Disclosing software vulnerabilities

Maria Canellopoulou-Bottis, Lecturer, DALS, Ionian University, Greece

Information can cause harm. A person may defame or defraud another. A person may use information offered to her by another on how to kill a person and kill, in fact, a person[1]. A person may kill herself upon learning that she has a terrible cancer[2]. A kid may be exposed to illegal pornographic material[3]. A textbook may contain dangerously inaccurate technical instructions or allegations[4]. A label on a T-shirt should have included the word 'flammable' but did not. A computer virus may cause millions of dollars damage. This is a very short list of examples: information, which has so many facets, transmission channels and meanings, has an equally diverse potential of causing very different kinds of damage.

Information may be speech, artistic expression, tool, product, good, code, image, signal, power, capital, service and so on. When information is seen as speech, freedom of speech in principle safeguards the free dissemination of information[5]. Information as an intangible is characterized as a non-rival good[6], since no one possesses less information, because another possesses the same information.

[1] *Rice v. Paladin,* 128 F. 3d 233 (4th Cir. 1997). For an extensive analysis of harms and liability because of the transfer of information in films or books see *Kunich J.,* Natural Born Copycat Killers and the Law of Shock Torts, 78 Wash.L.Q. 1157 (2000).

[2] This is the reason offered in support of the so-called physician's therapeutic privilege (not to disclose the truth about a patient's condition to her etc). See relevant analysis and criticism in *Katz J*., The Silent World of Doctor and Patient, New York: The Free Press, 1983.

[3] See discussion in *Reno, Attorney-General of the US v. American Civil Liberties Union,* 521 US 844 (1997), *ALA v. US*, 529 US 803 (2000). On the question of harm by pornography see (among many others) *McKinnon K.,* Only Words, Cambridge, Massachusetts, Harvard University Press, 1993 and *Becker M., Bowman C. & Torrey M., Cases and Materials on* Feminist Jurisprudence: Taking Women Seriously, American Casebook Series, West Publishing Company, March 1994, pp. 313-352*, Paul P*., Pornified: How Pornography Is Transforming Our Lives, Our Relationships, and Our Families Times Books, 2005.

[4] An aeronautical chart may have missed a geographical feature, *Brocklesby v. US*, 767 F. 2d 1288 (9th Cir. 1985), *cert. denied*, 474 US 1101 (1986); a mushroom may be inaccurately described as harmless (*Winter v. G.P. Putnam's sons*, 1033 F. 2d 928, 1033, 9th Cir. 1991, case of the mushroom *amanita phalloeides*'s picture which was negligently put next to another harmless mushroom's description, readers picked up the dangerous mushrooms, ate them and had liver transplants).

[5] See among others *Myers B.L.,* Read at Your Own Risk: Publisher Liability for Defective How-to Books, 45 Ark.L.Rev. 699 (1992).

[6] *Samuleson P. & Reichman J*., Intellectual Property Rights to Data? 50 Vand. L. Rev. 51 (1997), p. 59: '…commercial compilers of data have long suffered from a risk of market failure owing to the intangible, ubiquitous and, above all, indivisible nature of information goods….Information goods have the properties of so-called public goods: they are ubiquitous, inexhaustible, indivisible and nondepletable. A second comer's use of a new information good does not diminish or exhaust it. Once disclosed to the world, anyone can use an information good without the originator's permission....'.

Therefore, information as a good is quite different from, say, television sets-if I give you my television set, I will not have it any more, which is not true when I give you information. Information is therefore by nature[7] very different from a product[8] (for example, a car[9]); no product liability for information (as a product, which has caused damage) has been sustained as yet[10], because product liability presupposes a product. Information's intangibility, the lack's of a publisher's control over its content and the possible chilling effect strict product liability would have over free speech, has sustained until today the courts' position that information is not a product, with the (criticized) exception of information published in maps, navigational and aeronautical charts [11]. Apart from tortious product liability, in the special case of software, contractual clauses such as disclaimers of liability for damage have an excellent chance of being upheld by the courts[12].

---

[7] See the oft-quoted eloquent statement by Thomas Jefferson in a letter to Isaac McPherson, 1813: '….that ideas should freely spread from one to another over the globe, for the moral and mutual instruction of man, and improvement of this condition, seems to have been peculiarly and benevolently designed by nature, when she made them, like fire, expansible all over space..', copy of the entire letter at www.temple.edu/lawschool/dpst/mcphersonletter.html, last visit May 10, 2005.)

[8] A product, in the sense of what item may trigger strict product liability, as a rule must have a physical existence, but intangibles such as gas, naturals (pets) and writings (only navigational charts, though) are included in the relevant definition, see Legal Information Institute's site at www.law.cornell.edu/topics/products_liability.html, last visit May 10, 2005.

[9] On this particular comparison, see *Bruey*, '…a car can be seen as a car by anybody, and therefore respect for another's property can be claimed from anybody. Transferred to information, this would mean that the title to information has to be respected by persons not knowing it. This cannot be just by referring to the recipient…a car remains the same car when moved to another garage. Information, on the other hand, very much depends on the persons and the context…', Information Cannot be Owned, available at http://www.cyber.law.harvard.edu/home/uploads/339/Druey.pdf, research publications No 2004-2005, 4/2004, last visit June 28, 2006.

