What We Know About Bug Bounty Programs - An Exploratory Systematic Mapping Study

Ana Magazinius(✉), Niklas Mellegård, and Linda Olsson

RISE ICT Viktoria, Gothenburg, Sweden
{ana.magazinius,niklas.mellegard,linda.olsson}@ri.se
http://www.ri.se

Abstract. This paper presents a systematic mapping study of the research on crowdsourced security vulnerability discovery. The aim is to identify aspects of bug bounty program (BBP) research that relate to product owners, the bug-hunting crowd or vulnerability markets. Based on 72 examined papers, we conclude that research has mainly been focused on the organisation of BBPs from the product owner perspective, but that aspects such as mechanisms of the white vulnerability market and incentives for bug hunting have also been addressed. With the increasing importance of cyber security, BBPs need more attention in order to be understood better. In particular, datasets from more diverse types of companies (e.g. safety-critical systems) should be added, as empirical studies are generally based on convenience sampled public data sets. Also, there is a need for more in-depth, qualitative studies in order to understand what drives bug hunters and product owners towards finding constructive ways of working together.

Keywords: Bug bounty · Systematic mapping · Literature review

1 Introduction

In a digital and connected world, attempts to hack connected units are a problem for companies. Consequences range from economic ones such as patching costs, decreased revenue and plummeting stock prices, to damaged reputation and safety risks [1,63,67]. Meanwhile, what drives hackers to hack ranges from curiosity, to money [31], and reputation [3,4,31,52,57]. This has led companies to engage in constructive collaboration with the hacker community rather than getting into conflict. The earliest example of this type of collaboration was initiated by Hunter & Ready, who in 1983 offered a VW Beetle (Bug!) as a reward for bugs found in their VRTX operating system[1]. Although bug bounty programs (BBP) were not very common at first, with time, Internet giants such as

This research was funded by Swedish funding agency Vinnova, FFI program, HoliSec project (project number 2015-06894).

[1] https://techcrunch.com/2017/01/19/hacking-the-army/.

T. Groß and T. Tryfonas (Eds.): STAST 2019, LNCS 11739, pp. 89–106, 2021.
https://doi.org/10.1007/978-3-030-55958-8_5

Netscape, Google and Facebook initiated BBPs. Government agencies (e.g. the United States Department of Defense) have also initiated BBPs, as have automotive companies such as General Motors and Tesla. The general belief is that BBPs lead to discovery of vulnerabilities not detected in regular penetration testing, because of the size and the skillset of the bug hunter community. Middleman companies, which connect product owners with the bug hunter crowd and manage the bug-hunting process, have become part of the vulnerability discovery ecosystem. iDefense was the first middleman company, followed by many others. Today's white-market middleman companies, such as HackerOne and Bugcrowd, host hundreds of public and private BBPs where the bug-hunting crowd are invited to legally test the security of the involved companies' products.

The research on BBPs reflects this evolution; for the past two decades, researchers have provided theoretical and empirical contributions to the body of knowledge. However, a compilation of these research efforts is lacking. A 2018 search for literature reviews on BBP research only resulted in one minor study, compiling just eleven papers [28]. Hence, there is a need to more extensively map this research area, to illuminate what is known and what remains under-researched. In this paper, we address this by a systematic mapping study which may lay the grounds for future research. The aim of this study is to map the research area and answer the following research questions:

RQ1. What aspects of BBPs that relate to the product owner's perspective have been addressed by research?

RQ2. What aspects of BBPs that relate to the bug-hunting crowd's perspective have been addressed by research?

RQ3. What aspects of BBPs that relate to the mechanisms of vulnerability markets have been addressed by research?

2 Methodology

This study is based on the rigorous guidelines for systematic literature reviews (SLR) adapted to suit a mapping study [37,38]. They differ in that SLRs provide in-depth analysis and comparison of different categories of a topic, whereas mapping studies only identify and classify existing research.

A literature search was conducted in late June 2018, on four search engines: Scopus, IEEE Xplore Digital Library, ACM Digital Library and Google Scholar. Search terms were: "bug bounty", "vulnerability reward program" and "vulnerability disclosure". No limit was set for publication date, only material in English was considered. While non-academic reports provide interesting insights, they were excluded due to lack of methodology transparency, and lack of quality ensuring measures such as peer review. The search resulted in 2457 items.

Selection criteria were that the papers should concern 1) mechanisms of crowdsourced vulnerability discovery, or 2) mechanisms of vulnerability disclosure by external bug hunters, or 3) organisations' management of vulnerabilities discovered by external bug hunters. A first selection was made based on title and abstract. To ensure reliability in the selection, all items found in Scopus,

IEEE Xplore and ACM were reviewed independently by two researchers. Items found in Google Scholar (the source of most items), the top 15% were reviewed by two researchers and the remaining 85% by one researcher. This was considered sufficient as a validity check and the first selection resulted in 216 papers. All selected papers were examined by at least one researcher excluding papers which content did not match the selection criteria. The borderline papers were discussed within the research team. This process resulted in the final selection of 72 papers (see Appendix 4), approved by all three researchers. The papers were categorised into one, or more, of three main categories (corresponding to the three research questions); product owner, the bug-hunting crowd and vulnerability market mechanisms. This categorisation was chosen as it puts focus on the two main actors in a BBP and on the relationships between them and other actors. Each researcher was assigned a category to review in depth, after which all categories were discussed within the team. This was the point of departure for the analysis.

3 Results

While the research on bug bounties has been ongoing since 2000, there has been a noticeable increase in the number of published papers since 2016. The earliest paper included in this study focused on the product owner category, followed by the first paper on market mechanisms in 2004, and the first paper on crowd related topics in 2007 (see Fig. 1).

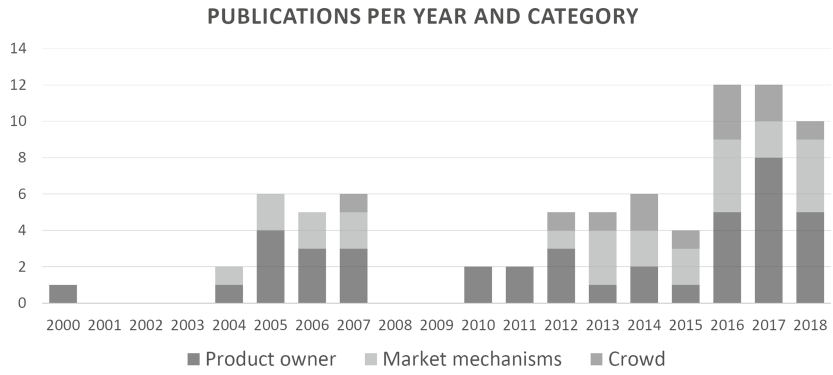

Fig. 1. Publications per year and category (one paper can appear in more than one category)

Out of the 72 papers included in this study 44 (61%) are based on empirical evidence, two (3%) are literature reviews, and 26 (36%) are purely theoretical (see Fig. 2). While all three categories used in this paper consist of both empirical and theoretical research, product owner and market mechanisms categories also include literature reviews (see Fig. 2).

