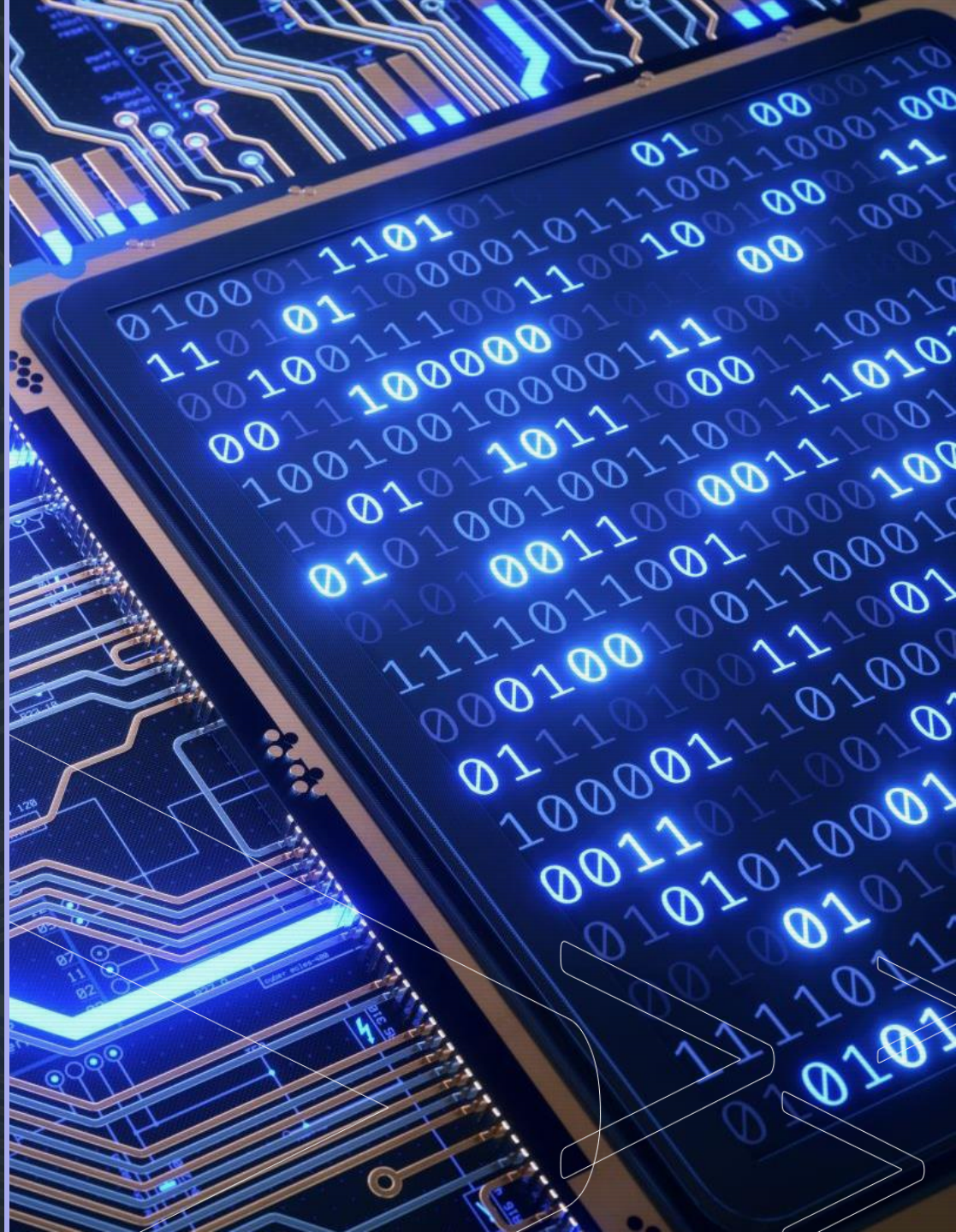
WiCyS: Intro to Cybersecurity and Cybersecurity Job Titles



Reminders

- Check in on GSP!
- Don't forget to join the WiCyS Slack!

Find the Slack invite link on our Facebook page, just click the "sign-up" button!

Cybersecurity: What is it?

Very broad umbrella for many subfields

Many different titles available

Not just stereotypical hacking

~11% women in the field

Some Basic Cybersecurity Terminology

- CTF: Capture-The-Flag
  - Participants solve puzzles or try to break into systems given to them
- Hats
  - White hat hacker: hacks to expose vulnerabilities so that they can be patched
  - Grey hat hacker: may violate laws or break rules, but not for unethical reasons
  - Black hat hacker: breaks into computer systems for unethical reasons
- Teams
  - Red team: hired to break into a system, considered outside of an organization
  - Blue team: focuses on defending a system from red teams

Cybersecurity Conferences!

- Most famous conferences are DEFCON, Black Hat
  - Both usually held in Las Vegas in August
  - DEFCON is more traditionally hacker-y
  - Black Hat is a bit more professional
  - Both have many interesting talks
- ACM/IEEE research conferences held for topics such as networks, HCI, etc.
- Women in Cybersecurity annual conference
  - Students must apply to receive a scholarship to attend, pay $40 to register
  - Better than GHC for networking because it has 3k attendees instead of 20k+

How to Get a Cybersecurity Internship?

- Apply to as many places as possible
- Slide into recruiter DMs
- Study for interviews/build up a great resume
  - Build side projects
  - Try CTF practice!
  - Understand basic data structures
  - Understand general computing concepts such as networks, architectures, operating systems

Some Common Titles

Security Engineer: Building secure systems; could be hardware or software focused

Network Engineer: Building and maintaining secure networks

Security Consultant: Consult for different companies to improve their security practices

System Administrator/DevOps/Security Analyst: Similarly to network engineering, though may involve securing overall systems

Security Researcher: Research new vulnerabilities, novel security techniques, etc.

