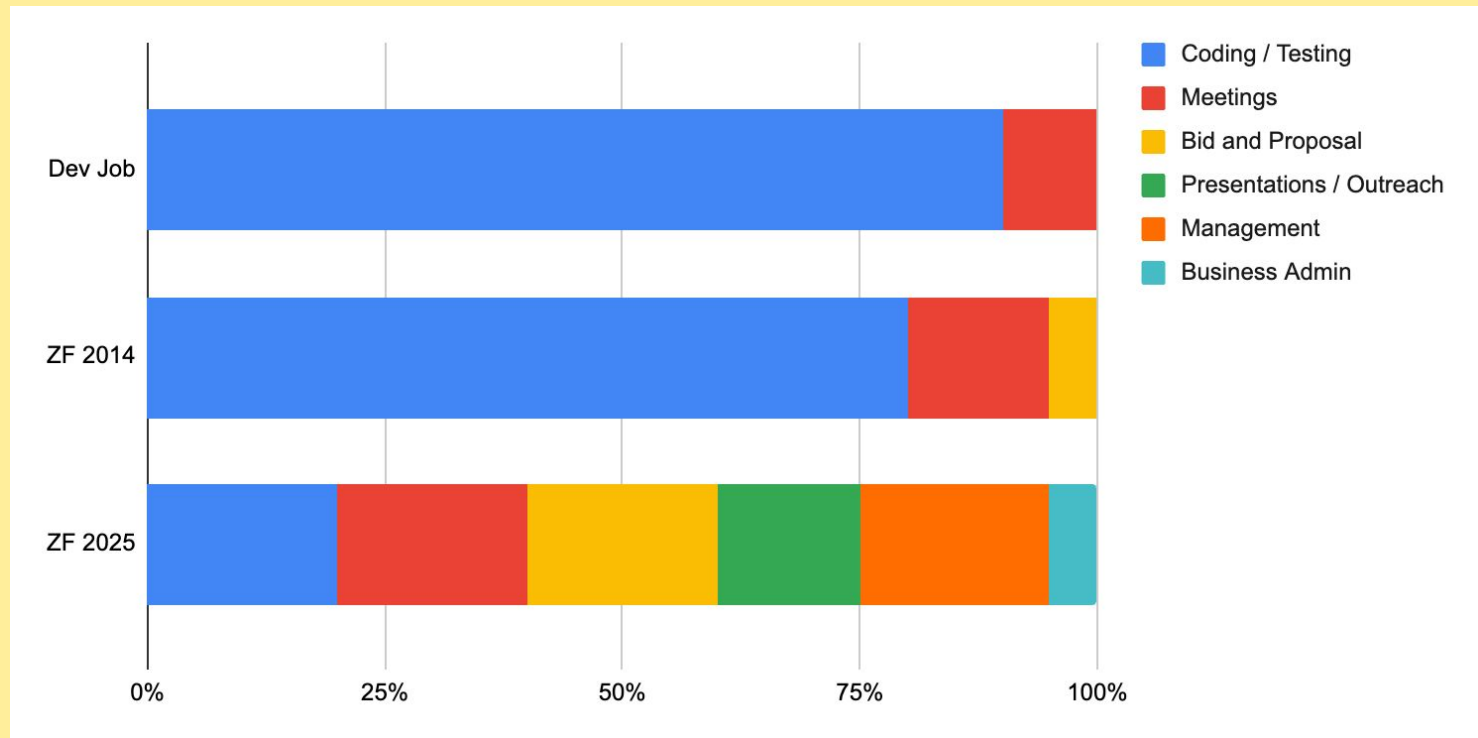
- Many sizes, shapes, focuses, funding models, job types, end-goals, etc.
- Too many axes/differences to list, but lots out there!
 - Likely a fit for anyone!



Differences/Considerations

- Company Size
 - Personal agency, creativity, stability, focus areas
- Company purpose/goals
 - Support internal products, drive cutting edge technique research, improve ubiquitous processes
- Ownership Model
 - Private, Private Equity, FFRDC/similar, Government
 - “Federally funded research and development center”
- Funding Model
 - Gov contracts, IR&D, support commercial tools
- Lifecycle / Follow-through
 - Long-term evolution, wild-west shotgun approach

Research vs. Development Jobs



Twist: industrial research can be a dev job!