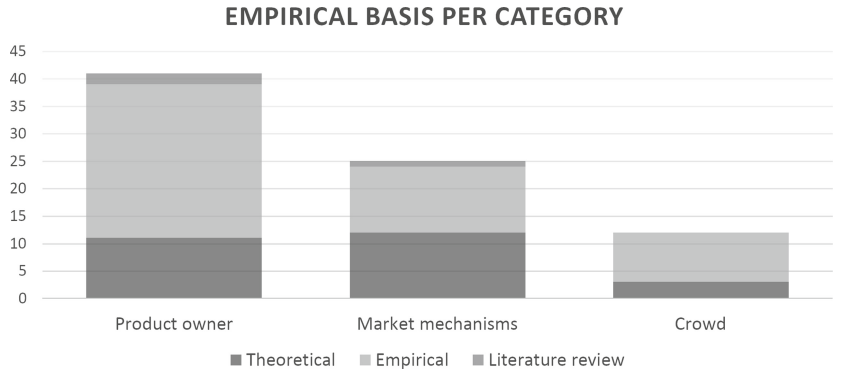

Fig. 2. Empirical basis per category (one paper can appear in more than one category)

Further, an increase in the amount of empirical papers can be observed in the past five years (see Fig. 3). These draw data from 28 different datasets, the top ones being CERT (seven cases), followed by HackerOne (five cases), and Wooyun and NVD (three cases respectively).

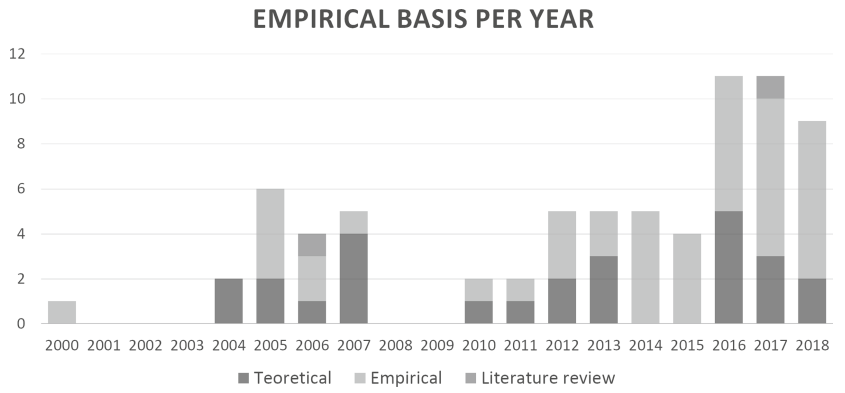

Fig. 3. Empirical basis per year (one paper can appear in more than one category)

3.1 Product Owner

Publications in the product owner category consider the perspective of the organiser of a BBP, and/or the owner of the product that is being tested. The category includes 41 papers published between 2000 and 2018 (see Fig. 4), which were classified in subcategories: guidelines, vulnerability life cycle, economic aspects and experience reports (see Fig. 5).

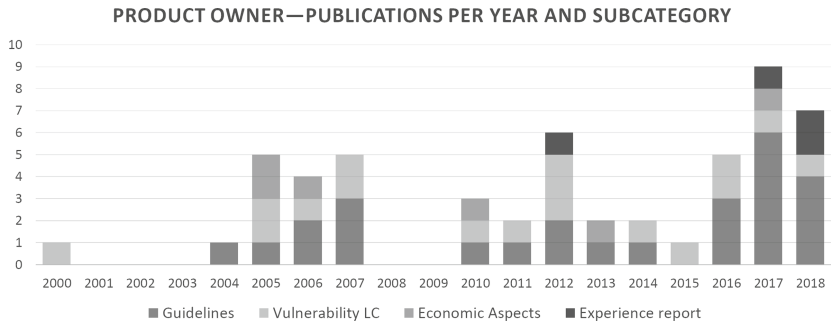

Fig. 4. Product owner, publications per year and subcategory (one paper can appear in more than one subcategory)

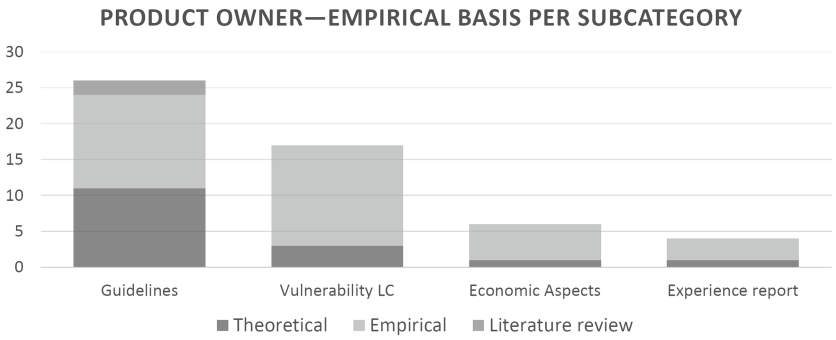

Fig. 5. Product owner, empirical basis per subcategory (one paper can appear in more than one subcategory)

Guidelines. Papers in this category provide guidelines and recommendations that are relevant to organisers of a bug bounty. [26,71,74] examine historical bug bounties and provide improvement suggestions, and [61] provides a checklist for the organisers. Other papers examine more specific aspects, [17,40,73] investigate how to incentivise a crowd, and [41] how to formulate a BBP announcement. General guidelines for vulnerability disclosure are provided by [7,18,21]. More specific aspects are provided in [30] where disclosure strategies in different domains are examined and mapped to the domain of control engineering. [27] provides a deterrent story about a company going to lengths to try to prevent disclosure rather than to acknowledge and fix vulnerabilities. The paper goes on to present a more efficient strategy applied by another company.

The impact of disclosure on patching practices is investigated in [10], and [14] maps disclosure with number of attacks. One paper examines ethics and moral obligations various actors have with regard to software vulnerabilities [66].

Another perspective is taken in [44] where the rate of discoveries as a BBP progresses is examined and recommendations on adaptation of rewards provided. [24] provides recommendations on how to formulate and communicate terms with a crowd. Some papers focus on risk assessment, [34] proposes a systematic approach to assessing the risk of a vulnerability causing adverse effects, while [63] investigates incidents in other domains and maps those to military systems.

One paper examines the methods of operation when detecting a vulnerability and provides recommendations on how to avoid vulnerabilities and improve security [25]. Another focuses on vulnerability reporting, providing recommendations on how to better manage vulnerability reports [65].

