

Abstract geometric lines forming various polygons and shapes, primarily in the upper left and center of the slide.

EMOTIONAL SUPPORT FOR “48 HOURS OF FAILURE”

(Dr?) Alex Dean Cybulski
Research Security Specialist
University of Toronto

ABOUT ME

Security research specialist
University of Toronto's Information Security Division
Design strategy & policy for securing high performance computing clusters

Also:
Sociologist studying: information security, hacker culture and games
Former prof @ the University of Toronto Mississauga: Hacker Culture
CTF Team: the 212s
Documentarian: Cyberwar on Viceland (2016)

alexander.cybulski@utoronto.ca
@adcylbulski on infosec.exchange the and the evil bird platform

MY RESEARCH

3 In-Person CTF Competitions

U.S. & Canada

200 hours of observation

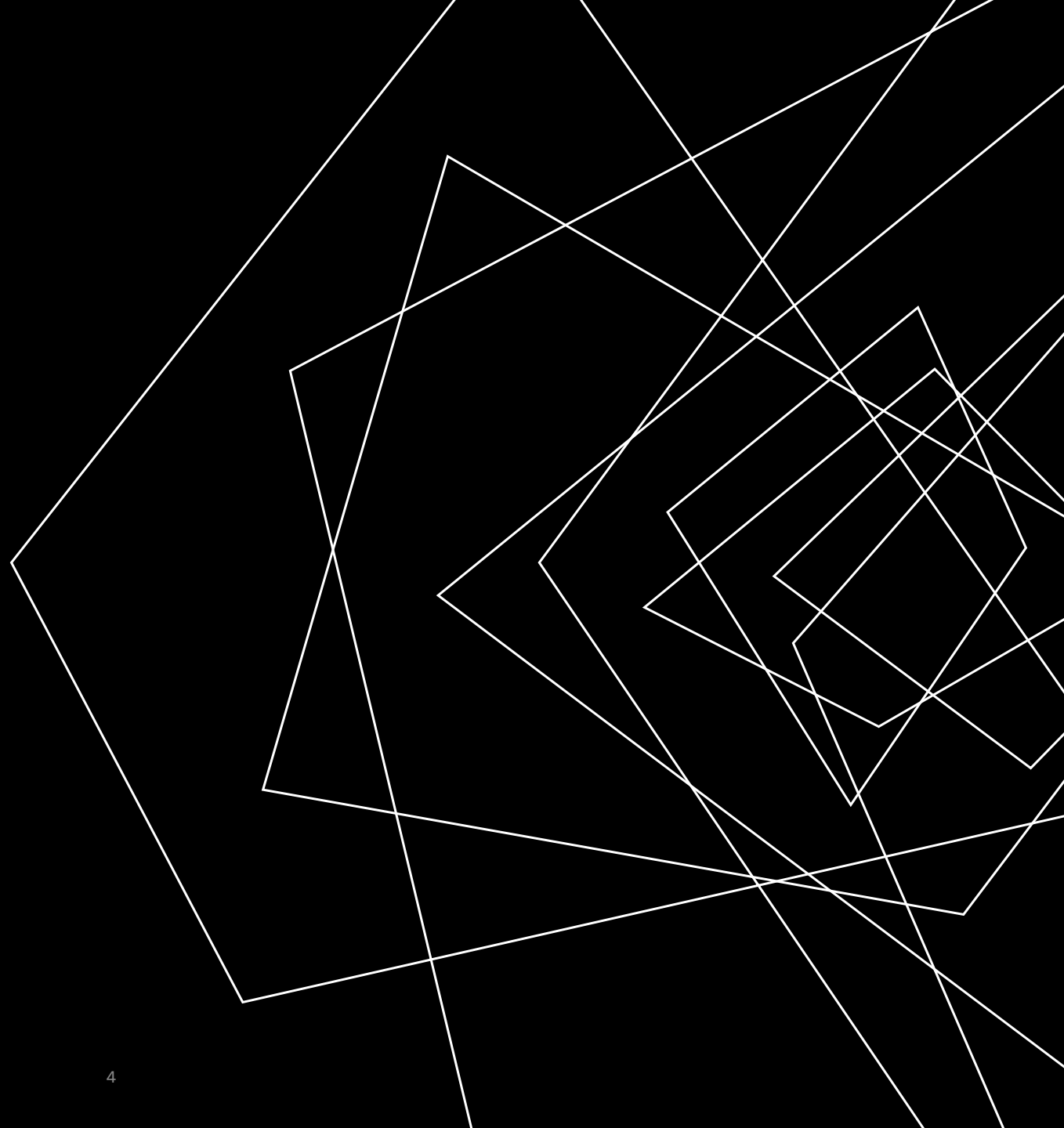
100 hours of interviews

w/ CTF Designers & Players

230-page research report

Sim Cyberpunk: Serious Play, Hackers and Capture the Flag

WHY DO PEOPLE PLAY IN CTFS?





