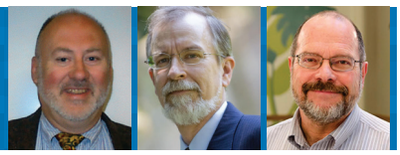
AFTERSHOCK

EDITORS
HAL BERGHEL University of Nevada, Las Vegas; hlb@computer.org
ROBERT N. CHARETTE ITABHI Corp.; rncharette@ieee.org
JOHN L. KING University of Michigan; jlking@umich.edu



Moral Hazards in Cyber Vulnerability Markets

Alex Hoffman and Hal Berghel, University of Nevada

The cyber vulnerability market arose from bug bounty programs initiated in the 1980s. Originally created to provide programmers, end users, and security professionals with an opportunity to report code vulnerabilities, it has since become a cottage industry that serves many masters with very different motives.

Bug-bounty programs may be distinguished by the nature of their management. Internal programs are run by software companies themselves, while third-party programs are managed by intermediaries or brokers that operate either as for-profit businesses or clandestine services. These third-party programs fuel the gray and black markets for software vulnerabilities that benefit software developers or cyber mercenaries, respectively, especially state actors who seek to acquire robust cyber warfare tools. The largest consumer of black-market software vulnerabilities is most likely the U.S. National Security Agency's (NSA's) Vulnerability Equities Process (VEP). The motives behind these two markets are very different; the former is primarily economic, whereas the latter is cyberpolitical.

THE NSA VEP

The most sought-after vulnerability to hackers, cyber mercenaries, and the military–industrial complex is the zero-day, which, by definition, has never been observed "in the wild" and for which there have been no identifying signatures or defensive measures developed. In short, the entire Internet is vulnerable. It has been speculated that the black market for zero-days began in late 2005, when the Windows metafile vulnerability was sold for US$4,000.[20] According to Curtis,[20] that began serious study on the economic potential of the zero-day market, and the rest, as they say, is history. It is not unusual for the most dangerous vulnerabilities to sell for hundreds of thousands (or even millions) of dollars. Cyber mercenaries discovered early on that the big money was in selling to the highest bidder,[29] and the highest bidders intend to use vulnerabilities offensively.

Digital Object Identifier 10.1109/MC.2019.2936635
Date of current version: 22 November 2019

The black market in vulnerabilities presents governments that purport to be democratic with a conundrum, the first of two identifiable moral hazards. They can report the vulnerabilities to developers to contribute to the safety and security of their citizens, or they can cloister the malware in an offensive stockpile for use as cyber weaponry against adversaries.[44] This was one of the key questions that the Obama administration sought to resolve when it commissioned the President's Review Group on Intelligence and Communications Technologies in 2013. The resulting report, "Liberty and Security in a Changing World,"[34] was relatively well balanced, given that it was the product of a bureaucracy led by proponents of government surveillance. As was written at the time, "This report falls in the Shakespearean category of much ado about nothing. Though it doesn't accomplish much, it doesn't seem to do much harm either, and that's a good thing."[5] That said, the report did reveal some interesting facts to the few citizens who were willing to read it. It actually recommends that the government do nothing to "subvert, undermine, weaken, or make vulnerable generally available commercial software," a point to which we now turn.

Although the report does not specifically refer to the VEP, the authors were thinking about it when they suggested that government security agencies not be given carte blanche in the use of zero-day vulnerabilities. The report recommended that "before approving use of the zero-day rather than patching a vulnerability, there should be a senior-level, interagency approval process that employs a risk-management approach." This sentence is the "government-ese," Orwellian double-talk, or political-psychobabble equivalent of saying that the interests of citizens should not be dismissed out of hand when the government stockpiles malware. For bureaucrats, this is an important consideration, for it recommends that at least some concern be given to the public interest in such matters. (Actually, we might more accurately use the expression "what the public considers the public interest," for the public and their elected officials frequently disagree on what the public interest actually is.)

