Vulnerability Hunting

Ryan Scott

Grand Canyon University  
Information Security II

Prof. Christine Bakke

**Part 1: Selling Vulnerabilities**

***Unique Perspective on Hacking***

A unique aspect of the podcast is its focus on the guest's experiences as a professional hacker as well as the different motives and incentives behind hacking. These include financial gain, personal challenge, and even spying, (Planet Money, 2017).

***Compensation for Vulnerabilities?***

According to the guest, the reward for finding security vulnerabilities in products is primarily the satisfaction and accomplishment that comes with finding and exploiting such vulnerabilities, (Planet Money, 2017). Additionally, vulnerabilities do have a market, and companies or governments can provide compensation if they are willing to buy vulnerabilities for their own use. There are also instances in which companies will pay hackers "bug bounties" to alert them to vulnerabilities within their own products, (Planet Money, 2017).

***Who’s Buying Vulnerabilities?***

Among the key buyers of vulnerabilities are governments and corporations, as they seek to protect or exploit systems by purchasing information about security weaknesses, (Planet Money, 2017). In the guest's opinion, vulnerabilities are in high demand, and the government and companies (such as Zerodium) are among the most important buyers of vulnerabilities, (Pagliery, 2016).

**Legal Action vs Reward**

***Apple Lawyer vs Hackers***

If I were a lawyer at Apple, I would cite the violation of the Computer Fraud and Abuse Act (CFAA), which prohibits bad actors from accessing unauthorized computer systems. Additionally, I may be able to accuse the hackers of misappropriating trade secrets if confidential information was involved.

***Apple + Exploits Market***

There are quite a few lucrative reasons for Apple to participate in the exploits market. Apple's products are more secure when exploits are disclosed responsibly. This market also provides access to a pool of talented hackers, as well as the potential for the purchase of exclusive rights to exploits straight from the source. Participating in the exploits market is a solid defensive option to better safeguard against exploits.

**Part 2: Vulnerability Hunting Techniques**

***The Value of Monkey Testing***

Monkey testing is a beneficial technique in the software development process that involves testing software with random inputs in order to uncover unusual behavior or errors that may not be detected by traditional testing methods, (media.ccc.de, 2018). An important purpose of monkey testing is to simulate how users might interact with software in unexpected ways. This can be done by using automated scripts to randomly input data and interact with the software, allowing developers to identify potential vulnerabilities or errors, (media.ccc.de, 2018). While types of data used for monkey testing can vary, it usually includes examples you'd find in real life, such as invalid or unexpected data.

The tests can be conducted using automated tools or manually, depending on the resources available. Ultimately, the hope of the monkey test is to identify any unexpected behavior or errors that may cause the software to fail (without finding out the hard way), (Sluiter, 2020b).

***“Smart Monkey” Fuzzing***

Fuzzing programs, like Radamsa, create data that is like a “smart monkey” rather than a “dumb monkey” using a combination of random inputs and heuristics in order to generate more focused test cases, (Sluiter, 2020b). The process of fuzzing involves generating data based on knowledge of the data format or protocol being tested, rather than blindly inputting random data. This results in generating data that is more likely to trigger edge cases or unexpected behaviors. For example, Radamsa can use machine learning to learn patterns in the data it is fuzzing, and then generate new test cases that are more likely to trigger vulnerabilities, (Sluiter, 2020b).

***Using Specific Crashes to Exploit Vulnerabilities***

It would be particularly advantageous for someone to create an exploit for an application vulnerability if they observed crashes that indicated memory corruption or buffer overflows. As a result of these types of crashes, attackers could exploit the vulnerability. A malicious attacker may also be interested in crashes that occur during privileged operations, such as accessing system resources or executing code with elevated privileges, (media.ccc.de, 2018).

***How AI and ML Assist Fuzzing Testers***

Artificial intelligence and machine learning can be particularly useful for a fuzzing tester by creating fake data to test against an application. This can be done by learning patterns in the data and generating new test cases based on that knowledge. For example, Radamsa can learn from previous test cases to generate new inputs that are more likely to trigger vulnerabilities, (media.ccc.de, 2018). By learning from successful test cases that resulted in a crash or other unexpected behavior, Radamsa may be able to improve itself as it is used more frequently. In this way, Radamsa is capable of generating new test cases with even greater potential to trigger similar vulnerabilities by analyzing the inputs that caused the initial crash, (media.ccc.de, 2018).

***How to Utilize a Vulnerability***

Unfortunately for hackers, knowing about a vulnerability is not enough to exploit it. In order to exploit a vulnerability, a hacker must have both a comprehensive understanding of how the vulnerability can be exploited and the technical expertise to accomplish this task. This may involve reverse-engineering the software to understand how it works, and developing a malicious program that can take advantage of the vulnerability, (media.ccc.de, 2018).

