Markets for Zero-Day Exploits: Ethics and Implications

Serge Egelman
University of California
Berkeley, CA, USA
egelman@cs.berkeley.edu

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot*
Carleton University
Ottawa, Ontario, Canada
paulv@scs.carleton.ca

ABSTRACT

A New Security Paradigms Workshop (2013) panel discussed the topic of ethical issues and implications related to markets for zero-day exploits, i.e., markets facilitating the sale of previously unknown details on how to exploit software vulnerabilities in target applications or systems. The related topic of vulnerability rewards programs ("bug bounties" offered by software vendors) was also discussed. This note provides selected background material submitted prior to the panel presentation, and summarizes discussion resulting from the input of both the panelists and NSPW participants.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection; K.6.0 [**Management of Computing and Information Systems**]: General—*Economics*; D.4.6 [**Software**]: Security and Protection

Keywords

Vulnerabilities; Exploits; Security Economics

1. INTRODUCTION

Zero-day exploits ("0-days") are techniques that exploit vulnerabilities in a target software program, where the vulnerabilities are not yet known by the developers of the target program or other parties, and for which fixes are therefore not yet available. The trading of software exploits between hackers is an activity with a long history; it has become more interesting as criminal elements have increasingly used such exploits for their own economic benefit. Selling of 0-days by security researchers as a supposedly "legitimate source of income" is an interesting spin on this—but already for several years now, some software companies have offered, to software experts wearing hats of various colors, *bug bounties* for private technical details of new exploits targeting that company's own products. Some may question the ethics and implications of this practice; the issues become even more interesting when the exploits are bought by parties other than the developers of the targeted software. Indeed, 0-day markets do not lead to public disclosure when the interests of the buyers are better served by having the vulnerabilities remain unpatched [16].

Our interest is in *markets* that facilitate the sale of 0-days—not the existence or mechanics of such markets per se, but rather the *implications and ethical issues* related to the development, promotion, use, and possible regulation of such markets. A primary motivation is the growing popularity of markets for 0-days as evident from recent media articles [4, 5, 6, 7, 14], the growing prices of exploits in such markets, and the lack of discussion to date by the mainstream academic community of the ethics and security implications.

We believe that this topic is timely, as it involves the relatively new paradigm of markets for 0-days. One of our goals is to increase awareness among researchers of such markets, and in particular, related ethical issues and implications. We believe that the general topic of ethics within computer security deserves greater attention in academic curricula, and thus discussion of interesting, novel ethical topics in major forums benefits the community, and students in particular.

Between them, the panelists represent academia (two currently at universities and all with active publication records), industrial views (two have extensive background in industry), and government (one has worked in, and all have worked with, government).

2. RELATED WORK AND RECENT PRESS

A brief chronological summary of selected related literature and media articles follows.

- Rescorla's 2003-2004 work [13] raises interesting questions about the utility and benefits of searching for software bugs, considering both whitehats and blackhats; in particular, he raises the possibility that effort spent finding vulnerabilities may not significantly increase software quality.

- Ozment's 2004 paper [11] summarizes Schechter's earlier formulation of vulnerability markets [15] (which included the "market price of vulnerability" concept), and proposes that there are advantages to considering vulnerability markets in terms of bug auctions.

*Author's version (Oct.24, 2013), posted for personal use; not for redistribution. The definitive version was published as below. http://dx.doi.org/10.1145/2535813.2535818.

NSPW'13, September 9–12, 2013, Banff, AB, Canada.

ACM 978-1-4503-2582-0/13/09 ...$15.00..

- Ozment's 2005 work [12] revisits Rescorla's view that vulnerability hunting may be of questionable social benefit, giving evidence of a higher likelihood of rediscovery of bugs by independent parties (e.g., blackhats finding the same bugs that whitehats might find), suggesting that hunting effort offers greater utility.

- Böhme's 2005-2006 work [1] gives terminology for four economic markets related to software vulnerabilities: bug challenges (including bug bounties and bug auctions), vulnerability brokers (buying details for circulation to other subscribers), exploit derivatives (contracts paying out fixed sums upon occurrence of security events), and cyber-insurance.

