Vulnerabilities and Their Surrounding Ethical Questions:
A Code of Ethics for the Private Sector

Alfonso De Gregorio
Security Labs
Zeronomicon
Milan, Italy
adg@zeronomi.com

Abstract: Zero-day vulnerabilities — weaknesses in software that are unknown to the parties who can mitigate their specific negative effects — are gaining a prominent role in the modern-day intelligence, national security, and law enforcement operations.

At the same time, the lack of transparency and accountability in their trade and adoption, their possible overexploitation or abuse, the latent conflict of interests by entities handling them, and their potential double effect may pose societal risks or lead to the breach of human rights.

If left unaddressed, these usage-related challenges call into question the legitimacy of zero-day vulnerabilities as enablers of national security and law enforcement operations and erode the benefits that their proportionate use have for the judiciary, defence, and intelligence purposes.

This work explores what the private sector involved in the trade of zero-day vulnerabilities can do to ensure the respect human rights and the benign and societally beneficial use of those capabilities. After reviewing what can go wrong in the acquisition of zero-day vulnerabilities, the article contributes the first code of ethics focused on the trade of vulnerability information, where the author sets forth six principles and eight corresponding ethical standards aimed respectively at guiding and regulating the conduct of this business.

Keywords: Software, Vulnerabilities, Ethics, Governance, National-Security, Intelligence, Law-Enforcement

1. INTRODUCTION

Who holds the moral low ground: the ruthless malefactors profiting from yet another remote code execution vulnerability, or the vendors practicing unrestrained vulnerability dumping onto the downstream market participants? [1] Who are the ones that exploit us the most: the foreign security services taking total control of our mobile handsets, or the vendors using patching to optimize market and legal protections by re-negotiating contract terms users could not negotiate in the first place and from which the users have no satisfactory way to escape? [2] If our governments introduce trade controls to administer the export of intrusion software, should we demand software manufacturers to internalise the cost of the insecure software that we import into our lives, for reasons of symmetry? Should we make them liable for the defects and flaws that allow the intrusion in the first place? [3,4]

With incomplete knowledge about the real-world security of systems we entrust our business, is it even ethical to refrain us from hunting vulnerabilities or prevent others from doing likewise? [5] And, what should do a security researcher with the vulnerabilities when they get found? [6] Is full disclosure an acceptable course of action? Does full disclosure become more acceptable if the affected vendor ignores the vulnerabilities that were reported responsibly or fails to provide a timely patch? [7] Does coordinated vulnerability disclosure provide a more ethically sound path to be taken? [8] Does the same path remains morally preferable if one of the parties, who receives the vulnerability information from the Coordinator prior to its public disclosure, decides to use it to exploit vulnerable entities? [9]

Are bug bounty programs exploiting bounty hunters? Should bug hunters pretend to get paid if the other party has not asked them to do their work?

What government security agencies should do with vulnerabilities:[10] should they exploit them [11, 12] or should they let everybody else mitigate them, in the way they already do? [13] Should they take advantage of those vulnerabilities to benefit a limited number of stakeholders,[14] or should they disclose them to all affected constituents? [15]

Has the power inequity in the vulnerability equation to be balanced? With entities affected by vulnerabilities spread all around the world, how to inform the public? With vendors threatening legal action and supported by their significant financial resources, how to protect the security researchers? [16]

With our society growing more data intensive, how to oversee not only material and technology but also knowledge? “How do the attempts to strike a balance between scientific openness and national security […] redefine science-security relations? How does scientific knowledge become subject to security governance? And how does this dynamic affect the links among scientific knowledge, security expertise and political decision?” [17]

Can we regard hacking to be an ethical practice and condemn, at the same time, the trade of capabilities enabling this practice as immoral?

Wherever we turn our attention in the vulnerabilities supply-chain, from software vendors — creating vulnerabilities during the products development lifecycle —, to vulnerability researchers — finding existing vulnerabilities and creating exploits to take-advantage of them —, to vulnerability brokers — trading vulnerability intelligence and exploits —, to government agencies and other entities — using or misusing the resulting capabilities —, all industry actors face their respective ethical issues related to the knowledge of zero-day vulnerabilities — weaknesses in software that are unknown to the parties who can mitigate their specific negative effects.

