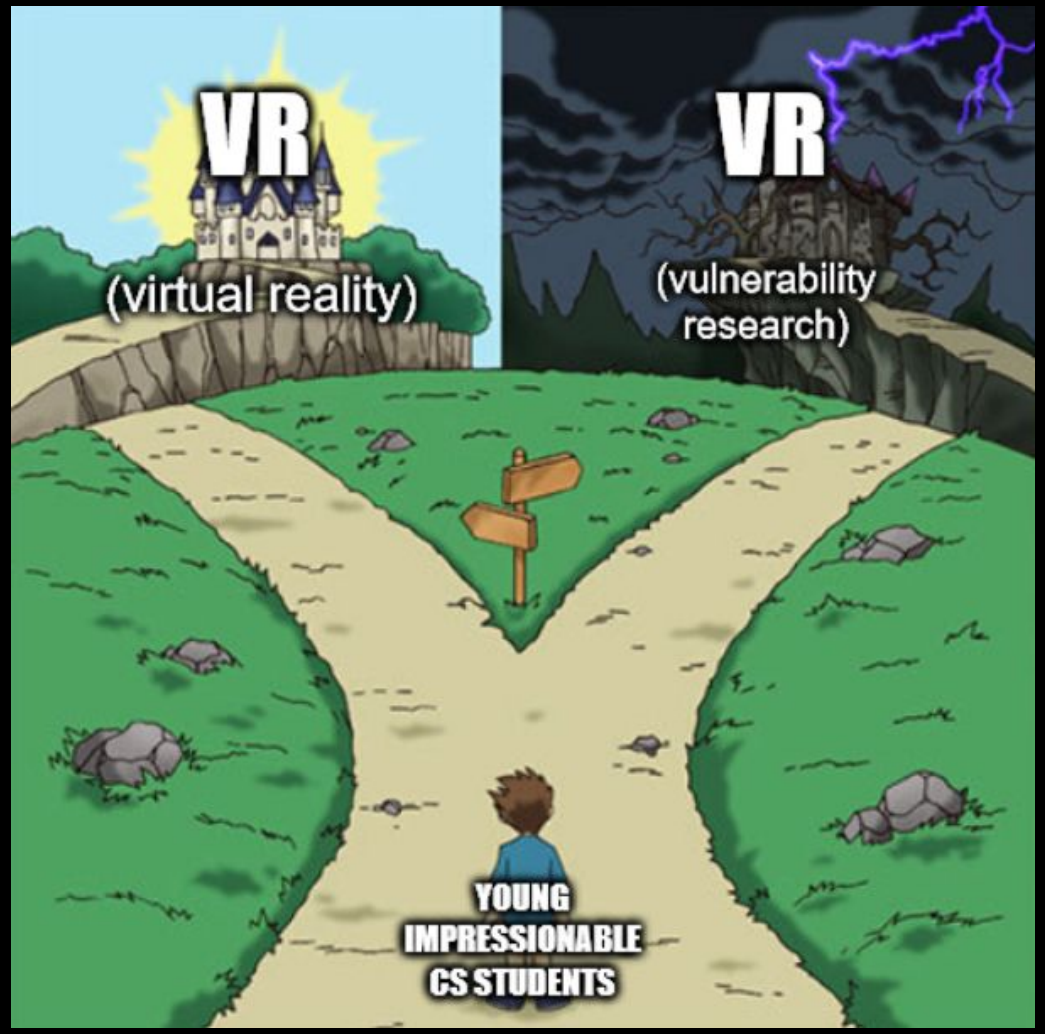
Week 09
Security Careers

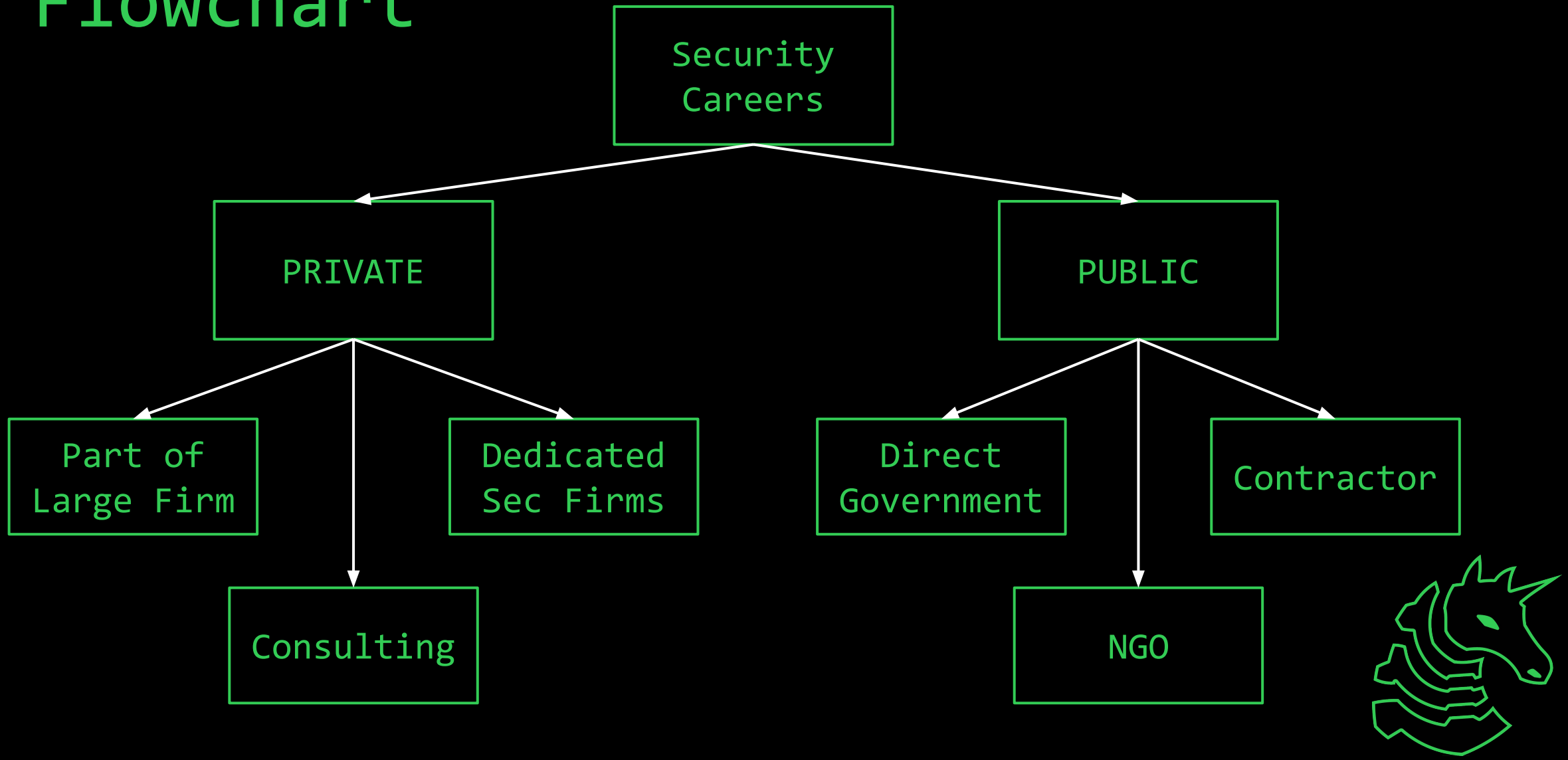
Announcements

- Check out Cyphercon interest poll in #club-general
- SIGPwny server down due to ACB outage last Saturday :(
  - Internal CTF down for now

sigpwny{give_job_please}



Flowchart


Security Careers
PRIVATE
PUBLIC
Part of Large Firm
Dedicated Sec Firms
Consulting
Direct Government
Contractor
NGO

Private Sector

"Part of Large Firm"

You are doing security work for a big company that doesn't necessarily specialize in security services

Software Security Engineer

Ensure that code being written is safe / integrated safely

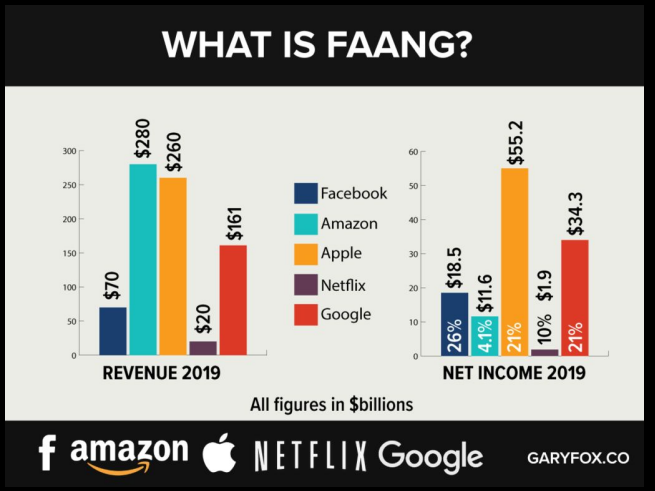
Tasks

- Develop software from a security-focused point-of-view
- Perform security audits on software

Companies to Look at

- FAANG (Facebook, Apple, Amazon, Netflix, Google) / Big Tech
- Most major firms that develop software want their code to be secure

Salary Expectation: **$80k-$500k+**



Security Engineer

Creates tools and solutions that help security analysts and executives identify threats

Tasks

- Design secure network infrastructure, including installing taps
- Configure system information and event monitoring (SIEM)
- Writing tools/scripts to automate repetitive analyst tasks

Companies to Look at

- All companies with mission-critical infrastructure need a dedicated security team to respond to threats

Salary Expectation: **$60k-$250k+**

Security Analyst

Ensures that systems and assets are secure, also known as Security Operations Center (SOC) analyst

Tasks

- Perform vetting of newly deployed servers
- Continuously audit servers and assets for vulnerabilities
- Alert others when patching is needed

Companies to Look at

- All companies with mission-critical infrastructure need a dedicated security team to respond to threats