Vulnerability Life-Cycle. Papers in this category describe life-cycle models and analyse the dynamics of a vulnerability in its various states of existence. This may provide valuable insights for understanding the dynamics of a vulnerability, such as correlations between disclosure and exploitation or rate of patch uptake. [58] examine whether the delay between disclosure and acknowledgement by the vendor cluster across vendors. [10] explore whether there is a correlation between delay in patching after a disclosure and find no support that instant disclosure means faster patching. They do however find support that open source vendors are quicker to provide patches and that more serious vulnerabilities do seem to receive patches quicker. A somewhat contradictory result was reported in [52]: vendors facing the threat of disclosure, as well as vendors that risk loss of value, tend to provide patches faster. [49] examine whether grace periods between vulnerability discovery and disclosure have an impact on the speed of providing a patch but find no clear relationship. [45] examines whether (and what) publicly available information about a vulnerability has an impact on exploitation, finding that the risk of exploitation increases with increased criticality of the vulnerability and when several vulnerabilities are related to each other. Similarly, [14] finds that zero-day attacks typically last for almost a year before disclosure, but mostly affect few product owners. However, the amount of attacks increases with several orders of magnitude after disclosure. [8,12] analyse the number of attacks over the vulnerability life cycle, and [12] finds that many intrusions occur long after a patch has been released. [46] analyse the time delays between the various stages of the vulnerability life-cycle. [8] present a life-cycle model for a vulnerability and, using empirical data, correlates number of detected attacks to the stages of the life-cycle. [18] provide a theoretical model for the information dissemination of a vulnerability and analyse it from different stakeholders' perspectives.

[6,11] examine factors that affect prioritisation of which vulnerabilities to patch, as well as typical delay between disclosure and the release of a patch. [68] provide a model for patching practices for embedded software industrial control devices which can be used by companies in deciding strategic patching management. Two papers examine patch uptake and explore the rate at which patches are applied by users. [51] examine factors affecting the rate of patch uptake, finding that security experts and developers (and software with automatic updating

mechanisms) have significantly lower median times to patch. [68] examines patch uptake for embedded internet-connected industrial control systems, finding that patch uptake is slow. One paper evaluates CVSS based on severity scoring from a number of public vulnerability reward programs, finding that CVSS can be a useful metric for prioritising patching [70].

Economic Aspects. Papers in this category examine economic aspects of vulnerability disclosure, such as the cost of a vulnerability and return on investment for organising a BBP. [26] compare the cost of organising a bug bounty with the results and conclude that the benefits are considerably greater that the cost. [1,67] correlate loss of market value with vulnerability disclosure and conclude that there is usually a brief loss of value. [56] compare the cost of proactively detecting vulnerabilities with the cost of responding to black market exploits and conclude that the reactive approach is more economical.

Experience Reports. Two papers describe the Pentagon BBP [19,20] and another one focuses on smart-grid vendors [30]. [2] provides insights into fears experienced prior to BBP and countermeasures taken by the vendors.

3.2 Bug Hunter Crowd

The papers in the crowd category provide insight into both the bug-hunting community as a whole and individual bug hunters. Researchers from diverse fields such as information security, software engineering, computer science, information economics and ethics have contributed to this research, which spans over eleven years. Out of twelve papers included in this category four are theoretical and eight are based on empirical evidence collected and analysed using quantitative as well as qualitative research methods (see Fig. 6). The empirical data comes from middleman companies and vulnerability databases. The first publication is from 2007, and the papers have been classified as belonging to one or more of the sub-categories crowd trends, incentives for bug hunting, bug-hunters' skill set and ethics (see Fig. 7).

Crowd Trends. Papers in this category describe the bug-hunter community over time. The interest in BBPs has grown over time and both active and the overall crowd are growing [32,71,72], most of which are hunters that are not employed by the companies whose products they test [3,4,33]. The growth in crowd has led to an increase in the number of reported vulnerabilities [32,33,71], in particular ones of medium and critical severity [33,71]. One of the papers suggests a model for organisations' and bug-hunters' utility, concluding that for both parties the utility decreases as more bug hunters join a BBP [74]. This is likely due to the increasing number of reported duplicates, which for product owners means more time spent on reports and for bug hunters means more time spent without reward [74] causing them to switch programs [31,44,71,74].

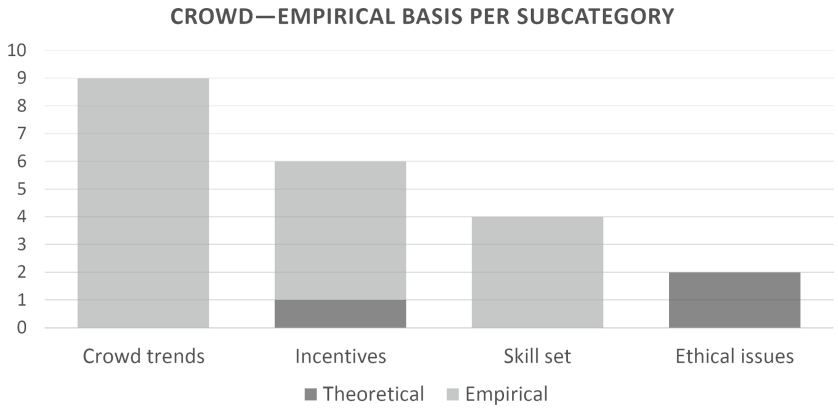

Fig. 6. Bug hunter crowd, empirical basis per subcategory (one paper can appear in more than one subcategory)

The most active bug hunters contribute to a majority of reports [31], in particular more critical ones [72], but still they are a minority of the crowd [31,33,71]. However, having a large crowd might still be preferable for a product owner, since that implies a sizeable contribution [72]. In particular middleman companies might benefit from this, since less active hackers tend to submit bug reports to a larger number of companies [72].

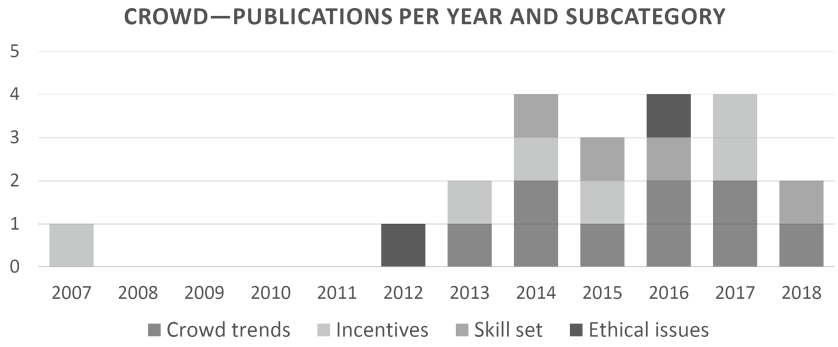

Fig. 7. Bug hunter crowd, publications per year and subcategory (one paper can appear in more than one subcategory)

Incentives for Bug Hunting. Papers in this category draw conclusions from both the behaviour of individual bug hunters as well as from the crowd as a whole. Monetary incentives are obviously important [3,4,44,72], particularly for the most active bug hunters [31]. Other incentives are: making products more safe and secure [31,72], building a reputation [72], and curiosity and having fun [3,4]. Further, one paper presents a theoretical model of how loss is reduced for both hunters and product owners [52].