- Miller's 2007 work [9] notes problems faced by a security researcher wishing to sell 0-day exploits to a "legitimate buyer." He mentions bug bounty programs that existed as early as 1995 (Netscape), and other organizations paying for vulnerability information in bug-buying programs (e.g., Mozilla, iDefense Labs (Versign), the Zero Day Initiative of the TippingPoint division of 3Com), as well as the details of his own sale of an exploit to the NSA for $50,000.

- (Jan. 31 2010) article on WRAL TechWire [14] discusses the underground market, and specifically mentions Google's bug-bounty program for Chrome browser bugs (and others as noted by Miller above).

- (Mar. 23, 2012) Greenberg [7] discusses the $250,000 sale of an iOS exploit arranged by exploit broker "the Grugq," and mentions the French company Vupens specializing in selling exploits as profiled in Forbes magazine (Apr. 9 2012). The raises the question whether 0-day markets should be regulated?[1]

- (Mar. 29 2012) soon thereafter, Hofman and Timm [8] cite Greenberg's discussion of the *"dangerous but largely underreported problem in internet security: the sale of 0-day exploits to customers not intending to fix the flaws."* Should laws disallow government agencies from any activities that discourage fixing of software vulnerabilities?

- (May 30, 2012) Schneier [16] notes that originally, bounties resulted in bugs being fixed, but now criminals—and governments[2]—buy bugs for private exploitation, benefiting from the bugs *not* being fixed and the details *not* being publicly disclosed. He suggests that the economics of 0-day markets are detrimental to society, as they motivate the private sale of exploits: previously when third parties found vulnerabilities, economics favored disclosure (for hacker notoriety, academic credit, and consulting credibility), pressuring vendors to patch and improve security.[3]

- (January, 2013) the popular CanSecWest Pwn2Own contests (e.g., see [5]), ongoing since about 2007, show the increasing popularity of big-dollar rewards for exploit details, with those details not always flowing back to the developers of the targeted software. In a twist on this, in September 2013, a website arose to crowdsource a reward for the first demonstrated defeat of the fingerprint sensor on Apple's new iPhone 5S phone.

- Finifter et al. [2] studied empirical data on the vulnerability rewards programs of Google Chrome and Mozilla Firefox—thus, both directly involving software developers of the target software, whose interest is presumably in fixing the vulnerabilities rather than exploiting them. Over a three-year period, 28% and 24%, respectively, of Chrome and Firefox patched vulnerabilities reported in security advisories resulted from these bug bounty programs. The authors suggest that both programs compare favorably (from the viewpoint of the software vendor) to hiring full-time security researchers, and correspondingly from the viewpoint of the flaw-finders in such bounty programs, the economic compensation is inferior to a full-time job.

- A Microsoft bug bounty program announced June 2013 offered rewards up to US$100,000 for identifying and fixing major product security flaws. In October 2013, it paid out [3] US$100,000 to James Forshaw related to a flaw he found in the Windows operating system.

For further discussion of related work, among other publications, we recommend Böhme [1] for an early view, and Finifter et al. [2] for more recent work.

3. PANEL FORMAT AND SET-UP

The panel format was as follows. The third author provided brief setting and background, serving as panel/session chair. He very briefly mentioned selected related work (see above), posed two questions for discussion (see next paragraph), and defined the following base terminology.

- A *Vulnerability Rewards Program (VRP)* is a program whereby a software vendor pays an outside researcher a "bug bounty" for disclosing details of a security-related software flaw.

- A *Zero-Day Market (ZDM)* is a market resulting in the sale of exploit or bug details; a vendor responsible for developing the software in question may (but often will not) learn these details as a result.

The first two authors were assigned as panelists to argue opposite sides of two intentionally broad/vague statements:[4]

1. *"VRPs are beneficial"*
2. *"ZDMs are beneficial"*

To focus and stimulate discussion, a set of background questions (see immediately below) were presented both in the workshop pre-proceedings, and at the start of the panel session itself. Example arguments *for* and *against* VRPs and ZDMs (see the following sub-sections) were also provided in

[1]See also March 15, 2013 article by Mueller [10].
[2]This is as well as agents buying the exploits as middlemen, for governments preferring to deal through contractors.
[3]This is especially true when done "responsibly," i.e., disclosure after sufficient advance notice to allow fixes *a priori*.
[4]One NSPW attendee suggested that the propositions were not ideally suited for the purpose, and that a better debate would result from a statement such as: "Be it resolved that ACM members should not participate in ZDMs."

the pre-workshop proceedings. After brief opening remarks by the two debating panelists, the NSPW attendees (participants) were asked to participate by contributing their own input, observations, or questions to the panelists.

