Software Vulnerability Lifecycle and Vulnerability Markets

Subjects: Computer Science, Software Engineering
Contributor: Abdullah M. Algarni

Vulnerability lifecycles and the vulnerability markets are related in a manner that can lead to serious security and economic risks, especially regarding black markets. The subject of software security has emerged as a primary concern and has once again been raised by individuals and government agencies in terms of risks of violations regarding information security, cybersecurity, and the consequences for the economy, especially in relation to attacks from actors with special agendas. Therefore, software vulnerabilities have major effects on the developmental paths of technology, development, and investment.

Keywords: software vulnerability ; vulnerability lifecycle ; vulnerability markets ; software security ; risk management

1. Introduction

A vulnerability is established when a code or specification error occurs. Therefore, the possible vulnerability lifecycle has many phases including discovery, disclosure, patching, and exploitation. These phases have several impacts, particularly discovery and exploitation, that could be critical phases for determining the degree of risk involved. Potential vulnerability exploitations will have a major economic impact on the software industry, including software vendors and end users (i.e., individuals and organizations). A data security breach can cause a loss of confidentiality, including leaks to groups deemed dangerous to society, leading to direct and indirect cost losses [1][2].

There is a relationship between the number of code development changes in such software, resulting from software development methods and the probability of discovering software vulnerabilities that can lead to changes in the software security [3]. Therefore, vulnerability disclosure policies that release patches for those discovered vulnerabilities are key to reducing the impact on security and the economy, especially if the disclosure is made by reliable agencies, since it has a direct effect on the vendor patch time [4]. If the vulnerabilities are not patched by the software vendor, zero-day exploits will have been identified, and the related security risks of vulnerability exploitation and disclosure will have increased [5]. Some studies have been conducted on the vulnerability lifecycle and the major players in a security ecosystem involving discovery motivations, along with search tools, vulnerability markets, criminals, vendors, security information providers (SIPs), and the public, based on thousands of publicly disclosed vulnerabilities [6].

Financial rewards are often the primary motivation for discoverers looking to detect vulnerabilities, and are frequently the reason for attacking people and organizations. Therefore, the discovery phase is becoming the main phase to focus on, since it has the most impact on vulnerability markets. Private organizations, and even several governments, now participate in vulnerability markets where vulnerabilities are traded. Vulnerability markets have expanded to include legitimate, grey, and black markets [7][8]. Legitimate markets are encouraged by creating vulnerability rewards programs (or bug bounty programs), especially in the investigation of crowdsourcing vulnerability discovery events [9] and the protection of smart cities and e-governments that use the Internet of Things (IoT) against any potential security attacks [10] [11] by investigating alternative economic solutions, encompassing everything from incentive systems to market-based solutions [12]. The average cost of running these reward programs for a year is currently less than the cost of recruiting two additional software engineers [13]. In addition, vulnerability rewards programs reduce the risks associated with using different types of markets, such as black markets, where discoverers can maximize their incentives and the main customers intend to use these vulnerabilities to attack specific targets for money. From this perspective, encouraging the establishment of many reward programs will minimize black transactions and their implications, and these programs can play a great role in supporting cybersecurity [14][15]. Based on this idea, searching for new, effective, and worthy vulnerability rewards based on a modern economics model should fill the gap between these types of markets [16][17].

Many studies illustrate that each phase of the vulnerability lifecycle is likely to have a correlation with some types of vulnerability markets, and that this can produce some risks to economics and security. For example, Munaiah and

Meneely [18] demonstrated, using empirical analysis, the weak relationship between the Common Vulnerability Scoring System (CVSS) and reward incentives based on 703 vulnerabilities across 24 products. However, Burkart and McCourt [19] and Allodi [20] conducted a study on the economics of vulnerability exploitation based on data collected from a cybercrime market. They found strong evidence of a correlation between vulnerability market activities and the probability of exploitation, which led to varying exploitation prices.

Other studies have strongly focused on the response of vendors' patching behaviour with regard to the impact of vulnerability disclosure threats and the presence of competitors [21]. Anderson et al. proposed 15 policies that tackle issues related to information security and that affect the security economics of the European Union [22]. In addition, they encourage internet service providers (ISPs) to take serious steps in terms of cleaning infected devices and taking care of all information or databases that contain cybersecurity incidents as well as breaches that hugely impact economics [23]. Even the reporting of software vulnerabilities in products can adversely affect the software vendors' market value [24].