[10] *Aetna Casualty v. Jeppesen*, 642 F. 2d 339 (9th. Cir. 1981), *Saloomey v. Jeppesen*, 707 F. 2d 671 (2nd Cir. 1983), *Brocklesby v. US*, 767 F. 2d 1288 (9th Cir. 1985), *cert. denied*, 474 US 1101 (1986) (airplane crashed with six victims, the pilot had used a defective but approved by the Federal Aviation Authority flight procedure, represented graphically on a chart), *Fluor Corp. v. Jeppesen & Co*, 216 Cal. App. 1985). In these cases, charts for airplanes (with geographical features etc to guide the flights) were considered as products and product liability for erroneous charts leading to severe damage was upheld. See also *Schultz R.,* Application of Strict Product Liability to Aeronautical Chartpublishers, Journal of Air Law and Commerce 64 (1999), pp. 431-458. While there are also comments against this kind of liability, see *Phillips J*., Information Liability: The Possible Chilling Effect of Tort Claims Against Producers of Geographic Information System Data, 26 Fla. St. UL Rev 743 (1999), others have urge exactly the opposite: the expansion of liability to other situations, *see e.g. Leadstrom, N. D*., Internet Web Sites as Products Under Strict Products Liability: A Call for an Expanded Definition of a Product, Washburn Law Journal, 40, (201), pp. 532-560.

[11] See critical analysis in *Leadstrom*, id, note 10.

[12] See *ProCD v. Zeidenberg*, US Court of Appeals, 7th Cir. 96 F. 3d 1447 (1996), upholding a 'shrink-wrap' clause dealing with permissions to use the software, sold off-the-shelf. The UCC also permits a seller to disclaim warranties otherwise provided for under the Code; if the software seller does disclaim liability and states that the software is sold 'as it is', this defeats the potential plaintiff's ability to sue for software failure. '..In boilerplate license agreements, buyers accept that they are buying the product as is..', *Haley C.,* Users Urge Disclosure of Security Flaws, June 28, 2002, available at http://boston.internet.com/news/print.php/1378631, last visit October 5, 2005.

But even if information has a nature 'pushing' it to freedom and even if the general idea is that this freedom is essential to a democracy, it is also generally accepted, again in principle that information can cause harm and therefore, its transfer may be subject to certain legal limitations.

Information published in the Internet has a distinct ability to cause enormous harm. This is so, because the recipients may form a very big and perhaps unknown number; also, information may be multiplied and transferred automatically to them. A classic example is the transmission of a computer virus. By its very nature, the virus multiplies by itself[13] and causes damage to the property of the recipients. Code Red I and II are examples of how information published in the Web may cause harm. Code Red I was a computer virus which had infected over 12.000 computers by July 18, 2001 and a different version of Code Red I infected an estimated over 359.000 computers within 14 hours of its release. Code Red II, a new and entirely different version, was more dangerous as it allowed the external unauthorized control of a computer. But other viruses have caused more damage than Code Red; ILOVEYOU virus is alleged to have caused losses up to $10 billion to deferral agencies and to major networks like Dow Jones[14]. It follows that, if censorship of information must adhere to some particular rules when information is transmitted, for example, through a book sold in the market, perhaps censorship of information transmitted through the net should adhere to different (more stringent) rules.

The case of disclosing information on security 'holes' presents special characteristics, quite different from the disclosure of other 'dangerous' information. I do not refer here to the obvious case of a hacker who 'frees' a 'malignant' virus in the Net; this is a crime, dealt with in criminal statutes all over the world. I refer to the rather controversial[15] case where a person acting in good faith[16] discovers certain

[13] For example, if in the first hour the victims of the virus are four and the virus requires one hour to be received by the next wave of victims, after ten hours these victims become 1.048.576, *see Stadler*, Examples of Malicious Computer Programs, 2002, available at www.rbs2.com/cvirus.htm, last visit July 3, 2006. *Stadler,* id, also notes that in this example, after 24 hours, there would be 10^{14} new victims, while there are only 10^9 people on earth.

[14] Computer Virus Hit 14 Agencies, Chi. Trib. C1 (May 10, 2000). See extensive analysis of the Code Red damage in *Preston E. & Lofton J.,* Computer Security Publications: Information Economics, Shifting Liability and the First Amendment, 24 Whittier Law Review 71, pp. 72-74 (2002).

[15] I refer to this case as controversial, as it has propelled a big debate among the security community, see, among many others, *Arbaugh W., Fitchen L & McHugh J.,* Windows of Vulnerability: A Case Study Analysis, Computer, December 2000, available at www.cs.umd.edu/~waa/pubs/Windows_of_Vulnerability.pdf, last visit June 28, 2006, pp. 52-58, p. 57, hereinafter sited as *Windows of Vulnerability,* (referring to this matter as 'the great debate').

vulnerabilities in a system and discloses these vulnerabilities, so that other people may learn about it and hopefully, engage in research, with the objective to 'patch' ('cure') these vulnerabilities. A vulnerability may be a lacking security requirement (e.g. lack of, or improper authentication, encryption etc) or a development error in the software (e.g. buffer overflow, race condition etc) [17]. The motive is benign; but when the vulnerability is disclosed, hackers may use it in order to take advantage of this vulnerability and cause very important damage.

