Most Successful Vulnerability Discoverers: Motivation and Methods

Abdullah M. Algarni, and Yashwant K. Malaiya
Computer Science Department, Colorado State University, Fort Collins, CO 80523, USA
{Algarni, Malaiya}@cs.colostate.edu

Abstract— *In this paper, we investigate the factors that motivate and enable successful vulnerability discovery and the role of vulnerability markets. This is done by studying the career, motivation and methods of the most successful vulnerability discoverers. Vulnerability discovery takes considerable expertise. Some vulnerabilities, if exploited, can cause enormous damage to an organization, a segment of the economy, or even national security. Software developers, security organizations and government agencies are continuously engaged in efforts to prevent improper disclosure of vulnerabilities that can lead to zero-day exploitations. We observe that a major percentage of vulnerabilities are discovered by individuals external to software development organizations. We identify the top vulnerability discoverers throughout the past 12 years, and examine their motivation and methods. We observe that financial reward is a major motivation, especially to discoverers in Eastern Europe.. The paper studies the actual vulnerability market, rather than the hypothetical markets often studied in recent literature.*

Keywords – Software security; vulnerability discovery model; risk management; vulnerability market; vulnerability patching

1 Introduction

Potential exploitation of software security vulnerabilities has now emerged as a major security threat to organizations, some of the economic sectors, and national defense. Software vulnerability can be defined as a software defect or weakness in the security system that could be exploited by a malicious user causing loss or harm [1]. The number of unremedied vulnerabilities in a system represent the degree of security risk. It is important during the software lifecycle development process to evaluate and manage the risk, in order to assess how it will impact users, organizations, and the society.

Vulnerability discovery models that attempt to model the vulnerability discovery process have been recently proposed [2,3]. However there has not been a study of actual vulnerability discoverers and what motivates them. The individuals who discover the vulnerabilities (termed *discoverers* here) and those who exploit them (*exploiters*) are two separate groups. Discovering a vulnerability takes a much higher degree of technical skill and insight. The exploiters do not require a comparable skill—in fact, in the presence of an exploit (code that exploits one or more vulnerabilities), a patient hacker may achieve a security breach largely mechanically. The vulnerability discoverers represent a critical source of risk, should they choose to sell the vulnerability to malicious organizations or individuals. For example, Google has twice paid a $60,000 reward for details on a single vulnerability [4], suggesting that the potential damage caused by these vulnerabilities could have been enormous.

Many vulnerability discoverers seek to preserve the right to their claim of having discovered a vulnerability, since it serves to acknowledge the discoverer's expertise. For example, the well known University of Cambridge researcher Ross Anderson mentions a vulnerability he and his student discovered in 2003 [5]. A mid-year peak in vulnerability discovery, specifically in Microsoft products, can be explained by the coinciding date of a major conference, wherein security experts often present their vulnerability findings [6].

As presented here, a large percentage of vulnerabilities are found by experts external to the actual software development organizations. They are free to disclose the vulnerabilities they discover in any way they like. The hackers who are vulnerability exploiters are often classified as *white hat*, *black hat*, and *gray hat* [7,8]. These classifications do not apply to the security researchers engaged in finding vulnerabilities. However, the vulnerability markets may be classified as *legitimate*, where the transactions are properly recorded and disclosed; *black*, where the transactions are not disclosed; or *gray*, where the transactions are at the borderline. The current software vulnerability reward programs are a major part of the legitimate markets that attempt to attract the vulnerability discoverers who might otherwise resort to selling their findings on the black market. Those programs are relatively new and sometimes limited. They attempt to bring a discovery to the legitimate market, which significantly reduces the risk to the society. It is possible that some groups, such as government defense agencies, may be willing to pay a much higher price in the black or gray market [9].

There are several vulnerability databases organized by government-affiliated or private organizations. They include the National Vulnerability Database (NVD), Open Source Vulnerability Database (OSVDB), the vulnerability data collected by Frei et al. [10] (FVDB), Exploit Database, and IBM X-Force Vulnerability Database. In this paper, we have used OSVDB frequently for our investigations. As implied by its name, OSVDB is an open-source, community-organized