Some Common Titles

Security Engineer: Building secure systems; could be hardware or software focused

Network Engineer: Building and maintaining secure networks

Security Consultant: Consult for different companies to improve their security practices

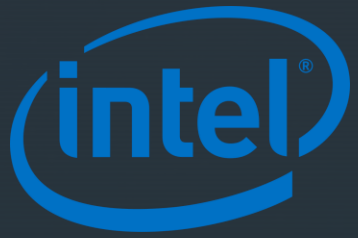
System Administrator/DevOps/Security Analyst: Similarly to network engineering, though may involve securing overall systems

Security Researcher: Research new vulnerabilities, novel security techniques, etc.

WARNING: there is no standard title; specific roles may change by company

Security Engineer

- Usually, apply to Software Engineering internship position and hope to be matched with a security team
- Interviews: expect typical technical interviewing/Leetcoding
- Example companies:
  - Tech companies - Microsoft, Google, Facebook
  - Literally anything involving finance – banks, brokers, the Federal Reserve
  - Hardware companies – Nvidia, Apple, Intel



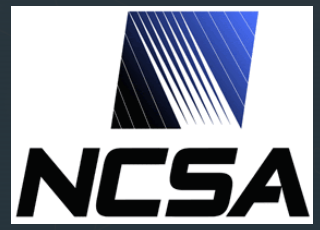


Security Analyst

- Not as much programming as security engineers
- Involves more manual checking for potential vulnerabilities, ensuring compliance with company security policies
- Interviewing: could be Leetcode or trivia questions
- Example companies:
  - Anything that wants to secure…anything
  - Booz Allen Hamilton, CrowdStrike

Network Engineer

- Similar to security analysts, with focus on network security/setup
- Interviewing: expect questions about the network stack
- Example companies:
  - Cisco, Huawei
  - T-Mobile, Verizon, AT&T
  - Research institutes; for example, National Center for Supercomputing Applications sent network engineers to South America recently to help set up a big telescope

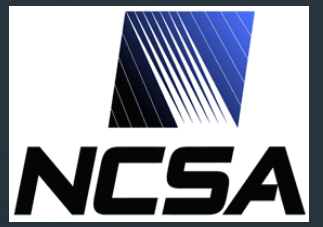


Security Consulting

- Could have more business flavor than other roles (but, be warned, sometimes ends up being software development)
- For example, a company might want help with improving their personnel access policy
- Interview: expect case interviews
- Example companies:
  - Big 4 of consulting
  - Other consulting firms, such as West Monroe, Grant Thorton

Security Researcher

- Specific area can vary; some search for vulnerabilities or develop secure technologies
- Interviews: could be coding or discussion of past research experiences
- Companies
  - National laboratories: Sandia National Labs, Pacific Northwest National Laboratory, MIT Lincoln Laboratory, MITRE
  - Universities: look for security REUs or positions at specific campus groups such as National Center for Supercomputing Applications



Being a Classic Hacker?

- [redacted]
- Interviews: usually not going to be Leetcode; the hard part is obtaining security clearance
- Programs such as SFS, DoD SMART scholarship offer to pay your tuition and match you with a government job in exchange
- Example companies:
  - US Government: FBI, NSA, etc.
  - Federal contractors
  - Any nation that uses computers

Relevant Skills

- Being comfortable in a Linux environment
- Knowledge of the network stack, how to use Wireshark (or any other network traffic monitoring tool)
- Knowledge of computer architecture, operating systems
- Low-level languages
- Object-oriented programming
- ...and a lot more!

A Side Note on Certifications

- Some people or companies want to see certifications for security
- If you want a certification, then go for it!
  - If you have a computer science degree, certifications aren't very important
  - Certifications are a great way for non-technical majors or applicants without a degree to show they have sufficient security knowledge

Interested?

- Attend future meetings!
- Try CTFs on your own if it interests you
- Prepare for interviews
- Pick 1 role type and start applying ASAP

Interview + Recruitment Tips!

To get an interview

- Introduce yourself to recruiters
  - Try to find UIUC campus recruiters, though any general university recruiter could probably help
  - Let them know when you have other deadlines/offers
  - Especially for research positions, it's likely you could get a job position by networking with full-time staff
    - For example: if you find an interesting paper, email the primary author

To Prep for Technical Interviews

- Practice Leetcode
  - Give it a serious try before checking the answer if you're stuck
  - Re-solve old questions to make sure you really understand the solution
  - Type in a Google Doc without a compiler to replicate whiteboard environment
  - Talk to yourself out loud while solving problems
- Brush up on basic theory/concept knowledge
  - Data structures, algorithm complexity
  - Web security/networking stack concepts, if the position expects them

To Prep for Behavioral Interviews

- Write down your answers to behavioral questions **in advance**
  - "Tell me about yourself"
  - "Tell me about a time you dealt with a team conflict"
- Read your resume, know which projects you would bring up if prompted about them
  - "Tell me about a project you're really proud of"
  - Remember the details; you don't want to stumble when asked how you implemented a certain feature
- **Be confident!**

To look for Security Opportunities

- **Look up companies of interest, find out their internship timelines**
  - For example: some PwC summer 2021 internships opened in 2020 spring
  - Meanwhile, national labs can make decisions a few months before start dates
- **Get started with on-campus or Research Park IT/security positions**
- **Email security professors about their research labs**
- **Apply for companies on WiCyS sponsor list**
  - Being a sponsor tends to mean a) they want more security roles filled and b) they want these roles to be filled by diverse candidates
  - If you're a national member, check for jobs on Job Board++
  - Attend WiCyS career fairs!