The importance of this point was brought home three years later when the hacking group Shadow Brokers published information on stolen NSA files (including archived zero-days) on the Internet.[39,45] According to Kaspersky Labs, the digital signatures of the hacking tools used by Shadow Brokers were similar to those found in software used by the Equation Group.[51] (Kaspersky Labs also provides an Equation Group FAQ.[52]) Dan Goodin has observed that "the use of zero-day exploits later used in both the Stuxnet worm that disrupted Iran's nuclear program and the Flame malware platform targeting the Middle East demonstrated that Equation Group had clear connections to the NSA or a related U.S. hacking arm."[26]

The Shadow Brokers case illustrates how much of a moral hazard the VEP presents. As Dave Aitel and Matt Tait have observed, the U.S. government "... has confused a public relations strategy with a security strategy, to the detriment of the nation."[2] As with all moral hazards, the problem appears when disincentives motivate conduct that is inconsistent with avowed objectives.[5] Specifically, it is not obvious that the VEP as it is currently instituted will make us safer than if the U.S. government were to remove itself from the zero-day supply chain.[3] The absence of confirmable positive advantage suggests that extensive future public discussion should be encouraged.

BUG BOUNTIES AND MORAL HAZARDS

The original bug bounty program was intended as a remunerative vehicle through which people could ethically report software defects (also known as *bugs*) to companies. Typically, such bugs are related to security vulnerabilities; so a bug bounty program, at least in the ideal case, incentivizes people to do the right thing and report bugs to the developer. Bug bounty programs tend to follow a typical crowdsourcing model, where there is an open call for people to anonymously test software.[33] Participating companies initiate their bug bounty programs by announcing them openly, which allows certain testing for security vulnerabilities without liability. Some companies, such as Oracle, are opposed to having their software examined for security vulnerabilities,[21] so security detectives should be careful not to breach licensing agreements or laws. To ameliorate legal concerns, disclose.io is attempting to "... standardize best practices around safe harbor for good-faith security research."[23]

In fact, disclose.io is working to provide a framework for ethical security research. Its work involves building a set of best practices so that people can collaborate with companies on bug bounty hunting. Such efforts to establish a vendor-neutral vulnerability reporting framework have no downside from the public's perspective; however, it would be naive to think that they would be universally welcomed by vendors as they violate the essential premise of faith-based security: security through obscurity.[4] It is not unusual for technology companies to avoid any investigation into the suitability of their product. The recent Theranos fraud investigation highlights the tenacity with which technology companies may attach themselves to corporate secrecy.[13]

It has been reported that the first known bug bounty program started in 1983.[35] Netscape launched the first modern crowdsourced bug bounty program,[25] offering tiered rewards to people in late 1995. Although Netscape's program was a way to discover all types of defects, there was one key difference between that version and the iterations that exist today: the

program was applicable only during the Netscape Navigator 2.0 beta testing. It took seven years for the next company, IDefence, to pick up where Netscape left off and, in so doing, take the modern approach of testing live-production software. Two years later, TippingPoint joined IDefence as a broker for security vulnerabilities. It would pay people a few hundred dollars for finding bugs, and, in turn, it would sell the information about the vulnerability to the target company.[25] Although Mozilla has the current longest-running bug bounty program, Google accelerated the movement in 2010 by enticing broad participation in crowdsourced vulnerability discovery.[25,32]

STATE OF THE ART

Current bug bounty programs are either internally managed programs (IMPs) or third-party-managed programs (TMPs). IMPs favor larger technology companies like Google, Microsoft, Facebook, and Intel, as they are able to devote adequate monetary and human resources to the task. TMPs, on the other hand, favor smaller or nontechnology-based companies; Starbucks, Netflix, General Motors, Twitter, and Snap are examples of companies that rely on TMPs. Examples of TMPs include Hackerone,[31] Bugcrowd,[10] and Cobalt.[14] Of course, there are exceptions to these rules. Johnson & Johnson is a company that does not specialize in computing but administers its own bug bounty program,[41] while Snap and Netflix are computing companies that use TMPs.[9,30] Even the U.S. federal government is getting in on the bug bounty action, with the U.S. Air Force, U.S. Department of Defense, and other agencies dabbling in the practice. There is discord at the federal level, with the U.S. Department of Homeland Security trying to work holistically across the government and private sector to mitigate cyber risk, while the U.S. Federal Bureau of Investigation considers bounty programs "a little overhyped" for the government[42]; thus, further discourse in this area will be saved for a subsequent work.