The following example questions were posed at the beginning of the panel session, as background to focus discussion. The panelists and NSPW attendees were asked to consider these questions, with respect to both VRPs and ZDMs (jointly, or individually).

1. Do they turn strong young programmers into blackhats— or motivate development of much-needed security skills?
2. Do they threaten in-house security careers?
3. For whom are they beneficial?
4. Do they result in the discovery of vulnerabilities that would otherwise remain dormant?
5. Do they result in fewer public disclosures of bugs?
6. Do they subsidize undesirable activities (e.g., criminal activities, or unethical government use of exploits), or are they a highly economical way to find bugs?
7. Should they be regulated markets?

Much of the ensuing discussion centred on these questions. A number of the example "for" and "against" arguments (see following subsections) similarly touch on these questions.

3.1 Example arguments "FOR"

The following example arguments for VRPs and/or ZDMs were given prior to the formal panel session.

- We need all the help we can get. The software industry spends a lot of effort discovering bugs. We can't afford to neglect any avenue to improving our discovery rate.
- Tournaments are the least-cost way of getting work done. We can get the maximum number of exploits for the minimum cost.
- Having good relations with more responsible members of the hacking community increases the chance of having eyes and ears into goings-on.
- Large-scale effort at discovering vulnerabilities is healthy. Regular sustained effort makes it less likely that unspent fuel accumulates. Assertion: the potential for catastrophic societal harm is less if vulnerabilities are exposed in an evenly spaced fashion than if they were used all at once. The potential for major hacks on critical infrastructure is reduced if an army of people is constantly looking and reporting.
- There's already a market for vulnerabilities, but hackers are paid in fame and notoriety. Blackhat, defcon, and dozens of other 'cons' are bazaars where hackers try to leverage their exploits into pen testing gigs, free drinks, book deals, interviews, blog traffic or twitter followers. Society would be better served if this process of monetizing exploits resembled a market more and "Keeping up with the Kardashians" less.
- Computer security does not need yet another topic which drives us to absolutist positions. Dealing with a world-of-grey morally ambiguous issue where the lines are unclear would be good for us. Lessons learned might be put to good use elsewhere.

3.2 Example arguments "AGAINST"

The following example arguments against VRPs and/or ZDMs were given prior to the formal panel session.

- Injecting money into dubious circles is morally suspect. Cybercriminal circles intersect with organized crime, drug cartels and terrorism. We should not be involved in financing these operations.
- The *cobra effect*:[5] paying for exploits creates an adverse incentive to plant bugs for later harvest. Humans are extraordinarily good at gaming any system put in place, and the chance of software that is less (vs. more) secure is very real.
- Is this just a way for companies like Microsoft, Google and Apple to outsource product testing on the cheap? If they can get away with getting work done without paying salary and benefits, they will. Is it good for society, or the industry, if that happens?
- 0-day markets encourage the private sale (and non-disclosure) of details of exploits, to better allow the buyer to execute the exploit for private benefit.
- Markets create attractive incentives for more smart people to spend time finding vulnerabilities—and if it is true that the more you look, the more bugs you will find, then such attractive markets will increase the number of (privately-known) vulnerabilities.
- If a software producer buys an exploit, they may require a signed NDA as a condition of the sale, which may result in a fix being developed much slower than if the vulnerability were simply publicized.
- Assertion: this isn't the most efficient way of allocating resources. It would be more efficient to use the bounties for other purposes, e.g., training developers to make fewer mistakes.

4. INTEGRATED DISCUSSION SUMMARY

As noted above, one panelist was assigned to argue *for* the case that VRPs and ZDMs are beneficial, while a second was assigned to argue *against* them being beneficial. After brief background from the panel chair and opening arguments from the two panelists, the chair took round-robin input from the NSPW participants, requesting that comments and discussion focus, as much as possible, on issues related to ethics and implications. Time allowed just over two-thirds of the NSPW attendees to provide their input; the remaining attendees were invited to submit remarks to the NSPW scribe (a standing option at NSPW), who recorded all comments (and provided same to the authors). The selective summary below combines discussion points raised, including observations, assertions, and questions.