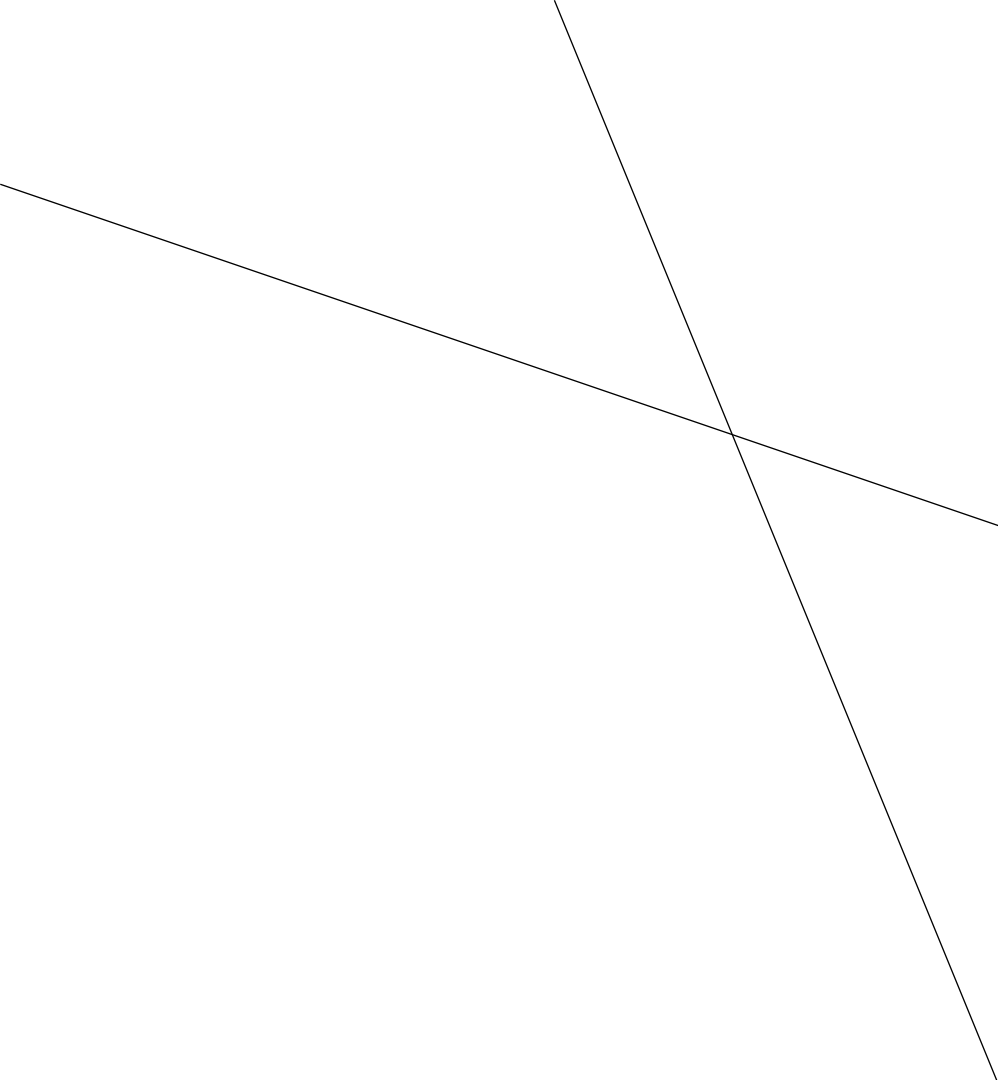
I DIDN'T LEARN ANYTHING NEW

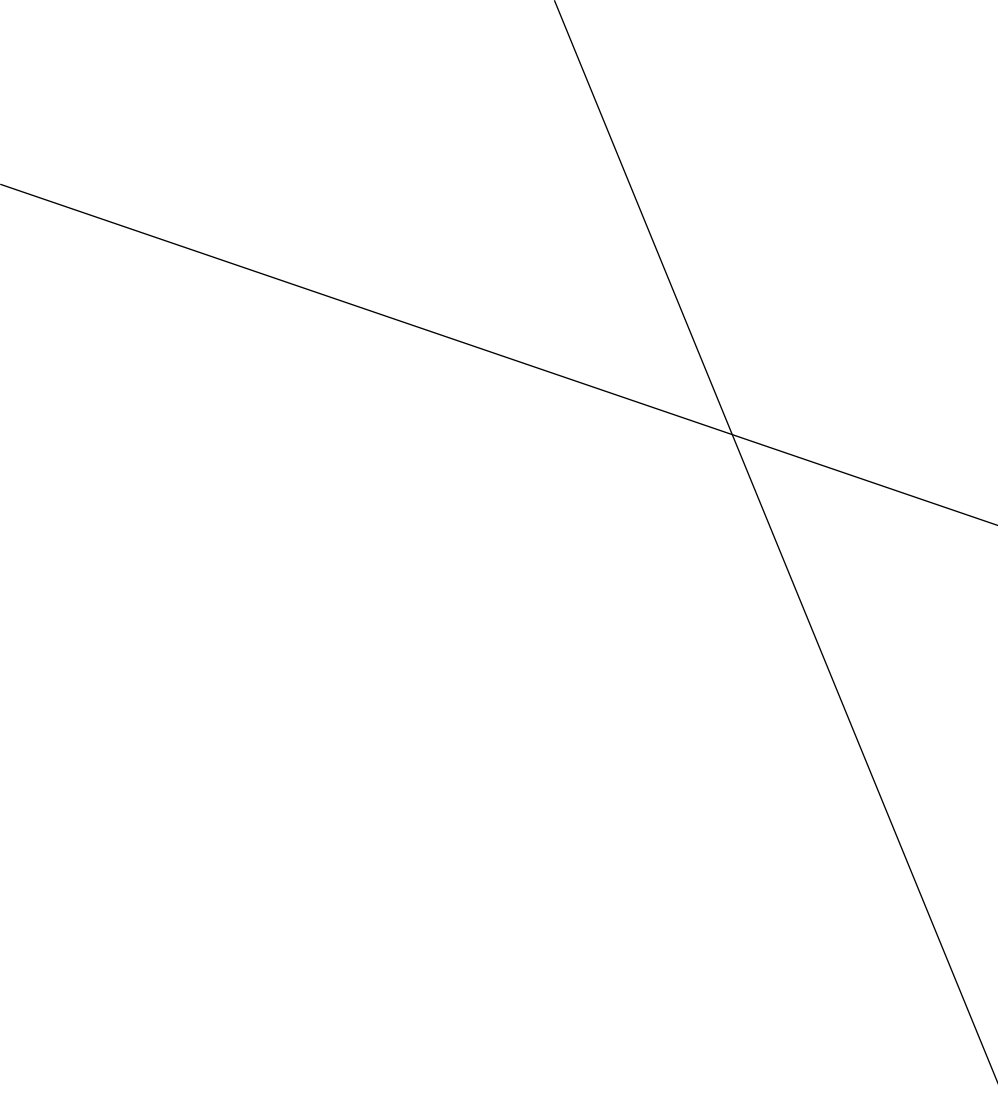
I DON'T THINK CTFS ARE FUN

I SPENT 8 HOURS SETTING UP A #@
\$ LINUX ENVIRONMENT ON MY LAPTOP AND
DIDN'T MEET ANYONE HIRING

I PLACED LAST IN THE DEFCON CTF
QUALIFIER



- 
- Two thin black lines intersect on the left side of the slide. One line is horizontal, and the other is diagonal, crossing it from the top-left towards the bottom-right.
- I love CTF
 - But it's easy to quit when your first competition goes poorly.
