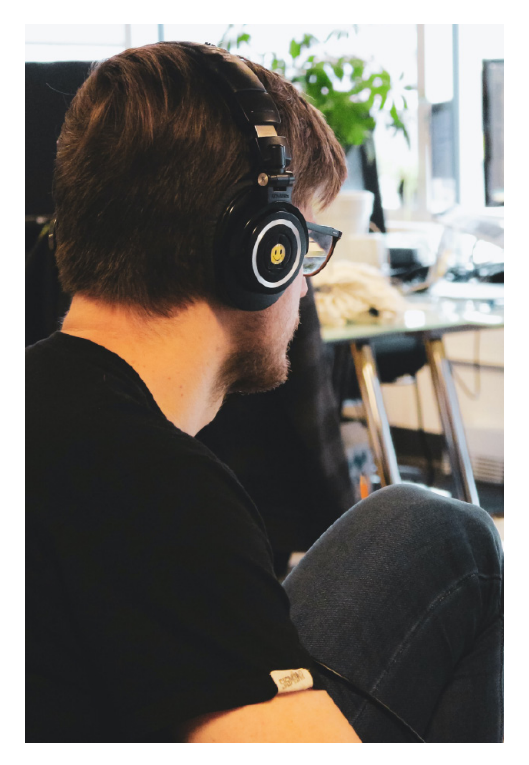
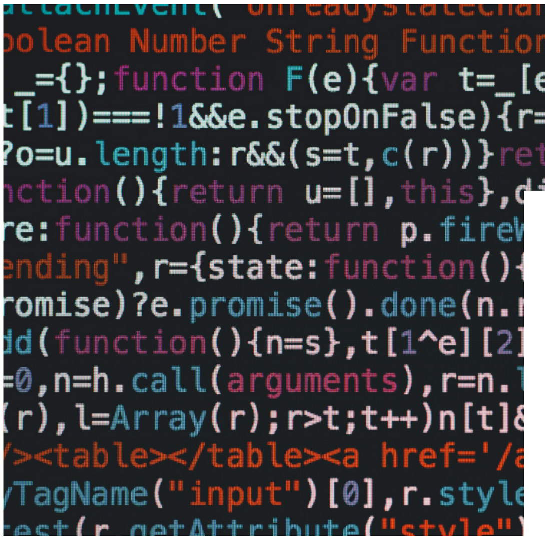
Carnegie Mellon University
Silicon Valley



SECURITY CAREER GUIDE

Student Affairs at Carnegie Mellon University Silicon Valley

CONTENTS



Carnegie Mellon University Silicon Valley
CARNEGIE MELLON UNIVERSITY

SECURITY CAREER GUIDE

Acknowledgment section

These career guides are adopted each year, and the career services team would like to sincerely thank the 2019 cohort of Peer Career Consultants for creating the first iteration. We appreciate the hard work of Chaitra Dinesh Pai, Nursultan Dyussebayev, Arpit Gupta, Sweta Hari Kumar, and Joseph Konan who researched specific fields of interest and compiled helpful tips and resources for students to enable them to make the most of their CMU-SV experience and navigate the internship and job search process in Silicon Valley. Their valuable contributions made these career guides possible. Additionally, the example resumes are compiled from recent alumni who also wanted to help our future students at CMU-SV. Thank you to everyone who contributed their time and effort.

Introduction

As cybercrime is growing at an exponential rate, and news of major breaches reach headlines nearly daily, information security professionals are in high demand. **Cybersecurity Ventures reports (https://cybersecurityventures.com/jobs/) that “the number of unfilled cybersecurity jobs grew by 350 percent, from one million positions in 2013 to 3.5 million in 2021. For the first time in a decade, the cybersecurity skills gap is leveling off. Looking five years ahead, we predict the same number of openings in 2025” wrote Editor-in-Chief, Steven Morgan.**

Security concerns are not new in the tech world. Security has been an **integral** part of organizations since early days. Individuals who are curious about how the technology works at a fundamental level, and are passionate about asking the question ‘why’, gain **success** in the field of security.

