



HACKING



YOUR SECURITY CAREER!





0 1 1 0 1 0 0 0
0 1 1 0 1 0 0 0
0 0 0 1 0 1 1 0
0 1 1 0 1 0 1 1
0 1 1 0 1 0 1 1

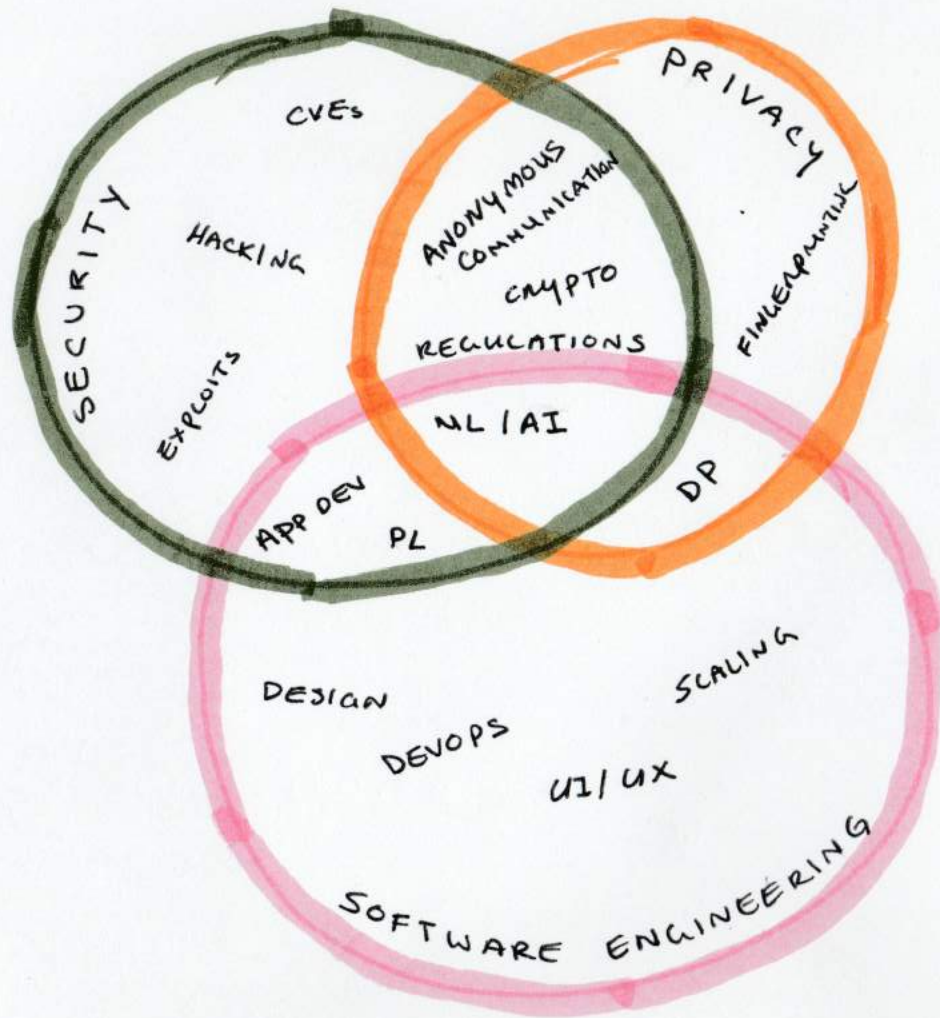
* HACKER VOICE *
I'M IN.

ABOUT ME:

- 
- PAST: WATERLOO CS (GRADUATED 2020)
 - CURRENTLY: SENIOR RESEARCH ANALYST
@ UCHICAGO
 - FUTURE: SECURITY / PRIVACY PHD STUDENT
- 



WHAT IS
SECURITY
? ? ?



★ SECURITY ISN'T AN ISOLATED FIELD !