[5]See `http://en.wikipedia.org/wiki/Cobra_effect`

1. *VRP benefits include expanding the field of experts.* A beneficial aspect of VRPs is that they provide new opportunities to developers and thus help expand the field. One NSPW participant had met developers who entered the field through bug bounty funding, in an environment where no companies employed developers; and Finifter et al. [2] note that several researchers who distinguished themselves through the VRP programs of Google and Mozilla were later hired by those organizations. One participant noted that this field expansion might be negative in the sense of "more jobs creating worse software;" a counterpoint was that corporate developers are rewarded better for jobs well done than for "burying Easter eggs."

2. *VRPs and ethics in embedded/other special systems.* Are ethical issues different for VRPs targeting vulnerabilities in embedded systems (vs. standard desktop client software, mobile device software, or server software)? Are there specific scenarios where we should avoid creating incentives for vulnerability discovery if the consequences are especially serious? Would it be ethical to sell, or trade in, vulnerabilities in voting systems? A general observation is that markets are most likely to be ethical when the producer of the system is the party who has the highest incentive to pay for vulnerabilities; thus a market for vulnerabilities in voting systems may not have favorable ethics.

3. *Ethics and markets.* A counter argument is that ethics are irrelevant to markets—markets exist whether we like it or not. Many corporations act independently of ethical considerations, motivated by profit goals. ZDMs themselves may be viewed as ethically neutral; what is important is the ethics of the actors involved including the discoverer and the parties willing to pay for information discovered, and how they play out; how does the discoverer choose what offer to accept? Ethical questions arise if buyers have ill intent. Bugs sold directly to a vendor retain residual value on a ZDM (patches aren't deployed immediately or universally).

4. *Vulnerability or exploit, environments, price discovery.* Software vulnerabilities often depend on environment, e.g., some are exploitable on specific platforms only. Working exploits typically command greater bounties than vulnerabilities which have not yet, or cannot, be turned into exploits. Vulnerabilities are not interchangeable nor directly comparable. Thus pricing and establishing efficient markets is difficult. One participant suggested that market regulations for VRPs should require buyers to publish, in advance, their evaluation criteria for (valuing) vulnerabilities. Price discovery is a potential challenge (the seller needs a way to provide convincing evidence of the existence and importance of his information, without revealing all details themselves). A type of zero-knowledge proof system would help (for a protocol, see Miller [9]).

5. *Markets independent of software vendors.* Some software has no formal vendor—e.g., open source or other free or community-maintained software. So, there may be no vendor willing to pay for vulnerability information. This motivates the need for markets independent of a software vendor. Companies smaller than Microsoft and Google might not be able to afford to participate in an efficient market. Should smaller vendors charge a premium to high-risk customers to subsidize their participation in the markets? Small developers may not have the capability to pay bug bounties.

6. *Fishing the bug pool vs. rewarding secure design.* Is it true that the more vulnerabilities that are found, the fewer there are left?[6] How big are the reserves of vulnerabilities—though they may get harder to find (i.e., the price may go up), with more work might we keep finding as many bugs as we want? (Is there an analogy to fossil fuel market; are we "in a fracking situation?") Is our energy not better spent finding a way to reward the creation of knowledge on how to create systems with stronger security properties?

7. *Markets with prices that reveal information.* Related to this, it was suggested that markets should be designed to reward secure development/deployment—i.e., market prices should reveal or reflect something about the security of the underlying products, extracting hidden information.[7] Cobra effects can be addressed by options contracts that reward vendors for deploying secure products—e.g., "We pay out a reward if no cobra is seen before the end of the week."

8. *Academia as a VRP.* It was suggested that academia is possibly the largest VRP. Professors are rewarded for papers that describe and analyze vulnerabilities; many security consultants also publicize their findings, to build up their credibility. Do VRPs broadly defined (including a culture bestowing benefits to academics and consultants) incentivize, in a "smart subpopulation," a "continuing to look for bugs" behavior over one of "learning how to build better systems?"