By way of comparison, Google's bounty program has paid out more than US$15 million since 2010,[43] with the highest payout associated with its Android platform. Facebook has spent US$7.5 million since 2011.[37] Microsoft was the last of the three to start a bug bounty program,[8,28] but it is already near the top of the annual payout scale, with US$2 million paid out in 2018 alone and plans to expand in 2019.[48] Like Google, it has multiple different programs and varying reward tiers within each of them, but unlike Google, it announced in 2019 that, although it will maintain an IMP, it is outsourcing the payment process to HackerOne.[48] Recognition for bounties will be rewarded on both Microsoft and HackerOne leaderboards.

At this writing, HackerOne.com is the largest of the TMPs by investment dollars. It was founded in 2012 by two Dutch hackers along with a Dutch entrepreneur and Facebook's head of product security.[40] It has raised US$110.4 million in venture funding[18] and employs the largest group of hacker/programmers. Starbucks, Twitter, Uber, Snap, and HBO all use HackerOne's bug bounty platform. Even Google employs HackerOne's help with the GooglePlay store, and as mentioned, Microsoft started using, HackerOne for its payment processing in 2019.

BugCrowd.com was also founded in 2012, but it trails HackerOne in investment dollars at US$48.7 million.[16] BugCrowd has a slightly different model, whereby it internally employs verification engineers to manually check every bug submitted through its platform to ensure a certain standard of defects being submitted.[12] It also boasts an impressive customer list headlined by Tesla, Cisco, Netgear, Atlassian, and Okta.[11]

Cobalt.io is the newest, and by far the smallest, of the three start-up companies by investment dollars. It was started in 2013, and it has raised only US$8 million in funding to date.[17] Notable companies using Cobalt include Sales Force, Credit Karma, and GoDaddy. Other companies, such as Synack,[47] compete in this market, but they do not strictly crowdsource their bug bounty programs. These "closed ecosystem" environments are not discussed here.

INCENTIVES

As with the VEP, both types of bug bounty programs discussed enable misplaced incentives, although IMPs are less assailable in this regard. This holds true for all bounty programs and is not unique to the software industry. The general problem is that open bounties may encourage participation by the wrong people for the wrong reasons, at least from the point of view of the principal's interests. There is a parallel in this regard between bug bounties and traditional bounty hunters (that is, bail/fugitive recovery agents, surety agents, skip tracers, and so on), which why the activity is banned in all but the United States and some of its territories. Although the parallel is not precise, drawing it is informative.

In the ideal case, bounties are offered to encourage people to do the right thing (show up for trial, report software bugs)—that is, what is in the best interest of the patron (society, the government, stockholders, and so on). However, in their zeal to satisfy these interests, bounty supporters frequently ignore potential moral hazards such as encouraging behavior as unlawful as that which justified the bounty. The arrest of the star of the TV series *Dog the Bounty Hunter* on charges of illegal detention and conspiracy for the alleged kidnapping of a fugitive cosmetics heir illustrates that the motives of a bounty hunter may be mixed and are not necessarily consistent with those of the sponsor.[7] The same applies to bug bounty hunters. The bounty may entice hunters to sell any discovered bugs to a higher bidder

than the sponsor, thereby defeating program objectives. The bounty program may be perceived as merely a fallback if no better price for detected bugs can be found.