INJECTION

STACK OVERFLOW

CANARIES

EXPLOITS

ZERO DAY

PUBLIC KEY CRYPTO

HACKING

VULNS


MALWARE

MALWARE

SUPPLY CHAIN

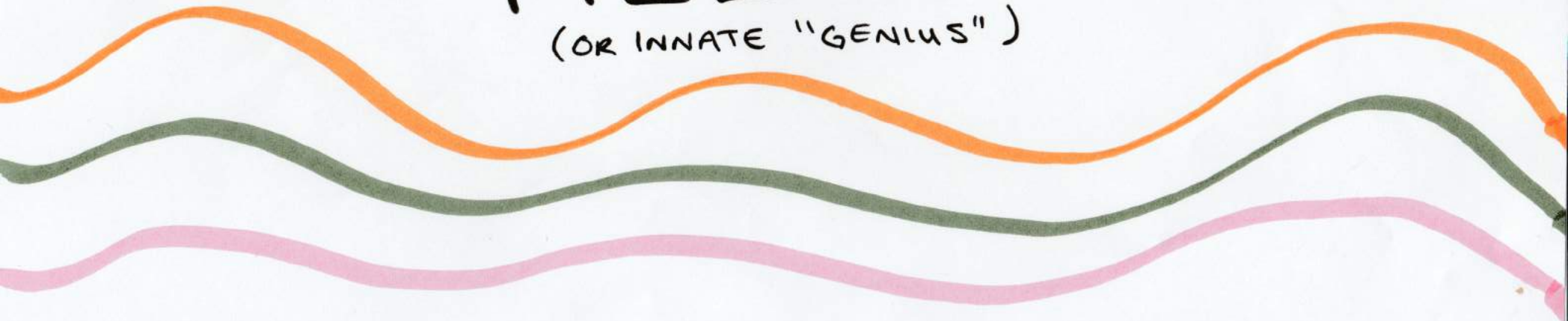
DEFCON


GDPR



EVERY
JOB
IS A
SECURITY
JOB

NO
REQUIRED
HEIGHT
(OR INNATE "GENIUS")



Three thick, hand-drawn diagonal lines in orange, pink, and green run from the top-left towards the bottom-right of the page. The orange line is the topmost, followed by the pink line, and then the green line at the bottom.

MY PATH*

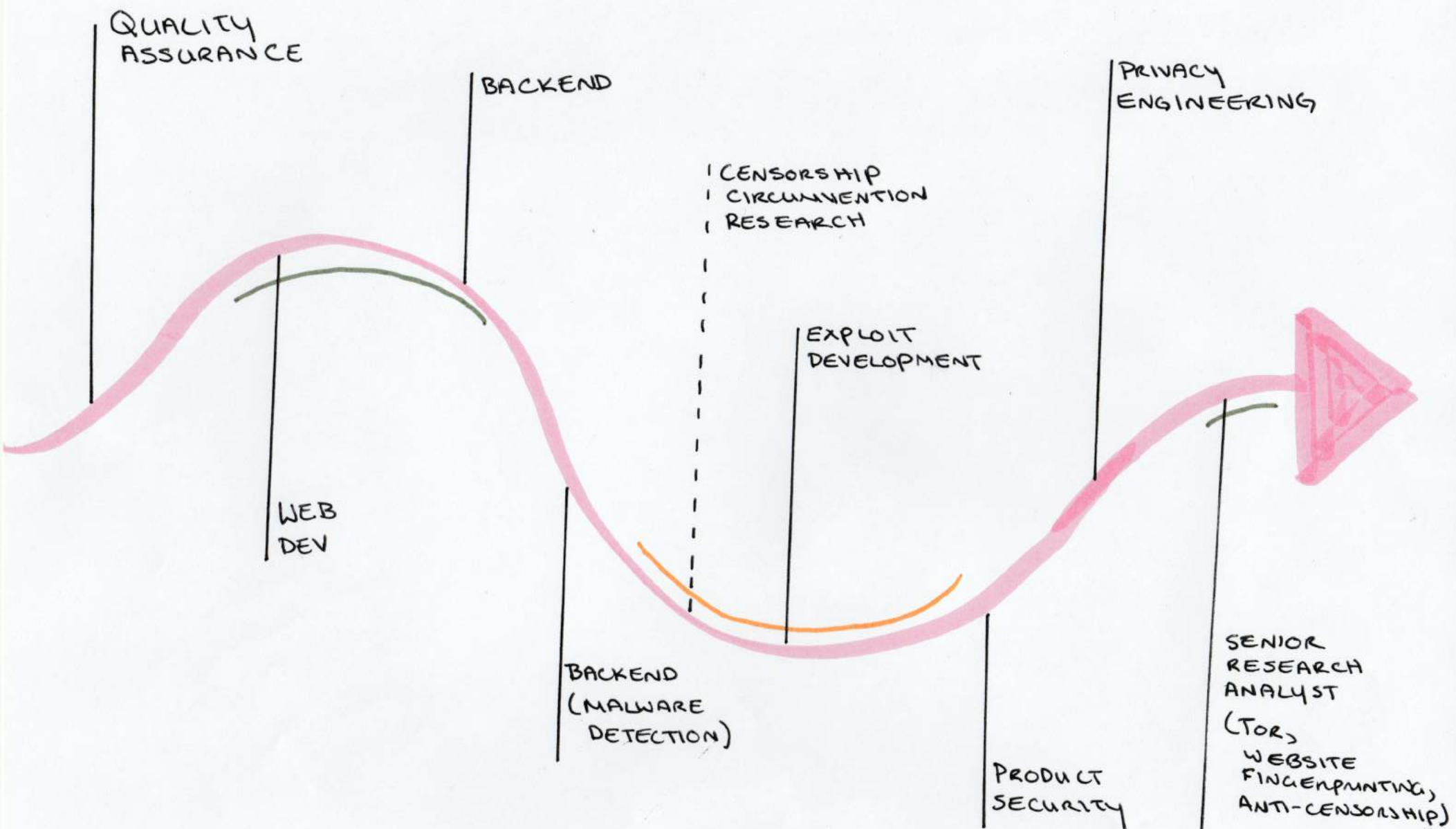
* THERE IS NO "CORRECT"
WAY, YOUR JOURNEY WILL LOOK
DIFFERENT, BUT HOPEFULLY THIS
SERVES AS A GUIDE OR
EXAMPLE 😊