Bug Hunters' Skill Set. This category describes the types of vulnerabilities that are addressed by the bug hunters and the skills that bug hunters possess. Most of the bug hunters are reported to have a single skill [33], but on a crowd level the diversity among skills is high [32]. The most commonly reported vulnerability types that bug hunters target are SQL injection, XSS and design flaws [32,33,71,72]. One paper reports that the bug-hunting crowd has a desire to increase their skill set when given the opportunity in form of public vulnerability reports or tutorials [72].

Ethical Issues. This category includes papers that provide suggestions on what moral issues to consider as a bug hunter. One paper offers guidelines for bug hunters [22] and the other one states which ethical issues to consider [57]. Both agree that the well-being of humans should be taken into consideration on small scale (e.g. privacy and safety) and large scale (e.g. political outcomes) and urge bug hunters to ensure that their findings are used for good.

3.3 Vulnerability Market Mechanisms

This category comprises papers that focus on the buying or selling of vulnerabilities or exploits, or on economic aspects of vulnerabilities. The 25 papers about market mechanisms have been classified as descriptive papers, theoretical models, market trends or ethics papers (see Fig. 8).

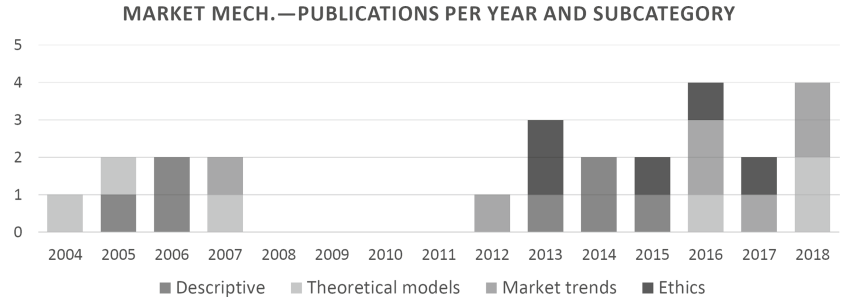

Fig. 8. Vulnerability markets, publications per year and subcategory

The research area has evolved since 2004 when the first paper was published. Early papers deal more with theory and descriptions of the area, while later papers examine empirical data and ethical implications. It seems that the area has become more applied with time, although theoretical models still seem to be of interest (see Fig. 9).

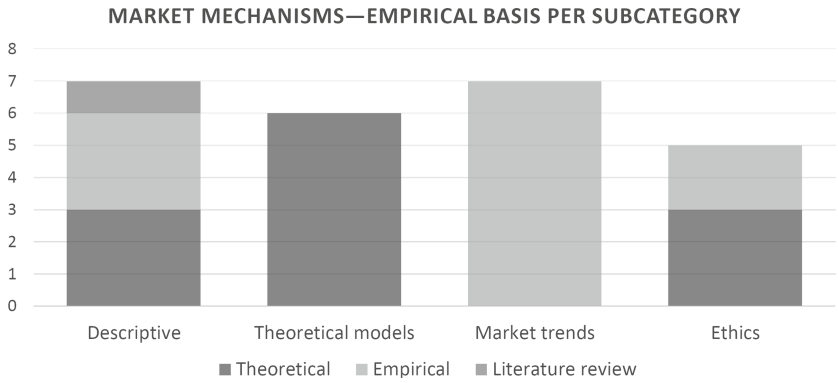

Fig. 9. Vulnerability markets, empirical basis per subcategory

Descriptive Papers. The papers in this category provide overviews and discussions of the area of vulnerability markets. Several are theoretical and based on economics. For instance, [7] establish that economics of information security is a new and thriving discipline. They apply classical economics theories to vulnerability markets and discuss how this can help understand the market mechanisms. This kind of analysis is also provided by [15,16], who further creates a typology of vulnerability markets: bug challenges, vulnerability brokers, exploit derivatives and cyber-insurance. [53] build on this when investigating the usefulness of different market types: vulnerability brokers, bug challenges, buyer's bug auction and seller's bug auction. [39] use institutional economics theory as a framework to understand vulnerability markets. Black and white markets are described by [9]. A different perspective is given by a discussion on black and white vulnerability markets as a basis for policy recommendations to reduce cybercrime [64].

Theoretical Models. These papers are based on mathematical models of market dynamics and agent behaviour. [35,36] use game theory to examine whether market-based mechanisms or a publicly funded intermediary performs better with regard to social welfare, suggesting that a publicly funded intermediary maximises social welfare. Another study models the vulnerability market as an optimisation problem of minimising social cost, attempting to explain why some vendors offer monetary rewards for vulnerabilities while others do not [62]. [54] develop a system dynamics model to describe the growth of a vulnerability black market and suggest that a white market may reduce black market trade. A more recent model covers the choice of selling vulnerabilities to software vendors (white market) or governments (grey market) [29]. [43] use game theory to examine who should foot the bill for information security - software vendors or the government.

Market Trends. The majority of these papers are published in recent years, suggesting that vulnerability markets are gaining interest within applied research. [42] analyse the effects of private (as opposed to publicly funded) intermediaries on disclosure and patching time, showing that disclosure time is not affected but time to patch may increase. Another study shows that market-based disclosure is beneficial for security, as it reduces the number of exploitation attempts [55]. [32] show that the more bug hunters that engage in a BBP, the more vulnerabilities are discovered. [50] examine the correlation between CVSS scores and bounties, concluding that the link between CVSS score and bounty is low. [59] examine and discuss exploit pricing, showing that many exploits are sold for a mere $50-100 on the white market. On the black market, exploits are priced equally high or higher [5]. However, [60] show that bug bounty programs can be successful even without monetary rewards.

Ethics. The papers in this category concern ethical aspects of vulnerability markets. One paper reports on an expert panel discussion which aimed at increasing awareness of the consequences of vulnerability markets [23]. Questions are raised, such as, can it be considered ethical to trade vulnerabilities in voting systems or in pacemakers? [69] argue that the selling of vulnerabilities may generally be considered ethical but that the selling of zero-day exploits may not. To reduce the market for zero-day exploits, they propose that software vendors should spend their money on in-house vulnerability discovery rather than on BBPs. Two papers concern American law: [13] argues that responsible disclosure infringes on freedom of speech, wherefore full disclosure is preferable, while [47] argues that a framework is needed to discern between criminal acts of disclosure and disclosure for the public good. Finally, one paper points out how society depends on information security and argues that information security should be viewed as a public good [48].