The publication therefore in fact increases the likelihood of malicious forceful intrusions. This likelihood logically increases, depending on what kind of information is made public: only that a certain vulnerability exists or, the 'worse' scenario, the code able to take full advantage of the vulnerability. In the Code Red events mentioned above, a company named *eBay* announced on its Web page and to BugTraq (a highly esteemed e-mail journal on computer security) that it had discovered a vulnerability in Microsoft's Internet Information Server. Three days later, an independent entity, self-called 'HighSpeed Junkie' released the actual buffer overflow (the code, Code Red) necessary to the exploitation of this vulnerability in a public Web site[18]. In another case, which attracted a lot of attention, within days of the publication of a bug in Netscape's Java implementation to a web site containing also the example code for how this bug operated, thousands of users' systems were reported as compromised[19].

A first response to the problem could be, in these cases, censor the publication of such information[20]. But publication of information in the vulnerability case has a

---

[16] That the particular person acts in good faith may not always be the case or it may be difficult to ascertain. For the purposes of the discussion in this particular paper though, good faith is a fact to be taken as such.

[17] See *Takanen A, Raasakka P., Laakso M. & Roning J.,* Agents of responsibility in software vulnerability processes, Ethics and Information Technology, vol. 6, n. 2, June 2004, 94, note 2. Types of vulnerabilities include access control errors, authentication errors, boundary error, configuration errors, exception handing errors, input validation errors, randomization errors, resource errors, state errors etc. On security in cyberspace, see generally *Tavani H.,* Ethics and Technology, Ethical Issues in an Age of Information and Communication Technology, 2004, 152. For particular cases on computer security see *Spinello R.,* Case Studies in Information and Computer Ethics, Prentice Hall, New Jersey, 1997, 165.

[18] See *Preston,* id., p. 73.

[19] *Ranum M*., Have a Cocktail: Computer Security Today, http://www.ranum.com, n. 2, 2000, last visit July 3, 2006.

[20] Actually eBay was criticized, among others, by Richard Smith, the director of Privacy Foundation, who sustained that disclosure was causally connected with the damage Code Red did, *Preston,* id. p. 76. But see also *Schneier B.,* Crypto-Gram Newsletter: Full Disclosure, http://www.schneier.com/crypto-gram-0111.html#1, last visit June 28, 2006, who supports, after

dual nature: it may be the only way this vulnerability may be cured and people may, therefore, enjoy a more secure system than before; it may also serve as a tool to great damage. It is true that a bomb maker reading about bombs is not also provided with an actual bomb to explode at will, whereas a hacker may be provided with dangerous exploit code, in full disclosure cases. Publishing how to make a bomb cannot, as a rule, help lessening the likelihood of damage by bombing. But disclosing information about a vulnerable system may lead to a quick resolution of this vulnerability and therefore, increase the security of this system. This particular 'bug-bomb' will be forever extinguished in the virtual world; bombs in the real world simply are not subject to a total 'disappearance'. The physical world cannot be made safer by disclosure-the virtual, can.

Software vendors are 'pushed', when their product's defect is publicly exposed, to issue a patch as fast as they can. But vendors are not the only ones to react; in fact, the more people learn about it, the higher the possibility is to end up quickly with an effective patch. It is this quality of the particular information that makes the regulation of its dissemination so hard. It is also this quality which has lead to an ongoing debate about whether, when, how and where a particular vulnerability could be safely as much as possible) be disclosed.

It follows that the resolution of the disclosure problem is not as easy as it may appear. In this respect, the discussion joins other difficult ethical conflicts about disclosure[21]. Under 1, I will present the current debate on disclosure or non-disclosure of system vulnerabilities. Under 2, I will describe the clash of interests in this debate. Under 3, I will discuss the general idea of silence.

1. The debate about disclosure

To disclose a software vulnerability may mean, mainly, two things[22]:

---

explaining why, that '…most criticisms of eEye are not based on fact, but are rooted in a dislike of their brash style, in-your-face advisories, and choice of hair coloring…'.

[21] Dealing with who has and why access to a particular kind of information (for example, physician/patient informational conflicts etc).

[22] Apart from the following options (inform the vendor and/or inform the public in general, through internet sites etc) another rather exceptional case has also been reported, where the identifier elected to inform only but all people affected by the particular vulnerability (a company's customers, where their emails were at risk), see *Rasch M.,* The Sad Tale of a Security Whistleblower, http://www.securityfocus.com/columnists/179, last visit July 3, 2006.

a. the discoverer (the 'benign identifier'[23]) elects to notify the software vendor, in secret, that her product suffers from a particular deficiency, so that the vendor issues, as quick as possible, a patch or

b. the discoverer opts to post the vulnerability in the Internet, in sites[24] usually constructed to deal with this and perhaps other, relevant, issues.

Intermediate solutions exist, such as a policy where the vendor is entitled to be the first to know and, after some time, if no real measures to correct the problem are taken, then the discoverer reports the vulnerability publicly. A middle solution is defended by CERT/CC[25], an organization very influential in disclosure vulnerabilities issues that publishes around 3.500 to 4.000 new vulnerabilities every year[26]. The policy advanced by CERT is to allow the vendor a window of time of 45 days, so that a patch may be, during this time, made available[27]. After this time limit, though, all vulnerabilities reported to CERT will be disclosed to the public, regardless of the existence or availability of patches or workarounds from affected vendors[28]. This is referred to as 'responsible disclosure'; the first option is sometimes called 'instantaneous' disclosure[29]. Full disclosure has been described as including exploit code whereas limited disclosure omits details on exploits. Full disclosure sometimes includes the disclosure of viruses (and not exploits only) in mailing lists[30]. Exact definitions of kinds of disclosure have not been commonly accepted[31].