I STARTED WITH ZERO

(ZILCH, NONE, HEAD EMPTY)

KNOWLEDGE . . .





QUALITY ASSURANCE

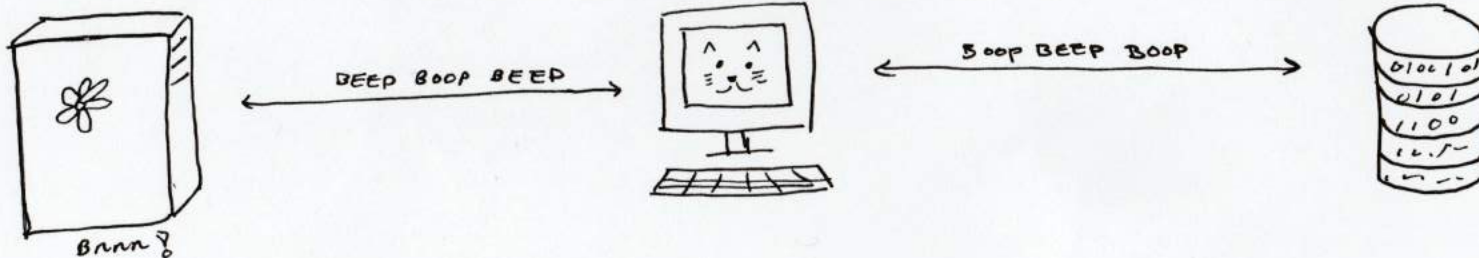
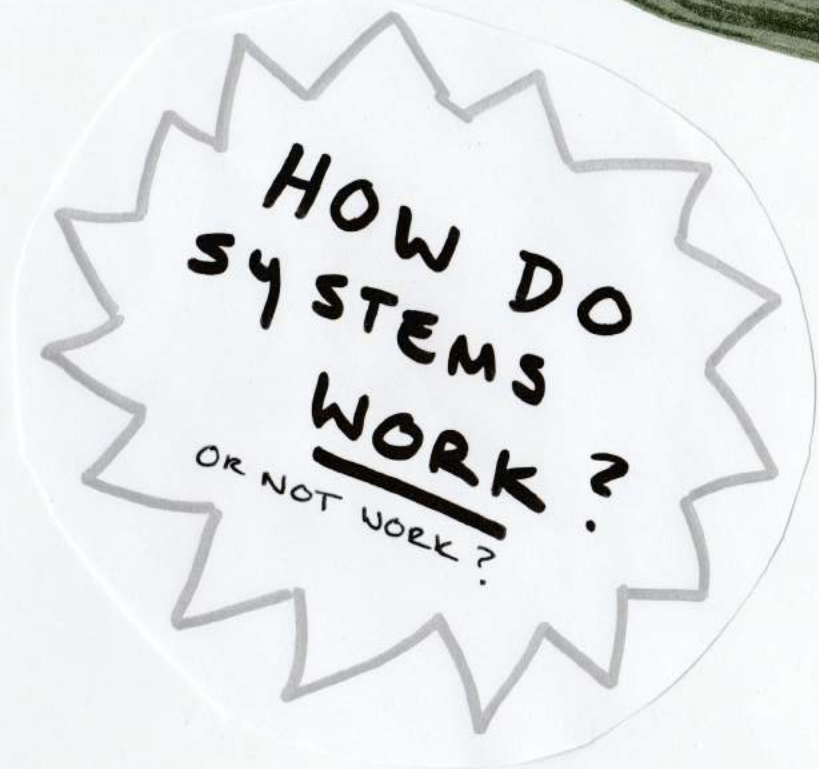
- How do you find bugs?
- What bugs are really common?
- What avenues are open for someone to mess with a system?