4 Discussion and Concluding Remarks

The number of BBPs has grown during the studied period, especially around the time when middleman companies increased their activity on the market. Examination of their public datasets has shown increased number of reported vulnerabilities over time, of medium and critical severity in particular. While the most active hunters tend to find not only more, but also more critical bugs, the contribution of the less active part of the crowd is still sizeable.

Product Owner. The increase in research is largest relating to guidelines for and economy of a BBP. It is crucial to know not only the cost of practically organizing a BBP, but also aspects such as: risks in vulnerability disclosure; cost of detecting a vulnerability in-house vs. in a BBP; cost comparisons between a reactive repair due to black market vulnerability discovery and proactive repair based on in-house BBP discovery. While [26] argue that benefits of a BBP greatly

overweigh the costs, in purely economic terms the reactive approach might be better as argued by [56], which appears quite cynical.

Vulnerability Market Mechanisms. White and black markets are in focus of this category [5,9,16,54,64]. While a white market is shown to be beneficial for establishing the price of vulnerabilities and to manage the "public good" [7,35,36], research also shows that it may be too easy to trade vulnerabilities on the black market instead [15,55,64].

Bug Hunter Crowd. While incentives for bug hunting include reputation, learning and fun, the most reported incentive is monetary [4,31,72]. For the most active hackers, monetary incentives are particularly important [31], which makes research on ethical aspects of bug hunting necessary. This type of research is found in all three main categories. Authors urge those selling bugs to consider safety and privacy aspects that otherwise might be in danger as a result of data leakage and vulnerabilities weaponisation [22,48,57].

Research Gaps. In order to fill the gaps in current understanding of BBP practice future research should include:

- Diverse data sets: A majority of empirical publications on BBP have used public data sets and open source projects. To our knowledge there are no academic publications examining BBPs for safety critical systems which are experiencing a dramatic increase in connectivity.
- Diverse research methods: Most of the empirical research, in particular that on bug hunters, is quantitative. Qualitative methods would provide more in-depth understanding of bug hunters' mind sets.
- Multidisciplinary research: Most authors have a background in information security or computer science. The literature is complemented by economics, law and philosophy researchers, who often contribute very different perspectives. Implications of BBPs for companies, individuals and states are complex, and multidisciplinary research can provide valuable insights.

Lastly, we believe that the ongoing increase in publications will likely require comprehensive systematic literature review in a few years time when the body of knowledge is substantial enough to draw relevant in-depth conclusions.

Appendix A

This appendix maps each publication included in the mapping study to the categories it was included in, product owner (PO), crowd (CR), and market mechanisms (MM).

Ref	Publication	PO	CR	MM
1	"*Is There a Cost to Privacy Breaches? An Event Study*", Acquisti, A., Friedman, A., Telang, R	X		
2	"*Friendly Hackers to the Rescue: How Organizations Perceive Crowdsourced Vulnerability Discovery*", Al-Banna, M., Benatallah, B., Schlagwein, D., Bertino, E., Barukh, M.C	X		
3	"*Most successful vulnerability discoverers: Motivation and methods*", Algarni, A.M., Malaiya, Y.K		X	
4	"*Software Vulnerability Markets: Discoverers And Buyers*, Algarni, A.M., Malaiya, Y.K		X	
5	"*Economic Factors of Vulnerability Trade and Exploitation*", Allodi, L			X
6	"*Comparing Vulnerability Severity and Exploits Using Case-Control Studies*", Allodi, L., Massacci, F	X		
7	"*The Economics of Information Security*", Anderson, R., Moore, T	X		X
8	"*Windows of vulnerability: a case study analysis*", Arbaugh, W.A., Fithen, W.L., McHugh, J	X		
9	"*0-Day Vulnerabilities and Cybercrime*", Armin, J., Foti, P. Cremonini, M			X
10	"*Economics of software vulnerability disclosure*", Arora, A., Telang, R	X		
11	"*An Empirical Analysis of Software Vendors' Patch Release Behavior: Impact of Vulnerability Disclosure*", Arora, A., Krishnan, R., Telang, R., Yang, Y.,	X		
12	"*Does information security attack frequency increase with vulnerability disclosure? An empirical analysis*", Arora, A., Nandkumar, A., Telang, R.,	X		
13	"*A Target to the Heart of the First Amendment: Government Endorsement of Responsible Disclosure as Unconstitutional*", Bergman, K			X
14	"*Before We Knew It: An Empirical Study of Zero-day Attacks in the Real World*", Bilge, L., Dumitraş, T	X		
15	"*Vulnerability markets*", Böhme, R			X
16	"*A Comparison of Market Approaches to Software Vulnerability Disclosure*", Böhme, R			X
17	"*Enter the Hydra: Towards Principled Bug Bounties and Exploit-Resistant Smart Contracts*", Breindenbach, L., Daian, P., Tramer, F., Juels, A.,	X		
18	"*Efficiency of Vulnerability Disclosure Mechanisms to Disseminate Vulnerability Knowledge*", Cavusoglu, H., Cavusoglu, H. Raghunathan, S	X		
19	"*Cybersecurity Innovation in Government: A Case Study of U.S. Pentagon's Vulnerability Reward Program*", Chatfield, A.T., Reddick, C.G	X		
20	"*Crowdsourced cybersecurity innovation: The case of the Pentagon's vulnerability reward program*", Chatfield, A.T., Reddick, C.G	X		
21	"*Network Security: Vulnerabilities and Disclosure Policy*", Choi, Jay Pil; Fershtman, C., Gandal, N	X		
22	"*Vulnerabilities and their surrounding ethical questions: a code of ethics for the private sector*", De Gregorio, A		X	
23	"*Markets for zero-day exploits: ethics and implications*", Egelman, S., Herley, C., van Oorschot, P.C			X
24	"*Private Ordering Shaping Cybersecurity Policy: The Case of Bug Bounties*", Elazari Bar On, A	X		
25	"*To Improve Cybersecurity, Think Like a Hacker*", Esteves, J., Ramalho, E., De Haro, G	X		
26	"*An Empirical Study of Vulnerability Rewards Programs*", Finifter, M., Akhawe, D., Wagner, D	X		
27	"*Vulnerability Disclosure: The Strange Case of Bret McDanel*", Freeman, E	X		
28	"*Web science challenges in researching bug bounties*", Fryer, H., Simperl, E., Fryer, H., Simperl, E	X		
29	"*Revenue Maximizing Markets for Zero-Day Exploits*", Guo, M., Hata, H., Babar, A			X
30	"*Cyber vulnerability disclosure policies for the smart grid*", Hahn, A., Govindarasu, M	X		
31	"*Understanding the Heterogeneity of Contributors in Bug Bounty Programs*", Hata, H., Guo, M., Babar, M. A		X	
32	"*A study on Web security incidents in China by analyzing vulnerability disclosure platforms*", Huang, C., Liu, J., Fang, Y., Zuo, Z.,		X	
33	"*Shifting to Mobile: Network-based Empirical Study of Mobile Vulnerability Market*", Huang, K., Zhang, J., Tan, W., Feng, Z		X	X
34	"*Defining and Assessing Quantitative Security Risk Measures Using Vulnerability Lifecycle and CVSS Metrics*", Joh, H., Malaiya, Y.K	X		
35	"*Economic analysis of the market for software vulnerability disclosure*", Kannan, K., Telang R			X
36	"*Market for Software Vulnerabilities? Think Again*", Kannan, K., Telang, R			X
39	"*Shifts in the Cybersecurity Paradigm: Zero-Day Exploits, Discourse, and Emerging Institutions*", Kuehn, A., Mueller, M			X
40	"*Banishing Misaligned Incentives for Validating Reports in Bug-Bounty Platforms*", Laszka, A., Zhao, M., Grossklags, J	X		
41	"*The Rules of Engagement for Bug Bounty Programs*", Laszka, A., Zhao, M., Malbari, A., Grossklags, J	X		
42	"*An examination of private intermediaries' roles in software vulnerabilities disclosure*", Li, P., Rao, H.R			X
43	"*Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets*", Li, Z., Liao, Q			X