 - CTF is so frustrating one of my interview subjects, Pawel, referred to playing in one as “48 hours of failure.”
 - My goal with this talk is:
 1. To teach you the stories that the cybersecurity / hacking community tells itself about CTF
 2. To help you push through failure & frustration & keep playing CTF

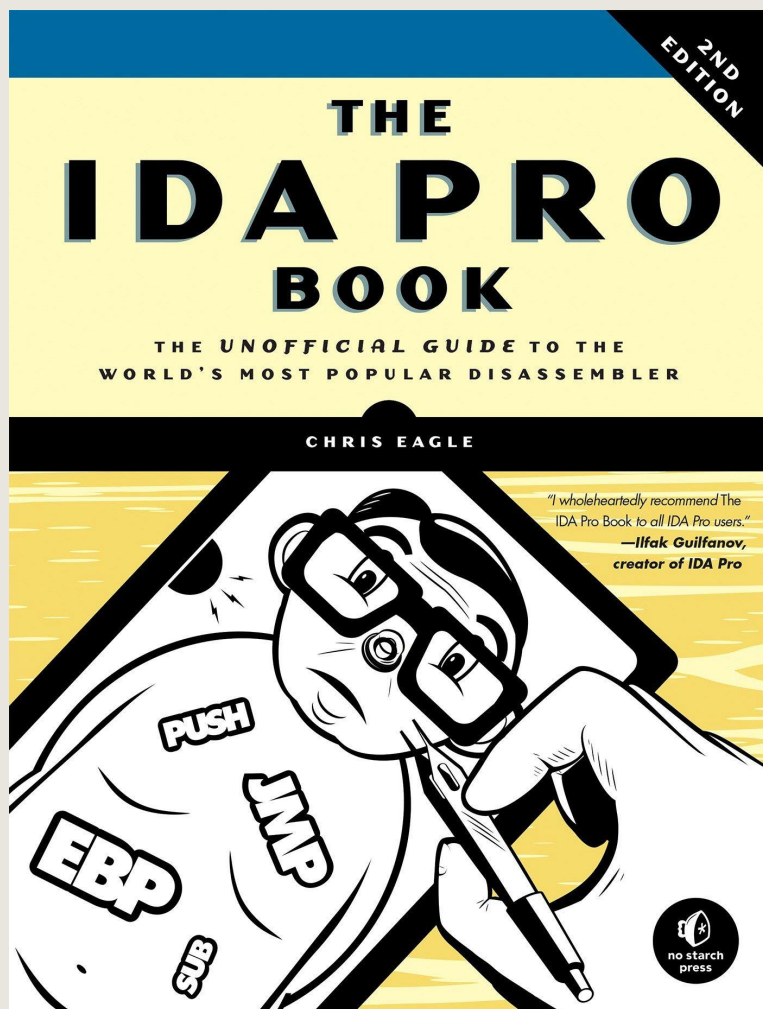
- 
- Learning, having fun and networking are stories we tell ourselves about games. In sociology we often say that play is “rationalized” we do it for a reason – we have stories for why, how and to what end we do certain things.
 - CTF is “serious play” which means that we have often rationalized doing something (hacking, coding, cybersecurity) that is laborious (like work), but for a specific reason (leisure, socializing, professionalization)
 - When those stories we tell ourselves about doing something don’t line up with our experiences doing that thing AND when play is so much like doing work, we usually stop
 - Why bother?



“FUNDAMENTALLY, YOU'RE WASTING YOUR TIME WHEN YOU COULD BE READING PAPERS [LAUGHS HARD]. AND THAT'S A THAT'S A FINE WAY OF APPROACHING IT TOO.