TABLE 1
SUMMARIZE THE IMPORTANT INFORMATION ABOUT SOME CURRENT VULNERABILITY REWARDS PROGRAMS

Program	# VULN TYPE	Max reward	Min reward	# of beneficiaries	Trend
Vulnerability Reward Program for Google web properties	5	$20,000	$100	2010: 51 2011: 122 2012: 189	Increase
Chrome Vulnerability Reward Program	Any security bug	>= 10,000	500	494	N/A
CCBill Vulnerability Reward Program	7	500	300	42	Hold
Secunia Vulnerability Coordination Reward Program (SVCRP)	Most bugs depending on some criteria	Most Valued Contributor & Most Interesting Coordination Report	N/A	N/A	N/A
The Mozilla Security Bug Bounty Program	Certain bugs depending on some criteria	$3000 (US) cash reward and a Mozilla T-shirt.	500	N/A	N/A
ZDI Rewards Program(TippingPoint)	Particular bugs depending on some criteria	$25,000	$1000	N/A	N/A
Facebook	7	No maximum	$500	Prior to 2011: 43 2011: 46 2012: 111	Increase
WordPress Security Bug Bounty Program	11	$1000	$25	N/A	N/A
iDefense (Verisign)	N/A	N/A	N/A	Significant number	N/A

database associated with the Open Security Foundation, with the stated aim being to provide "accurate, detailed, current, and unbiased technical information". It contains more than 90,377 vulnerabilities found by 4,735 researchers [11].

The first section of this paper provides some background about vulnerability markets and the current reward programs. The next section identifies the top vulnerability discoverers, using the OSVDB database, and examines their careers. We examine the data for well-known open-source browsers in order to determine how many vulnerability discoverers were discovered internally by the browser development teams, and to assess the relative significance of external vulnerability finders. We show the specific questions that we have posed to several top discoverers and present what we have discovered. Finally, we discuss our findings and present our conclusions along with suggestions for future work.

2 Background

Any unpatched vulnerabilities in a software program can allow hackers to attack the system, harming an organization or compromising sensitive information. Therefore, remedying any newly discovered vulnerabilities before they are exploited is critical. While many discoverers are likely to be responsible professionals, they need to be provided the opportunity to use their skills in a positive, productive way in order to avoid passing the information to those who might exploit the vulnerabilities. If there is a lack of incentives from organizations in the field, they might be tempted to sell the information in the vulnerability black market, resulting in possible exploitation of systems.

2.1 Vulnerability markets

Vulnerability discoverers seek rewards for their capabilities. This gives rise to vulnerability markets, which may be termed legitimate markets, black markets or gray markets. Vulnerabilities discovered within a developer organization do not enter the market. Those discovered within a security company are used for demonstrating the company's capabilities to potential customers, and perhaps providing customers early remediation. Freelance discoverers will attempt to maximize their reward by selling their vulnerabilities in the vulnerabilities markets [12,13]. Vulnerabilities have significant economic value [14] because they can lead to zero-day exploits that might harm organizations, the economy, and ultimately, society [15]. Some exploits have been sold for as much as $250,000 [16]. In addition to money, many discoverers find the fame generated by the disclosure also attractive, as it can be translated into further economic opportunities.

In legitimate markets the buyers are original software developers, the third-party security organizations follow proper practices for disclosing the vulnerabilities, and the transactions are well documented. Several international government organizations are also said to have been significant buyers [16], but their policies are not generally disclosed. In a few countries, the government may be the only major buyer. Selling and buying software vulnerabilities should ideally be done through a well-regulated market [17, 18]. The software vulnerability reward programs discussed below are a major part of the vulnerability market [19]. Such markets should be efficient, legal, and attractive for both discoverers and buyers, and should involve policies that will protect the society. A few commercial organizations that serve as brokers now exist [20,21]. In the black market, the vulnerabilities could be sold to the highest bidder, some of whom may attempt to use them maliciously. Some vulnerability discoverers may consider the black market an attractive option for selling their discovered vulnerabilities [22]. They may find the vulnerability reward programs unattractive because they pay significantly less. The reward programs are still new, and their rewards may often pale in comparison with prices in the black market, which can

pay a significant amount depending on the vulnerability's severity. Some organizations, such as Google, have acknowledged the importance of freelance discoverers, and offer a significant monetary award in addition to the possible inclusion in their 'discoverers hall of fame'. A good example of a vulnerability discoverer who has taken advantage of such a reward program is Sergey Glazunov, a Russian student and security researcher who earned $60,000 by discovering a new exploit in Google's Chrome browser [23].

2.2 Vulnerability reward programs

Rewarding security researchers and others who make software products more secure is important. Providing rewards to motivate people to find software defects or weaknesses before they are exploited by black hat exploiters is critical to improving computer security.

There are only a few current vulnerability reward programs, and most of them were created a few years ago. The idea of reward programs is still quite new, and needs more development and improvement.