**Part 3: Policy Questions About Vulnerability Reporting**

***National Security vs Consumer Safety***

In general, national security and consumer safety should not be viewed as mutually exclusive goals, as both are important and can often be achieved simultaneously with some nuance. However, there may be situations where prioritizing one over the other is necessary, such as in cases of imminent national security threats. As indicated by the RAND research presented in this video, national security concerns drive the vulnerabilities market, with government agencies and military organizations being among the largest buyers of zero-day exploits, (Sluiter, 2020b). This does not, however, mean that consumer safety should be overlooked. In fact, the consequences of an exploit of a vulnerability can be significant for both national security and consumer safety.

Therefore, the search for vulnerabilities must be done in a manner that strikes a balance between national security and consumer safety. Through responsible vulnerability disclosure practices, vulnerabilities can be disclosed to vendors with sufficient time to patch them before they are publicized. A collaborative and responsible approach to the identification and mitigation of vulnerabilities can also be used by government agencies and private companies.

***How Liable Should Companies Be?***

As no two vulnerabilities are the same, software companies should be held responsible to some extent for vulnerabilities in their products. The extent of liability varies depending on several factors, such as the severity, potential harm to consumers, and whether the company was aware of the vulnerability and did not take reasonable steps to address it.

The Zerodium and Zero Day Initiative (ZDI) are both examples of vulnerability brokers that buy and sell zero-day exploits. Zerodium specializes in purchasing high-value exploits, whereas ZDI focuses on finding and reporting vulnerabilities to vendors for a monetary reward. Although both companies are involved in the vulnerability disclosure ecosystem, they approach the issue very differently.

As part of Zerodium's business model, zero-day exploits are sold to customers, which may include government agencies and other organizations interested in national security. Consequently, they pay more for vulnerabilities that they can verify are causing considerable damage, (ZERODIUM FAQ, n.d.). Buying and selling exploits with the potential to be misused for malicious purposes raises many ethical concerns. In contrast, ZDI's approach is to notify vendors of vulnerabilities so that they can be patched, thus enhancing consumer product security.

***Risk Profile and Vulnerabilities***

The impact of vulnerabilities on a business' risk profile cannot be overstated. Vulnerabilities can lead to data breaches, financial losses, reputational damage, and legal liability. In addition, the impact of a vulnerability can be amplified exponentially if it is exploited by a malicious actor, such as a hacker or cybercriminal, (Pagliery, 2016).

The unfortunate truth for businesses is that vulnerabilities have a high market value, with zero-day exploits fetching millions of dollars in some cases. This creates a market incentive for hackers and other malicious actors to search for vulnerabilities and exploit them for profit, (Hat, 2017). As a business, you must implement strong cybersecurity measures in order to mitigate your risk profile. This can include patching vulnerabilities regularly, monitoring your networks for suspicious activity, and training your employees on cybersecurity best practices.

# References

Computer Fraud and Abuse Act Reform. (n.d.). Electronic Frontier Foundation. <https://www.eff.org/issues/cfaa>

Hat, B. (2017, December 29). Zero Days, Thousands of Nights: The Life & Times of Zero-Day Vulns and Their Exploits. YouTube. <https://youtu.be/8BMULyCiSK4>

media.ccc.de. (2018, December 29). 35C3 - The Layman’s Guide to Zero-Day Engineering. YouTube. <https://www.youtube.com/watch?v=WbuGMs2OcbE&feature=youtu.be>

Pagliery, J. (2016, April 7). Meet Zerodium, the company that pays $1 million for Apple hacks. CNNMoney. <https://money.cnn.com/2016/04/07/technology/zerodium-apple-hacks/index.html>

Planet Money. (2017, March 8). Episode 596: Hacking The iPhone For Fun, Profit, And Maybe Espionage. <https://www.npr.org/sections/money/2017/03/08/519298871/episode-596-hacking-the-iphone-for-fun-profit-and-maybe-espionage>

Removals and SafeSearch reports Tool - Search Console Help. (n.d.). <https://support.google.com/webmasters/answer/9689846?hl=en>

Sluiter, P. W. P. (2020b, May 31). How to find Zero Day exploits. YouTube. <https://youtu.be/oeEEZWI3cfM>

Sluiter, S. (2021). GitHub - shadsluiter/GoogleHacking: Related to Google Hacking aka Dorking. GitHub. <https://github.com/shadsluiter/GoogleHacking>

ZERODIUM - FAQ About How to Sell Your Zero-Day (0day) Research and Exploits. (n.d.). <https://zerodium.com/faq.html>