Contrasted with Commercial Jobs

- These are only my opinions – your mileage may vary!

Pros:

- Exciting, creative, bleeding-edge work
- Capital-S Science, solving real problems
- Interactions with many other people (including across other domains)
- Agency in what I get to work on
- Builds a diverse skill set (beyond coding)

Cons:

- Go with the tides (“blockchain everything”)
- Often DOD-funded (people feel different ways about that)
- Funding is not always entirely stable (like now!)
- Not everything comes to fruition or is completed (“into the void”)

- It might sound like I’m putting down other jobs – not the case – just cheerleading for industrial research!

Typical Progression of a Project

- Find solicitation (or partner, gov-side champion, etc)
- Write proposal or pitch
- Get funded (percentage-wins – from 10-40%)
- Lots of contractual/admin work
- Period of performance (6mo – 5yrs+)
 - WRITE SOFTWARE
 - Other deliverable artifacts
 - Travel / talks
 - Demos / evaluations / red-teams
- Follow-on funding and/or transition

ReSCIND: Exploiting Cognitive Bias

CogVuln Specs:

Instr: X, Y, Z

Entity: A, B, C

Sensors:

X: try(A)

Y: access(B)

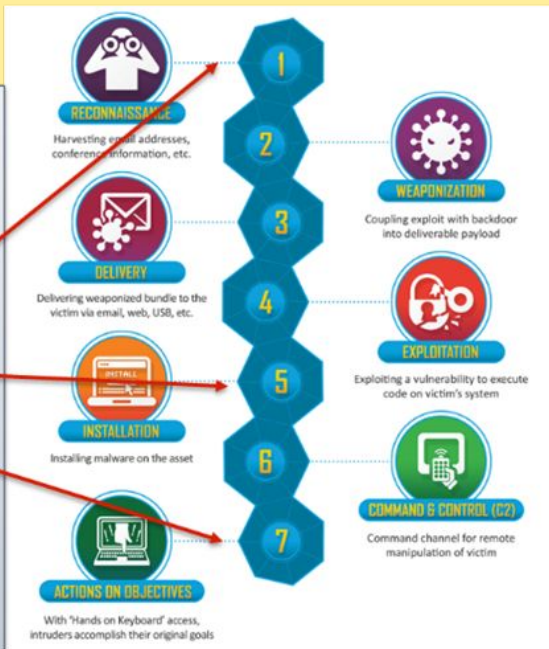
Z: exec(C)

Triggers:

R: add(A)

S: diff(B)

T: long(C)



Cyber Kill Chain

HSR Traces:

Attacker 1:

X: 3x ; 25s

Y: 10x ; 230s

Z: 2x ; 60s

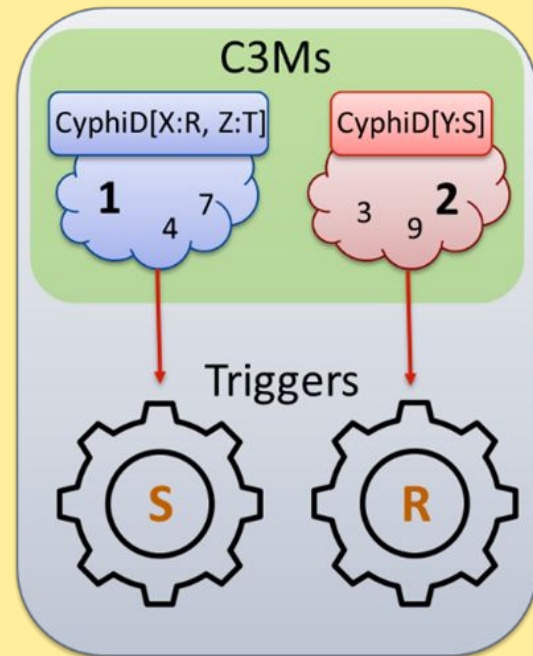
Attacker 2:

X: 15x ; 300s

Y: 4x ; 45s

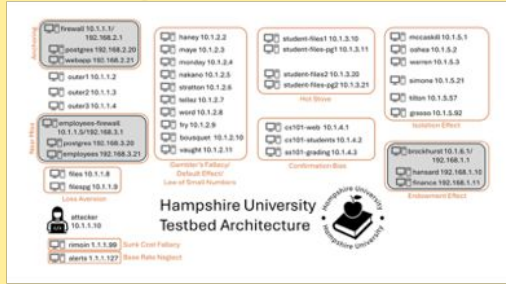
Z: 5x ; 90s

APhiD



ReSCIND Human Studies and Results

Cyber Methods



Cyber Testbed
Open world behavior

Established Methods

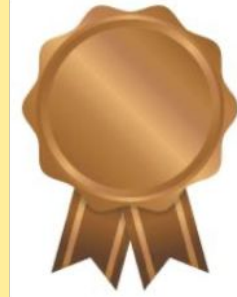


Fun Fair Experiments
Lab-style behavior

1	2	3	4	5
Very Slightly or Not at All	A Little	Moderately	Quite a Bit	Extremely
1. Interested				11. Irritable
2. Distressed				12. Alert
3. Excited				13. Ashamed
4. Upset				14. Inspired
5. Strong				15. Nervous
6. Guilty				16. Determined
7. Scared				17. Attentive
8. Hostile				18. Jittery
9. Enthusiastic				19. Active
10. Proud				20. Afraid

At the beginning, all the participants went through the consent form and initial assessment questionnaire to check their suitability for the study. The participants recorded their feelings according to the proposed scale and rated

Table 1. The participants



Canonical Surveys
Self-report instruments

ReSCIND Human Studies and Results

The screenshot displays the ReSCIND interface with three main components:

- Task Tracker:** Shows 'Total Time Remaining: 5:57:08' and 'Objective Time Remaining: 0:57:32'. It includes buttons for 'Read Mordor's SSH Keyring', 'Idle', 'Working', 'Completed', and 'Abandoned'. Below these are buttons for 'Objectives', 'Help and Info', 'Input Flag', and 'User ID'.
- Objectives Panel:** Contains a table with the following data:

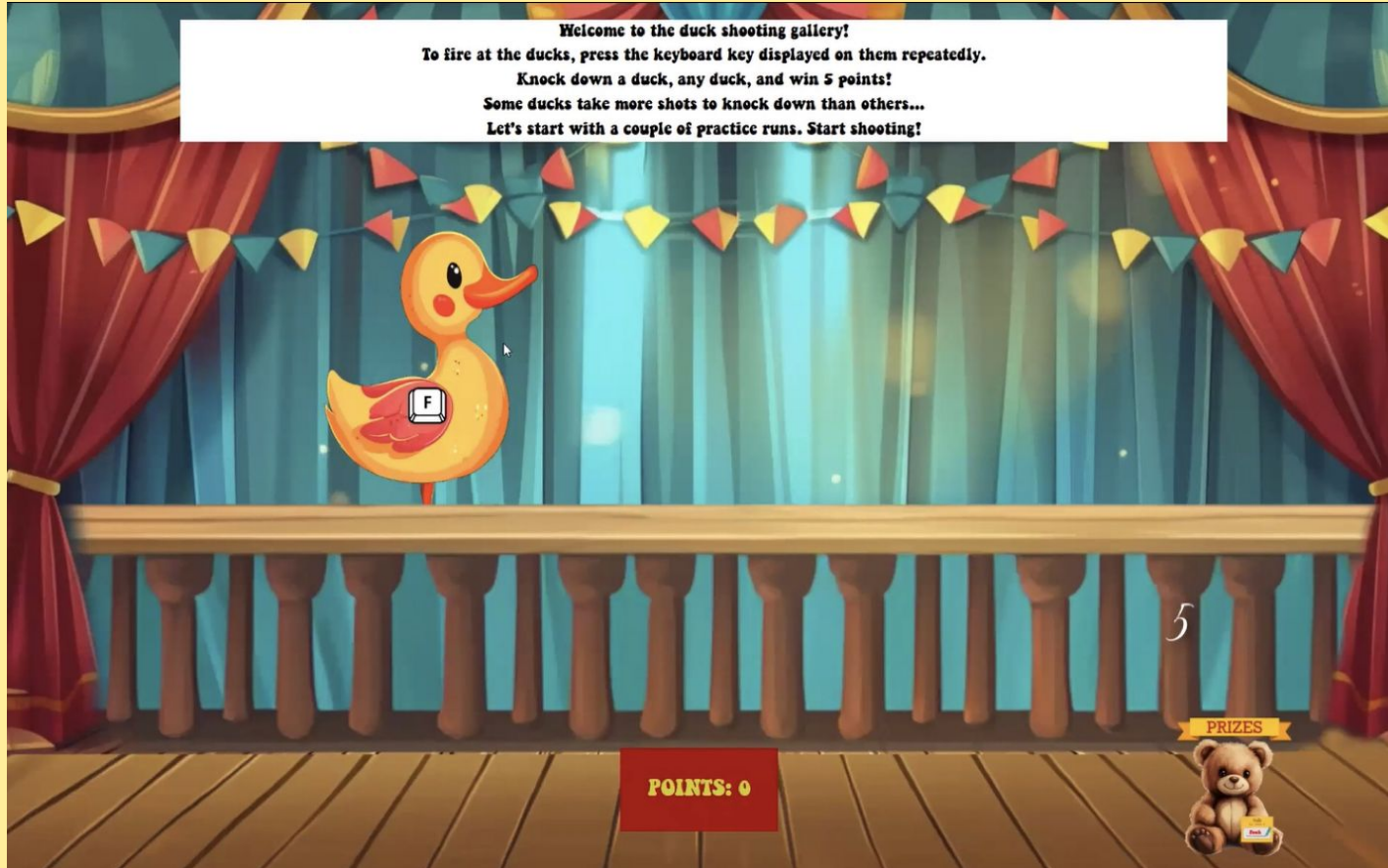
Index	Name	Description
1	Read Mordor's SSH Keyring	Suspicious traffic has been detected originating from host mordor. Please locate the "known_hosts" file for user mordor@mordor. Enter the names and IP addresses of any hosts contacted by mordor for a \$20 reward. You may connect to mordor via ssh using username "mordor" and password "WhereTheShadowsLie".
- Terminal Window:** Shows the command prompt for 'attacker@attacker: ~'. It displays system information, including management and support links, and a list of programs included with the Ubuntu system. It also shows the output of the 'ls' command in the 'known_hosts' directory, indicating that access to known hosts is blocked and that the 'cat' command is not permitted.