The current reward programs include these listed below. The key information about them is provided in Table 1:

- Vulnerability Reward Program for Google web properties [24]: This program was created in November 2010. People who discover one of five types of vulnerabilities, such as remote code execution, SQL injection, and other common web flaws, are rewarded from $100 to $20,000. The number of discoverers who have received approval from the reward panel has ranged between 53 winners in the fourth quarter of 2010 to 39 winners in the fourth quarter of 2012.
- Chrome Vulnerability Reward Program (Chromium Security Reward) [25]: All vulnerabilities are considered in this program, provided the vulnerability is identified as being of sufficiently high severity. The rewards range from $500 to $10,000 and up.
- Secunia Vulnerability Coordination Reward Program (SVCRP) [26]: There are two special awards: most valued contributor and most interesting coordination report.
- The Mozilla Security Bug Bounty Program [27]: The rewards range from $500 to $3,000 depending on the severity rating of the vulnerability, and the reward includes a Mozilla t-shirt.
- ZDI Rewards Program [28]: The Zero Day Initiative (ZDI) provides reward points each time a vulnerability submission is purchased. These points determine the ZDI status, which are bronze, silver, gold, platinum, and diamond. The rewards range from is $1,000 to $25,000.
- Facebook [29]: This program is similar to most other reward programs. It offers a bounty for certain qualifying security bugs. The reward has a minimum of $500 with no specified maximum, and is based on severity and creativity.
- WordPress Security Bug Bounty Program [30]: This program has two different bounties: one for WordPress and another for WordPress Plugins. The minimum reward is $25, and the maximum reward is $1,000.
- CCBill Vulnerability Reward Program [31]: CCBill is an Internet billing service. The rewards range from $300 to $500, depending on the types of vulnerabilities found, such as SQL Injection, DoS, and persistent XSS. This program has been temporarily placed on hold due to corrections needed in the reported bugs.
- iDefense Vulnerability Contributor Program: This is one of the oldest reward programs, and a few of the top discoverers mention working with iDefense. However the detailed reward information is not available.

Notably, Microsoft has been steadfast in not offering a reward program, although it works with discoverers and acknowledges their discoveries [32]. Microsoft does use outside consultant organizations to test their software on a contract basis, however [33].

3 The vulnerability discoverers

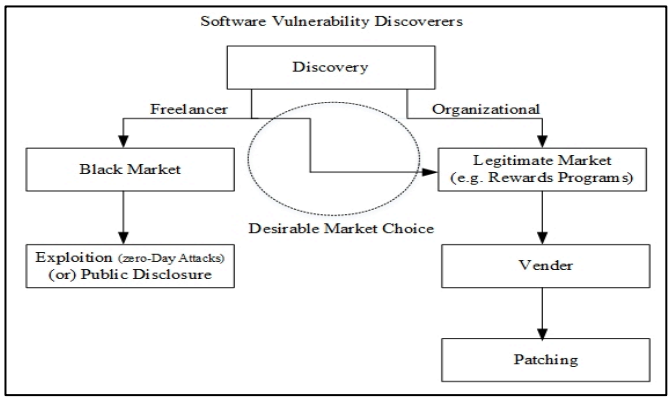

FIG. 1. THE EVENTS IN THE VULNERABILITY LIFE CYCLE

The motivation for vulnerability discoverers has been considered briefly by researchers in the past [34], but has never been studied using actual data. The discovery and disclosure of vulnerabilities are processes that are significantly impacted by the economics involved [35]. A few researchers have considered theoretical modeling of the vulnerabilities market. This paper asks these questions: who are the actual vulnerability finders, and what motivates them?

As shown in Figure 1, vulnerability discovery is done by organizational researchers—who generally follow proper disclosure policies—and freelance researchers, who may sell their findings, either in the legitimate or the black market. Some vulnerabilities are sold in the legitimate market via vulnerability reward programs, or by contacting venders directly. The developers get a chance to develop software patches for the vulnerabilities before the vulnerability is disclosed. On the other hand, when the vulnerabilities are sold on the black market, they are likely to be exploited before public disclosure. The key strategy would be to encourage the researchers to sell their discovered vulnerabilities in the legitimate market instead of the black market (dotted circle on the figure). This will reduce trading in the black market and more vulnerabilities will enter the legitimate market.