---

[23] As described by *Ozment A.,* The Likelihood of Vulnerability Rediscovery and the Social Utility of Vulnerability Hunting, working paper presented at the Workshop on Economics and Information Security, June 2-3, 2005, Cambridge MA, USA, available at at infosecon.net/workshop/pdf/10.pdf, last visit June 28, 2006, p. 2, the benign identifier is a person interested in computer security who decide to discover and report software vulnerabilities and who is not necessarily employed by or associated with a vendor and who is not an attacker, with malicious intent to cause harm.

[24] 'Bugtraq', operated by SecurityFocus, one of the most comprehensive and trusted sources of security information on the Internet, is one of these mailing lists, devoted to fulfill the aims of a policy towards full instant disclosure. Another one is the Full Disclosure mailing list, see *Ozment A.,* id.

[25] Computer Emergency Response Team Coordinating Center, established in 1988, a center of Internet security expertise, federally funded, see www.cert.org.

[26] *Shawn Hernan*, of CERT, Roundtable, the Disclosure Debate, 2002, available at http://infosecuritymag.techtarget.com/2002/jul/roundtable.shtml, last visit July 3, 2006.

[27] This policy is characterized as a de facto, but unofficial policy, see *Arora A., Telang R & Xu Hao,* Optimal Policy for Software Vulnerability Disclosure, http://www.dtc.umn.edu/weis2004/xu.pdf, p. 2, last visit May 14, 2005.

[28] See CERT/CC Vulnerability Disclosure Policy, www. cert.org/kb/vul_disclosure.html, last visit June 28, 2006.

[29] See *Ozment,* id., p. 3.

[30] *Gordon S. & Ford R*., When Worlds Collide Information Sharing for the Security and the Anti-virus Communities, available at http://vx.netlux.org/lib/asg06.html, last visit July 3, 2006.

[31] See *Cooper, '...*we do not have a common, accepted definition of full disclosure…the problem is, there's all these questions about full disclosure and yet no definition of what we are talking about…', in Roundtable, the Disclosure Debate, available at http://infosecuritymag.techtarget.com/2002/jul/roundtable.shtml, last visit July 3, 2006.

Any decision about when, how and to whom a software vulnerability should be disclosed or not must take into account:

a. the interests of the software vendors of the defective product
b. the public's right to know when a particular system is compromised and how and
c. the public's interest against attacks made possible *because* the vulnerability (perhaps along with a very convenient for hackers exploit) was reported.

In this last respect (c), empirical evidence on, for example, whether it is a fact that the disclosure of an exploit inescapably leads to very harmful security attacks, is necessary, as part of the foundation of an efficient disclosure legal or ethical rule. The lack of appropriate, comprehensive empirical evidence on these issues has been reported as in fact, a major problem; it also seems that we do not have evidence on the severity of damages caused by attacks [32]. Some commentators are careful to note that their data are noisy and problematic[33]. One should also take into account that there is reason to believe that security incidents are massively under reported[34]. Still, the assumption that once a computer program capable of bypassing an access control system is disseminated via the Internet, it will be used[35] is truly reasonable, but it is equally truly, until more concrete data are available, an assumption. Lastly, arguments for or against disclosure reasonably carry different weight among their supporters, depending on who their evaluator is[36].

---

[32] *Arora A., Krishnan R., Nandkumar A., Telang R. & Yang Y.*, Impact of Vulnerability Disclosure and Patch Availability – An Empirical Analysis, Workshop on Economics and Information Security, Minneapolis, May 2004, MN, USA, available at www.dtc.umn.edu/weis2004/weis-arora.pdf, last visit July 3, 2006.

33 *Wiik J., Gonzalez J. Lipson H. & Shirneall T.,* 2004, Dynamics of Vulnerability – Modeling the Life Cycle of Software Vulnerabilities, P. International System Dynamics Conference, Oxford, UK, p. 4, *Ozment A*., id.

[34] *Mitchell D., & Banker E.,* Private Intrusion Response, 11 Harv. J. T. & Tech. 699, 704 n. 10, 1998, one in ten violations is detected, one in ten is reported to the police etc.

[35] *Universal City Studios v. Reimerdes,* 111 F. Supp. 2d 294, 331 (S.D.N.Y. 2001).

[36] See diverse opinions on disclosure in a survey*, Goens T*., The Full Disclosure of Computer Security Vulnerabilities-An Examination of the Debate, an abbreviated version of the undergraduate distinction project, BSBA 2001, available at http://fisher.osu.edu/people/goens_1/results.htm, last visit October 5, 2005. '…Perceptions of the degree of risk involved with full disclosure announcements vary by association with certain computer security groups. BugTraq subscribers do not feel full disclosure is as harmful as those in professional membership computer security groups, such as the ISSA. Not surprisingly, BugTraq subscribers feel the strongest that *not* (emphasis in the original text) releasing vulnerability information will cause a high degree of risk for those involved with computer security. These results show that there is no strong consensus regarding the possible effects of full disclosure across the various types of persons employed in computer security…'. In another survey by Hurwitz Group of more than 300 software security professionals, it is also reported that users (another interest

Arguments for full or 'responsible'[37] disclosure view include:

1. Early disclosure has been reported as having a significant positive impact on the vendor patching speed. Vendors respond slower to vulnerabilities not disclosed by CERT/CC-they always choose to patch later than a socially optimal disclosure time[38]. Open source vendors patch more quickly than closed source vendors and severe vulnerabilities are patched faster[39].
2. Responsible disclosure best safeguards the critical infrastructure of the Internet[40] whereas full disclosure necessarily leaves a large number of users vulnerable; simultaneously, it has been reported that
3. The frequency of attacks after disclosure decreases over time[41].
4. Early and full dissemination of vulnerabilities allows for extensive research to correct them faster; apart from promoting academic freedom of information, disclosure offers as an end result more security, not less[42].
5. Crackers already know the vulnerabilities; systems administrators do not[43]. Vulnerabilities are often rediscovered independently within a relatively short

---

group in this debate) strongly supported prompt notification of potential problems, 39% said immediately, another 29% within a week, whereas the industry standard is about a month, see *Haley C.,* Users Urge Disclosure of Security Flaws, June 28, 2002, available at http://boston.inetrnet.com/news/print.php/1378631, last visit October 5, 2005. The respondents to the survey opted for disclosure, even if their own companies would be endangered by it, see Security Vulnerabilities: is Full Disclosure the Best Path? date of publication not available, text available at http://advisorevents.com/doc/10190, last visit July 3, 2006.

[37] The exact meaning of the terms 'full' and responsible' disclosure is not clarified in the relevant literature; generally, full disclosure may mean the immediate disclosure of all details about a vulnerability (also, for example, an exploit) whereas responsible disclosure may mean the delayed (for example, after 45 days, under CERT rules) disclosure of some characteristics of a certain vulnerability (or only its existence).

[38] *Arora A., Telang R. & Xu H*., Optimal Policy for Software Vulnerability Disclosure, in Workshop on Economics and Information Security, May 2004, Minneapolis, MN USA, available at www.dtc.umn.edu/weis2004/xu.pdf, last visit June 28, 2006. The writers support, however, that instant disclosure is equally sub-optimal. It is reported that security vendors often ignore vulnerabilities and that network administrators do not bother to install patches, *Shneider*, id.

[39] *Arora A., Krishhnan R., Telang R. &Yang Y.,* An Empirical Analysis of Vendor Response to Disclosure Policy, p. 1, available at. http://infosecon.net/workshop/pdf/41.pdf, last visit June 28, 2006.

[40] *Duncan J.,* Responsible Vulnerability Disclosure: Challenges for Vendors Whose Products Are Infrastructural, Secure Business Quarterly, issue three, Defining the Value of Strategic Security, third quarter 2002 at www.sbq.com, last visit September 27, 2005, p. 5.

[41] See *Arora A., Krishhnan R., Telang R. &Yang Y.,* An Empirical Analysis of Vendor Response to Disclosure Policy, p. 1, available at. http://infosecon.net/workshop/pdf/41.pdf, last visit June 28, 2006.

[42] *Grannick*, id. Also, generally, *Schneier B.,* Secret Lies-Digital Security in a Networked World, 2000, *Schneier B*., Full Disclosure and the Window of Exposure, available at http://www.schneier.com/crypto-gram-0009.html, last visit September 29, 2005. There does not appear to be, however, clear empirical evidence to support the end result of 'more security'.

[43] *Windows of Vulnerabilities,* p. 57. See also *Levy E.,* Full Disclosure is a Necessary Evil, 2001, http://securityfocus.com/news/238, last visit July 3, 2006, noting that '…The Code Red worm is based on an earlier worm that exploited another vulnerability in Microsoft's IIS server. The vulnerability was a buffer overflow in the .htr ISAPI filter. No details about this vulnerability were public. Yet, someone

period of time; vulnerability hunting is therefore socially useful and full disclosure pressures vendors into more rapidly providing patches[44].

6. Secrecy leads to a market for early notification of vulnerabilities only to a small number of willing payers[45]; a black market for security information may also be the result of secrecy policies[46].
7. Vulnerabilities are a demonstration of faulty products; producers should produce better code, as a first priority, and not care so intensively that the defect of their product is not publicly exposed[47].

Arguments against disclosure include the following:

1. Immediate publication of a security advisory has been shown to cause an equally immediate exploitation, which reoccurs on a regular cycle because of poor maintenance – malware never truly goes away[48]. This effect is avoided with a responsible disclosure policy.
2. Even when a patch *is* available, disclosing a vulnerability increases the frequency of attacks-clearly, attackers believe that users will not patch in time[49].
3. Vulnerability disclosure increases the frequency of attacks[50]; users are defenseless against attackers[51]; hackers, when only

---

wrote a worm to exploit the vulnerability anyway…'. See also *Vidstrom A.,* Full Disclosure of Vulnerabilities-pros and cons and fake arguments, http://216.239.59.104/search?q=cache:x14tDa-KLNkJ:ntsecurity.nu/papers/disclosure/+Full+Disclosure+of+Vulnerabilities-pros+and+cons+and+fake+arguments&hl=el, last visit October 5, 2005, '…How could we keep vulnerabilities secret when so many people at so many different places and organizations have them? The vulnerability details may already be in circulation in the computer underground…'.

[44] *Ozment A.,* id., see note 23, p. 1.

[45] *Levy E.,* Full disclosure is a necessary evil, id, '...for $2.500 a year any black hat with a business name, PO BOX and a web site can get advance notice of vulnerabilities before most of the general public – at least in theory…'.