WEB DEV

- How are systems built?
- What frameworks are commonly used?

BACKEND

- What makes a system reliable?
- How do certain languages enable particular exploits?



MALWARE

- How do users get infected / fall victim to attacks and exploits?
- How are attacks detected?

EXPLOIT DEV

- How do hackers (good or bad) find attacks?
- Are new attacks common?
- How do I responsibly disclose?
- How do I effectively communicate?

PRODUCT SECURITY

- What security/privacy issues happen at scale?
- What regulations have to be met?
- What are the software engineering problems that need to be solved?

PRIVACY ENGINEERING

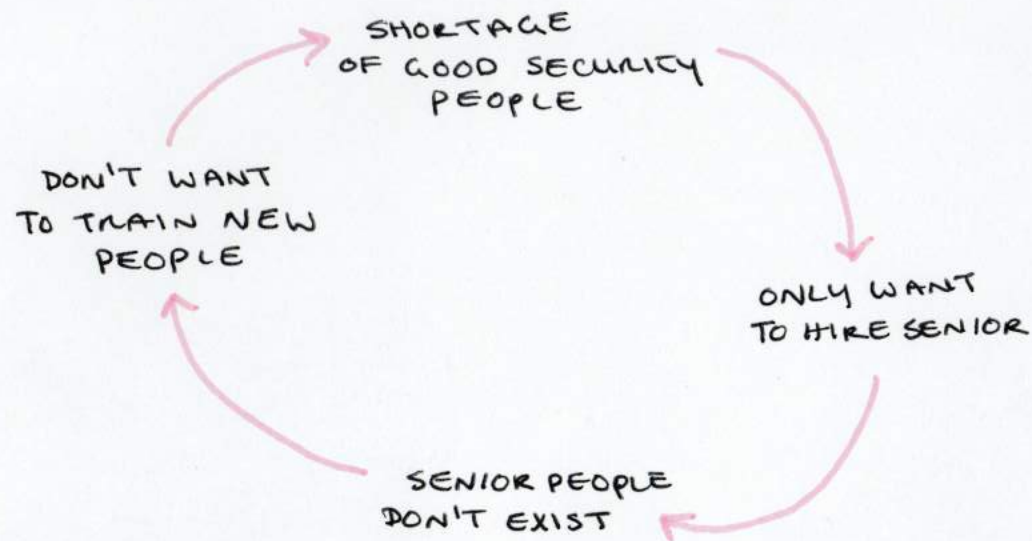
- What are the privacy risks?
- How do we achieve goals without exploiting users?
- How do we prevent information leakage?



FOUNDATIONAL
KNOWLEDGE!

