# Hacking Laws and Rules

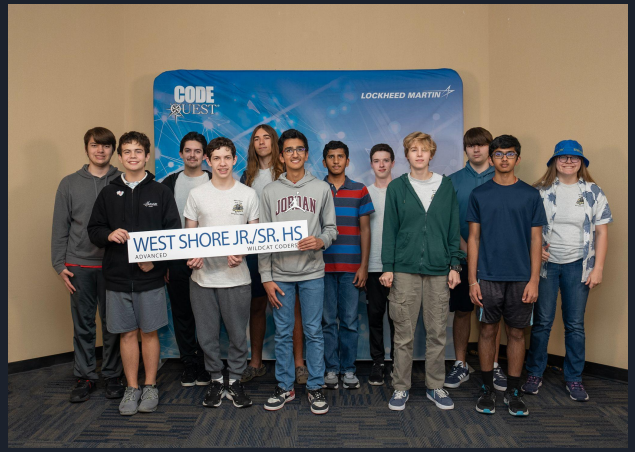
Level 0x09

# Quick Overview

- Events / Planning
- Laws and Hacking Rules

# Upcoming Events

- Code Quest
  - Saturday, March 1
  - Teams are 2-3 people
- Spring Break.  March 17-21st
- Cyber Quest
  - March 29
  - Teams are 3-5 students
- We need to setup teams and get a list of who is going




# Code Quest

- 4 Teams (2-3 students per team), 5th team is maybe / waitlist
  - Team name
  - Novice or Advanced
- Light breakfast, and lunch are provided
- Each team member can bring 1 computer, 1 monitor
- No cell phones, no cameras, no family members
- Lockheed Requirements
  - Bring IDs / Passports
  - Non-US citizens are allowed (need additional information for registration)
  - Liability Waiver and Photo Release
- Brevard County Public Schools
  - Field Trip Permission Form for BCPS

# Charlie Miller

- BS and PhD in math.  Notre Dame alum
- Apple hacking
  - Macbook Air
  - Safari Browser
  - IPhone via SMS
  - Malicous iPhone apps on Apple store
- Charlie and Chris Valasek
  - Vehicle hacking


WIRED

# Ethics and Responsibilities

- Borrowing heavily from Dr. O'Connor's Cyber Camp 2024 Slides
  - Former Florida Tech professor of Cyber Security

# Computer Fraud and Abuse Act

- Law passed in 1986, updated in 1996, 2001, 2008
- Prohibits unauthorized access (trespass) to computers and networks, extortion or threats of attack
- Transmission of code or programs that cause damage to computers or other related actions to protected computers
- Addresses unauthorized access to government, financial institutions, and other computer and network systems

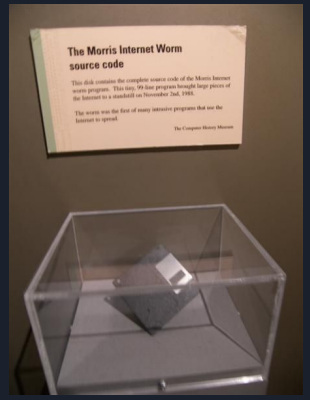
# US vs Robert Morris

What happened

- Morris wanted to demonstrate how a computer attack could spread, created one of the first computer worms
- Worm spread across university, government, and military networks

Consequences

- Prosecutors claim 10 million dollars in damages / economic impact
- Guilty under CFAA in 1990
- 3 years probations + fines




# Dangers of CFAA

- Very broad prosecutions
  - Cyber-bullying cases
  - Stealing academic papers
  - Downloading contacts from ex-employer
  - Exploiting gambling machines
  - Game console hacking
  - Google dorking
- Other possible violations?
  - Guessing friends facebook logins and using their accounts
  - Accessing teachers computer when they aren't looking
  - Flight tracking celebrities

# Digital Millennium Copyright Act (DMCA)

- Law in 1998, updated in 2000, 2003, 2006, 2010, and 2013
- Criminalizes the act of unlawful reproduction or distribution of copyrighted material
- No one should tamper with and break an access control mechanism that protects copyrighted material
- Provides an explicit exemption for encryption research for identifying flaws

# Sony vs George Hotz (GeoHot)

What happened

- Sony sued him for jailbreaking PS3
- Hotz bypassed copy protection functions
- Hotz argued he owned the PS3 and can do with it as he pleases