9. *Goods of different value to different actors.* VRPs and ZDMs are not new. An old question is: How do we resolve any incentive mismatch whereby exploiters pay a higher price than defenders? The goods don't have equal value to all market participants. This market has characteristics of extortion, and needs transparency in terms of the same information to all participants (cf. Miller [9]). For example, would a vulnerability allowing shut-down of a pacemaker be worth much more to the patient than the device manufacturer? (This may depend on any liability the manufacturer may bear.) For vulnerabilities that can be leveraged into powerful exploits, there may be a stronger incentive to use them as such rather than to sell them to vendors; but some researchers may do the latter for ethical or reputational (vs. monetary) reasons.

10. *Vendor interaction with bug finders.* How does industry deal with actors who find these bugs; what incentives are offered to bring vendors the details, rather than to the public or black markets? It ranges widely from relying on perceptions of "public good," "ethics" and "the right thing to do," to bug bounties, to peer and societal pressure. Not all individuals are equally

[6] See Rescorla [13] for discussion.

[7] See Böhme [1] for discussion.

sensitive to such pressures. This may argue in favor of regulating VRPs and ZDMs.

11. *Cobra effect on credit card fraud.* It was asserted that credit card systems provide a big incentive to create detectable fraud because in many countries, merchants must pay for fraud through a service fee to the issuer. Thus the issuing bank benefits from greater volumes of detectable fraud.

12. *Cobra effect and anti-virus industry.* It was observed that fears of a cobra effect (by way of planting bugs) are analogous to long-standing accusations that anti-virus vendors create viruses to help sell their products.

13. *Avoiding cobra effect.* Incentives in ZDMs should be designed to preclude cobra effects. The incentive to plant Easter eggs (developers coding bugs intentionally in order to later benefit from their discovery), might be decreased if the payment of a bounty decreases the developers' bonus pool for the vulnerable product, or if bug bounties paid were deducted from developers' pay. On the other hand, the resourcefulness of devious developers to find ways to personally benefit from any system should not be underestimated.

14. *Other unintended consequences.* Aside from the cobra effect of planting Easter eggs, we should consider other side effects arising from the law of unintended consequences. Money paid for vulnerabilities may remove money from preventing vulnerabilities; and VRPs or reactions to ZDMs may divert resources from design activities in general, e.g., to respond to sensational market or public events that might possibly impact a corporate reputation through negative publicity. Consider as an analogy radar-jamming in WWII: you could jail people who jam radar, or create jam-proof radios (the latter was done, via spread-spectrum techniques).

15. *Openness of markets, and motives.* Rather than argue whether or not markets for vulnerabilities should exist, we should acknowledge that they already do (whether we like it or not), and instead ask: Should such markets be in the open? One opinion is that open markets result in many more attacks—but there is disagreement on this, and also on whether attackers always have greater monetary resources—some large, profitable or well-funded vendors may have greater financial resources and incentives than attackers. Facebook presumably is more interested in paying for vulnerability information than most potential Facebook attackers. A bug seller's motivation might not be entirely financial—e.g., a seller might even wish to sell a vulnerability to a party who *desires* that it be used to harm the software manufacturer. Development of a finer understanding of the intrinsic motivations of those who "work" in grey areas that may effect good or ill is more likely if such activities are in the open.

16. *Modeling.* A better understanding of ZDMs may result from pursuit of a precise, mathematical model of actors: vendors, employees of vendors, researchers (bug finders), criminals, etc.

17. *Regulating prices to avoid ZDMs.* Can prices be regulated, e.g., by VRPs or other mechanisms, in such a way as to avoid the need for ZDMs?

18. *Rewards change behaviors.* Experiments have shown that rewards change actors' approaches to tasks; e.g., kids enjoy tasks more if rewarded for doing the task well. An example noted was that vulnerabilities discovered in response to incentive programs have been more sophisticated than others.

19. *ZDMs as art markets.* Financial markets are not as good an analogy for ZDMs as the art market: there are a lot of private buyers, frequent over-the-counter sales, and a requirement for rigorous quality control.

20. *VRPs signalling software quality.* Might software customers eventually come to choose their vendor based on the quality of its VRP program?