(*continued*)

Ref	Publication	PO	CR	MM
44	"*Given enough eyeballs, all bugs are shallow? Revisiting Eric Raymond with bug bounty programs*", Maillart, T., Zhao, M., Grossklags, J., Chuang, J	X	X	
45	"*Software Vulnerability Disclosure and its Impact on Exploitation: An Empirical Study*", Mangalaraj, G.A., Raja, M.K	X		
46	"*Security-related vulnerability life cycle analysis*", Marconato, G. V., Nicomette, V., Kaâniche, M	X		
47	"*Hacking Speech: Informational Speech and the First Amendment*", Matwyshyn, A.M			X
48	"*Stockpiling Zero-Day Exploits: The Next International Weapons Taboo*", Maxwell, P			X
49	"*Are Vulnerability Disclosure Deadlines Justified?*", McQueen, M., Wright, J. L., Wellman, L	X		
50	"*Vulnerability Severity Scoring and Bounties: Why the Disconnect?*", Munaiah, N., Meneely, A			X
51	"*The Attack of the Clones: A Study of the Impact of Shared Code on Vulnerability Patching*", Nappa, A., Johnson, R., Bilge, L., Caballero, J., Dumitras, T	X		
52	"*To disclose or not? An analysis of software user behavior*", Nizovtsev, D., Thursby, M.,	X	X	
53	"*An Assessment of Market Methods for Information Security Risk Management*", Pandey, P., Snekkenes, E.A			X
54	"*Understanding Hidden Information Security Threats: The Vulnerability Black Market*", Radianti, J., Gonzalez, J.J			X
55	"*Are Markets for Vulnerabilities Effective?*", Ransbotham, S., Mitra, S., Ramsey, J			X
56	"*Is finding security holes a good idea?*", Rescorla, E	X		
57	"*Ethical Issues in E-Voting Security Analysis*", Robinson, D.G., Halderman, J.A		X	
58	"*Exploring the clustering of software vulnerability disclosure notifications across software vendors*", Ruohonen, J., Holvitie, J., Hyrynsalmi, S., Leppänen, V	X		
59	"*Trading exploits online: A preliminary case study*", Ruohonen, J., Hyrynsalmi, S., Leppänen, V			X
60	"*A Bug Bounty Perspective on the Disclosure of Web Vulnerabilities*", Ruohonen, J., Allodi, L			X
61	"*Current data security issues for financial services firms*", Sipes, E.K., James, J., Zetoony, D	X		
62	"*Economic Motivations for Software Bug Bounties*", Sprague, C., Wagner, J			X
63	"*Identifying self-inflicted vulnerabilities: The operational implications of technology within U.S. combat systems*", Stevens, R	X		
64	"*Curbing the Market for Cyber Weapons*", Stockton, P.N.; Golabek-Goldman, M			X
65	"*Doing What Is Right with Coordinated Vulnerability Disclosure*", Suárez, R.A., Scott, D	X		
66	"*Agents of responsibility in software vulnerability processes*", Takanen, A., Vuorijärvi, P., Laakso, M., Röning, J	X		
67	"*Impact of Software Vulnerability Announcements on the Market Value of Software Vendors - an Empirical Investigation*", Telang, R., Wattal, S	X		
68	"*Characterizing and Modeling Patching Practices of Industrial Control Systems*", Wang, B., Li, X., de Aguiar, L.P., Menasche, D.S., Shafiq, Z	X		
69	"*Ethics of the software vulnerabilities and exploits market*", Wolf, M.J., Fresco, N			X
70	"*Evaluating CVSS Base Score Using Vulnerability Rewards Programs*", Younis, A., Malaiya, Y., Ray, I	X		
71	"*An Exploratory Study of White Hat Behaviors in a Web Vulnerability Disclosure Program*", Zhao, M., Grossklags, J., Chen, K	X	X	
72	"*An Empirical Study of Web Vulnerability Discovery Ecosystems*", Zhao, M., Grossklags, J., Liu, P		X	
73	"*Devising Effective Policies for Bug-Bounty Platforms and Security Vulnerability Discovery*", Zhao, M., Laszka, A., Grossklags, J	X		
74	"*Crowdsourced Security Vulnerability Discovery: Modeling and Organizing Bug-Bounty Programs*", Zhao, M., Laszka, A., Maillart, T., Grossklags, J	X	X	

References

1. Acquisti, A., Friedman, A., Telang, R.: Is there a cost to privacy breaches? An event study. In: Proceedings of International Conference on Information Systems, p. 19 (2006)
2. Al-Banna, M., Benatallah, B., Schlagwein, D., Bertino, E., Barukh, M.C.: Friendly hackers to the rescue: how organizations perceive crowdsourced vulnerability discovery. In: Proceedings of the Pacific Asia Conference on Information Systems, p. 15 (2018)

