Activity 8: Part 3

Ryan Coon

CST-407

Professor Ty Howard

February 11, 2024

How are Software Vulnerabilities Discovered?

a.Research resources for “How to Find Zero Day Exploits." Describe the value of “Monkey Testing” in the software development process.

Monkey Testing is a software testing technique where the application is tested with random, unexpected, or invalid inputs to uncover unexpected behaviors or vulnerabilities. Monkey Testing is valuable because it can reveal issues that may not be discovered through traditional testing methods. By subjecting the software to random and unexpected inputs, the testing process can uncover unanticipated bugs, edge cases, or vulnerabilities that may not have been considered during the development phase.

b.Describe how a fuzzing program, such as Radamsa, creates data that is like a “smart monkey.”

Fuzzing programs, such as Radamsa, are designed to generate random or mutated data to be used in software testing. This creates data much like a “smart monkey” as Radamsa  generates diverse and meaningful input variations that can effectively uncover unexpected behaviors and vulnerabilities in the software under test.

c.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?

d.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 in order for a hacker to utilize the program flaw?

The phrase "A known vulnerability is a necessary condition, but not a sufficient condition, for an exploit" implies that the existence of a known vulnerability in a software program is a critical prerequisite for a potential exploit to occur, but it alone is not adequate to launch an exploit. In other words, while the presence of a vulnerability provides a starting point for a potential attack, additional steps and factors are typically required for an exploit to be successfully carried out. The next step after discovering a vulnerability would be that the attacker would have to learn about the nature of it. What causes it, potential impact, and how it can be triggered. Only then can the attacker devise an exploit strategy for the vulnerability.

The video "Zero Days, Thousands of Nights" raises three questions based on the research. These are open-ended questions that require well-supported answers. Use the facts presented by RAND to support valid answers for the following:

a.Should we prioritize national security or consumer safety and company liability?

In my opinion, I do not feel that it should escalate to national security level unless the threat is to a valid government system. We should however prioritize consumer safety and put companies liable for their handling of vulnerabilities and exploits brought on by them. The only way the government should be brought in is if a company cannot handle the attacks, which could potentially put their consumers at risk of losing more than just money, should be called to step in and mitigate the attacks and penalize the company. According to the video zero-day exploits have an average life span of around 7 years, it should not take this long to find flaws in their systems. If a company looked more into securing their products rather profits, I feel that exploits would be handled in a more timely manner.

b.Should software companies be liable for vulnerabilities in their products?

In my opinion they should be liable to an extent. If they are actively trying to sort out their vulnerabilities and paying off site ethical hackers to help them locate them, then I feel that they should not be held liable. If say the company has had that system up and running for 10 years plus and they are doing nothing to stop or even intercept their vulnerabilities, then yes they should be held totally liable and face whatever consequences come their way.

c.What is the impact to a business’ risk profile?

If a business has a known vulnerability and it gets exposed to the public, the business’ profile can take a big hit among other things. They can lose business, lose trust in their past, present, and future customers, and possibly even go bankrupt due to this.

Section B: How Much are Vulnerabilities Worth?

1.Review the associated resources located in the Topic Materials. Then address the following questions making sure to justify your rationale with supporting evidence:

a.Hacking isn’t new or news. How does "Episode 596: Hacking the iPhone for Fun, Profit, and Maybe Espionage," provide a unique perspective on the world of hacking?

This podcast is about the million-dollar Apple vulnerability in that the hacker who found the vulnerability was able to sell information for a million dollars. This opens our eyes to the black-market sales of zero-day exploits. Knowing that there is a black market for these vulnerabilities, companies now employ a team to find these zero-day exploits without having to pay a “ransom” for them.

b.According to the guest of the show, what type of compensation is fair for people who find vulnerabilities in products?

The guest on the podcast did not mention a fair price. However he did state Johnny Mnemonic would find zero-day exploit and sell them for a few thousand dollars. The podcast goes on to play a recorded business deal where “Ty” negotiated an Apple exploit for $350,000.

c.What does the show say who are important buyers of vulnerabilities?

According to the podcast, he states that the Chinese businessmen are willing to pay a lot of money for exploits. With this information, one can only assume that these are the most important buyers of vulnerabilities.

d.How closely does the podcast's conclusions compare with those of "Thousands of Nights" presentation by RAND in regard to the effectiveness of services like Zerodium?

When you compare the conclusions of the two, you can see that they differ in a few ways. The employee of RAND stresses the need to collect real-world data on zero day exploits so that the public is better informed and more prepared to deal with them. The hacker on the NPR podcast leads me to believe that he would sell to Zerodium, as they seem to be the highest paying among buyers. I was also stated that vulnerabilities have no end date and are possibly still being sold to governments or other buying entities.

e.Your Opinion: Companies have several options for protecting their assets. One is legal; they can sue people who find exploits. Another option is reward; they can play the market for buying vulnerabilities. Which of these has the stronger case? Support your answer with facts presented in the resources.

I feel that if a company would go the legal route and sue anyone who finds exploits, would just push more of the activity to the black market. There is a way they can keep it legal by offering bounties for exploits. This way they don’t have to pay a ransom which would make it illegal of having to employ a team that could potentially cost double what these bounties would. This is my opinion and could save a company a lot of money in salaries and ransom payments while still remaining legal.

References:

Black Hat. (2017, December 29). Zero Days, Thousands of Nights: The life & times of Zero-Day Vulns and their exploits [Video]. YouTube. <https://www.youtube.com/watch?v=8BMULyCiSK4>

Npr. (2017, March 9). Episode 596: Hacking the iPhone for fun, profit, and maybe espionage. NPR. https://www.npr.org/sections/money/2017/03/08/519298871/episode-596-hacking-the-iphone-for-fun-profit-and-maybe-espionage

Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2018). Security in Computing: 5th Edition. <https://dl.acm.org/citation.cfm?id=2756777>

Programming w/ Professor Sluiter. (2020, May 31). How to find Zero Day exploits [Video]. YouTube. https://www.youtube.com/watch?v=oeEEZWI3cfM