From securing nation state networks and systems to protecting a user’s data and devices, different corporations have different objectives, while academia focuses on improving existing cryptography protocols or implementing new ones. Security is inherently **interdisciplinary**. Different companies have different requirements for entry. Thus, the field is wide open for both recent graduates and people looking to make a career change. Here are a few **different job options** to explore:

- **Application Security**: Provides engineering teams with the security expertise necessary to make confident product decisions via code reviews and audits. Develops tools and frameworks to integrate security into applications software during the design and development process.

- **Corporate Security**: Helps in detection and prevention of internal and external threats against the company systems and infrastructure; by designing scalable security solutions.

- **Incident Responder**: Works with a host of forensics tools to find the root cause of problems like intrusions or malwares, limit the damage and see that it never happens again.

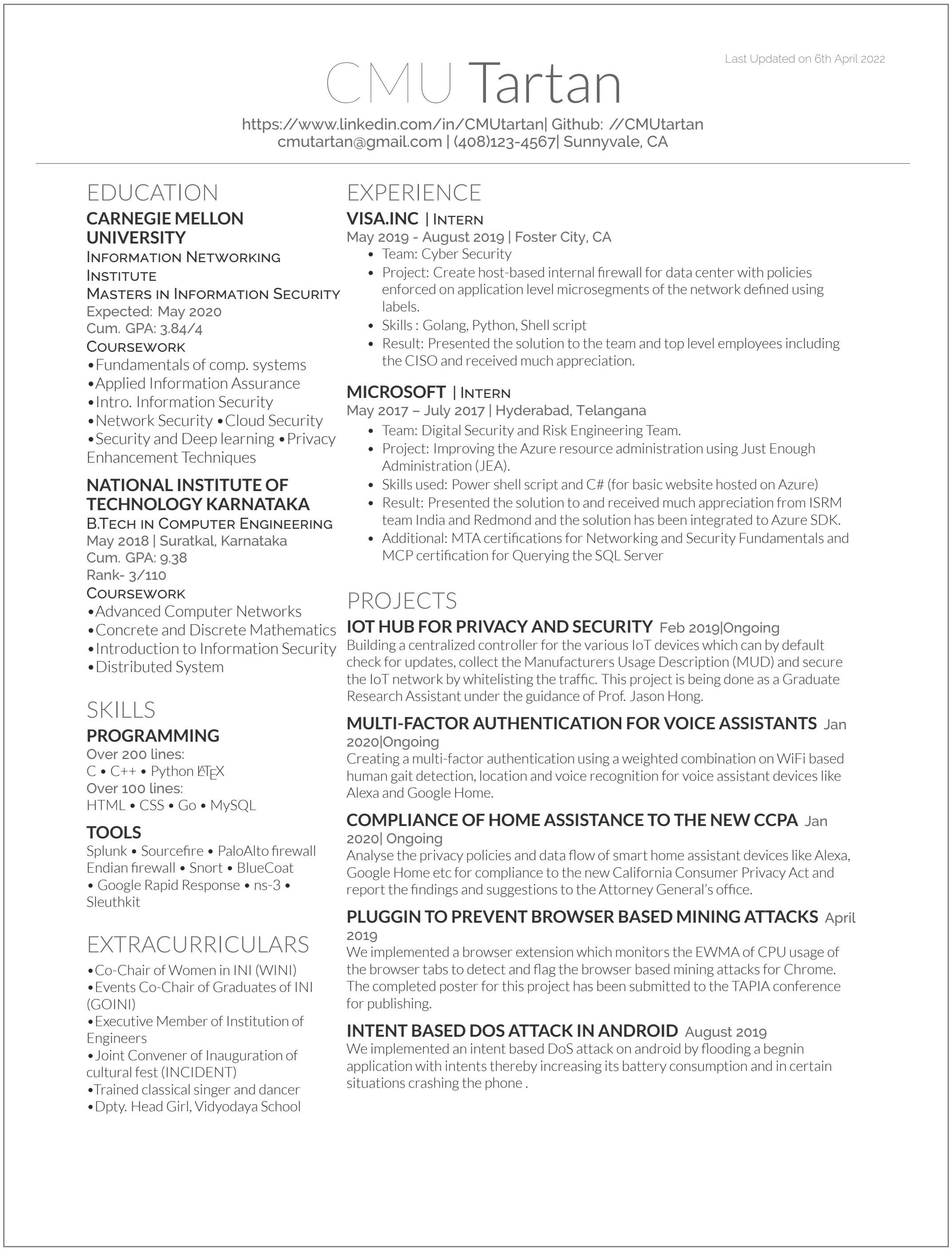
- **Penetration Tester**: Responsible for legally hacking into an organization’s applications, networks, and systems to discover security vulnerabilities and report to the stakeholders.