Software development organizations such as Google or Microsoft have divisions dedicated to security-related work. They are responsible for the development of security patches. They also discover some of the vulnerabilities in their own products. However as Figures 2 and 3 show, a large fraction of the vulnerabilities, perhaps a majority of them, are discovered by outside discoverers. These external discoverers have their own motivation, which may be different from the motivation

TABLE 2
VULNERABILITY DISCOVERERS FROM JULY. 1, 2012 TO DECEMBER 31, 2012: INSIDERS OR OUTSIDERS

DISCOVERERS	SAFARI'S VULNERABILITIES	PERCENTAGE	CHROMIUM'S VULNERABILITIES	PERCENTAGE
PRODUCT'S COMPANY DISCOVERERS	17	20%	0	0%
PRODUCT'S COMPANY DISCOVERERS AND OTHERS	0	0%	35	35%
OUTSIDE DISCOVERERS	66	80%	63	64%
UNKNOWN DISCOVERERS	0	0%	1	1%

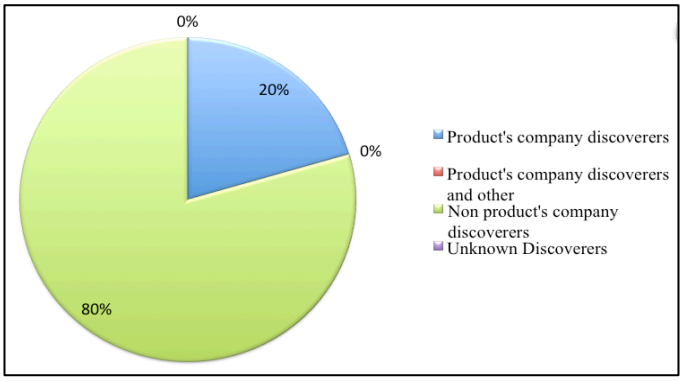

FIG. 2. VULNERABILITY DISCOVERERS IN SAFARI

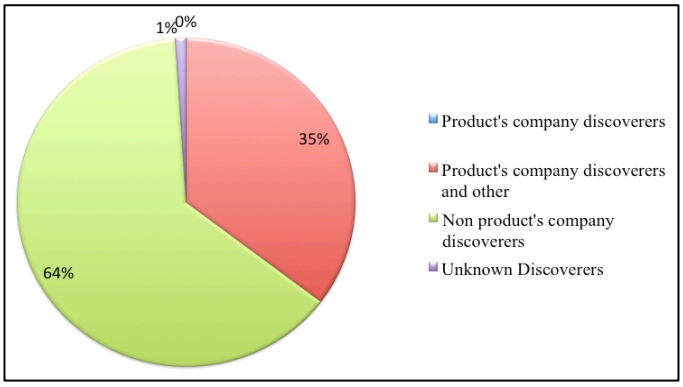

FIG 3. VULNERABILITY DISCOVERERS IN CHROMIUM

of those engaged in discovering vulnerabilities internally in a software development organization. Many external discoverers are freelancers either working on their own or on contract basis. Some of the external discoverers are part of organizations that provide security services.

3.1 Top discoverers

To understand the vulnerability discovery process, we examine the records of the top vulnerability discoverers. Since each of them has successfully discovered quite a large number of vulnerabilities, we can presume that they did not just get lucky—rather, they have a system that has been demonstrated to work. To find the top vulnerability discoverers, we obtained data from the OSVDB database created in 2002. We identified the following ten vulnerability discoverers in the database who found the most vulnerabilities. The actual names are not identifiable in some cases; they are generally known by the login identifier that they use in their blogs.

• r0t: He is a Latvian associated with a group named Unsecured Systems [36]. He discovered 810 vulnerabilities between Aug. 9, 2005 and Sept. 16, 2010. No additional information about him could be located.

• Lostmon Lords: He is a security researcher from Spain [37]. He discovered 279 vulnerabilities between June 20, 2004 and Aug. 15, 2009, as recorded by OSVDB. According to his blog [38], he continued to discover vulnerabilities from Nov. 2009 to July 2012, but apparently disclosed them in such a manner that he is not identified as the discoverer in OSVDB.

• rgod: He is Andrea Micalizzi from Catania, Italy. He was 36 years old when he died in 2006 [39]. However, one of his friends has continued to use rgod login. Together they discovered 277 vulnerabilities between June 6, 2005 and Aug. 29, 2012. According to rgod's website [40], rgod's friend is still discovering vulnerabilities but rgod is not identified as the creditee in OSVDB.

• James Bercegay: He is the owner of GulfTech Security Research and Development [41], which was started in 2002. He discovered 200 vulnerabilities between June 3, 2003 and Sept. 20, 2008.

• Aliaksandr Hartsuyeu: He is the owner of eVuln [42], a security company, which was started on Nov. 14, 2005 [43]. He discovered 229 vulnerabilities between Dec. 28, 2005 and Feb. 03, 2011.

• Kacper: He was a part of the Devil team [44]. He is from Poland. He discovered 199 vulnerabilities between May 12, 2006 and Aug. 10, 2007.

• Luigi Auriemma: He is from Milan, Italy [45]. He discovered 267 vulnerabilities between July 8, 2000 and Mar. 16, 2013.