These capabilities are gaining a prominent role in the modern-day intelligence, national security, and law enforcement operations. [18] At the same time, the lack of transparency and accountability in their trade and adoption, their possible overexploitation or abuse, the latent conflict of interests by entities handling them, and their potential double effect [19] may pose societal risks or lead to the breach of human rights. [20]

If left unaddressed, these usage-related challenges call into question the legitimacy of zero-day vulnerabilities as enablers of national security and law enforcement operations and erode the benefits that their proportionate use have for the judiciary, defence, and intelligence purposes. [21]

This work explores what the private sector involved in the trade of zero-day vulnerabilities can do to ensure the respect human rights and the benign and societally beneficial use of those capabilities. After reviewing what can go wrong in the acquisition of zero-day vulnerabilities, the article contributes the first code of ethics focused on the trade of vulnerability information, where the author sets forth six principles and eight corresponding ethical standards aimed respectively at guiding and regulating the conduct of this business.

2. Zero-days and Their Non-Zero Societal Risks

Zero-days vulnerabilities are not *ipso facto* beneficial or harmful. They can be used for beneficial purposes and misused for harmful aims, and, as such, are a dual-use knowledge enabling dual-use technology. Yet, in the context of Computer Network Operations (CNOs), what makes the use of any given capability beneficial or harmful is very much a matter of perspective. Depending from which side of the playing field we look at things, the use of the same capability might be considered differently if it goes towards the creation or the detriment of political, military, diplomatic, economic, or business advantages.

Notwithstanding the weak or uneven regulatory global landscape, the public international law and the international treaties form a backbone of principles that

should be followed by the private sector in the acquisition of zero-day vulnerabilities.

To begin with, traders of vulnerability information and security capabilities shall mitigate the risk to enable with their tools or knowledge the cyber security strategies of entities willing to abuse human rights. Also, they should contribute to the realisation to the right to health, by controlling which capabilities they provide to whom, if those capabilities may pose a direct danger to the health of human beings. [22] Finally, in consideration of the time-sensitiveness and value of the traded commodities, the suppliers of zero-day vulnerabilities will need to honour the highest integrity standards, avoiding latent conflicts of interest that may erode the asymmetric advantage of the customers against targets that heavily dependent on IT, and preserving the confidentiality of the entities they do business with and the confidentiality of the acquired capabilities.

The following section intends to address these usage-related challenges and to contribute towards the establishment of a culture of responsibility.

3.CODE OF ETHICS

As an ethically concerned founder of an acquisition platform for security capabilities, the present author established a code of business ethics and he holds to its principles and standards in the conduct of his business.

The present section sets forth six principles and eight corresponding ethical standards. The principles are aspirational goals aimed at guiding and inspiring the conduct of business, and they underpin the ethical standards. The ethical standards are enforceable rules for the day-to-day business operations.

Principle A: Respect Human Rights — Clean Hands

Respect all human rights proclaimed by international human rights treaties, including The International Bill of Human Rights, and strive to ensure no complicity in any human rights abuses.

Standard 1: Vetting and Monitoring of Customers

Do not engage in any business with entities known for abusing human rights and reserves the right to suspend or cease business operations with entities found to be involved at a later time in human rights abuses.

Principle B: Do Not Pose a Danger to Human Health

Champion the health of human beings and commit to do not enable your Customer entities with capabilities that may pose a direct danger to human health.

Standard 2: Inadmissible Capabilities

Do not engage in any trade of capabilities that exploit vulnerabilities in medical devices or in systems to which human life is entrusted, unless the Vendor of the affected device or system is the Acquiring Entity or the Acquiring Entity was authorised by the Vendor to be the recipient of the vulnerability disclosure process, vulnerability information, or risk mitigation strategy.

Standard 3: Trade Secrets

You will never trade in stolen trade secrets, and require your suppliers to certify that they have independently found the vulnerability and autonomously developed any related technology, and that they are not employees of the targeted software manufacturer, nor have they received access to the confidential information through a disclosure by the same.