21. *VRPs grooming blackhats.* Do bug bounties turn developers into blackhats? This resembles questions about pen testing and ethics—not all pen testers are motivated by money, and there's a fine line between good pen testers and hackers.

5. CONCLUDING REMARKS

Vulnerability rewards programs (bug bounties) are gaining popularity in the commercial world, along with interest in related zero-day markets (vulnerability markets). These may have important implications on the software industry, and raise interesting ethical issues. Our goal in this note has been to raise awareness of these topics across a broader audience, and to renew academic pursuit of these topics which received early attention a decade ago [1, 11, 15].

Acknowledgements. The authors thank NSPW 2013 participants for their active and passionate discussion of this topic, and their keen insights, and especially Bob Blakley for the invaluable detailed notes of the session's discussion. The first author thanks the Intel Science and Technology Center for Secure Computing. The third author is Canada Research Chair in Authentication and Computer Security, and acknowledges NSERC for funding the chair and a Discovery Grant.

6. REFERENCES

[1] Rainer Böhme. A comparison of market approaches to software vulnerability disclosure. Proc. ETRICS 2006: Emerging Trends in Information and Communication Security, Freiburg, Germany, June 6-9 2006, Springer LNCS 3995, pp.298-311. Earlier version: Proc. of 22C3, Berlin (Dec.27-30 2005), Vulnerability Markets: What is the economic value of a zero-day exploit?

[2] Matthew Finifter, Devdatta Akhawe, David Wagner. An empirical study of vulnerability rewards programs. USENIX Security, 2013.

[3] J. Finkle. Hacking expert wins more than US$100,000 exposing Microsoft security holes. http://www.theglobeandmail.com/

[4] Ryan Gallagher. Cyberwar's gray market: Should the secretive hacker zero-day exploit market be regulated? Jan.16, 2013, Slate magazine. http://www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html

[5] Brian Gorenc. Pwn2Own 2013 (blog). Jan.17, 2013. http://dvlabs.tippingpoint.com/blog/2013/01/17/pwn2own-2013

[6] Andy Greenberg. Meet the hackers who sell spies the tools to crack your PC (and get paid six-figure fees). March 21, 2012 online; also in April 9, 2012 issue of Forbes magazine. http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees

[7] Andy Greenberg. Shopping for zero-days: A price list for hackers' secret software exploits. March 23, 2012 online; also in April 9, 2012 issue of Forbes magazine. http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/

[8] Marcia Hofmann and Trevor Timm. "Zero-day" exploit sales should be key point in cybersecurity debate. Mar.29, 2012. https://www.eff.org/deeplinks/2012/03/zero-day-exploit-sales-should-be-key-point-cybersecurity-debate

[9] Charlie Miller. The legitimate vulnerability market: Inside the secretive world of 0-day exploit sales. WEIS 2007.

[10] Milton Mueller. Regulating the market for zero-day exploits: look to the demand side. March 15, 2013. http://techliberation.com/2013/03/15/regulating-the-market-for-zero-day-exploits-look-to-the-demand-side/

[11] Andy Ozment. Bug auctions: Vulnerability markets reconsidered. WEIS 2004.

[12] Andy Ozment. The likelihood of vulnerability rediscovery and the social utility of vulnerability hunting. WEIS 2005.

[13] Eric Rescorla. Is finding security holes a good idea? *IEEE Security and Privacy* 3(1):14-19 (Jan.2005). WEIS 2004 version available (18 pages, updated 7 Feb. 2005). See also: E. Resorla, "Security Holes ... Who Cares?", USENIX Security 2003.

[14] Jordan Robertson. 'Zero-day' black market—Where hackers buy secrets to exploit tech flaws. Jan.31, 2010. WRAL TechWire. http://wraltechwire.com/business/tech_wire/news/blogpost/6931357/

[15] S. Schechter. *Computer Security Strength and Risk: A Quantitative Approach*. Ph.D. thesis, Harvard, 2004.

[16] B. Schneier. The vulnerabilities market and the future of security. May 30, 2012. http://www.forbes.com/sites/bruceschneier/2012/05/30/the-vulnerabilities-market-and-the-future-of-security/

[17] Z.Xu, Q.Hu, C.Zhang. Why computer talents become computer hackers. *C.ACM* 58(4):64-74 (Apr.2013).