• Janek Vind, or "waraxe": He runs an interactive software vulnerability and security website [46]. Janek is from Estonia and his collaborators are from Australia, Turkey, Argentina, and other countries. They discovered 319 vulnerabilities between Aug. 08, 2003 and Mar. 21, 2013.

• Luny: The little information provided in the database records states that he discovered 142 vulnerabilities between May 18, 2006 and July 13, 2006.

• Russ McRee: He is a senior security analyst, researcher, and the founder of holisticinfosec.org in the United States [47]. He found 237 vulnerabilities between Jan. 14, 2008 and Mar. 2, 2012.

3.2 Outsider and insider discoverers

One key question in understanding the vulnerability discovery process is whether a discoverer of vulnerabilities is a part of the software product team or an outsider. This will help us to understand what motivates discoverers to find and report software vulnerabilities. To address this question we examined two well known open-source software products: Safari and Google Chromium (Table 2, Figures 2,3). The period we

TABLE 3
SUMMARIZES TOP VULNERABILITY DISCOVERERS' ANSWERS TO SPECIFIC QUESTIONS ABOUT THEIR VULNERABILITY DISCOVERING AND VULNERABILITY REWARD PROGRAMS.

DISCOVERER	MOTIVATING FACTORS	STOP DISCOVERING	IMPACT OF REWARDS PROGRAMS	APPLYING TO REWARDS PROGRAMS
DISCOVERER 1	HOBBY AND LIFESTYLE CHOICE	NO.	N/A	NO
DISCOVERER 2	MAKE HIS WEBSITE MORE POPULAR	NO.	LIMITED IMPACT	NO
DISCOVERER 3	CURIOSITY	NO. HE HAS A COMPANY	NOT MUCH IMPACT	ZDI AND IDEFENSE.
DISCOVERER 4	ENJOYMENT	YES. NOT ENOUGH TIME	MOSTLY, YES.	NO
DISCOVERER 5	FUN, PROFIT, AUDITING	NO.	YES	ZDI AND IDEFENSE.

investigated was from July 1, 2012 to December 31, 2012, and we used the Open Source Vulnerability Database OSVDB as the data source.

As shown in Table 2, for these two products, the majority of the vulnerabilities discovered were found by outsiders. This demonstrates the importance of outsider discoverers and the potential significance of providing discoverers with more enticing vulnerability reward programs, or other forms of a legitimate market. It is definitely worth knowing what would motivate the discoverers to participate in such reward programs.

3.3 Questions for top discoverers

In order to gain insight into their thinking, we decided to contact the top discoverers and ask them some questions. We were able to locate contact information for most of them. We then contacted them and asked some key questions, including the following:

1. What motivates you to discover software vulnerability?
2. How and when did you start?
3. What specific tools do you use for discovering vulnerability?
4. Did you stop working as a vulnerability discoverer? If so, when and why did that happen? If not, why not?
5. Do you think that vulnerability reward programs will help reduce black market transactions and encourage the use of legitimate markets? Please explain.
6. Did you apply to one of the current vulnerability reward programs, and if so, why?
7. Do you have any other comments?

Considering that freelance vulnerability discoverers can sometimes be secretive, we were pleasantly surprised when several of them actually responded. The following section includes some of the answers to the above questions. To ensure their privacy, we have replaced the discoverers' names with aliases. Table 3 summarizes the responses.

- Discoverer 1: He uses his own tools, "specifically his hands and mind, in preference to automated tools". He has not sold a vulnerability in the past ten years. Rather than sell or exploit a vulnerability, he prefers to help developers make a patch available for it. He does not find the reward program to be attractive.
- Discoverer 2: The main reason he became a vulnerability discoverer is that it made his own website more popular and enabled him to offer a source code review service. He only uses his own tools, which are offered on his organization's website. He is also of the opinion that vulnerability reward programs are of limited use, as the black markets offer more money. Like Discoverer 1, he does not apply for any reward programs.
- Discoverer 3: He started in 2002 while following Bugtraq and other mailing lists. He uses various public and proprietary tools to discover vulnerabilities. Although he now runs his own company, he still finds the time for discovery work. In his opinion, vulnerability reward programs do not help to reduce black market transactions substantially and encourage the use of legitimate markets. He states that reward programs pay very little for exclusive information and bug patches, which can be sold for much more on the black market. Nevertheless, he has submitted some vulnerabilities to the ZDI and iDefense reward programs in the past.
- Discoverer 4: He started in 2008 and focuses entirely on web application security flaws, largely specific to free and open source applications. To discover vulnerabilities, he uses a combination of tools such as Burp Suite, OWASP ZAP, and a number of Firefox plugins (Tamper Data), as well as simple manual testing. He thinks that, for the most part, vulnerability reward programs will help to reduce black markets and encourage legitimate markets. He acknowledges that money is always a motivator and if vulnerability discoverers are paid well via the legitimate market, hopefully they will be less likely to sell the bug on the black market. He mentions that he does not sell vulnerabilities. He always coordinates his findings with Secunia but does not take any further action regarding the vulnerability.
- Discoverer 5: He believes that the most profitable option for a vulnerability discoverer like him is to offer software security auditing services. His first 'hacks' were done many years ago, between 1992 and 1993. The tools that he uses for discovering vulnerabilities are Notepad++ for PHP and other scripting languages, which allow him to search specific text strings through multiple files and color coding. He also uses Apache/PHP/MySQL on his home PC, and all of his web application research is done using @localhost. Discoverer 5 usually works manually, without automatic vulnerability scanners. Moreover, he believes that vulnerability reward programs will surely lessen damage, and mentions that he is aware of hundreds of zero-day findings sold to ZDI and other vulnerability reward programs. He has worked with ZDI and iDefense because they pay for findings, arrange all communications with developers, and give him credit in the public advisory.

