Benevolent Hackers: Careers in Cybersecurity

Jennie Kam, Security Researcher
Jay Koehler, Engineering Manager

Abstract

We aim to educate students about the challenging but lucrative careers in cybersecurity and inspire those staying in academia to tackle the larger cybersecurity issues of tomorrow. Security professionals are highly sought-after by companies, government, and academia alike and the demand rises with each additional device connected to a network. We will share our experience in the industry and suggest methods of getting into cybersecurity without a formal university track.

Introduction

Cybersecurity is a term becoming more prevalent in our everyday news, but what exactly does it entail? Google defines it as "the state of being protected against the criminal or unauthorized use of electronic data" and Merriam-Webster says it was first used in 1994. A decade later, cybersecurity can translate to a challenging and constantly evolving career path since it's become obvious that both the Internet and criminals are here to stay.

The Internet of Everything is alive and blossoming. As more nontraditional devices (e.g., thermostats, insulin monitors, clothes) and services (e.g. credit card payments, telephone calls) incorporate electronics and Internet connections, the need for understanding electronic security is rapidly increasing as well. An obvious need for cybersecurity is online banking, but would you want someone else to be able to control the temperature in your house through your Internet enabled thermostat? Watching your networked baby monitors? Stealing your identity through your RFID enabled passport? Tampering with the electronics in your car? Changing the dosage on your wireless insulin pump? All of these threats are becoming a reality and it is critical to society that the knowledge of "white hat" (or ethical) hackers surpasses the knowledge of "black hat" (or malicious) hackers.

Careers in this industry include, but aren't limited to:

- Secure product development: Hardware and software designers
- Penetration testing: Finding vulnerabilities in computer systems and networks
- Computer forensics: Investigation of computer crimes
- Reverse Engineering: Product and malware analysis
- Defenders: Security monitoring of IT networks and secure network design
- Research (Industry, government, & academia): Solving for the seemingly impossible e.g.,
  "Can we create stronger encryption algorithms?"
  "Is biometric authentication the future or are passwords still necessary?"
  "Who or what should be a root of trust on the Internet?"

These broad career paths can be applied to a myriad of different technologies and applications – such as mobile technologies (e.g. GSM and CDMA,) wired and wireless networks, RFID, embedded systems, GPS/satellite systems used by planes, critical infrastructure systems such as the power grid. Since malicious attacks affect corporations, governments, and academia, all have a vested interest in

developing and sharing this knowledge. That is to say, you'd be hard pressed not to find a technology job that doesn't involve security.

Practical tips for exploring a career in Cybersecurity

If your school offers courses in cybersecurity, start there. If not…

- Most universities hire computer savvy students to intern with their IT department – you'll likely be exposed to real world security problems there.
- Join or start a cybersecurity club at your university so that you can gather with like-minded students and learn together. There are several university level challenges called "Capture the Flag" competitions that will provide practical experience – one of the most popular is the CSAW CTF hosted by NYU-Poly each fall (https://ctf.isis.poly.edu/).
- Stanford and the University of Maryland both offer courses on cryptography and cybersecurity through Coursera.org either free or for a small fee.
- Check out the Women in Cybersecurity organization and conference: http://www.csc.tntech.edu/wicys/resources
- FSU has a free offensive security course complete with videos, slides, and readings online (http://www.cs.fsu.edu/~redwood/OffensiveComputerSecurity/lectures.html)
- The U.S. government has formed the National Initiative for Cybersecurity Careers and Studies (http://niccs.us-cert.gov) with plenty of scholarship, internship, camp, and job opportunities listed.
- Kali Linux (formerly known as BackTrack) is a mostly free collection of penetration tools for the Linux-inclined.
- Defcon is a ~$200 conference held in Las Vegas each year where security professionals and newbies from both sides of the ethics fence descend upon each year.

There are a number of paid entry-level certifications that are respected in the industry if you've got extra cash lying around (or can find an internship with a company willing to pay for it) - Certified Ethical Hacker (CEH), RedHat Certified Security Specialist (RHCSS), Cisco Certified Network Associate (CCNA) Security, Certified Information Security Manager (CISM)

Additional Resources

Some books that provide an excellent introduction to a variety of cybersecurity areas:

- Cybersecurity and Cyberwar: What Everyone Needs to Know by Singer, Friedman
- Anything published by Syngress as they cover a wide variety of topics – The Basics of…
- Hacking: The Art of Exploitation by Jon Erickson
- The Art of Security Assessment by Dowd, McDonald, Schuh
- The Web Application Hacker's Handbook by Stuttard, Pinto

Find the complete list here: http://www.amazon.com/gp/registry/wishlist/37UGL5AYUNACB/

Send an e-mail to iwtlas@gmail.com
(**I** Want **T**o **L**earn **A**bout **S**ecurity) to get all the links and more!