Another downside is that a bounty program can create a free-for-all for bug detection, including the reporting of inconsequential bugs, which might delay software release or distract the manufacturer from important product development. In addition, software testers involved in bounty programs may not have the ability to discriminate the potential for negative consequences of bugs.[49] Reporting low-potential (LOPO) bugs may become more of a distraction for developers than an asset. For legal reasons, when developers ignore reported bugs of any stripe, they increase their liability. Developers may also be unwilling to pay to eliminate every possible bug in a software prior to release, so the effect of the program may be only to increase the number of people who are aware of noncritical LOPO bugs. Finally, there is the issue of the vetting of participants in bug bounty programs. As with their extrajudicial counterparts, there are no certifications or background tests involved.

COMPENSATION

Compensation is either a monetary reward or an informal in-kind exchange. Many companies publish a price list for bug bounties based on type of bug, severity, and reporting status. Companies will usually pay only for the initial bug report, although there are exceptions. In 2019, Microsoft offered fractional compensation for a report of an internally known bug.[36] In-kind exchange may involve discounts of products and services, air miles, or public recognition (for example, leaderboards).[22] Some programmers consider bug reporting to be part of their professional responsibility. The Association for Computing Machinery's code of ethics, for example, holds that computing professionals have a responsibility to report "any signs of danger from systems."[1]

Bug detection may be remunerative outside of the aforementioned bug bounty programs. Brokers and resellers, such as TippingPoint and IDefence (purchased by Verisign),[25] work in much the same way as news aggregators; they repackage source material (in this case, software bugs) for particular audiences (in this case, developers) for a commission or fee. Exodus Intelligence even provides a zero-day subscription service with a guaranteed minimum of relevant reports to enterprise networks.[24]

A variation on this theme is the gray/black market industry, where all manner of computer threat vectors (bugs, malware, threat signatures, compromises, and so on) are sold for profit to state actors and their constituencies.[19] In our view, distinctions between the *gray* and *black* labels seem ad hoc, arbitrary, and motivated by public relations more than policy considerations. Perhaps a better term would be *taupe market*. In any event, the same motives are involved in both black and gray markets: sell the information to the highest bidder consistent with global political bias and personal agenda, whether it be a sale to a broker for the industry (the gray part of the scale) or the sale to a state sponsor, cyber mercenary, or criminal organization (the black component). We emphasize that in neither case is the motivation the health of the software industry or security of the end user.

These markets are driven by the consumers: the NSA VEP, other government agencies, intelligence/defense "pure plays" (that is, companies whose primary revenue is government contracts), foreign governments, and occasional independent bad actors. This industry contributes to the cyber-mercenary backbone of the much larger military–industrial-complex spine and involves many of the same players. As mentioned, there is a lot of money involved in the gray market. It has been reported that Zerodium offers up to US$2 million for high-risk, zero-day vulnerabilities,[27,50] the ultimate destination for and use of which would not be disclosed. At this writing, no definitive assessment has been published on the economics of the gray/black market. It is not even known how companies account for their bounty budgets.

The study of bug bounty programs offers insights into many different perspectives on security within the technology sector and technology programs within other sectors. Each perspective seems to carry with it unique moral hazards. Industry-supported bug bounty programs send mixed messages and attract participants with varying skill levels and different agendas, not all of which are entirely consonant with industry objectives and the interests of end users. On the other hand, the gray/black market operates independently and at cross purposes with industry initiatives, and it draws on the skills of what one would assume to be a largely independent group of participants. A thorough analysis of the identities of these two groups (bug bounty participants and gray/black market operatives) and their interrelationships would be fascinating, and, in our view, is essential to any risk analysis worthy of the name. We hope that social scientists are drawn to such study. In the meantime, ground-truth data are minimal, and our understanding is necessarily fragmentary. C

REFERENCES

1. Association for Computing Machinery, "ACM Code of Ethics and Professional Conduct," ACM, New York, June 22, 2018. [Online]. Available: https://ethics.acm.org/
2. D. Aitel and M. Tait, "Everything you know about the vulnerability equities process is wrong," Lawfare, Brookings Institution, Washington, D.C., Aug. 18, 2016. [Online].