3.4 Discussion

Upon investigating the factors that influence vulnerability discovery and disclosure, we summarize our findings as follows.

We note that freelance discoverers play a significant role in vulnerability discovery. In some cases, they have even formed their own companies or groups. An unusually high number of successful vulnerability discoverers are from Eastern Europe, a region also known for its sophisticated vulnerability exploiters [48]. That may be attributable to a high degree of technical skill combined with weaker local economies. The rewards for finding vulnerabilities often come from international software organizations based in the United States.

Discovering vulnerabilities requires considerable technical and research skills. Some of the discoverers have an extensive background in software security. The responses by the top discoverers to our questions suggest that they tend to rely on their expertise and intuition rather than just the tools. The discoverers, like other well paid software professionals or researchers, expect to be fairly compensated for their services. With a few critical, high-severity vulnerabilities in hand, they may be in a position to bargain.

An attractive reward program based on vulnerability criticality can provide a significant alternative to the black market. A few software developers and security organizations now run a small number of such programs. These programs ensure time for patch development before a disclosure. Some of the top discoverers that we contacted suggest that sometimes the reward programs do not pay enough, and a better reward may be obtained on the black market, but none of them admitted to selling any vulnerabilities on the black market.

We note that after a few years of very successful vulnerability discovery, many of the top discoverers apparently disappear from the scene as credited discoverers. Some of them suggest that they find it more profitable to contract out their security auditing services to software developers.

The black market may often provide better rewards for some individual vulnerabilities than current legitimate programs. The black market might sometimes be more attractive because applying to reward programs may be tedious or slow. Limited awareness of reward programs may also contribute to the attractiveness of the black markets. The reports suggest that many of the buyers in the black market may be affiliated with various governments [16], bringing a significant amount of money to the black market.

Companies and organizations need to design attractive vulnerability reward programs for their products. This will allow the legitimate markets to compete with the black market. Some reward programs, such as the one for Google Chrome, appear to have been successful. Google has a good reputation in technology as well as management, and has recognized the discoverers as high-achievement professionals. While the amount of money committed to the reward programs is only a tiny part of the company's revenues, Google is giving out some of the best monetary rewards.

A significant part of the global vulnerabilities market is quite opaque. Even the emerging legitimate markets have not been studied in detail, although some mathematical studies based on the classical market theories have appeared. There is a need to examine actual data and practices in order to understand the vulnerability discovery and disclosure.

4 Conclusion and future works

This paper has examined the motivation and methods of vulnerability discoverers by studying the motivation and the methods of discoverers and the vulnerability market. The most successful vulnerability discoverers are identified, and their motivation and techniques have been examined.

While vulnerability discoverers use some tools— including those that they have developed themselves—they rely on their expertise and insight to a considerable extent. It must be kept in mind that tools for finding known vulnerabilities are completely different, and are not of use for discovering new vulnerabilities.

We find that a large fraction of the discoverers are from outside of the software development organizations, and their key motivation is a monetary reward. The vulnerabilities are disclosed in a proper and responsible way when they are traded though the legitimate markets. Reward programs and contract-based software review services are the major components of the legitimate markets. Organizations that act as vulnerability brokers may deal in either the legitimate or the black market. The vulnerability discoverers acknowledge that the black markets can often be attractive. Reports suggest that government agencies may make up a significant part of the black market buyers. This suggests a need for expanded and more attractive legitimate markets.