Principle C: Avoid Conflicts of Interest

Strive to benefit those with whom you do business and take care to avoid possible conflicts of interest that could cause your Company, its Employees, or Contractors to pursue goals not in the interest of the Company business peers.

Standard 4: Conflict of interests and overexploitation

You will protect the value of the traded capabilities. You will specify the maximum number of entities to which the same capabilities may be sold, within a given time-frame (unless in case the capabilities are intended for risk prevention).
Furthermore, you shall strive not to sell a vulnerability to one party, and the technology to defend against that vulnerability to another party which is a likely target of the first.

Standard 5: Unintended Use

Prohibit yourself, your employees and contractors to use the information or the capabilities, traded in the fulfilment of the service, for the pursuit of personal goals. Authorised personnel shall use such capabilities only to test and validate them, and more generally only for research and development purposes.

Principle D: Obey the Law

Comply with all applicable legal requirements and understands the major laws and regulations that apply to your business, including laws related to: trade controls, anti-bribery, competition, trade secret, money laundering and insider trading.

Standard 6: Exporting

Comply with trade laws controlling where the you can send products and services, strive to meet the criteria required to hold export licenses, where applicable, and stay alert to changes to the applicable export licensing systems.

Principle E: Preserve Confidentiality

Protect the confidentiality of the identity of entities you do business with and the the confidentiality of the information and intellectual properties received from, or provided to, your business peers in the fulfilment of your Service. At the same time, recognize that the extent and limits of confidentiality may be regulated by applicable laws and regulations.

Standard 7: Maintaining Confidentiality

At the extent and limits regulated by applicable laws and regulations, preserve the confidentiality of the identity of entities you do business with. Restrict access to the information and the intellectual property received from or provided to your business partners on a need-to-know basis, enforcing a principle of least privilege.

Principle F: Doctrine of Double Effect and Dual Use

Acknowledge that the capabilities you provide may be used within goods that, just like any and all information security tools, are inherently dual purpose and potentially dual use, and therefore may serve also military purposes, police investigations and the like; the military use of the traded capabilities may have a double effect: the intended effect and the foreseen but genuinely unintended consequence. While discouraging against harmful side effects, you acknowledge the inherent duality of the effects resulting from the use of those capabilities and you trade them, unless they are in conflict with other principles set forth in the present Ethics Code.

Standard 8: Duality

Acknowledge that the capabilities you provide can be used within goods that are inherently dual purpose and accept to supply them, as long as it is foreseeable that those capabilities will be used only for legitimate purposes in line with international standards for the respect of human rights, and unless their trade is in conflict with principles set out in the present Ethics Code.

4. Conclusions

Ayn Rand once remarked: “Every aspect of Western culture needs a new code of ethics — a rational ethics — as a precondition of rebirth.” [23]

The author feels similarly with regard to the debate surrounding vulnerabilities: Every aspect of the vulnerabilities supply chain needs a new code of ethics — a rational ethics — as a precondition of rebirth.

In this spirit, the present author established the first code of ethics focused on the trade of vulnerability information and offered its principles and standards up for comments and criticism. If, as noted by Earl Warren, “[i]n a civilised life, law floats in a sea of ethics” [24], it is both the author’s hope and wish that the present and future reflections will inform policy makers.

References

[1] De Gregorio, A.; “Andy, the Polluters, Rick Deckard, and Other Bounty Hunters”, PHDays VI, 2016, Moscow, https://youtu.be/R3tuEdX3fdg

[2] Rice, D. “Geekonomics — The Real Cost of Insecure Software”, 2007, Addison Wesley, ASIN: B01A659S42

[3] Terrence, A; Tunca, T. I.; “Who Should Be Responsible for Software Security? A Comparative Analysis of Liability Policies in Network Environments”, WEIS 2011, http://dx.doi.org/10.1287/mnsc.1100.1304

[4] Mudge; Zatko, S.; “Measuring Adversary Costs to Exploit Commercial Software: The Government-Bootstrapped Non-Profit C.I.T.L.”, https://www.blackhat.com/us-16/briefings/schedule/#measuring-adversary-costs-to-exploit-commercial-software-the-government-bootstrapped-non-profit-citl-4514

