**Vulnerability Hunting**

Austin Johns

ITT-306

Professor Kris Peters

3 March 2021

**Part 1: Selling Vulnerabilities**

Listen to “Episode 596: Hacking the iPhone for Fun, Profit, and Maybe Espionage,” explore the “Zerodium Questions and Answers (Q & A),” and read “Meet Zerodium, the Company that Pays $1 Million for Apple Hacks,” then answer the questions below. Use full sentences and supporting evidence to justify your responses.

1. Hacking is not new or news. How does the podcast “Episode 596: Hacking the iPhone for Fun, Profit, and Maybe Espionage” provide a unique perspective on the world of hacking?
   1. The podcast offers a unique perspective because they brought on the individual that found out about the bug in Apple’s system. The perspective was opinion and fact-based, but this mix showed a unique perspective on the situation. The hacker found the hole in the operating system and kept this idea secret to profit off of the information. He went into business with another person that betrayed this plan and sold the information to Chinese hackers that created Jailbreaking.
2. According to the guest of the podcast “Episode 596: Hacking the iPhone for Fun, Profit, and Maybe Espionage,” what type of compensation is fair for people who find vulnerabilities in products?
   1. The guest on the podcast stated that there is a huge market for this kind of bug. In the podcast, the guest detailed that the Chinese market had many restrictions in the App Store provided by Apple. By finding this bug, the hackers can bypass Apple’s App Store and implement any changes to the device that they would like. For this kind of information that will lead to these types of freedoms, there is a lot of money involved.
3. What does the podcast identify as important buyers of vulnerabilities?
   1. The buyers of the vulnerabilities are hackers in other countries. These hackers create backdoors into the operating system by allowing any applications to be downloaded to the operating system. In this context, the app market has a much larger opportunity for profit, so the “Jailbreakers” would be very interested in this vulnerability.

**Legal Action versus Rewards**

Companies have several options for protecting their assets. One is legal; they can sue people who find exploits. Another option is a reward; they can play the market for buying vulnerabilities.  The following two questions allow you to weigh in with your opinion.

1. Suppose you are a lawyer for Apple. What arguments might be made for pursuing legal action against hackers who expose vulnerabilities? What is the legal case against the buyers of these exploits?
2. What arguments might be made to Apple executives for participating in the exploits market and offering rewards to hackers who discover exploits?

**Part 2: Vulnerability Hunting Techniques**

Watch “Bug Finder Bounties, Fuzzing Software Security, Zero-Day Exploits and a Radamsa Demonstration,” and the first 34 minutes of “35C3 – The Layman’s Guide to Zero-Day Engineering” for an overview of techniques used to find vulnerabilities in a piece of software. Answer the questions below using full sentences and supporting evidence to justify your responses.

1. Describe the value of monkey testing in the software development process. What types of data are used for the test? How are tests conducted? What resources are needed? What results does the test hope to find?
   1. In software development, monkey testing is valuable because it highlights any unplanned or accidental bugs in the way a program handles input. “Monkey Testing” refers to randomly inputting a set of numbers, characters, etc. into a program to find a handling error. Tests are conducted at random. Different parts of an app are clicked, tapped, and different inputs are included to test how the application handles it. There aren’t many resources needed, just a tester that is willing to sit and randomly mess with a program. Hopefully, this testing yields a result. Most likely, the result will be a logic discrepancy that requires debugging.
2. Describe how a fuzzing program, such as Radamsa, creates data that is like a “smart monkey” rather than a “dumb monkey.”
   1. A fuzzing program helps to generate broken and invalid inputs for the program to handle. If error handling is designed into the program, there should be an error that results. However, if some errors are not planned for, the fuzzing program is designed to help detect them.
3. Based on features of operating systems security, what types of application crashes would be interesting to a person trying to create an exploit of a vulnerability of an application?
   1. Application crashes that a hacker would want to exploit usually surround security. For example, Shell Shock was a fuzzing hack that allowed for access to the shell of a Unix operating system. Furthermore, there are many cases when hackers will attempt to exploit vulnerabilities in web browsers. Many web browsers harbor sensitive information that hackers would be interested in like card numbers, emails, birthdays, etc.
4. Describe how artificial intelligence, using machine learning, helps a fuzzing tester create fake data to test against an application? Give a machine learning scenario in which a program like Radamsa could improve itself with more usage.
   1. In an environment that fuzzing is used, the fuzzing program could be much more effective if it were self-learning. For example, designing a program that would be recording information about how the program responds to some of the inputs would allow the program to make more targeted “decisions.” In these decisions, the program could find the vulnerability or bug in the program without much interference from the user.