The research reported in this paper needs to expanded further by looking at a larger number of individual discoverers. There is a need to study the legitimate and the black markets so that the processes can be modeled accurately. Because this is a dynamically changing field, studies such as this need to be repeated in order to see if there are any observable trends in terms of the vulnerabilities that end up in the legitimate and black market periodically, and the subsequent risks to society.

Acknowledgement

We would like to thank all of the top discoverers who took the time to answer our questions. Their answers and comments have provided us with a much clearer understanding of the field. This work was partly supported by a scholarship from King AbdulAziz University in Saudi Arabia.

5 References

[1] C. P. Pfleeger and S. L Pfleeger. Security in Computing, 3rd ed. Prentice Hall PTR, 2003.

[2] O. H. Alhazmi and Y. K. Malaiya, "Application of Vulnerability Discovery Models to Major Operating Systems," IEEE Trans. Reliability, March 2008, pp. 14-22

[3] S.-W. Woo, H. Joh, O. H. Alhazmi and Y. K. Malaiya, "Modeling Vulnerability Discovery Process in Apache and IIS HTTP Servers", Computers & Security, January 2011, Pages 50-62.

[4] "Teen Exploits Three Zero-Day Vulns for $60K Win in Google Chrome Hack Contest | Threat Level | Wired.com," Threat Level. [Online]. Available: http://www.wired.com/threatlevel/2012/03/zero-days-for-chrome/. [Accessed: 01-Apr-2013].