Available: https://www.lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong
3. S. Anthony, "The first rule of zero-days is no one talks about zero days (so we'll explain)," Ars Technica, Oct. 20, 2015. [Online]. Available: https://arstechnica.com/information-technology/2015/10/the-rise-of-the-zero-day-market/2/
4. H. Berghel, "Faith-based security," *Commun. ACM*, vol. 51, no. 4, pp. 13–17, Apr. 2008. [Online]. Available: https://cacm.acm.org/magazines/2008/4/5432-faith-based-security/abstract
5. H. Berghel, "Moral hazards, negative externalities, and the surveillance economy," *Computer*, vol. 47, no. 2, pp. 73–77, Feb. 2014. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6756872
6. L. Bilge and T. Dumitras, "Before we knew it: An empirical study of zero-day attacks in the real world," in *Proc. 2012 ACM Conf. Computer and Communications Security*, pp. 833–844. doi: 10.1145/2382196.2382284.
7. A. Bonawitz, "Duane 'Dog' Chapman arrested," *CBS News*, Sept. 15, 2006. [Online]. Available: https://www.cbsnews.com/news/duane-dog-chapman-arrested/
8. P. Bright, "Microsoft pays $100K for new exploit technique, patches IE 0-day," Ars Technica, Oct. 9, 2013. [Online]. Available: https://arstechnica.com/information-technology/2013/10/microsoft-pays-100k-for-new-exploit-technique-patches-ie-0-day/
9. Bugcrowd, "Netflix," San Francisco, CA. Accessed on: Oct. 23, 2019. [Online]. Available: https://bugcrowd.com/netflix
10. Bugcrowd, "Bugcrowd cybersecurity platform," San Francisco, CA. Accessed on: Oct. 23, 2019. [Online]. Available: https://www.bugcrowd.com/
11. Bugcrowd, "The most trusted crowdsourced security company," San Francisco, CA. Accessed on: Oct. 23, 2019. [Online]. Available: https://www.bugcrowd.com/customers/
12. Bugcrowd, "Getting started with Bugcrowd | FAQs," San Francisco, CA. Accessed on: Oct. 23, 2019. [Online]. Available: https://docs.bugcrowd.com/docs/getting-started-with-bugcrowd#section-once-your-program-is-live
13. J. Carreyrou, *Bad Blood: Secrets and Lies in a Silicon Valley Startup*. New York: Knopf, 2018.
14. Cobalt, "Cobalt application security platform," San Francisco, CA. Accessed on: Oct. 23, 2019. [Online]. Available: https://cobalt.io/
15. M. Coppock, "Microsoft and Google are paying more than ever to those who find bugs in their systems," Digital Trends, Mar. 6, 2017. [Online]. Available: https://www.digitaltrends.com/computing/google-microsoft-increase-payouts-in-bug-bounty-programs/
16. Crunchbase, "Bugcrowd." Accessed on: Oct. 23, 2019. [Online]. Available: https://www.crunchbase.com/organization/bugcrowd
17. Crunchbase, "Cobalt (Cobalt.io)." Accessed on: Oct. 23, 2019. [Online]. Available: https://www.crunchbase.com/organization/cobalt-io
18. Crunchbase, "HackerOne." Accessed on: Oct. 23, 2019. [Online]. Available: https://www.crunchbase.com/organization/hackerone
19. S. Curtis, "Hackers tap into 'grey market' for legal bug sales," *Telegraph*, June 10, 2015. [Online]. Available: https://www.telegraph.co.uk/technology/internet-security/11664677/Hackers-tap-into-grey-market-for-legitimate-bug-sales.html
20. D. Danchev, "Black market for zero day vulnerabilities still thriving," ZDNet, Nov. 2, 2008. [Online]. Available: https://www.zdnet.com/article/black-market-for-zero-day-vulnerabilities-still-thriving/
21. M. Davidson, "No, you really can't," Oracle Blogs, Nov. 2, 2008. [Online]. Available: https://web.archive.org/web/20150811052336/ https://blogs.oracle.com/maryanndavidson/entry/no_you_really_can_t