- **Privacy Engineer**: Works to ensure that the data collection and usage practices are transparent, protect user privacy, and mitigate risk.

- **Security Policies**: Researches, develops, and supports company-wide security capabilities, especially those dealing with policy, risk, and compliance, while integrating with customers.

EXAMPLE RESUME

To give you an idea of what a security focused role resume can look like before it's tailored to the job description, please see the example below. *Please note, these roles may not have occurred in 2019-2020. This is a resume example from a real CMU-SV student, however, other data points are edited each year. Please recognize that this is not a real candidate. Please email career-services@sv.cmu.edu if you have any questions about this example resume or if you need to schedule a resume appointment, please do so through Handshake.



Last Updated on 6th April 2022

CMU Tartan

https://www.linkedin.com/in/CMUtartan| Github: //CMUtartan
cmutartan@gmail.com | (408)123-4567| Sunnyvale, CA

EDUCATION

CARNEGIE MELLON UNIVERSITY
Information Networking Institute
Masters in Information Security
Expected: May 2020
Cum. GPA: 3.84/4
Coursework
•Fundamentals of comp. systems
•Applied Information Assurance
•Intro. Information Security
•Network Security •Cloud Security
•Security and Deep learning •Privacy Enhancement Techniques

NATIONAL INSTITUTE OF TECHNOLOGY KARNATAKA
B.Tech in Computer Engineering
May 2018 | Suratkal, Karnataka
Cum. GPA: 9.38
Rank- 3/110
Coursework
•Advanced Computer Networks
•Concrete and Discrete Mathematics
•Introduction to Information Security
•Distributed System

SKILLS

PROGRAMMING
Over 200 lines:
C • C++ • Python LaTeX
Over 100 lines:
HTML • CSS • Go • MySQL

TOOLS
Splunk • Sourcefire • PaloAlto firewall Endian firewall • Snort • BlueCoat • Google Rapid Response • ns-3 • Sleuthkit

EXTRACURRICULARS

•Co-Chair of Women in INI (WINI)
•Events Co-Chair of Graduates of INI (GOINI)
•Executive Member of Institution of Engineers
• Joint Convener of Inauguration of cultural fest (INCIDENT)
•Trained classical singer and dancer
•Dpty. Head Girl, Vidyodaya School

EXPERIENCE

VISA.INC | Intern
May 2019 - August 2019 | Foster City, CA

- Team: Cyber Security
- Project: Create host-based internal firewall for data center with policies enforced on application level microsegments of the network defined using labels.
- Skills : Golang, Python, Shell script
- Result: Presented the solution to the team and top level employees including the CISO and received much appreciation.

MICROSOFT | Intern
May 2017 – July 2017 | Hyderabad, Telangana

- Team: Digital Security and Risk Engineering Team.
- Project: Improving the Azure resource administration using Just Enough Administration (JEA).
- Skills used: Power shell script and C# (for basic website hosted on Azure)
- Result: Presented the solution to and received much appreciation from ISRM team India and Redmond and the solution has been integrated to Azure SDK.
- Additional: MTA certifications for Networking and Security Fundamentals and MCP certification for Querying the SQL Server

PROJECTS

IOT HUB FOR PRIVACY AND SECURITY Feb 2019|Ongoing
Building a centralized controller for the various IoT devices which can by default check for updates, collect the Manufacturers Usage Description (MUD) and secure the IoT network by whitelisting the traffic. This project is being done as a Graduate Research Assistant under the guidance of Prof. Jason Hong.

