Zero-day Workshop 2017, 27 January, Brussels — Nominal delivery draft

Vulnerabilities and Their Surrounding Ethical Questions: What the Private Sector Can Do

Alfonso De Gregorio

Opening

Good morning and thank you for the invitation.

Zero-day vulnerabilities — weaknesses in software or hardware that are unknown to the parties who can mitigate their specific negative effects — are gaining a prominent role in modern-day intelligence, national-security, and low-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, defense, and intelligence purposes.

With your help, what I want to do today is to briefly review the vulnerability supply chain, its main actors, and their surrounding ethical questions. After setting the context, I will share with you how I decided to approach these questions in my occupation and report on the ethical principles and standards I set forth in Code of Business Ethics that I adopted in my day-to-day business operations.

In doing so, it is not my intention neither to lecture anybody about how you are expected to behave, nor to provide definitive answers to pressing challenges. I will be happy if will have asked more questions than given answers, or if I will have contributed some meaningful ethical principles and standards to build upon.

So, let’s get started.

The Vulnerability SupplyChain

As already noted, zero-day vulnerabilities are enablers of today cybersecurity strategies.

A supply-chain emerged to serve the particular demanders of this valuable information.

To begin with, due to economic, regulatory, and legal incentives that are misaligned distorted or ineffectual, software makers create an unknown number of vulnerabilities during the products’ development lifecycle.

In our society growing more interconnected and interdependent, vulnerabilities are like pollutants, whose private cost is near zero to polluters but whose public cost is almost unbearable for the society.

That is to say that the private cost of poorly written insecure software is near zero to software makers that, as a result, are practicing an unrestrained vulnerability dumping onto the downstream market participants.

In the absence of a policy discouraging the unrestrained vulnerability dumping onto the downstream market participants, defenders are too busy mopping the floor to turn off the faucet.

Precisely because software products have among the highest level of defects of any product sold today, defenders need to patch them.

Yet, patching plays as a perverse incentive, allowing software manufacturers to optimize market and legal protections by re-negotiating contract terms buyers could not negotiate in the first place.

This is how, every time a vulnerability comes out, we find ourselves signing a new licensing agreement. But this gives the manufacturers the ability to re-negotiate contract terms we could not negotiate in the first place and from which we have no satisfactory way to escape.

Vulnerability hunters discover in the aftermarket defects and flaws that software manufacturers failed to detect themselves.

High-performance organisations, both in the government and in the industry sector, demand the findings of these researches, to enable their security strategies.

And various types of marketplaces compete with each other in order to win the preference of vulnerabilities hunters towards their specific idea of which security strategies should be enabled by the disclosure of any given vulnerability.

The reality is that vulnerabilities are the unknown currency of the security aftermarket.

Ethical Questions

My contention is that wherever we turn our attention in the vulnerabilities supply chain, from software vendors, to vulnerability hunters, to government agencies, all industry actors face their respective ethical issues related to the vulnerabilities affecting networked devices and the knowledge of their existence.

Therefore, I want to ask you:

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? 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? 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?

With incomplete knowledge about the real-world security of systems we entrust our business, is it ethical to refrain us from hunting vulnerabilities or prevent others from doing likewise? And, what should do a security researcher with the vulnerabilities when they get found? Is full disclosure an acceptable course of action? Does full disclosure becomes more acceptable if the affected vendor ignores the vulnerabilities that were reported responsibly or fails to provide a timely patch? Does coordinated vulnerability disclosure provide a more ethically sound path to be taken? 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?

Are bug bounty programs exploiting bounty hunters? What are fair terms? Should bug hunters pretend to get paid if the other party has not invited them to do their work?

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

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?

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?”

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

Today, I want to explore with you 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.

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-purpose 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. 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.

With the code of ethics it is my intention to address these usage-related challenges and to contribute towards the establishment of a greater culture of responsibility.

Code of Business Ethics

I set 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.

Let’s give a look to them.

The first and foremost governing principle that today I want to offer to you today is the clean hands principle, which asks the private sector, and me, to…

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.

No, it is not my aspiration to run a company involved in any human rights abuse. Therefore I vet and monitor my Customers.

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 discovered 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.

All of which is to say that, no, I don't want software maker employees to join the bug bonanza and to write them a new minivan this afternoon

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, 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 use 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.

And that is pretty much it as far as my code of ethics goes.

Concluding Remarks

Today I am honoured to be with you in Brussels and I am reminded about the Russian-born Али́са Зино́вьевна Розенба́ум, who once remarked:

> "Every aspect of Western culture needs a new code of ethics — a rational ethics — as a precondition of rebirth." — Ayn Rand

I feel 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, I established the first code of ethics focused on the trade of vulnerability information and, today, I offered its principles and standards up for your comments and criticism.

If, as noted by Earl Warren, "[i]n a civilised life, law floats in a sea of ethics", it is both my hope and wish that our reflections will inform policy markers.

As recently remarked by Steven Aftergood on Nature, "Expanding the scope of ethical deliberation over new technology may seem like a daunting prospect bound to impede innovation." Today, there is no doubt, that I raised questions more quickly than they can be answered. "But experience suggests that many such questions will be worth asking."

I welcome all your thoughts. Thank you.

References

[1] http://www.br-insight.com/an-analysis-of-blade-runner
[2] http://www.br-insight.com/a-study-of-blade-runner
[3] Shoshana Zuboff, In The Age Of The Smart Machine, http://www.shoshanazuboff.com/new/books/in-the-age-of-the-smart-machine/
[4] David Rice, Geekonomics
[5] http://guykawasaki.com/the_art_of_boot/
[6] http://guykawasaki.com/the_art_of_inno/
[7] David Rice, Geekonomics: The Real Cost of Insecure Software, A Keynote for Everyone