PIPELINE PROBLEM

* DUN, DUN, DUUUNN *



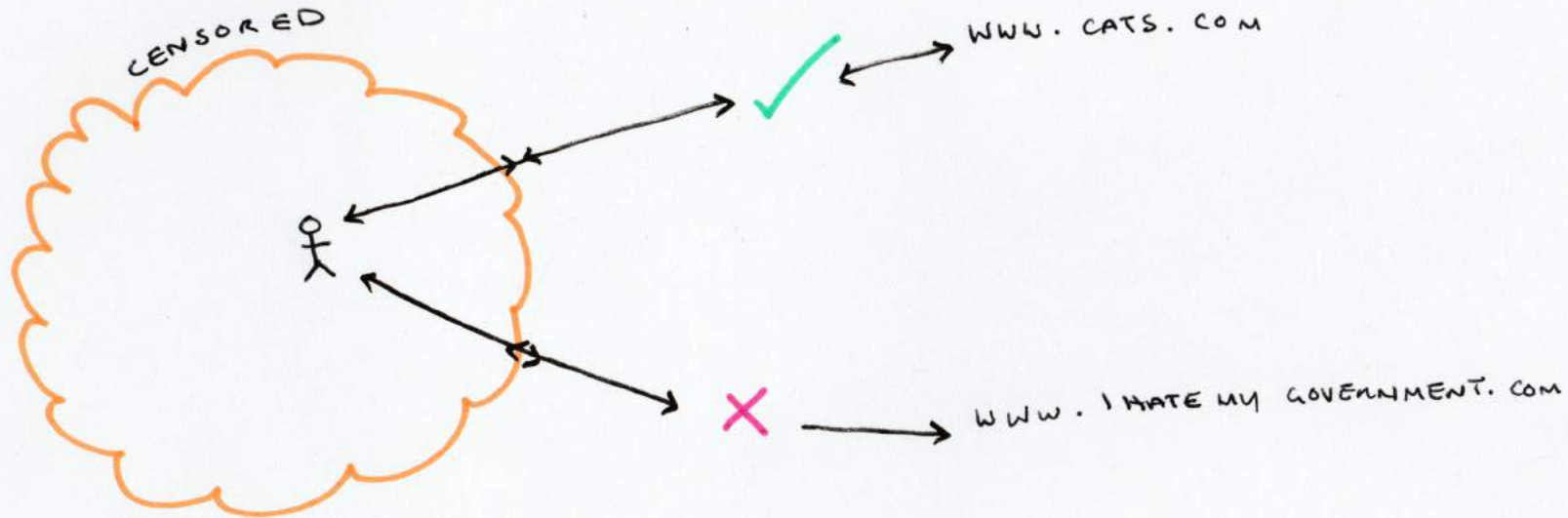
- GOOD NEWS ! LOTS OF MENTORING OPPORTUNITIES
- MOST PEOPLE ARE SUPER NICE
- IF YOU ENCOUNTER A WORKPLACE THAT IS UNWILLING TO TEACH OR MENTOR, RUN AWAY
- LOTS OF ONLINE RESOURCES TO LEARN SKILLS
- BE ENTHUSIASTIC AND PERSISTENT !

RESEARCH

- ACADEMIC SECURITY / PRIVACY RESEARCH IS THRIVING
- OFTEN WHERE THE MOST CUTTING EDGE STUFF HAPPENS
- SOME RESEARCH AREAS
 - CRYPTOGRAPHY
 - SECURE MESSAGING
 - NOVEL EXPLOITS
 - ANONYMOUS COMMUNICATION
 - SECURE AND PRIVATE ML / AI
 - AND MORE !

CHECK OUT: crisp.uwaterloo.ca

CENSORSHIP CIRCUMVENTION



SECURITY: HOW DO WE PREVENT CENSORS FROM DEPLOY CENSORSHIP ATTACKS?

PRIVACY: HOW DO WE HIDE THAT A USER IS CIRCUMVENTING CENSORSHIP?

TAKE AWAYS:

- SECURITY | PRIVACY | ETC. IS FOR EVERYONE !
- EVEN SEEMINGLY UNRELATED COOPS / INTERNSHIPS CAN GIVE YOU IMPORTANT SKILLS !
- NOT ALL SECURITY JOBS ARE HACKING, THERE'S SO MUCH VARIETY !
- TRY OUT DIFFERENT THINGS !
- LOTS OF PEOPLE ARE EXCITED TO HELP YOU FLOURISH !



RESOURCES:

- ★ [GITHUB.COM/ANNA LORIMER/SECURITY-RESOURCES](https://github.com/annalorimer/security-resources)
- ★ [DEFCON.ORG](https://defcon.org)
- ★ [CRISP.UWATERLOO.CA](https://crisp.uwaterloo.ca)
- ★ [PETESYMPOSIUM.ORG](https://petesymposium.org)
- ★ INFOSEC PEOPLE HANG OUT ON TWITTER
- ★ SLIDES ARE AT: [ANNA LORIMER.COM/HACKING YOUR SECURITY CAREER](https://annalorimer.com/hacking-your-security-career)