Security Research

Antonio Zea Jr

In my odysse to transition from a high school math teacher to a software developer of some sort I first fell in love with the ethical hacking side of technology. My first introduction was through a periodical called Hackin9. At the time the magazine was fairly new on the sceen and the article that got me started was on a newish tool called aircrack-ng. That got me started on installing my first linux distro and trying to setup and run aircrack-ng and other tools along that vein(nmap, nessus, john the ripper, etc). Now that I have an opportunity in graduate school many years later to explore this topic I finally can fullfill my wish of creating/exploring exploits. My goal in this project will be to use the Metasploit framework to identify an exploit and create a local target for testing. Once I can successfully run exploit on the target machine I will try to rewrite the exploit and test my implementation on the target. My goal is to learn the process of creating and packaging an exploit within the context of the Metasploit framework.

In this paper I will outline the relevant legal and ethical issues related to researching, writing, and posting exploits. I will seek articulate my stance on these issues and then offer support evidence as well as alternative perspective related to these issues.

Lets start off by outlining some of the legal issues associated with researching, writing and distributing exploits. Park and Albert cite two types of legal liability relevant to security researchers, civil liability and criminal liability. Lawsuits initiated by private parties incur civil liability, while criminal liablity occurs in cases initiated by the government accusing the defendant of a crime(Park and Albert, 3-4). They outline seven main areas of U.S. law researchers need to take into account when developing exploits.

Area of law	Potentially risky activities
The Computer Fraud and Abuse Act (CFAA) (§3.1) The CFAA is the federal anti-hacking / anti-computer-crime statute.	Accessing devices that you do not own, without the owner's permission
Copyright law (§3.2) Copyright law creates legal protections for "creative" works, including software.	Copying, modifying, or running software that you didn't write and do not have the permission of the copyright holder (often, the software author) to copy, modify, or run
Anti-circumvention provision of the Digital Millennium Copyright Act (DMCA §1201) (§3.3) The anti-circumvention provision prohibits bypassing certain access-control measures.	Circumventing measures designed to prevent or restrict access to software or other copyrighted works, such as encryption or password requirements
Contract law (§3.4) Contract law imposes liability for breaching a contract you agreed to.	Experimentation that violates a contract that you may have agreed to (including terms of use/service or non-disclosure agreements)
Trade secret law (§3.5) Trade secret law aims to protect confidential business information from misappropriation.	Using or disclosing information about software or a system design that a company keeps secret from a competitor
The Electronic Communications Privacy Act (ECPA) (§3.6) ECPA is a federal statute that aims to protect the privacy of electronic communications.	Collecting, observing, or analyzing third-party data flowing over a network
The Export Administration Regulations (§3.7) Federal law imposes certain conditions on publishing or transferring cryptography/security information and technology from the U.S. to abroad.	Transferring non-published information, code, or equipment related to cryptography to a foreign destination, outside the ordinary course of research. The government has never invoked export regulations against researchers; it seems highly unlikely they would do so absent very unusual circumstances.

Table 1: Potential areas of legal risk for security researchers

All this goes to summerize that there is a lot in place to stymie security research. Even the existence of a company bug bounty programs does not implicitly guarantee that a company supports software security research. Although the process of security research can be rife with legal pitfalls the value added by the research can in many cases outweigh possible legal liability. The U.S. Department of Justice(DOJ) this summer announced a revision of its policy regarding charging violations of the Computer Fraud and Abuse Act (CFAA).

> The policy for the first time directs that good-faith security research should not be charged. Good faith security research means accessing a computer solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in a manner designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices, machines, or online

services to which the accessed computer belongs, or those who use such devices, machines, or online services. (DOJ 2022-05-19)

Under that doctrine, security research is better able to improve cybersecurity without the threat of criminal liability. I intend to use a local virtual instance of an OS I own running on a private network for pentesting purposes. Specifically, I will use virtiabox running on Arch linux host to run a Kali linux guest and a vulnerable image of Ubuntu and/or Windows XP. By running this project in a virtual network I mitigating some of possibility of creating outcomes that can impact systems outside of this local virtual network. I believe this establish the good faith standard alluded to by the DOJ.

Although that touches on the criminal liablity incured, civil liability seems like the wild west of the legal system. Companies can file cease and desist letters(C&D) as one common way of nudging a researcher to stop publishing or furthering their work. Accoridng to Park and Albert, who offer some questions that can be helpful deciding how to proceed in such instances:

- Who sent it?
- How much information does it have about your research? How much knowledge does it demonstrate about the area?
- What law does it cite and how much detail does it go into?
- Does it ask for a response by a particular date?

Park and Albert go on to point out that a C&D letter does not create any legal obligation but it can serve as a starting point for assessing any further possibility of action from a given entity. Either way their advice is to retain legal counsel, which is exactly what lawyers would say.

As we move onto the ethical implications of security research a good starting point is the Association for Computing Machinery's Code of Ethics and Professional Conduct.

- Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.
- Avoid harm.
- Be honest and trustworthy.

- Be fair and take action not to discriminate.
- Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.
- Respect privacy.
- Honor confidentiality.

From this list I will focus on Avoiding harm, Contributing to society, because I feel they highlight my thoughts on ethics of security research as they apply to my prospective final project.

In the study of vulnerabilities and exploits it is possible to accidentally damage not only my own systems but systems that maybe connected to my setup. Every reasonable step needs to be taken to mitigate this eventuality. Even though studying these artifacts can create serious issues, the gains that can made by research in security benefit all users.

By studying security and finding flaws in our practices and protocols we can develop computer systems that give society the freedom to utilize technology safe and securely. Without safety and security, culture and its development are held back. Allcott, Gentzkow, and Yu postulated that misinformation through social media was a potential threat to democracy and broader society. Their research in quantifying the amount misinformation present before, during and after the previous U.S. election cycle helps put the problem into perspective(6-7).

After discussing the legal and ethical issues inherint in the research of exploits some key take aways are as follows. The good faith doctrine adopted by DOJ in regards to the Computer Fraud and Abuse Act (CFAA) will promote privacy and cybersecurity. Avoiding harm needs to be a high priority in the pursuit of security research due to potential harm that out of control vulnerabilities can incur. Lastly, security research helps create a safer more secure system where culture can flourish.

Bibliography

Allcott, H., Gentzkow, M., & Yu, C. (2019). Trends in the diffusion of misinformation on social media. Research & Politics, 6(2). https://doi.org/10.1177/2053168019848554

“Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act.” *The United States Department of Justice*, 19 May 2022, https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act

Park, Sunno, and Kendra Allen. *A Researcher’s Guide to Some Legal Risks of Security Research*. https://clinic.cyber.harvard.edu/files/2020/10/Security_Researchers_Guide-2.pdf