2. Vulnerability Lifecycle Phases

The vulnerability lifecycle model [25][26] shows how a vulnerability evolves over time. The lifecycle of a vulnerability is divided into phases based on distinctive points in time, where each of them indicates a state and an associated risk [25]. Thus, the term vulnerability lifecycle denotes a fixed and linear progression from one phase to the next in order to comprehend vulnerability behavior. The following have been addressed as possible states of vulnerability:

- Birth: this refers to the occurrence of a software defect or flaw.
- Discovery: the vulnerability in the software product is discovered. The vulnerability discoverers can be either black hats or white hats.
- Disclosure: the discoverers have the option of exposing the details of the vulnerability to the developer or to the general public.
- Correction (patching): the vulnerability is fixed by releasing a software modification through software vendors or developers.
- Publicity: a vulnerability can be made public in different ways.

  Scripting (exploitation): anyone with moderate skills can successfully exploit a new vulnerability.
- Death: this state occurs when the vulnerability has been patched or the attackers have lost interest.

Vulnerability lifecycle discussion can aid the development, deployment, and maintenance of software systems, as well as the formulation of future security rules and the auditing of previous incidents. As a result, security concerns regarding different software products from various vendors can be assessed [27].

The sequence states of exploitation, disclosure, and patching are not always fixed [28] as sometimes the exploitation and patching can occur at a time that is earlier than, at the same time as, or after the disclosure state.

3. Vulnerability Market Types

Depending on the motivation of vulnerability discoverers, different types of vulnerability markets emerge. Algarni and Malaiya [7] studied discoverers' motivations and described current vulnerability markets where sellers (discoverers) and buyers (consumers) trade vulnerability.

In general, vulnerability markets are divided into legitimate (including regulated and unregulated markets) and illegitimate markets. A brief description of these is provided below.

3.1. Regulated Vulnerability Markets

These are controlled by conventions and laws to prevent any non-suitable actions against society as a whole. These types of market include the following:

- Publicity: the discoverer submits the vulnerability to an authority, such as software developers. money or a reward is not the main motivation for the discoverers. They always focus on building their reputations as capable researchers.

- Captive market: the discoverers belong to organizations. Thus, they are not allowed to reveal the discovered vulnerabilities externally.
- Vulnerability rewards from vendors: the discoverers can sell their findings directly to software vendors through some current rewards programs. These programs provide a good and legitimate option for discoverers to obtain rewards as opposed to resorting to other illegitimate alternatives.
- Rewards by security service companies: these companies discover a vulnerability for two main reasons: to provide a high level of security for their subscribed customers or to sell the vulnerability to software developers only.

3.2. Vulnerability Gray Markets (Brokers)

These are considered a legitimate market but are partially regulated by some general rules. A broker may sell a vulnerability to software developers or to some government agencies depending on who can pay more.

3.3. Online Forums

These online places are classified as an illegitimate market because the main objective of these forums is to exchange vulnerability information and exploit hacktivists, who plan to attack specific organizations globally, achieve a special agenda, or send specific messages, such as when the LulzSec group attacked several global websites in 2011. Thus, money is generally not the main goal in these cases.

3.4. Vulnerability Black Markets

These are not regulated and are therefore illegitimate markets because they are not controlled by any rules or laws. Thus, any unknown groups or organizations can buy zero-day vulnerabilities that might harm targeted organizations in several countries. Many black markets or forums exist solely to facilitate underground transactions for the exchange of malware, information theft, and other services [29]. Therefore, the vulnerability price paid to discoverers is much higher than in other vulnerability markets, and this will encourage them to sell their vulnerabilities in these black markets, which is the main risk source.

References

1. Algarni, A.M.; Malaiya, Y.K. A consolidated approach for estimation of data security breach costs. In Proceedings of the 2nd International Conference on Information Management (ICIM), London, UK, 7–8 May 2016; pp. 26–39.
2. Algarni, A.M.; Thayananthan, V.; Malaiya, Y.K. Quantitative assessment of cybersecurity risks for mitigating data breaches in business systems. Appl. Sci. 2021, 11, 3678.
3. Arnold, B.; Qu, Y. Detecting software security vulnerability during an agile development by testing the changes to the security posture of software systems. In Proceedings of the 2020 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 16–18 December 2020; pp. 1743–1748.
4. Arora, A.; Telang, R.; Xu, H. Optimal policy for software vulnerability disclosure. Manag. Sci. 2008, 54, 642–656.
5. Kuehn, A.; Mueller, M. Shifts in the cybersecurity paradigm: Zero-day exploits, discourse, and emerging institutions. In Proceedings of the 2014 New Security Paradigms Workshop, Victoria, BC, Canada, 15–18 September 2014; pp. 63–68.
6. Frei, S.; Schatzmann, D.; Plattner, B.; Trammell, B. Modeling the security ecosystem-the dynamics of (in) security. In Economics of Information Security and Privacy; Moore, T., Pym, D., Ioannidis, C., Eds.; Springer: Berlin/Heidelberg, Germany, 2014; pp. 79–106.
7. Algarni, A.; Malaiya, Y. Software vulnerability markets: Discoverers and buyers. Int. J. Comput. Inf. Sci. Eng. 2014, 8, 71–81.
8. Algarni, A.M.; Malaiya, Y.K. Most successful vulnerability discoverers: Motivation and methods. In Proceedings of the 2013 International Conference on Security and Management (SAM), Washington, DC, USA, 2–6 September 2013; p. 1.
9. Fryer, H.; Simperl, E. Web science challenges in researching bug bounties. In Proceedings of the ACM Web Science Conference, New York, NY, USA, 25–28 June 2017; pp. 273–277.
10. Zhou, J.; Hui, K. Bug bounty programs, security investment and law enforcement: A security game perspective. In Proceedings of the 2019 Workshop on the Economics of Information Security (WEIS), Boston, MA, USA, 3–4 June 2019.