Consequences

- Sony and Hotz settled out of court
- Hotz barred from hacking Sony products
- Linux / OtherOS removed from PS3, lead to class action lawsuit, and $10 checks

# Dangers of DMCA

- Other possible violations?
  - Downloading a movie that you do not own from Internet
  - Game console hacking
  - Jailbreaking phones to use unofficial app stores
  - Decompilation projects
  - Emulators
  - Fan games / mods

# Types of Hackers / Security Researchers

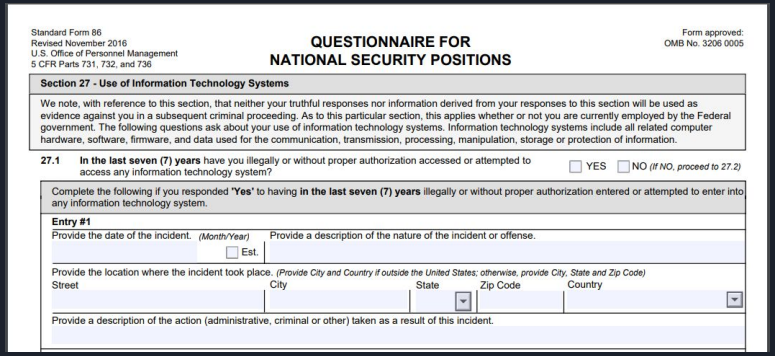
- White Hat - Ethical Hackers
  - Hired by companies / bug bounties
  - Have explicit permission to access computer systems
  - Find and secure weaknesses before others find them
- Grey Hat
  - Gain access to systems without permission
  - Motivated for fun, LOLZ, cred, or financial
  - May even report and disclose vulnerabilities to owners
  - Generally not stealing or damaging systems
- Black Hat
  - Use vulnerabilities / social engineering to gain access to system without permission
  - Steal data, financial info, and passwords
  - Destroy, encrypt, or ransom information systems
  - Botnets / DDOS

# My guidance / rules for CS Club

- Don’t break the law / or school’s rules
- **Only perform research on platforms that you are allowed / have permission**
  - CTF / training systems
  - Your own systems / computers
  - Your own door locks
- What if I find a vulnerability?
  - Don’t access systems that you are not authorized
  - **Responsible disclosure and reporting**
  - Proof of concepts only after vendor has chance to release fix
- Bug bounties / rewards for responsible research

# Hack the Planet!  sorta...

- Hack for the government
  - Intelligence communities
  - Join Cyber units of any military branch
  - DoD research labs
- Gov't contractors
- Pentesters
  - Software / networking
  - Physical security
- Bug Bounties
- Any Large companies with hacking risks (ALL)
  - Defenders
  - Internal attackers / auditors

Standard Form 86
Revised November 2016
U.S. Office of Personnel Management
5 CFR Parts 731, 732, and 736

**QUESTIONNAIRE FOR NATIONAL SECURITY POSITIONS**

Form approved:
OMB No. 3206 0005

**Section 27 - Use of Information Technology Systems**

We note, with reference to this section, that neither your truthful responses nor information derived from your responses to this section will be used as evidence against you in a subsequent criminal proceeding. As to this particular section, this applies whether or not you are currently employed by the Federal government. The following questions ask about your use of information technology systems. Information technology systems include all related computer hardware, software, firmware, and data used for the communication, transmission, processing, manipulation, storage or protection of information.

27.1 **In the last seven (7) years** have you illegally or without proper authorization accessed or attempted to access any information technology system? ☐ YES ☐ NO *(If NO, proceed to 27.2)*

Complete the following if you responded **'Yes'** to having **in the last seven (7) years** illegally or without proper authorization entered or attempted to enter into any information technology system.

**Entry #1**

Provide the date of the incident. *(Month/Year)* ☐ Est.

Provide a description of the nature of the incident or offense.

Provide the location where the incident took place. *(Provide City and Country if outside the United States; otherwise, provide City, State and Zip Code)*

Street | City | State | Zip Code | Country

Provide a description of the action (administrative, criminal or other) taken as a result of this incident.

# Attributions

- https://github.com/tj-oconnor/gencyber-camp/blob/main/slides/day-1/1-Ethics.pdf
-