ANITA BORG INSTITUTE
GRACE HOPPER
CELEBRATION OF WOMEN IN COMPUTING

Student Opportunity Lab: White Hat Hackers: Careers in Cybersecurity (in conjunction with "Checking out a Career in Cybersecurity?")

Jennie Kam | Security Researcher | Cisco Systems, Inc. | jkam@utexas.edu

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 policy making 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 - Breakers

"Breakers" spend their days either breaking systems or analyzing compromised systems. Often times "breakers" come from a computer science or engineering background. There are many specializations within "breakers" that include, but aren't limited to:

Security testing | These are the "white hat hackers" who are given explicit permission to test and document the different ways a system is vulnerable. System is a broad term that could mean a wide range of things – a physical device (e.g., iPhone or Xbox), a network (e.g., university intranet), or an e-mail server (e.g., company servers). Technical knowledge of programming languages, networking, and operating systems can be useful for this field. However, soft skills can be important too. Social engineering, the art of influencing people into breaking normal security procedures, has become an

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

effective method of gaining initial entry to a system. These jobs often have titles such as security consultant, security researcher, red team member, information security analyst, or penetration tester.

Reverse engineering | This field may interest those who like puzzles and/or working backwards. Companies, academia, and government alike want malware to go from 1's and 0's to human readable code such that the good guys can learn about it. This knowledge could be used to create anti-virus or intrusion prevention products, or to learn more about what was compromised in a system breach. Knowledge of computer architecture, C/C++/Java, and algorithms can be useful in this field. Reverse engineering can have a hardware component as well – taking apart a system and looking for ways to change system firmware is a common attack. These jobs are often listed as security researcher or security engineer.

Digital Forensics | This field involves data recovery and analysis from any sort of computing system (traditional PCs to network traffic logs). Private corporations looking for insider threats, military agencies collecting global intelligence, and law enforcement are all examples of potential employers in this area. Scripting languages, networking, and big data knowledge could be particularly useful, as well as interest in the human psychology aspect. These jobs will likely require significant documentation as results are used for legal proceedings. Often, there are citizenship requirements for working in these kinds of positions.

Career Path Details - Researchers

Research happens in all sectors (government, academia, industry) to solve tomorrow's cybersecurity problems. Advances in technology increase the need for entities to stay ahead of bad actors' capabilities as well as the growing number of bad actors. Unskilled persons, often called "script kiddies", can take advantage of the widely available scripts and open source tools that automate attacks on computer systems and networks. Highly skilled actors, such as nation states and vigilante groups, are getting more sophisticated as storage and processor power become cheaper. Cryptographic algorithms that are secure due to physical computing limitations will eventually be broken, possibly by quantum computing. Some examples to read about: Logjam, Angler Exploit Kit, and Carnegie Mellon's password research team.

Practical Tips: The 3 E's

Education: Stanford's cryptography course, University of Maryland's 5-course cybersecurity series both available Coursea.org for free.
Certifications: Certified Ethical Hacker, Cisco CCNA Security, Global Information Assurance Certifications

Experience: Capture the flag (CTF) competitions: PicoCTF, CCDC, CSAW CTF

Exposure: Conferences! ACM CCS, IEEE Symposium on Security and Privacy, Defcon, Black Hat (Europe, USA, Asia), WiCyS, ShmooCon, DerbyCon, Bsides (many cities), local hackerspaces, CanSecWest (Canada), AppSecUSA, 44CON (UK), Chaos Communication Congress (Germany), ToorCon, REcon (Canada), Ruxcon (Australia), Ekoparty (Argentina)

Resources

Women in Cybersecurity (WiCyS) community:	https://www.csc.tntech.edu/wicys/resources/
Women's Society of Cyberjutsu community:	http://womenscyberjutsu.org/
Social Engineering:	http://www.social-engineer.org/
Amazon list for "Breaker" books:	http://amzn.com/w/FUVVRK2NKBIU
Reddit hiring threads:	https://reddit.com/r/ReverseEngineering https://reddit.com/r/netsec
Logjam Research	https://weakdh.org/
ACM Conference on Computer & Comm. Security	http://www.sigsac.org/ccs.html