3. Algarni, A.M., Malaiya, Y.K.: Most successful vulnerability discoverers: motivation and methods. In: Proceedings of the International Conference on Security and Management (SAM), p. 1. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp) (2013)
4. Algarni, A.M., Malaiya, Y.K.: Software vulnerability markets: discoverers and buyers. Int. J. Comput. Inf. Sci. Eng. **8**, 71–81 (2014). Zenodo
5. Allodi, L.: Economic factors of vulnerability trade and exploitation. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security - CCS 2017, pp. 1483–1499 (2017)
6. Allodi, L., Massacci, F.: Comparing vulnerability severity and exploits using case-control studies. ACM Trans. Inf. Syst. Secur. **17**(1), 1:1–1:20 (2014)
7. Anderson, R., Moore, T.: The economics of information security. Science **314**(5799), 610–613 (2006)
8. Arbaugh, W.A., Fithen, W.L., McHugh, J.: Windows of vulnerability: a case study analysis. Computer **33**(12), 52–59 (2000)
9. Armin, J., Foti, P., Cremonini, M.: 0-day vulnerabilities and cybercrime. In: 10th International Conference on Availability, Reliability and Security, pp. 711–718 (2015)
10. Arora, A., Telang, R.: Economics of software vulnerability disclosure. IEEE Secur. Priv. **3**(1), 20–25 (2005)
11. Arora, A., Krishnan, R., Telang, R., Yang, Y.: An empirical analysis of software vendors' patch release behavior: impact of vulnerability disclosure. Inf. Syst. Res. **21**(1), 115–132 (2010)
12. Arora, A., Nandkumar, A., Telang, R.: Does information security attack frequency increase with vulnerability disclosure? An empirical analysis. Inf. Syst. Front. **8**(5), 350–362 (2006). https://doi.org/10.1007/s10796-006-9012-5
13. Bergman, K.M.: A target to the heart of the first amendment: government endorsement of responsible disclosure as unconstitutional. Northwest. J. Technol. Intellect. Property **13**, 38 (2015)
14. Bilge, L., Dumitraş, T.: Before we knew it: an empirical study of zero-day attacks in the real world. In: Proceedings of the 2012 ACM Conference on Computer and Communications Security, CCS 2012, pp. 833–844. ACM, New York (2012)
15. Böhme, R.: Vulnerability markets. Proc. 22C3 **27**, 30 (2005)
16. Böhme, R.: A comparison of market approaches to software vulnerability disclosure. In: Müller, G. (ed.) ETRICS 2006. LNCS, vol. 3995, pp. 298–311. Springer, Heidelberg (2006). https://doi.org/10.1007/11766155_21
17. Breindenbach, L., Daian, P., Tramer, F., Juels, A.: Enter the hydra: towards principled bug bounties and exploit-resistant smart contracts. In: 27th USENIX Security Symposium, pp. 1335–1352 (2018)
18. Cavusoglu, H., Cavusoglu, H., Raghunathan, S.: Efficiency of vulnerability disclosure mechanisms to disseminate vulnerability knowledge. IEEE Trans. Softw. Eng. **33**(3), 171–185 (2007)
19. Chatfield, A.T., Reddick, C.G.: Cybersecurity innovation in government: a case study of U.S. Pentagon's vulnerability reward program. In: Proceedings of the 18th Annual International Conference on Digital Government Research - DGO 2017, Staten Island, NY, USA, pp. 64–73. ACM Press (2017)
20. Chatfield, A.T., Reddick, C.G.: Crowdsourced cybersecurity innovation: the case of the Pentagon's vulnerability reward program. Inf. Polity **23**(2), 177–194 (2018)
21. Choi, J.P., Fershtman, C., Gandal, N.: Network security: vulnerabilities and disclosure policy*. J. Ind. Econ. **58**(4), 868–894 (2010)

22. De Gregorio, A.: Vulnerabilities and their surrounding ethical questions: a code of ethics for the private sector. In: 2016 International Conference on Cyber Conflict (CyCon U.S.), pp. 1–4 (2016)
23. Egelman, S., Herley, C., van Oorschot, P.C.: Markets for zero-day exploits: ethics and implications. In: Proceedings of the 2013 Workshop on New Security Paradigms Workshop - NSPW 2013, Banff, Alberta, Canada, pp. 41–46. ACM Press (2013)
24. Elazari Bar On, A.: Private ordering shaping cybersecurity policy: the case of bug bounties. SSRN Scholarly Paper ID 3161758, Social Science Research Network, Rochester, NY (2018)
25. Esteves, J., Ramalho, E., Haro, G.D.: To improve cybersecurity, think like a hacker. MIT Sloan Manage. Rev. **58**(3), 71 (2017)
26. Finifter, M., Akhawe, D., Wagner, D.: An empirical study of vulnerability rewards programs. In: 22nd USENIX Security Symposium, pp. 273–288 (2013)
27. Freeman, E.: Vulnerability disclosure: the strange case of Bret McDanel. Inf. Syst. Secur. **16**(2), 127–131 (2007)
28. Fryer, H., Simperl, E.: Web science challenges in researching bug bounties. In: Proceedings of the 9th ACM Conference on Web Science, WebSci 2017, pp. 273–277. ACM (2017)
29. Guo, M., Hata, H., Babar, A.: Revenue maximizing markets for zero-day exploits. In: Baldoni, M., Chopra, A.K., Son, T.C., Hirayama, K., Torroni, P. (eds.) PRIMA 2016. LNCS (LNAI), vol. 9862, pp. 247–260. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-44832-9_15
30. Hahn, A., Govindarasu, M.: Cyber vulnerability disclosure policies for the smart grid. In: 2012 IEEE Power and Energy Society General Meeting, pp. 1–5 (2012)
31. Hata, H., Guo, M., Babar, M.A.: Understanding the heterogeneity of contributors in bug bounty programs. In: 2017 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM), pp. 223–228 (2017)
32. Huang, C., Liu, J., Fang, Y., Zuo, Z.: A study on Web security incidents in China by analyzing vulnerability disclosure platforms. Comput. Secur. **58**, 47–62 (2016)
33. Huang, K., Zhang, J., Tan, W., Feng, Z.: Shifting to mobile: network-based empirical study of mobile vulnerability market. IEEE Trans. Serv. Comput. **13**(1), 144–157 (2018)
34. Joh, H., Malaiya, Y.K.: Defining and assessing quantitative security risk measures using vulnerability lifecycle and CVSS metrics. In: Proceedings of the International Conference on Security and Management, p. 7 (2011)
35. Kannan, K., Telang, R., Xu, H.: Economic analysis of the market for software vulnerability disclosure. In: Proceedings of the 37th Annual Hawaii International Conference on System Sciences, p. 8 (2004)
36. Kannan, K., Telang, R.: Market for software vulnerabilities? Think again. Manage. Sci. **51**(5), 726–740 (2005). https://www.jstor.org/stable/20110369
37. Kitchenham, B., Charters, S.: Guidelines for performing systematic literature reviews in software engineering. EBSE Technical report (2007)
38. Kitchenham, B.A., Budgen, D., Brereton, O.P.: Using mapping studies as the basis for further research - a participant-observer case study. Inf. Softw. Technol. **53**(6), 638–651 (2011). Special Section: Best papers from the APSEC
39. 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, pp. 63–68. ACM, New York (2014)