[46] *Grannick J.*, working paper, untitled, available at islandia.law.yale.edu/isp/digital%20cops/papers/granick_newcrimescene2.pdf, last visit September 29, 2005.

[47] *Edwards*, id.

[48] *Windows of Vulnerability, id.*

[49] *Arora A., Krishhnan R., Nandkumar A., Telang R. & Yang Y.,* Impact of Vulnerability Disclosure and Patch Availability - An Empirical Analysis, Workshop on Economics and Information Security, Minneapolis, May 2004, MN, USA, available at www.dtc.umn.edu/weis2004/weis-arora.pdfl, last visit June 28, 2006, p. 19.

[50] *Arora A., Krishhnan R., Nandkumar A., Telang R. & Yang Y.,* id, p. 3-5.

[51] *Elias L.,* Full Disclosure is a Necessary Evil, SecurityFocus.com, 2001-08-16, www.securityfocus.com/news/238, 2001, last visit September 27, 2005, *Farrow R.*, The Pros and Cons of Posting Vulnerability, the Network Magazine, 2000, available at www.networkmagazine.com/shared/article, last visit September 27, 2005, *Gordon S. & Ford R.,* When

given minor details about a bug, can produce a working exploit in a relatively short amount of time[52]. Therefore, one must be aware that throwing exploit information out freely in the Internet means information anarchy[53].

4. The data on the effectiveness of disclosure, in terms of its effect on the software security defect rate, are not positive: the effort being spent on vulnerability finding has been documented as sustained by weak evidence[54]. Even when a vulnerability is reported, large sections of users either do not respond at all or respond only when an exploit is circulating. Therefore, it is never 'safe' to release immediately all the details of vulnerability[55].

5. If vendors are pressed by public disclosure to release a patch, then the will release it before it is researched throughout and tested; the patch may not fix the problem completely or it may cause compatibility problems[56].

2. The clash of interests in the disclosure debate

Sellers sell; their interests lie in persuading that they sell the best products available at the best market price. Any negative publicity about their product causes them, as a rule, losses. Software has been marketed as an information product where defects will always be present, defects not due to any negligence by its producer, but inherent in the very nature of the product. This particularity has sustained so far the lack of legal liability of software producers for their products, a liability, which would

---

Worlds Collide: Information Sharing for the Security and Anti-Virus Communities, research paper, 1999, available at http://vx.netlux.org/lib/asg06.html, last visit September 27, 2005.

[52] *Edwards M.,* To Disclose or Not to Disclose, That is the Question, available at http://www.windowsitpro.com/Articles/Print.cfm?Article ID=21618, last visit September 27, 2005.

[53] *Culp S.*, It's Time to End the Information Anarchy, available at http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/security/noarch.asp, last visit September 29, 2005.

[54] *Rescorla E.,* Is Finding Security Holes a Good Idea?, Workshop on Economics and Information Security, Minneapolis 2004, MN, USA, available at http//www.rtfm.com/burgate.pdf, last visit September 27, 2005.

[55] *Rescorla E.,* Security Holes…Who Cares? Proceedings of the 13th USENIX Security Symposium, August 2003, available at http://www.rtfm.com/upgrade.pdf, last visit June 28, 2006.

[56] *Vidstrom A.,* Full Disclosure of Vulnerabilities-pros and cons and fake arguments, http://216.239.59.104/search?q=cache:x14tDa-KLNkJ:ntsecurity.nu/papers/disclosure/+Full+Disclosure+of+Vulnerabilities-pros+and+cons+and+fake+arguments&hl=el, last visit October 5, 2005.

have been logically strict (irrespective of the proof of the vendor's negligence) for probably great customer's losses.

Perhaps it would be reasonable to assume that a software company would immediately react to a private vulnerability disclosure: thank and/or reward the benign identifier[57], instantly produce a proper patch and then, notify its customers. After all, one could think that a software company needs to produce a product as secure as possible, because otherwise, the product will not sell. This argument may hold true in the case of other products (for whose failings, notably, sellers do bear product liability, such as for example, cars) but the evidence does not support it in the case of software. What computer security professionals have noted, and been frustrated by, was the vendors' lack of interest in timely correcting their software, unless they were pressed by a public disclosure of the vulnerability[58]. Administrators do not always apply available patches[59]. Indeed, a more general comment is that software vendors systematically disregard consumers' safety and hide behind lax legal codes[60]-they are also reported as making, in software construction, 'the same mistakes over and over again[61]'. The Hurwitz survey was indicative of users' frustration with

[57] Companies are not always eager to truly thank the identifier or to compensate her: 'Typically hackers do a lot of research to figure out all the details about a security risk they have discovered. When they hand that research over to a vendor they generally do not receive other compensation other than a simple written thanks from the vendor..', *Edwards M. J*., To Disclose or not to Disclose, That Is The Question, June 27, 2001, available at http://windowsitpro.com/Articles/Print.cfm?ArticleID=21618, last visit October 5, 2005.