MULTI-FACTOR AUTHENTICATION FOR VOICE ASSISTANTS Jan 2020|Ongoing
Creating a multi-factor authentication using a weighted combination on WiFi based human gait detection, location and voice recognition for voice assistant devices like Alexa and Google Home.

COMPLIANCE OF HOME ASSISTANCE TO THE NEW CCPA Jan 2020| Ongoing
Analyse the privacy policies and data flow of smart home assistant devices like Alexa, Google Home etc for compliance to the new California Consumer Privacy Act and report the findings and suggestions to the Attorney General's office.

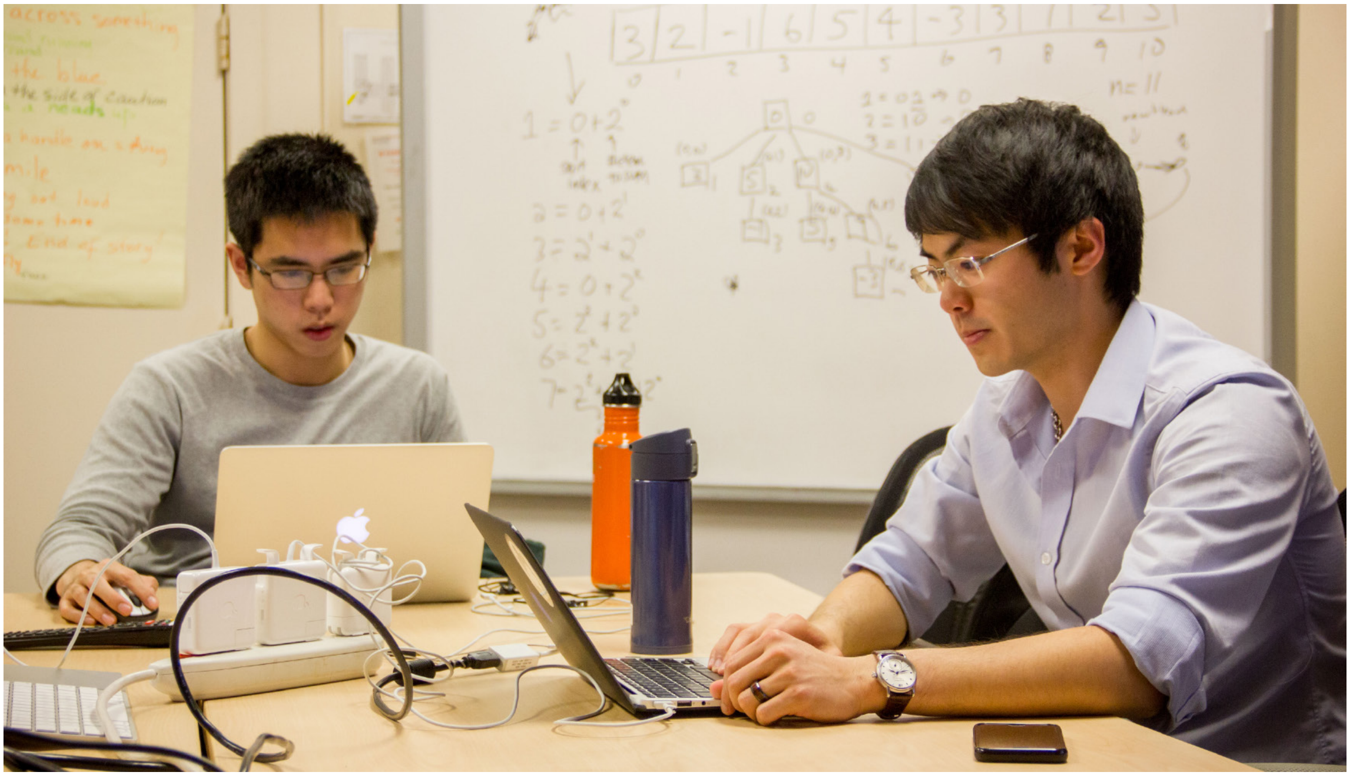
PLUGGIN TO PREVENT BROWSER BASED MINING ATTACKS April 2019
We implemented a browser extension which monitors the EWMA of CPU usage of the browser tabs to detect and flag the browser based mining attacks for Chrome. The completed poster for this project has been submitted to the TAPIA conference for publishing.