40. Laszka, A., Zhao, M., Grossklags, J.: Banishing misaligned incentives for validating reports in bug-bounty platforms. In: Askoxylakis, I., Ioannidis, S., Katsikas, S., Meadows, C. (eds.) ESORICS 2016. LNCS, vol. 9879, pp. 161–178. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-45741-3_9
41. Laszka, A., Zhao, M., Malbari, A., Grossklags, J.: The rules of engagement for bug bounty programs. In: Meiklejohn, S., Sako, K. (eds.) FC 2018. LNCS, vol. 10957, pp. 138–159. Springer, Heidelberg (2018). https://doi.org/10.1007/978-3-662-58387-6_8
42. Li, P., Rao, H.R.: An examination of private intermediaries' roles in software vulnerabilities disclosure. Inf. Syst. Front. **9**(5), 531–539 (2007). https://doi.org/10.1007/s10796-007-9047-2
43. Li, Z., Liao, Q.: Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets. Gov. Inf. Q. **35**(1), 151–160 (2018)
44. Maillart, T., Zhao, M., Grossklags, J., Chuang, J.: Given enough eyeballs, all bugs are shallow? Revisiting Eric Raymond with bug bounty programs. J. Cybersecur. **3**(2), 81–90 (2017)
45. Mangalaraj, G.A., Raja, M.K.: Software vulnerability disclosure and its impact on exploitation: an empirical study. In: Proceedings of AMCIS 2005, p. 9 (2005)
46. Marconato, G.V., Nicomette, V., Kaâniche, M.: Security-related vulnerability life cycle analysis. In: 2012 7th International Conference on Risks and Security of Internet and Systems (CRiSIS), pp. 1–8 (2012)
47. Matwyshyn, A.M.: Hacking speech: informational speech and the first amendment. Northwestern University Law Review, p. 52 (2013)
48. Maxwell, P.: Stockpiling zero-day exploits: the next international weapons taboo. In: Proceedings of 5th International Conference on Management Leadership and Governance, p. 8 (2017)
49. McQueen, M., Wright, J.L., Wellman, L.: Are vulnerability disclosure deadlines justified? In: 2011 Third International Workshop on Security Measurements and Metrics, pp. 96–101 (2011)
50. Munaiah, N., Meneely, A.: Vulnerability severity scoring and bounties: why the disconnect? In: Proceedings of the 2nd International Workshop on Software Analytics, SWAN, Seattle, WA, USA, pp. 8–14. ACM, New York (2016)
51. Nappa, A., Johnson, R., Bilge, L., Caballero, J., Dumitras, T.: The attack of the clones: a study of the impact of shared code on vulnerability patching. In: 2015 IEEE Symposium on Security and Privacy, pp. 692–708 (2015)
52. Nizovtsev, D., Thursby, M.: To disclose or not? An analysis of software user behavior. Inf. Econ. Policy **19**(1), 43–64 (2007)
53. Pandey, P., Snekkenes, E.A.: An assessment of market methods for information security risk management. In: Proceedings of 16th IEEE International Conference on High Performance and Communications (2014)
54. Radianti, J., Gonzalez, J.J.: Understanding hidden information security threats: the vulnerability black market. In: 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07), p. 156c (2007)
55. Ransbotham, S., Mitra, S., Ramsey, J.: Are Markets for Vulnerabilities Effective? MIS Q. **36**(1), 43–64 (2012)
56. Rescorla, E.: Is finding security holes a good idea? IEEE Secur. Priv. Mag. **3**(1), 14–19 (2005)
57. Robinson, D.G., Halderman, J.A.: Ethical issues in e-voting security analysis. In: Danezis, G., Dietrich, S., Sako, K. (eds.) FC 2011. LNCS, vol. 7126, pp. 119–130. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-29889-9_10

58. Ruohonen, J., Holvitie, J., Hyrynsalmi, S., Leppänen, V.: Exploring the clustering of software vulnerability disclosure notifications across software vendors. In: 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), pp. 1–8 (2016)
59. Ruohonen, J., Hyrynsalmi, S., Leppänen, V.: Trading exploits online: a preliminary case study. In: 2016 IEEE Tenth International Conference on Research Challenges in Information Science (RCIS), pp. 1–12 (2016)
60. Ruohonen, J., Allodi, L.: A bug bounty perspective on the disclosure of web vulnerabilities. In: Proceedings of 17th Annual Workshop on the Economics of Information Security (2018)
61. Sipes, E.K., James, J., Zetoony, D.: Current data security issues for financial services firms. J. Invest. Compliance **17**(3), 55–59 (2016)
62. Sprague, C., Wagner, J.: Economic motivations for software bug bounties. Econ. Bull. **38**(1), 550–557 (2018)
63. Stevens, R.: Identifying self-inflicted vulnerabilities: the operational implications of technology within U.S. combat systems. In: 2017 International Conference on Cyber Conflict (CyCon U.S.), pp. 112–118 (2017)
64. Stockton, P.N., Golabek-Goldman, M.: Curbing the market for cyber weapons. Policy Rev. **32**, 29 (2013)
65. Suárez, R.A., Scott, D.: Doing what is right with coordinated vulnerability disclosure. Biomed. Instrum. Technol. **51**(s6), 42–45 (2017)
66. Takanen, A., Vuorijärvi, P., Laakso, M., Röning, J.: Agents of responsibility in software vulnerability processes. Ethics Inf. Technol. **6**(2), 93–110 (2004). https://doi.org/10.1007/s10676-004-1266-3
67. Telang, R., Wattal, S.: Impact of software vulnerability announcements on the market value of software vendors - an empirical investigation. SSRN Scholarly Paper, Social Science Research Network (2005)
68. Wang, B., Li, X., de Aguiar, L.P., Menasche, D.S., Shafiq, Z.: Characterizing and modeling patching practices of industrial control systems. In: Proceedings of the 2017 ACM SIGMETRICS/International Conference on Measurement and Modeling of Computer Systems, p. 9. ACM, New York (2017)
69. Wolf, M.J., Fresco, N.: Ethics of the software vulnerabilities and exploits market. Inf. Soc. **32**(4), 269–279 (2016)
70. Younis, A., Malaiya, Y.K., Ray, I.: Evaluating CVSS base score using vulnerability rewards programs. In: Hoepman, J.-H., Katzenbeisser, S. (eds.) SEC 2016. IAICT, vol. 471, pp. 62–75. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-33630-5_5
71. Zhao, M., Grossklags, J., Chen, K.: An exploratory study of white hat behaviors in a web vulnerability disclosure program. In: Proceedings of the 2014 ACM Workshop on Security Information Workers, pp. 51–58. ACM, New York (2014)
72. Zhao, M., Grossklags, J., Liu, P.: An empirical study of web vulnerability discovery ecosystems. In: Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp. 1105–1117. ACM (2015)
73. Zhao, M., Laszka, A., Grossklags, J.: Devising effective policies for bug-bounty platforms and security vulnerability discovery. J. Inf. Policy **7**, 372–418 (2017)
74. Zhao, M., Laszka, A., Maillart, T., Grossklags, J.: Crowdsourced security vulnerability discovery: modeling and organizing bug-bounty programs. In: The HCOMP Workshop on Mathematical Foundations of Human Computation, Austin (2016)