Explain the following phrase: “A known vulnerability is a necessary condition, but not a sufficient condition, for an exploit.” What next step needs to be completed after a vulnerability is discovered for a hacker to utilize the programming flaw?

The phrase means that the vulnerability must exist for a hacker to exploit, but the vulnerability itself is not the exploit. The hacker has to be able to exploit the vulnerability. A vulnerability can exist without any issues happening. That’s when the hacker steps in. The hacker has to have the knowledge and take the action. When a vulnerability is found, there are multiple steps that the hacker must take to exploit it. There is an infinite number of possibilities, but the hacker has to figure out how they would like to use the vulnerability. For example, if a hacker finds a hole in the sign-in of a program, they still need to figure out how to manipulate data/systems to their benefit.

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

The video “Zero Days, Thousands of Nights: The Life & Times of Zero-Day Vulns and Their Exploits” raises three questions based on the RAND Corporation research. View the video and use the facts presented by RAND to support your answers to the following questions. These are open-ended questions that require a well-supported answer.

1. Should we prioritize national security, or consumer safety and company liability when hunting for vulnerabilities?
   1. In a conversation about national and personal security, both sides have valid opinions and views. However, to protect the individuals of a nation, I believe that national security should be prioritized. I think that there is a larger negative effect if there are vulnerabilities in national systems. If information falls into the wrong hands, there is a potential for a much larger negative impact than if the information of a few, or more than a few, individuals have their information exposed. However, I do believe that the importance of protecting the consumer cannot be understated. In a vulnerability surrounding the consumer, there could be other vulnerabilities for other consumers, so this could have a larger effect. Overall, for the well-being of the country that the consumer lives in, I think that national security is slightly more urgent than the security of individual consumers for the lone factor that it protects the country they reside in. Without the security of the country, the consumers may not have an opportunity to be consumers.
2. To what extent should software companies be liable for vulnerabilities in their consumer products? How do the Zerodium and Zero Day Initiative relate to this question?
   1. In consumer products, if software companies are putting consumers at risk, they should be liable. If the software company stores sensitive information, they should understand the importance of protecting this information. If the protection of the information is not well planned for and not well-tested, the company should be held accountable. However, in the event that the company did not have control of the situation, the company should have some grace. Zerodium pertains to this question because they are a leading company in the force preventing Zero-Day disasters. In many areas, the company is uncovering vulnerabilities, and they have the power to go public or keep information private. Zerodium has an opportunity to protect companies or protect the public. For this reason, Zerodium must assess the effects of the vulnerabilities, and using a moral compass, decide whether or not to share the information with more than just the company it involves.
3. What is the impact on a business’ risk profile concerning vulnerabilities?
   1. A business’ risk profile is a detailed report that describes threats that can expose a business. If a vulnerability is exposed about a business, this would be added to the risk profile. In investment and marketing, a risk profile is ideally non-existant. In the world we live in, with many online connections, unfortunately, this is rarely the case. A business with zero risk would have to be very small and simple. However, in a technology era, there are many ways that a business’ risks can be exposed and exploited. Therefore, a business with many risks may have a hard time finding investors and keeping customers.