-Tony (plays in 2-3 CTFs a month)

WHY ARE CTFs ARE A POOR LEARNING ENVIRONMENT



- CTFs are fundamentally competitions
 - Winning is inherently rivalrous
 - No hints
 - Time-limited
- The expectation is that most players will come with the knowledge they need to win
- “[CTF] organizers seldom offer to prepare competitors for the event... it’s incumbent upon them [players] to acquire the skills necessary to compete well” (p. 69) – **Chris Eagle**
- A survey of 15 “vulnerability discovery” exercises (CTFs) found that almost none satisfied basic pedagogical goals (Votipka, Zhang & Mazurek, 2021)
- Challenges are heuristic
 - They require us to know, or figure out something for ourselves

CTF HISTORY

- The term CTF was coined in 1996 at the hacker conference Defcon
 - But Hackers have always been making games out of breaking security controls
 - CTF emerges out of a culture known as the computer underground – pirates, hackers & phreakers (phone hackers)
 - The original CTF was more like a skateboarding contest than a game (no points, no rules, no scoreboard)
 - Started out as a sideshow for a LAN party
 - CTF was created to let hackers show off their skills
 1. To impress their peers
 2. And not get arrested in the process
- CTF was created a time when there weren't a lot of jobs (1990s) in information security
 - So CTF isn't necessary about work and/or learning
 - It's about impressing people



CTF CHALLENGES ARE DISCURSIVE



- CTF challenges are created by subject matter experts
- These experts think that the problem at the heart of the challenge: the method/methodology for vulnerability identification is interesting or meaningful
- For the most part CTFs use ‘constructed’ vulnerabilities that do not exist in the real-world
 - If the problems were identical to real-world ones there would be a lot of tools to automate their exploitation (Metasploit, for example)
- So solving a CTF challenge involves analyzing problems using real-world methods, methodologies and software

CTF CHALLENGES AS COMMUNICATION

- “CTF is really good to get you to learn about problems that need solving” – Tim
- CTF challenges are about applying & demonstrating problem solving skills & techniques
 - Demonstrating the intellectual capital of players
- To the things that other people think are meaningful (social capital)
- In playing, winners demonstrate expertise, they demonstrate cultural capital – their ability to navigate knowledge
- So playing in a CTF is about translating knowledge through meaningful problems to create recognition

CTFS AS NAVIGATION & PRACTICE

- CTFs are a check on your knowledge of contemporaneous problems
 - Essentially your ability to navigate all of the knowledge that is freely produced and circulated through hacker communities
- CTFs are a bad place to acquire new knowledge
- But they are great for refining existing skills:
 - “It's just learning, **getting better, getting better at all those exploitation [and] reversing tasks.**” – **Holden**
 - It's a “style of thinking” where” the tools and skills you use to solve the problem tend to be the same ones you would use to solve a real-world problem.” - **Jonah**



TAKEAWAYS

CTF is a game about cybersecurity, sure, but *really* it's a form of communication, which translates local knowledge (intellectual capital) into recognition (cultural capital) and expertise (social capital)

CTFs aren't great for traditional learning (developing new skills)

But they are good at refining skills (practice), understanding contemporaneous skills and building a culture of cybersecurity for learners.

- This doesn't mean if you want to learn you should quit and go home!
- Just don't be discouraged if/when you struggle! That's normal.



THANKS & HAPPY HUNTING

Alex Dean Cybulski

alexander.cybulski@utoronto.ca

@adcylbulski

www.adcybulski.com

WHO THIS TALK IS FOR

- This talk assumes you know nothing, or a bit about CTF
 - But want to know more
 - You want to develop cybersecurity / hacking skills
- I provide some critiques of CTF
 - But I do that to help you understand what you'll get out of participating
- My arguments are made based on observation & other people's experiences
 - Blended with a little teaching theory
 - But it's worth saying: your experience may vary!
- The talk is largely non-technical
 - But CTF is mostly non-technical
 - Sociologists define things, they help us create meaning and understand patterns
 - Terms from economics, psychology and even gaming are the product of ideas sociologists created

