The Economics of Cybersecurity — Lecture 13 Notes

Adam Hastings

April 16, 2024

1 Introduction: Types of Exploits

Let's clarify some terminology:

- **Bug** — unintended behavior. Could be a security issue, often times is not. Example:
- **Vulnerability** — A specific instance of a bug that has the potential to be exploited. Makes the device running the code vulnerable. Example: Memory safety violations, integer overflow, executing untrusted unsanitized input (e.g. SQL injection). *What is the name of the database that tracks vulnerabilities?* Technically the NVD (National Vulnerability Database — run by NIST!) is the *database*, but the entries are generally known by their *CVE* number (e.g. CVE-2021-44228).
- **Exploit** — Something that takes advantage of a vulnerability to achieve some goal. Important to note though that oftentimes there is a large gap between a vulnerability and an exploit! *Why?* A vulnerability can be thought of as a "foot in the door", but a vulnerability alone is rarely enough to do anything useful.

2 Characterising 0-Day Exploit Brokers

Ask: What's a 0-day? Why are they important in security and in security economics?

This paper is an empirical study of the marketplace for 0-day exploits. Specifically, it tracks prices from public 0-day brokers, which facilitate exchanges beteween 0-day buyers and 0-day sellers. *This is fairly similar to the Hack-for-Hire paper we read, but what are some of the key differences?* (Empirical, not experimental; 0-day market, not hacking-as-a-service market.)

- *Who are the buyers?* Zerodium claims to sell to "Western governments". Don't know how to verify this claim. Generally as part of the terms of agreement, the buyer is supposed to get exclusive rights to the exploit. *How do you ensure no double-selling?* I don't know. Maybe a research project.

- *Who are the sellers?* A bit unclear; My understanding is that there are private hackers out there who are good at finding and exploiting vulnerabilities and are willing to sell to the highest bidder.
- *What is the role of the broker? Are they just a middleman?* They serve a key role actually! Stockpiling and modulating the rate of 0day releases. Useful for offensive actors to have a steady supply of resources, because they usually have a limited shelf life. Who does this help economically? The sellers! The brokers create a market and can keep prices high. Don't need to worry about gluts or timing the market. Also, the buyer wants a steady supply too. So yes a middleman but one that actually improves outcomes for both buyers and sellers. Not just rent seeking!!)

2.1 Methods

Figure 1: Data was collected from snapshots on the Wayback Machine.

Threats to the validity of this data?

- Shows max prices only

2.2 Results

Figure 2: Prices are in the millions and have been for several years.

Figure 3: Spikes are an artifact of data collection. *Which types of applications have the highest-priced 0-days?* Browser and messengers apps. *Why are browser and messenger exploits worth more?*

- Maybe because more people use them?
- more universal?
- Others?

They actually quantitatively address this later in the paper.

Figure 4: *Which types of exploits are most valuable?* (zero click, persistence). What does this mean? Let's define some of these acronyms:

- **rce** — *Remote Code Execution.* Attacker has the ability to execute code on the victim's device.
- **lpe** — *Local Privilege Escalation.*
- **sbx** — *Sandbox Escape or Bypass. Can someone tell me what a sandbox is here in this case?* E.g. web browser, containers.

- **persistence** — Some types of malware may only be active for a few seconds or less; others may become malicious processes that inject themselve into memory and may try to hide themselves. *If a process exists only in memory and the machine is rebooted, what happens?* The malware is gone. If the attacker was trying to spy on the user, or just keep the malware alive with the intention of doing something malicious later, then simply rebooting will remove this malicious process from the device.
- **vme** — *Virtual Machine Escape.* A form of sbx?
- **zero click** — Exactly what it sounds like. Victim requires no interaction or "mistake".
- **requires local access** — Exactly what it sounds like. (Note the price is lower)
- **bypass** — bypasses specific security mechanisms (ASLR? NX-bit? Not sure which ones; unspecified)

Is it surprising or expected that zero-click and persistence are the most valuable? Why or why not?

How does this data compare to what is currently on Zerodium's home page?

What other trends do we notice? Growth (although they show max prices only? So of course these will be monotonic.)

Figure 5: *Which types of OS are most valuable?* IoS and Android. Both mobile! *Why?* Phone calls are sensitive; things are said that deliberately don't get written in text, perhaps? *Or is it because these platforms are harder to attack?* Probably not. General impression is that iOS is pretty secure, Android is insecure. Yet prices are very similar! I find this interesting.

2.3 Linear regression

I think CS people think of themselves as quantitative people yet are often a bit lacking when it comes to knowing quantitative methods (or maybe I'm just telling on myself). I could easily skip over the next part of this paper but it's so common in economics but also so common in data science and machine learning that I'm going to cover it here too.

Poll: Who knows what linear regression is? This is a really fundamental technique in data analysis you all should know. OLS is "curve fitting" — finding a line that minimzes distance betwen line and datapoints.

When fitting a curve, you want to find the line that most closely follows the data and "punish" the distance between the line and the datapoint. One common method is RSS (residual sum of squares):

$$RSS(b) = \sum_{i=1}^{N} (y_i - x_i^T b)^2$$

where β is the coefficients to the polynomial.

In OLS you are trying to minimize RSS, i.e. find

$$\hat{\beta} = arg\, min_b RSS(b) = (X^T X)^{-1} X^T y$$

which fortunately has a closed for equation.

2.3.1 Goodness of fit

The next part talks about R^2 values. *Show of hands—who knows what an R^2 score is?* R^2 is a measure betwen 0 (no correlation) and 1 (perfect correlation) that tells you how well the line whose parameters you found in OLS fits the data. It's defined as:

$$R^2 = 1 - RSS/TSS$$

where TSS is the Total Sum of Squares, defined as

2.3.2 Log-linear regression results

- Properties of the exploit (functionality it achieves) has the most explanatory power
- Targeted system has comparably little explanatory power.
- Some of the results are questionable (local access being a positive indicator of price?)

2.4 Extended discussion

- *Why advertise prices at all?* Authors pose this question. For attention perhaps? Might be surprising that buyers are OK with information leakeage (e.g. upped prices in niche email application)
- *Can we use prices as a predictor of risk?* If Zerodium is upping the price of exploiting some piece of software that you write, how should you react? What if you use the software in question?

3 Hacking for good: Leveraging HackerOne data to develop an economic model of Bug Bounties

Let's talk about bug bounties. Many companies have bug bounty programs where they will pay researchers money for disclosing bugs (especially security bugs). This is a mechanism for measuring the costs of security (not a very good one though).

What is HackerOne? Or Bugcrowd? Crowdsourced bug bounty programs.

How is this different from Zerodium or Crowdfense? Recall: Bugs != exploits (although some bug bounties require proof of exploit before paying). Biggest difference is the buyers. In crowdsourced bug bounty programs, the product vendor themselves are the ones paying for the disclosure, with the intention of **patching** rather than **exploiting**.

My impression from being around the cybersecurity community is that bug bounties are a nice little extra cash for people but no one treats them as a job.

3.1 Extended Discussion

4 Post-Paper Reading Discussion

Some questions to chew on:

- *Why do exploits pay so much more than bug bounties?* There's almost no limit to the amount the US will pay to read Putin's emails. Whereas companies have no liability for vulnerabilities (yet—remember National Cybersecurity Strategy?) so paying bug bounties at all is almost just pure altruism (or is it?).

5 Pwn2Own

Pwn2Own is an annual hacking competition with low millions of prize money. Participants