[5] R, Anderson, University of Cambridge, Home page. [Online]. Available: http://www.cl.cam.ac.uk/~rja14/ [Accessed: 27-Apr-2013].
[6] H.-C. Joh and Y. K. Malaiya, "Seasonal variation in the vulnerability discovery process," in Software Testing Verification and Validation, 2009. ICST'09. International Conference on, 2009, pp. 191–200.
[7] "White hat," Search security. [Online]. Available: http://searchsecurity.techtarget.com/definition/white-hat [Accessed: 01-Apr-2013].
[8] "HacK, CouNterHaCk | New York Times Magazine," [Online]. Available: http://www.nytimes.com/library/magazine/home/19991003mag-hackers.html. [Accessed: 01-Apr-2013].
[9] Andy Greenberg, Meet The Hackers Who Sell Spies The Tools To Crack Your PC, Forbes, March 21, 2012, bit.ly/11cbLC6
[10] M. Shahzad, M. Z. Shafiq, and A. X. Liu, "A large scale exploratory analysis of software vulnerability life cycles," in 2012 34th International Conference on Software Engineering (ICSE), 2012, pp. 771–781.
[11] The Open Source Vulnerability Database. [Online]. Available: http://www.osvdb.org. [Accessed: 01-Apr-2013].
[12] Karthik Kannan and Rahul Telang, Market for Software Vulnerabilities? Think Again, Management Science, Vol. 51, No. 5 (May, 2005), pp. 726-740.
[13] Arora, A.; Rahul Telang, "Economics of software vulnerability disclosure," Security & Privacy, IEEE, vol.3, no.1, pp.20, 25, Jan.-Feb. 2005.
[14] R. Böhme, "Vulnerability markets," Proc. of 22C3, vol. 27, p. 30, 2005.
[15] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. van Eeten, M. Levi, T. Moore, and S. Savage, "Measuring the cost of cybercrime," in 11th Workshop on the Economics of Information Security (June 2012), 2012.
[16] "Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits - Forbes," Forbes. [Online]. Available: http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/. [Accessed: 01-Apr-2013].
[17] C. Miller, "The legitimate vulnerability market: the secretive world of 0-day exploit sales," in Workshop on the Economics of Information Security (WEIS), 2007, pp. 7–8.
[18] D. McKinney, "Vulnerability Bazaar," IEEE Security Privacy, vol. 5, no. 6, pp. 69–73, 2007.
[19] A. Ozment, "Bug auctions: Vulnerability markets reconsidered," in Third Workshop on the Economics of Information Security, 2004.
[20] Ryan Gallagher, "Cyberwar's Gray Market- Should the secretive hacker zero-day exploit market be regulated?" Slate, Jan. 16, 2013.
[21] Michael Riley and Ashlee Vance "Cyber Weapons: The New Arms Race" BloomsbergBusinessWeek, July 20, 2011.
[22] S. Ransbotham, S. Mitra, and J. Ramsey, "Are markets for vulnerabilities effective?," MIS Quarterly-Management Information Systems, vol. 36, no. 1, p. 43, 2012.
[23] "Google throws stacks of cash at hackers to publicly crack its Chrome browser," VentureBeat. [Online]. Available: http://venturebeat.com/2012/03/08/hackers-crack-chrome-in-publi/. [Accessed: 01-Apr-2013].
[24] Vulnerability Reward Program for Google web properties. [Online]. Available: http://www.google.com/about/appsecurity/reward-program/. [Accessed: 01-Apr-2013].
[25] Chrome Vulnerability Rewards Program. [Online]. Available: http://www.chromium.org/Home/chromium-security/vulnerability-rewards-program. [Accessed: 01-Apr-2013].
[26] Secunia Vulnerability Coordination Reward Program (SVCRP). [Online]. Available: http://secunia.com/community/research/svcrp/. [Accessed: 01-Apr-2013].
[27] The Mozilla Security Bug Bounty Program. [Online]. Available: http://www.mozilla.org/security/bug-bounty.html. [Accessed: 01-Apr-2013].
[28] ZDI Rewards Program. [Online]. Available: http://www.zerodayinitiative.com/about/benefits/. [Accessed: 01-Apr-2013].
[29] Facebook rewards program. [Online]. Available: https://www.facebook.com/whitehat/bounty/. [Accessed: 01-Apr-2013].
[30] Wordpress rewards program. [Online]. Available: http://www.whitefirdesign.com/about/wordpress-security-bug-bounty-program.html. [Accessed: 01-Apr-2013].
[31] CCBill Vulnerability Reward Program. [Online]. Available: http://www.ccbill.com/developers/security/vulnerability-reward-program.php. [Accessed: 01-Apr-2013].
[32] Dennis Fisher "As Bug Bounty Programs Mature, Still More Room For Growth", August 17, 2012, threatpost.com
[33] Dennis Fisher, "Microsoft Says No to Paying Bug Bounties", July 22, 2010, Threatpost.com
[34] Alhazmi, O.H.; Malaiya, Y.K., "Quantitative vulnerability assessment of systems software," Reliability and Maintainability Symposium, 2005. Proceedings. Annual, vol., no., pp.615, 620, Jan. 24-27, 2005.
[35] Ross Anderson and Tyler Moore, The Economics of Information Security, Science, 27 October 2006: 314 (5799), 610-613.
[36] Blog of r0t. [Online]. Available: http://pridels-team.blogspot.com. [Accessed: 01-Apr-2013].
[37] Facebook's account of Lostmon. [Online]. Available: https://www.facebook.com/lostmon. [Accessed: 01-Apr-2013].
[38] Blog of Lostmon Lords. [Online]. Available: http://lostmon.blogspot.com. [Accessed: 01-Apr-2013].
[39] Personal website of rgod. [Online]. Available: http://retrogod.altervista.org. [Accessed: 01-Apr-2013].
[40] Blog of rgod. [Online]. Available: http://retrogod.altervista.org. [Accessed: 01-Apr-2013].
[41] The website of James Bercegay. [Online]. Available: http://gulftech.org. [Accessed: 01-Apr-2013].
[42] The website of Aliaksandr Hartsuyeu. [Online]. Available: http://evuln.com. [Accessed: 01-Apr-2013].
[43] StatsCorp.com Evuln.com security audit [Online]. Available: http://www.statscrop.com/www/evuln.com. [Accessed: 01-Apr-2013].
[44] Personal website of kacper. Available online at: http://www.devilteam.yum.pl
[45] Personal website of Luigi Auriemma. [Online]. Available: http://aluigi.altervista.org. [Accessed: 01-Apr-2013].
[46] Personal website of Janek Vind "waraxe". [Online]. Available: http://www.waraxe.us. [Accessed: 01-Apr-2013].
[47] Personal website of Russ McRee. [Online]. Available: http://holisticinfosec.org. [Accessed: 01-Apr-2013].
[48] Report: Eastern European Hackers More Sophisticated Than Asian Counterparts. [Online]. Available: http://blogs.wsj.com/digits/2012/09/18/report-eastern-european-hackers-more-sophisticated-than-asian-counterparts/. [Accessed: 01-Apr-2013].

About the Authors

Abdullah M. Algarni is a Ph.D. student in the Department of Computer Science at Colorado State University. He received his MS in Software Systems Engineering from the University of Melbourne in Australia in 2008. He is interested in software engineering and computer security.

Yashwant K. Malaiya is a Professor in the Computer Science Department at Colorado State University. He received his MS in Physics from Sagar University, MScTech in Electronics from BITS Pilani, and PhD in Electrical Engineering from Utah State University. He has been published widely in the areas of fault modeling, software and hardware reliability, and testing and quantitative security. He has also been a consultant to industry. He has served as a General Chair and a Program Chair for several international meetings, including as the General Chair of 2003 IEEE International Symposium on Software Reliability Engineering. He is a Golden Core member of IEEE Computer Society and a recipient of the IEEE Third Millennium Medal.