22. R. Dennis and G. Owen, "Rep on the block: A next generation reputation system based on the blockchain," in *Proc. 2015 10th Int. Conf. Internet Technology and Secured Transactions (ICITST)*, pp. 131–138. doi: 10.1109/ICITST.2015.7412073.
23. Disclose.io, San Francisco, CA. Accessed on: Oct. 23, 2019. [Online]. Available: https://disclose.io/
24. Exodus Intelligence, "Capabilities: Detect the undetectable – zero-day subscription," Austin, TX. Accessed on: Oct. 23, 2019. [Online]. Available: https://www.exodusintel.com/zeroday.html
25. E. Friis-Jensen, "The history of bug bounty programs," Cobalt Blog, Apr. 11, 2014. [Online]. Available: https://blog.cobalt.io/the-history-of-bug-bounty- programs-50def4dcaab3
26. D. Goodin, "Confirmed: Hacking tool leak came from 'omnipotent' NSA-tied group," Ars Technica, Aug. 16, 2016. [Online]. Available: https://arstechnica.com/information-technology/2016/08/code-dumped-online-came-from-omnipotent-nsa-tied-hacking-group/
27. D. Goodin, "Wanted: Zeroday exploit prices are higher than ever, especially for iOS and messaging apps," *Ars Technica*, Jan. 7, 2019. [Online]. Available: https://arstechnica.com/information-technology/2019/01/zeroday-exploit-prices-continue-to-soar-especially-for-ios-and-messaging-apps/
28. D. Goodin, "Now there's a bug bounty program for the whole internet," *Ars Technica*, Nov. 6, 2013. [Online]. Available: https://arstechnica.com/information-technology/2013/11/now-theres-a-bug-bounty-program-for-the-whole-internet/
29. A. Greenberg, "Meet the hackers who sell spies the tools to crack your PC (and get paid six-figure fees)," *Forbes*, Apr. 9, 2012. [Online]. Available: https://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/#7cec83841f74
30. HackerOne, "Snapchat," San Francisco, CA. Accessed on: Oct. 23, 2019. [Online]. Available: https://hackerone.com/snapchat
31. HackerOne, "Bug bounty - hacker powered security testing," San Francisco, CA. Accessed on: Oct. 23, 2019. [Online]. Available: https://www.hackerone.com/
32. C. Hopping, "Teenage hacker makes $1m from bug-bounty rewards," *IT PRO*, Mar. 4, 2019. [Online]. Available: https://www.itpro.co.uk/bugs/33127/teenage-hacker-makes-1m-from- bug-bounty-rewards
33. T. D. LaToza and A. van der Hoek, "Crowdsourcing in Software Engineering: Models, motivations, and challenges," *IEEE Softw.*, vol. 33, no. 1, pp. 74–80, Jan.–Feb. 2016. doi: 10.1109/MS.2016.12.
34. R. Clarke, M. Morell, G. Stone, C. Sunstein, and P. Swire, "Liberty and security in a changing world: Report and recommendations of The President's Review Group on Intelligence and Communications Technologies," The White House, Dec. 12, 2013. [Online]. Available: https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf
35. P. Marks, "Bounties mount for bugs," *Commun. ACM*, Aug. 23, 2018. [Online]. Available: https://cacm.acm.org/news/230582-bounties-mount-for-bugs/fulltext
36. MSRC, "Microsoft bounty program updates: Faster bounty review, faster payments, and higher rewards," Microsoft Security Response Center, Redmond, WA, Apr. 2, 2019. [Online]. Available: https://blogs.technet.microsoft.com/msrc/2019/04/02/microsoft-bounty- program-updates-faster-bounty-review-faster-payments-and-higher-rewards/
37. L. Newman, "Facebook, under scrutiny, pays out largest bug bounty yet," *Wired*, Dec. 12, 2018. [Online]. Available: https://www.wired.com/story/facebook-bug-bounty-biggest-payout/