INTENT BASED DOS ATTACK IN ANDROID August 2019
We implemented an intent based DoS attack on android by flooding a begnin application with intents thereby increasing its battery consumption and in certain situations crashing the phone .

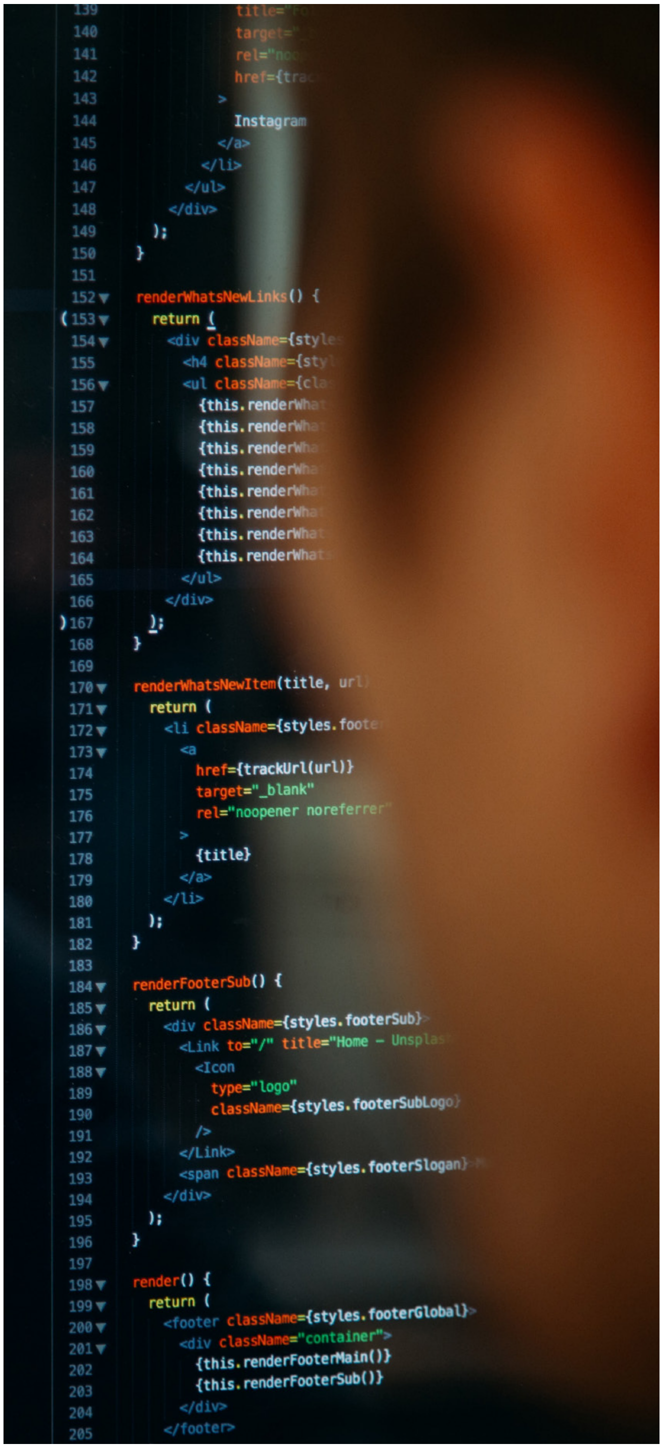
SKILLS, COMPETENCIES, AND APTITUDE

There is something new in the field of security every day. Thus, it requires individuals to be self motivated and have an ever learning spirit. Some **specific skills** to focus on:

- **Programming** in C, Java, Python, Bash (Linux/ Unix commands): Ability to jump into the codebase and understand what's happening in the given context in a short amount of time
- Components of a **Cryptosystem**: Symmetric/Asymmetric key cryptography, Hashing, Block/Stream ciphers, CIA (and other properties)
- **System Design**: Overview of how Applications, Backend, Database, Services (APIs) integrate together and work.
- **Network Stack**: Knowledge of TCP/IP layers, commonly used protocols (TCP, UDP, IP, HTTP/s, FTP, TLS, SSH, IMAP etc), Bluetooth
- **Fundamentals** of how different technology works and have evolved in terms of the networking concepts used, the web applications and the infrastructure involved
- Awareness of latest **security trends and best practices**
  - try to see where the world is going
  - an idea of what went wrong and why
- Top **Vulnerabilities** for web apps, mobile apps, network etc: OWASP, MITRE and their **mitigations**
- **Critical Thinking**: What can go wrong in the given system?
- Strong **communication** skills: Being able to explain very technical concepts in an easy way to different teams and stakeholders



SUPPLEMENTAL RESOURCES



```
              title="Fo
              target="_b
              rel="noo
              href={trac
            >
              Instagram
            </a>
          </li>
        </ul>
      </div>
    );
  }

  renderWhatsNewLinks() {
    return (
      <div className={style
        <h4 className={sty
        <ul className={cla
          {this.renderWhat
          {this.renderWha
          {this.renderWha
          {this.renderWha
          {this.renderWha
          {this.renderWhat
          {this.renderWhat
          {this.renderWhat
        </ul>
      </div>
    );
  }

  renderWhatsNewItem(title, url)
    return (
      <li className={styles.foote
        <a
          href={trackUrl(url)}
          target="_blank"
          rel="noopener noreferrer"
        >
          {title}
        </a>
      </li>
    );
  }

  renderFooterSub() {
    return (
      <div className={styles.footerSub}>
        <Link to="/" title="Home - Unsplas
          <Icon
            type="logo"
            className={styles.footerSubLogo}
          />
        </Link>
        <span className={styles.footerSlogan}>
      </div>
    );
  }

  render() {
    return (
      <footer className={styles.footerGlobal}>
        <div className="container">
          {this.renderFooterMain()}
          {this.renderFooterSub()}
        </div>
      </footer>
```

Articles:

- https://www.techrepublic.com/article/rise-of-the-accidental-cybersecurity-professional/
- https://www.techrepublic.com/article/cheat-sheet-how-to-become-a-cybersecurity-pro/
- https://www.zdnet.com/article/security-experts-explain-how-to-make-it-in-infosec/
- https://www.purevpn.com/blog/top-cybersecurity-experts/

Conferences:

- DefCon
- Blackhat
- WiCyS
- USENIX Security
- SOUPS (Symposium on Usability, Privacy, and Security)
- Networks@Scale (FB-run conference; great for network security and free; invite-only)

Lookout for Hackathons. Many online and onsite hackathons happen all round the year.

Educational Materials:

- HackTheBox
- PenTester Academy
- SANS Institute courses

CO-CURRICULAR ACTIVITIES

• **CTFs/Wargames**: PicoCtf, CtfTime, OverTheWire, BlackHat, Pwnable.kr, LiveOverflow
Play these CTFs and Wargames for hands-on experience to challenge yourself in real-world like scenarios. These are hosted online and you will find great write-ups on how to get started.

• **Coding**: LeetCode, HackerRank
Solve at least 100-200 easy-medium questions to be consistent in your development skills. It will help you during the interview process and while reviewing code.

• **Podcasts**: SecurityNow (weekly), Darknet Diaries
Be a regular listener! Even go back and start from episode 1. You will learn about the fundamentals of many technologies and how they evolved. Also, you will be up-to-date with the latest trends and affairs.

• **News**: Twitter (@schneierblog, @lorenzofb, @briankrebs, @BillBrenner70, @DanielMiessler, @kevinmitnick, @e_kaspersky, @mikko, @k8em0, @Shirastweet, @juliettekayyem, @lennyzeltser, @dangoodin001)
Follow famous security analysts. They share about the latest trends and affairs.

• **Internship**:
An internship in a particular security role gives you insights of how an organization looks at security internally and also how other security roles come into play. It is a good platform to explore your interests and benchmark your skills.

• **Projects**:
Most security classes at CMU involve a project component. Try to make the best out of these projects by learning something nascent or novel. Don't be afraid to dive in the layers.