Salary Expectation: **$50k-$250k+**

DFIR - Digital Forensics and Incident Response

Investigate cybercrime incidents

Tasks

- Set up tools to enable sufficient logging + alerts
- Inspect logs, filesystems, and traffic to discover method and extent of incidents
- Figure out who is behind attack

Companies to Look at

- Any big tech

Salary Expectation: **$40k-$200k+ (glassdoor)**

Security Research Scientist

Conduct research in company interest

Tasks

- Explore security risks of novel technology
- Publish papers and interact closely with academia
- Work with product teams to implement/test findings

Companies to Look at

- Most big tech

Salary Expectation: **$80k-$200k+ (glassdoor)**

Dedicated Security Firms

You work for a company that provides security services for another company

Security Software Development

Build software and services that security people use

Tasks

- Normal software dev: programming + unit testing
- Example software is IDA, Binja, Maltego, etc
- Example services are Qualys VMDR, Crowdstrike Falcon, Synack Red Team

Companies to Look at

- Vector35, Maltego, Qualys, antivirus companies

Salary Expectation: **$119k+ (ziprecruiter)**

Consulting

You work for a company that specifically provides security consulting to another company

Pentesting - Traditional

Your firm gets hired to try to find vulnerabilities in clients' software so they can fix them

Tasks

- Look for vulnerabilities in client software (web vulns, binary exploitation, **crypto**, etc)
- Present research and suggested fixes to client

Companies to Look at

- Rapid7, ScienceSoft, CyberHunter
- Deloitte, Plante Moran, PwC, etc.

Salary Expectation: $119k+ (glassdoor)

Pentesting - Independent

Go crazy on bug bounties, or be your own consultant

Tasks

- Choose bug bounties which are interesting, and then look for bugs in that scope
- Submit bug to bug bounty portal
- Get paid
- You could also do traditional consulting but independantly

Companies that have bounties

- Nearly all of them, but be sure to check what is in scope

Salary Expectation: $??? (Highly dependent on bounties + skill + time spent + you)

Big Firm Consulting - Cyber Risk

Design and implement solutions to various cybersecurity problems for businesses all over the world!

Tasks

- Assess and implement identity access management policies
- Architect and manage infrastructure security
- Attack surface management
- Cloud sec, data privacy management, appsec, etc.

Companies to look into

- Deloitte, McKinsey, other big4 and tier 1/2 consulting firms

Salary Expectation: $80k+ (way more with experience)

Pentesting - Specialized **(IAN)**

Public Sector

Direct Government Work

Working for the Government

Pros: Pension, easier taxes, working for the government benefits go here

Cons: Stuck on the GSA payscale

Government - Investigation

Exactly the same as DFIR from earlier

Tasks

- Inspect logs, filesystems, and traffic to discover method and extent of incidents
- Figure out who is behind attack

Government - Cyber Command

- Part of the Department of Defense (DoD)
- Split into attack and defense teams

Tasks

- If defense, work to protect the DoD network
- If offense, likely researching and stockpiling 0-days until it's time to weaponize them

Government - General

Government - Policy Design

- Office of Science and Technology Policy
  - Government wants people that are knowledgeable about technology and security to help make decisions
- CISA (Cybersecurity and Infrastructure Security Agency)
- NIST (National Institution of Standards and Technology)

NGOs / Government Contracting

You work for a private company that works for the government

General Government Research

Research as directed by the government, looking into cutting edge fields of computer security and how they can be used. Research also often pertains to other government work (DoD, DoE etc). Def/Off

Tasks

- Wildly vary
- Generally like research at universities but with government interests / objectives

Salary Expectation: Significantly higher than working direct for government, you get contractor money >:)

Vulnerability Research

Find and productize 0-days

Tasks

- Write fuzzers to find bugs in specific target
- Write reliable exploits to attack the vulnerability
- Write patches to fix vulnerabilities

Companies to Look at

- **REDLattice, Battelle, Raytheon, Lockheed Martin, Trail of Bits, Dataflow Security**

Salary Expectation: $70k-$200k + bug sale commission (can 2x or 3x salary)

Government - Research (Defense)

Making sure our stuff doesnt get popped

Government - Research (Offense)

Other Jobs in Security...

Security Influencer

- Push cybersecurity related media
- Examples: SwiftOnSecurity, LiveOverflow
- Content may be educational or funny

Salary Expectation: $??? Depends on size of following + amount of media and sponsorships

Computer Security Law

- Represent people who are prosecuted for cyber crimes

- Need to know all the laws + interpretations related to computers
  - Computer Fraud and Abuse Act (CFAA)
  - Some laws are pretty outdated

Academic Researcher / Professor

- Do cybersecurity research
- Don’t get paid much
- Not tied to financial interests of a company
- Work on problems that actually matter

Good cybersec research schools

- **MIT, CMU, UIUC**

Talk to Ravi for more info

Next Meetings

Sunday Seminar: UIUCTF Planning

- Find volunteers to implement specific chal ideas
- Set up team for web theming

Next Thursday: UIUC Tech Services

- Tech Services talking about their work, war stories, career pathways, and having a Q&A
- Use the link in #announcements to ask questions