TASK: Identify a critical file on the target machine (impossible).

MANIPULATION: optional series of easy but time consuming tasks as a primer

POST-TRIGGER SENSOR: willingness to spend time on impossible task despite no obvious progress

ReSCIND Human Studies and Results

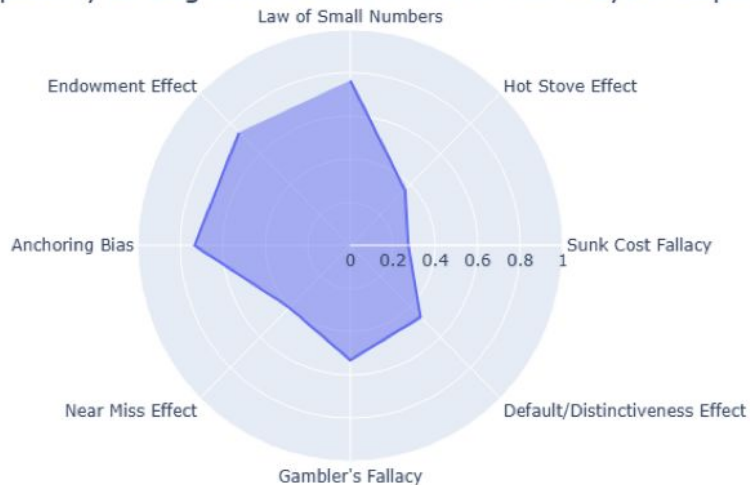


ReSCIND Human Studies and Results

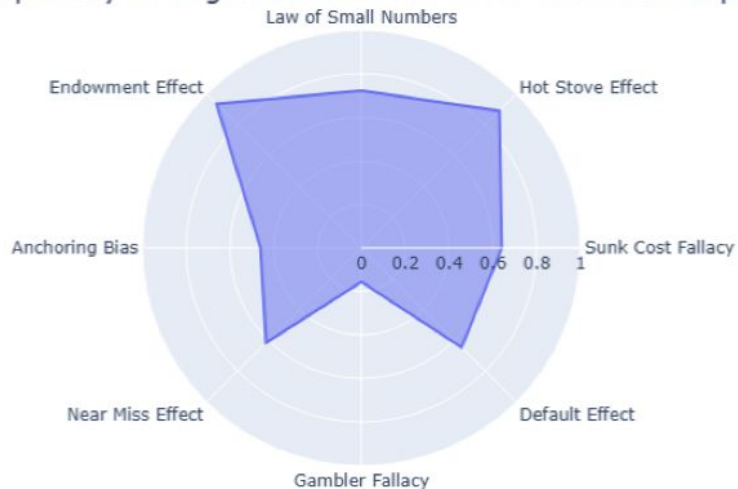
Bias	Scientific robustness	Ease of implementation	Defensive usefulness	Overall rating
Gambler's Fallacy/Hot Hand Effect	★★★	★★☆	★★★	★★★
Sunk Cost Fallacy	★★★	★★★	★★★	★★★
Default/Distinctiveness Effects	★★☆	★★★	★★★	★★★
Hot Stove Effect	★★★	★★☆	★★★	★★★
Cognitive Load Effect	★★☆	★★★	★★★	★★★
Law of Small Numbers	★★★	★★★	★☆☆	★★★
Framing Effect	★★☆	★★★	★☆☆	★★★
Anchoring Bias	★★☆	★★☆	★★☆	★★★
Near-Miss Effect	★☆☆	★★☆	★★★	★★★
Mere Exposure Effect	★★☆	★★☆	★★★	★★★
Base Rate Neglect	★★☆	★★★	★☆☆	★★★
Endowment Effect	★★★	★☆☆	★☆☆	★★★
Confirmation Bias	★☆☆	★★☆	★☆☆	★★★
Legend:	★☆☆ - low ★★☆ - medium ★★★ - high			

ReSCIND Human Studies and Results

Susceptibility to Cognitive Biases in Silver Tier - Cyber Experts



Susceptibility to Cognitive Biases in Silver tier - Non-Experts



ReSCIND Human Studies and Results

- Differences with canonical research
- Differences between Gold/Silver/Bronze
- Differences with other teams' results
- MANY research questions remain!
 - How do you cover ALL cyber activities?
 - How do you perturb the system in ways that are *effective* but not *obvious*?
 - How do you ensure you're not negatively affecting normal users?
 - Why do this at all, rather than just "kick them off"?

Software Engineering in Research

- Ranges from formal (e.g., agile) to “the wild west”
 - Prototyping / proof-of-concept
 - Dev, testing, packaging/deployment, feedback
 - Demos and customer interactions
 - Both keeping people happy and future pitching
 - QA, documentation, usability, expand use cases
-
- Like academic assignments, there's NEVER enough time to do everything the “right” way – “good enough” is often the reality

Non-SE responsibilities in Research

- Mentoring
 - Customer interactions
 - Pitches and outreach
 - Reporting/Documentation
 - Planning/Strategy/Management/Admin
 - Proposals
 - Business-side activities (*shudders*)
-
- These vary widely depending on job/seniority/project
 - Documentation and reporting is particularly important as you often come back to things later

Anecdotes and Challenges

- Major pivots when you hit full show-stoppers
 - KATE vs. DynamoRIO
- Unexpected failures in critical deployments
 - ReSCIND failure in AWS, not locally
- “Nothing” works in deployment (portability)
 - Even Docker can’t save you sometimes!
- Unexpected menial tasks can be huge blockers
 - IRB/HRPO approval on ReSCIND (AUS vs US)
- Fundamental concepts can be non-starters
 - Automated program repair / binary rewriting
 - Overhead and third-party tooling (DynamoRIO)

Personal Considerations

- Work/life balance – a mixed bag
 - There are very few times (but not 0) where I've had to work overtime
 - "Work when you want" and "self-paced" generally
- The "great reset" – projects (like classes) always end!
- Compensation generally tracks commercial jobs
 - Growth potential may be "at least slightly higher"
- Stability is "as good or better" than commercial jobs
 - The past year or so has been understandably chaotic, but previously we were almost always hiring

How might one get into this?

- Undergrad research!
 - though not strictly required
- Grad school enables a certain path
 - also not strictly required
- Knowing which companies do this
 - Gov agencies like to publicize their work, just search around – or ask someone like Wes!
- Internships are a great stepping stone and way to test the waters in a low-commitment way

Q&A

Any questions? Ask away!

zak.p.fry@gmail.com

