ANITA BORG INSTITUTE

GRACE HOPPER

CELEBRATION OF WOMEN IN COMPUTING

Student Opportunity Lab:

Checking out a Career in Cybersecurity?

Sunitha Kumar
Technical Lead
Cisco Systems, Inc.
sunithak@cisco.com
@sunitwitt

Tolu Onireti
Security Engagement Manager
Cisco Systems, Inc.
tonireti@cisco.com
@tolutop

Introduction

According to a Peninsula Press analysis (a Stanford project) of the U.S. Bureau of Labor Statistics (BLS), more than 209,000 Cybersecurity jobs in the U.S. are unfilled and the demand for information security professionals is expected to grow by 53% through 2018. With more jobs than there are trained people to fill them, information security analysts are compensated well. The U.S. BLS reported the 2012 median wage for information security analysts was $86,170, compared to the 2012 national median salary of $34,750.

Merriam Webster defines Cybersecurity as "the state of being protected against the criminal or unauthorized use of electronic data." However, as an industry, it is so much more than the dramatically stylized hackers featured in today's movies and television shows. Here are some major career paths within the information security industry:

- **Builders*** are those building security products, infrastructure, and services.
- **Breakers*** include ethical hackers conducting security tests, reverse engineers, and digital forensic specialists.
- **Defenders*** work on tools and techniques that help detect and respond to attacks against applications and infrastructure.
- **Leaders** include those from business and IT with the common goal of championing security efforts via policymaking and thought leadership.
- **Influencers** include project and program managers with the common goal of coordinating, influencing and managing security-related programs.
- **Researchers** can be found in academia, government, and private sectors working on Cybersecurity issues of the future.

Career Path Details

Builders

Every solution needs security builders. Builders identify threat to the solution and provide mitigations. Encompasses hardware, software, hosted services, and virtual platforms. When designing any system, cover the use cases from where your system is hosted, all the way to how it is used. Understand what security constraints are in your reach and what is outside. For instance, a SAAS application hosted in a cloud service provider is dependent on the cloud service provider for hardware

*Key security groups "builders, breakers, and defenders" are terms coined by OWASP: See owasp.org for more details.

security, defining its tenants for accountability, among other things. The SAAS application however, on the other hand has complete control over its web security.
In the areas of embedded solutions, there is complete control for defining hardware security, with hardware trust anchor, and secure boot.
Identify the exposure your solution has by understanding the privilege the processes should have. Aim for least privilege. Adopt secure coding mechanisms in order to avoid buffer overflow attacks.
In the area of software, more and more solutions encompass plug-and-play, wherein modules are sourced from open source or third party vendors to form the solution. Understand the security mechanisms in the sourced code, methodology to update them in the event of security vulnerabilities. Most solutions require an interface to trouble shoot. Ensure this interface in itself does not open up back doors.
Be aware that it is easy for hackers and script-kiddies to find the tools to attack and break systems, and as a builder, it is our responsibility and endeavor to make our systems hack-proof.

Defenders

Every asset of value is worth defending against exploitation. The role of the Cybersecurity Defender is to protect applications and infrastructure, by leveraging the Defense-in-depth approach to Security. Knowledge of the risk - which is vulnerabilities present and the likelihood of exploitation of the vulnerability - is crucial in determining the level of Security defense required to protect an application or infrastructure.
Defenders are trained to know steps they should and should not take during, before and after a cyber attack. Analysis of information gather before, during and after a cyber attack helps to provide feedback in developing better defense system that are adaptive to unknown vulnerabilities. The role of a defender is very crucial, it could be seen as a shield. The need to continue to evolve in this space is also crucial because, being a step ahead of the bad guys is very important, as our lives have become very interwoven with technology.

Below are some roles for a Cybersecurity Defender:

- Security Monitoring and Event Analysis
- Information Security Investigator
- Threat Analyst/Counter Intelligence
- Security Research Engineer/Data Scientist
- Malware Reverse Engineer
- Incident Responder In-depth

Practical Tips: The 3 E's – Opportunities for Education, Experience and Exposure:

- Undergraduate or Graduate degree in Computer Science, Engineering, or Cybersecurity
- Online courses to learn specific skills or learn about a Security tool, e.g. Coursera
- Take a course that will lead to certification, e.g. CISSP, CompTIA Security+, CSSLP,
- Look for a security organization that offers mentoring like CyberJutsu
- Be a member of a local chapter of $(ISC)^2$, ISACA, IEEE Computer Society.
- Network at work, organizations, conferences, meet-ups or online discussion groups. Grace Hopper Conference, RSA, DefCon are conferences to network for exposure and learn.
- Some high-schools and junior colleges offer programs such as NetAcad
- Include elements of Security in school projects. E.g. Confidentiality, Authentication and / or Integrity

Resources

Women in Cybersecurity (WiCyS) community: https://www.csc.tntech.edu/wicys/resources/
Women's Society of Cyberjutsu community: http://womenscyberjutsu.org/

*Key security groups "builders, breakers, and defenders" are terms coined by OWASP: See owasp.org for more details.