38. C. Osborne, "United Airlines showers air miles on bug bounty researchers," ZDNet, July 14, 2015. [Online]. Available: https://www.zdnet.com/article/united-airlines-showers-air-miles-on-bug-bounty-researchers/
39. N. Perlroth and D. Sanger, "Hacks raise fear over N.S.A.'s hold on cyberweapons," *NY Times*, June 28, 2017. [Online]. Available: https://www.nytimes.com/2017/06/28/technology/ransomware-nsa-hacking-tools.html
40. N. Perlroth, "HackerOne connects hackers with companies, and hopes for a win-win," *NY Times*, June 7, 2015. [Online]. Available: https://www.nytimes.com/2015/06/08/technology/hackerone-connects-hackers-with-companies-and-hopes-for-a-win-win.html
41. Johnson & Johnson, "Product vulnerability disclosure reporting," Johnson & Johnson Product Security, New Brunswick, NJ. Accessed on: Oct. 23, 2019. [Online]. Available: https://www.productsecurity.jnj.com/
42. J. Heckman, "FBI senior IT official: Bug bounties still useful, but 'a little over-hyped'," *Federal News Network*, July 18, 2019. [Online]. Available: https://federalnewsnetwork.com/cybersecurity/2019/07/fbi-senior-it-official-bug-bounties-still-useful-but-a-little-over-hyped/
43. E. Protalinski, "Google has paid security researchers over $15 million for bug bounties, $3.4 million in 2018 alone," VentureBeat, Feb. 8, 2019. [Online]. Available: https://venturebeat.com/2019/02/08/google-has-paid-security-researchers-over-15-million-for-bug-bounties-3-4-million-in-2018-alone/
44. B. Schneier, "Should U.S. hackers fix cybersecurity holes or exploit them?" *The Atlantic*, May 19, 2014. [Online]. Available: https://www.theatlantic.com/technology/archive/2014/05/should-hackers-fix-cyber security-holes-or-exploit-them/371197/
45. B. Schneier, "Who are the shadow brokers?" *The Atlantic*, May 23, 2017. [Online]. Available: https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/
46. Silent Circle, "The importance of bug bounty programs," Jan. 25, 2018. [Online]. Available: https://www.silentcircle.com/blog/importance-of-bug-bounty-programs/
47. Synack, Redwood City, CA. Accessed on: Oct. 23, 2019. [Online]. Available: https://www.synack.com/
48. L. Tung, "Microsoft: Our bug bounty payouts hit $2m in 2018 and we're offering more in 2019," ZDNet, Apr. 4, 2019. [Online]. Available: https://www.zdnet.com/article/microsoft-our-bug-bounty-payouts-hit-2m-in-2018-and-were-offering-more-in-2019/
49. D. Votipka, R. Stevens, E. Redmiles, J. Hu, and M. Mazurek. "Hackers vs. testers: A comparison of software vulnerability discovery processes," in *Proc. 2018 IEEE Symp. Security and Privacy (SP)*, pp. 374–391. doi: 10.1109/SP.2018.00003.
50. Zerodium, Washington, D.C. Accessed on: Oct. 23, 2019. "Our exploit acquisition program." [Online]. Available: https://zerodium.com/program.html
51. GReAT, "The equation giveaway," Moscow, Russia, Aug. 16, 2016. [Online]. Available: https://securelist.com/the-equation-giveaway/75812/
52. Kaspersky Lab, "Equation Group: Questions and answers," Moscow, Russia, Feb. 2015. [Online]. Available: https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf

ALEX HOFFMAN is a Ph.D. student in computer science at the University of Nevada, Las Vegas. Contact him at alex.hoffman@unlv.edu.

HAL BERGHEL is a Fellow of the IEEE and ACM and a professor of computer science at the University of Nevada, Las Vegas. Contact him at hlb@computer.org.