[5] Zetter, K; “A Bizarre Twist in the Debate Over Vulnerability Disclosures”, September 11, 2015, Wired, https://www.wired.com/2015/09/fireeye-enrw-injunction-bizarre-twist-in-the-debate-over-vulnerability-disclosures/

[6] Rey, E.; “Reflections on Vulnerability Disclosure”, Insinuator, July 14, 2015, https://www.insinuator.net/2015/07/reflections-on-vulnerability-disclosure/

[7] Northcutt, S.; Madden, C.; “IT Ethics Handbook: Right and Wrong for IT Professionals”, July 29, 2004, Syngress, ISBN-10: 1931836140

[8] Microsoft, “Coordinated Vulnerability Disclosure”, https://technet.microsoft.com/en-us/security/dn467923

[9] Cox, J.; "Confirmed: Carnegie Mellon University Attacked Tor, Was Subpoenaed By Feds", February 24, 2016, https://motherboard.vice.com/read/carnegie-mellon-university-attacked-tor-was-subpoenaed-by-feds

[10] Schwartz, A.; Knake, R.; "Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process", http://belfercenter.ksg.harvard.edu/publication/26725/governments_role_in_vulnerability_disclosure.html

[11] Friedman, A.; Moore, T.; and Procaccia A. D.; "Cyber-Sword v. Cyber-Shield: The Dynamics of US Cybersecurity Policy Priorities", Center for Research on Computation & Society, Harvard University, http://web.mit.edu/ecir/pdf/Friedman%20cyberwar-governance.pdf

[12] Aitel, D.; Tait, M.; "Everything You Know About the Vulnerability Equities Process Is Wrong", Lawfare, August 18, 2016, https://lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong

[13] Daniel, M.; "Heartbleed: Understanding When We Disclose Cyber Vulnerabilities", White House Blog, April 28, 2014, https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities

[14] "Commercial and Government Information Technology and Industrial Control Product or System Vulnerability Equity Policy and Process", https://www.eff.org/files/2015/09/04/document_71_-_vep_ocr.pdf

[15] Schneier, B.; "Disclosing vs. Hoarding Vulnerabilities", Schneier on Security, May 22, 2014, https://www.schneier.com/blog/archives/2014/05/disclosing_vs_h.html

[16] Thomas, C.; "The Vulnerability Disclosure Debate", http://www.tenable.com/blog/the-vulnerability-disclosure-debate

[17] Rychnovská, D.; "Governing dual-use knowledge: From the politics of responsible science to the ethicalization of security", Security Dialogue, 2016, Vol. 47(4) 310-328

[18] De Gregorio, A.; "The Bazaar, the Maharaja's Ultimatum, and the Shadow of the Future: Extortion and Cooperation in the Zero-Day Market", October 12-16, 2015, HITB GSEC, Singapore

[19] Lin, H; "Governance of Information Technology and Cyber Weapons'', in Harris, E. D.; "Governance of Dual-Use Technologies: Theory and Practice", American Academy of Arts and Sciences, https://www.amacad.org/content/publications/publication.aspx?i=22228

[20] Collins, K.; "Hacking Team's Oppressive Regimes Customer List Revealed in Hack", July 6, 2015, Wired, http://www.wired.co.uk/article/hacking-team-spyware-company-hacked

[21] Bellovin, S.M.; Blaze, M.; Clark, S; and Landau, S; "Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet", 12 Nw. J. Tech. & Intell. Prop. 1 (2014). http://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1

[22] Moe, M.; Leverett, E.; "Unpatchable: Living with a vulnerable implanted device", 32C3, https://events.ccc.de/congress/2015/Fahrplan/system/event_attachments/attachments/000/002/832/original/2015-12-28-CCC.pdf

[23] Rand, A.; Hull, G. (Editor); Peikoff, L. (Illustrator); "The Ayn Rand Reader", January 1, 1999, NAL, ISBN-10: 0452280400

[24] Warren, E.; New York Times, November 12, 1962