[58] *Schneier B*., Crypto-Gram Newsletter: Full Disclosure, November 15, 2001, available at http://www.schneier.com/crypto-gram-0111.html#1, last visit June 28, 2006, *Morgenstern M., Parker T. & Hardy S.,* It's Time to Be Responsible, available at http://securityfocus.com/guest/10711, last visit October 5, 2005, who mentions as an example the case of a vulnerability of Microsoft's Windows XP which was reported to Microsoft but was kept secret for almost two moths-Microsoft elected not to alert the general public, notwithstanding that tools to get around the problem were available the entire time. Another example is the case of Tornado Development, Inc., a company notified by an employee about a major flaw in their web-mail which did nothing at all to correct the vulnerability for more than six months (when the then ex-employee sent an e-mail on the matter to all 5.600 of Tornado's customers; Tornado first attempted to deleted the emails to the customers, so that they do not learn about the flaw and then, finally, fixed the vulnerability, see *Rasch M.,* The Sad Tale of a Security Whistleblower, 2003-18-08, available at http://www.securityfocus.com/columnists.179, last visit October 5, 2005.

[59] '…There are many reasons for an administrator not to apply all available patches. They include worries that the patches will introduce new errors into the system, a high work load, plain laziness, and that patches for example the OS are not fully supported by application program vendors. Knowledge about the fact that vulnerability details are in circulation out there also gives the administrator an argument against management/vendors for more resources in security issues...', *Vidstrom A.,* id.

[60] *Morgenstern M., Parker T. & Hardy S.,* id.

[61] *Hernan S*., of CERT, in Roundtable, the Disclosure Debate, July 2002, available at http://infosecuritymag.techtarget.com/2002/jul/roundtable.shtml, last visit July 3, 2006.

unresponsive vendors[62]. Software vendor unresponsiveness is commonly mentioned in the relevant literature.

Software vendors may suffer market losses when their stock falls. Research has shown that vulnerability disclosures lead to a negative and significant change in market value for a software vendor[63]. In this respect, software products fall into the same class as automobiles or drugs, when their vendors recall them. On average, a vendor loses around 0.6% value in stock price when a vulnerability is reported, a number which equals a loss of $0,86 billion per vulnerability announcement[64]. Losses are greater when no patch is simultaneously announced.

Therefore, while a threat of a dangerous negligence or product liability lawsuit is not available, in order to urge sellers to correct product deficiencies, a threat by a vulnerability disclosure exists and has been reported as a real one. Powerful economic interests are aligned on the side of (at least) limited disclosure[65]. Microsoft is one of the major companies pressing for limited disclosure[66] and it has the government as an ally[67]; so do a number of other companies, allegedly pushed by Microsoft to join the 'war' against disclosure[68]. But consumers are reported, however, to have contributed to the problems of software security, because they do not demand enough of it: '..if the vendors do not supply security, it's not because they do not want to sell it; it is because it is not expected..'[69]. Under this view, consumers care far more for functionality and features-not security. A parallel view is expressed in connection to

---

[62] See *Haley C*., id. On unresponsiveness see also, among others, *Rasch M.,* 'Responsible Disclosure' Draft Could Have Legal Muscle, 2002, at http://online.securityfocus.com/columnists/66, last visit Jule 3, 2006, '...Fixing security vulnerabilities may not be the vendor's highest priority, particularly where the product involved is freeware or shareware, previously released and unsupported software, or otherwise unprofitable to support. The vendor may not feel it is a worthy use of limited engineering resources to fix a vulnerability that is theoretical, or represents only a minor threat…'.

[63] *Telang R.. & Wattal S.,* Impact of Software Vulnerability Announcements on the Market Value of Software Vendors – an Empirical Investigation, Carnegie Mellon University, working paper, February 2005.

[64] Id., p. 1.

[65] *Grannick*, id., p. 7.

[66] *Culp S*., id.

[67] *Olavsrud T*., Government Against Full Disclosure of Vulnerabilities, 2002, available at http://internetnews.com/dev-news/print.php/1437841, last visit July 3, 2006.

[68] *Martin B*., Microsoft's Responsible Vulnerability Disclosure, The New Non-Issue, 2001, available at http://attrition.org/security/rant/z/ms-disclose.html, last visit July 3, 2006: '..if SecurityCompany A does not support Microsoft in this initiative, then certain negative things will happen. This could be anything from not sharing security information, revoking 'partner' status or anything else that hurts the company….It is clear that Microsoft's vulnerability disclosure initiative is nothing more than a PR stunt. They are trying to side step the onslaught of negative press surrounding their security practices. Negative press that originates because Microsoft's track record of releasing shoddy products that receive inadequate testing, no auditing and wide distribution'.

[69] Per Cooper Russ, TruSecure, in Roundtable, the Disclosure Debate, 2002, available at http://infosecuritymag.techtarget.com/2002/jul/roundtable.shtml, last visit July 3, 2006.

the average Internet user: '..(users) do not want to worry about security. It is not interesting to them. They do not care particularly about security and have better things to do their time than to constantly patch their system against security bugs. It's largely academic to them…'[70].

3. The choice of silence: costs in freedom of choice, costs in free speech

No matter how much or how little the public cares about security in their software, it is legitimate to argue that it has the right to know that their software is vulnerable[71]. People should, in principle, be offered the chance not only to know that a product they bought is compromised but also, the chance to repair it by themselves[72], to stop using it, to use it with caution, to engage in relevant research etc. As in other cases of 'the right to know' problems[73], improperly harming the interest in knowledge means harming the interest in freedom of choice. Ultimately, deprivation of choices means wrongful substitution in decision-making: the wrong party (the vendor, the discoverer etc) makes a decision, which legitimately and again, in principle, belongs to the individual citizen. The burden of proof that such deprivation is legitimate falls upon the parties arguing for silence and the justification needs to be supported by clear empirical evidence of harms-in principle, again, *actual* harms and not only the increase of a chance to harm, from reporting[74]. Such clear empirical evidence, as mentioned, is at present, lacking.