11. Li, Z.; Liao, Q. Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets. Gov. Inf. Q. 2018, 35, 151–160.
12. Li, Z.; Liao, Q. An economic alternative to improve cybersecurity of e-government and smart cities. In Proceedings of the 17th International Digital Government Research Conference on Digital Government Research, Shanghai, China, 8–10 January 2016; pp. 455–464.
13. Walshe, T.; Simpson, A. An empirical study of bug bounty programs. In Proceedings of the 2020 IEEE 2nd International Workshop on Intelligent Bug Fixing (IBF), London, ON, Canada, 18 February 2020; pp. 35–44.
14. Ruohonen, J.; Allodi, L. A bug bounty perspective on the disclosure of web vulnerabilities. In Proceedings of the 17th Annual Workshop on the Economics of Information Security, Innsbruck, Austria, 18–19 June 2018.
15. Arora, A.; Telang, R. Economics of software vulnerability disclosure. IEEE Secur. Priv. 2005, 3, 20–25.
16. Kesan, J.P.; Hayes, C.M. Bugs in the market: Creating a legitimate, transparent, and vendor-focused market for software vulnerabilities. Ariz. Law Rev. 2016, 58, 753–830.
17. Ransbotham, S.; Mitra, S.; Ramsey, J. Are markets for vulnerabilities effective? Mis Q. 2012, 36, 43–64.
18. Munaiah, N.; Meneely, A. Vulnerability severity scoring and bounties: Why the disconnect? In Proceedings of the 2nd International Workshop on Software Analytics, Seattle, WA, USA, 13 November 2016; pp. 8–14.
19. Burkart, P.; McCourt, T. The international political economy of the hack: A closer look at markets for cybersecurity software. Pop. Commun. 2017, 15, 37–54.
20. Allodi, L. Economic factors of vulnerability trade and exploitation. In Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, Dallas, Texas USA, 30 October–3 November 2017; pp. 1483–1499.
21. Arora, A.; Forman, C.; Nandkumar, A.; Telang, R. Competition and patching of security vulnerabilities: An empirical analysis. Inf. Econ. Policy 2010, 22, 164–177.
22. Anderson, R.; Böhme, R.; Clayton, R.; Moor, T. Security economics and European policy. In ISSE 2008 Securing Electronic Business Processes; Pohlmann, N., Reimer, H., Schneider, W., Eds.; Springer: Berlin/Heidelberg, Germany, 9 October 2008; pp. 57–76.
23. Moore, T. The economics of cybersecurity: Principles and policy options. Int. J. Crit. Infrastruct. Prot. 2010, 3, 103–117.
24. Telang, R.; Wattal, S. An empirical analysis of the impact of software vulnerability announcements on firm stock price. IEEE Trans. Softw. Eng. 2007, 33, 544–557.
25. Arbaugh, W.A.; Fithen, W.L.; McHugh, J. Windows of vulnerability: A case study analysis. Computer 2000, 33, 52–59.
26. Marconato, G.V.; Kaâniche, M.; Nicomette, V. A vulnerability life cycle-based security modeling and evaluation approach. Comput. J. 2013, 56, 422–439.
27. Shahzad, M.; Shafiq, M.Z.; Liu, A.X. A large scale exploratory analysis of software vulnerability life cycles. In Proceedings of the 34th International Conference on Software Engineering (ICSE), Zurich, Switzerland, 2–9 June 2012; pp. 771–781.
28. Frei, S.; May, M.; Fiedler, U.; Plattner, B. Large-scale vulnerability analysis. In Proceedings of the 2006 SIGCOMM Workshop on Large-Scale Attack Defense, New York, NY, USA, 11–15 September 2006; pp. 131–138.
29. Yue, W.T.; Wang, Q.; Hui, K. See no evil, hear no evil? Dissecting the impact of online hacker forums. Mis Q. 2019, 43, 73–95.