• **Certifications**:
There are online certifications offered by Comptia and Cisco. They focus on particular skills and you can use them to benchmark your knowledge.

• **Teaching Assistant**:
Being a TA demonstrates your grasp of the course material and team player skills. Also, it can help you further understand the material by evaluating different solutions.

• **Research Assistant**:
Doing research related to security under a CMU professor shows your willingness to learn and explore. It also helps you in building trust and connection with the professor.

INTERVIEW PREPARATION

Some companies go through the interviews very quickly, about or less than a month from start of interview to decision, while others take a long time. Govt organizations usually take more than a month, unless a candidate is in a rush, similarly Google is famous for its 2-3 months long procedure. Interviews typically happen in the Fall for most companies, but a few also have interview slots in the Winter and fewer yet in the Spring. Due to a big shortage, there are many openings all around the year.

Typical interview schedule: phone screening followed by onsite interview(s) (often a full day of interviews), then get a decision in a few days to weeks. Some companies will require you to do a technical assessment/coding interview first while others will ask more questions related to your cybersecurity knowledge and how to approach certain security situations.

For internships, typically a few phone screens for most places, but some companies host interns day where they bring in candidates from different schools at the same time for onsite interviews.

Websites:

- LeetCode
- OWASP
- PortSwigger
- CloudFlare Technical blogs
- https://github.com/gracenolan/Notes

Books:

- Introduction to C by Dennis Ritchie
- Hacking: The Art of Exploitation by Jon Erickson
- Cracking the Coding Interview by Gayle Laakmann McDowell
- Building Secure and Reliable Systems

PRACTICE QUESTIONS

Coding
https://www.programcreek.com/2012/11/top-10-algorithms-for-coding-interview/

- Array Operations
- String traversal
- Sorting
- Stacks/Queues
- Linked list traversal
- Binary tree traversal
- Graph traversal

Basic

- Encoding vs encryption
- Symmetric vs asymmetric cryptography
- Authentication vs authorization
- Block vs stream cipher
- PKI Infrastructure
- 2-DES vs 3-DES
- 3-DES Meet-in-the middle attack
- TCP vs UDP
- Proxy vs VPN
- Strong vs weak hash (Hash collision: Birthday paradox)
- ECB vs CBC mode
- Padding oracle attack
- SSL Pinning
- Buffer Overflow
- SQL injection
- XSS (Cross site scripting)
- CSRF
- SSRF
- MITM (Man in the Middle)
- Ransomware
- Phishing
- RCE (Remote Code Execution)

Advanced

- Why is RSA secure? Why is Quantum Computing a threat?
- How does ARP Cache Poisoning work?
- How do Heap overflow, Format string attacks work?
- What is TPM (Trusted Platform Module), Secure bootchain?
- What happens when I type Google.com in my browser?
- How does PGP work? What are the different components?
- How do you build a botnet? How do you defend against one?
- How does Row Hammer Attack work?
- How does TOR work?
- How does SSH work?
- Explain how SSL works.
- What is perfect-forward-secrecy?
- Working examples of applying STRIDE threat model
- MITRE ATT&CK framework
- Cyber Kill chain
- Secure coding on buffer overflow, stack overflow
- Anti-analysis techniques used by malwares

NEXT STEPS/CONCLUSIONS

Live and breath security! **Security is an Art of Living~**

Talk about any security related topics with your peers and learn how they feel about it. Aim of the conversation should be to learn something new and to walk away with something you can look up and go in a little more detail. Focus on different perspectives.

Also, during your time at CMU, you should explore these great **courses** directly or indirectly related to security:

- Introduction to Information Security
- Introduction to Computer Systems
- Advanced-Real Word Data Networks/Network Security/ Wireless Security
- Distributed Systems/Operating Systems
- Host/Network Based Forensics
- Introduction to Software Reverse Engineering
- Insure Cybersecurity Research
- Secure Software Systems
- Network security engineering

Up and coming **trends** in security to explore:

- Automation: security analysis via manual evaluation vs fuzzy evaluation and invariance detection
- ML/DL: security analysis and attack detection via machine/deep learning models
- Push Left: solving security vulnerabilities at the framework level to provide DRY design: (don't repeat yourself)