There is though some evidence that the evaluation of the general benefit from reporting (public benefit deriving, for example, from a quicker patch and the public's right to know) has been evaluated differently, depending on the status of the evaluator: those reporting vulnerabilities hold a higher esteem for these values (they

---

[70] *Ranum M.*, Have a Cocktail: Computer Security Today, n. 2, 2000, available at http://www.ranum.com, last visit June 28, 2006.

[71] *Grannick*, id.

[72] On this point see Levy's comments in *Olavsrud,* id.

[73] Compare, for example, with deprivation of patient choices, when the physician breaches the obligation to inform the patient, in detail in the seminal work of *Katz J.,* The Silent World of Doctor and Patient, New York: The Free Press, 1984.

[74] In principle, the law forbids behavior, which causes damage or is certain to cause damage; not behavior, which increases the likelihood of damage (relevant crimes are the exception to the rule). Similarly, a statute or a tort which punishes speech which has the propensity to be misused by some unknown recipient would be problematic, from a constitutionally significant respect, see Department of Justice, Report on the Availability of Bombmaking Information, the Extent to Which its Dissemination is Controlled by Federal Law and the Extent to Which Such Dissemination May be Subject to Regulation Consistent With the First Amendment to the US Constitution, April 1997, available at http://derechos.org/human-rights/speech/bomb.html., last visit July 3, 2006.

see their work as useful for the whole society) than that granted by those who receive the reports. Receivers usually see the issue as most important to the company they work for, first and foremost, and they see the company's role as promoting the general benefit-not theirs[75]. Opposite positions are also taken, as it seems, depending on whether the person expressing them is a member of the computer security or the anti-virus community[76].

As the public must be able to know, professionals and researchers in particular (and not only) must also be able to speak. Computer security researchers and professionals should not be deprived from their constitutional right to free speech. The clash between the sellers' and the public's interest in freedom from hacker activity and scientific freedom under the First Amendment has also been exposed[77]. Civil and criminal liability under the Digital Millennium Copyright Act and the Computer Fraud and Abuse Act has been a real threat against publishers of software vulnerabilities[78]. The law on liability for publications has not offered any clear solution yet, as there are instances where the First Amendment may not protect a certain publication (which is considered a 'tool' for a criminal act and not free scientific speech). Intent to harm is a crucial part of these crimes; as a rule, it is lacking in scientific publications, but sometimes courts may infer intent. The current 'map' of the relevant jurisprudence points to no safe direction[79]. Cases like

---

[75] See study reports of 157 valid answers from both reporters/receivers in questionnaire, *Havana T.,* Communication in the Software Vulnerability Reporting Process, April 2003, available at http://www.oulou.fi/research/ouspg/protos/sota/reporitng/gradu.pdf, last visit September 29, 2005.

[76] '..influential members of the security world in a position to contain the dissemination of viral code believe that disclosure is a necessary evil; the anti-virus industry believes that publication is unethical and harmful…', *Gordon S. & Ford R*, id., noting the diametrically opposed positions regarding information sharing.

[77] *Preston E. & Lofton J*., Computer Security Publications: Information Economics, Shifting Liability and the First Amendment, Whittier Law Review 24 (2002), pp. 71-142. Until today, the influential question whether software is more like a can opener (no First Amendment protection) or a recipe (First Amendment protection) has not been totally resolved, see *Kaplan C*., Is Software Like a Can Opener or a Recipe, Cyberlaw Journal, 1998, http://partners.nytimes.com/library/tech/98/07/cyber/cyberlaw/17law.html, last visit June 28, 2006.

[78] See for example the letter sent by HP to SnoSoft, when it published in securityfocus.com a buffer overflow exploit of Tru64 UNIX, threatening with federal criminal liability under both DMCA and CFAA, at http://politechbot.com.docs.hp.dmca.threat.073002, last visit September 29, 2005. SnoSoft had, however, waited for three months for HP to issue a patch; this never happened, but HP did issue a patch within 48 hours after publication by SnoSoft, see *Preston*, id, p. 139.

[79] See *Rice v. Paladin*, 128 Fed. 3nd 233, 4th Cir. 1997, where the publisher (Paladin) of a book called 'Hit Man: A Technical Manual for Independent Contractors' was held civilly liable, for the tort of aiding and abetting. The case involved the death of three persons, killed after an independent contractor followed the book's instructions. In this case, Paladin, who relied unsuccessfully on a First Amendment defense, had impressively stipulated intent. Compare to *Brandenburg v. Ohio*, 395 US 444 (1969), the 'classic' case attempting to set a line between abstract 'dangerous' advocacy (speech) and a crime (act), where abstract advocacy was held protected speech. In *US v. Freeman,* 761 F.2d 549, 5529th Cir.

Reimerdes[80] and *Corley*[81] where the Digital Millennium Copyright Act was successfully used as a legal foundation to sustain an injunction against the publishing of the computer program DeCSS (code permitting access to data from DVDs on unlicensed platforms) show us that a First Amendment defense is not always available, when the governmental interests, here in protecting legal copyrights, are opposed to it; perhaps, the governmental interest in public safety from hacking would be held equally superior.

Rules suppressing the free dissemination of information have not always been successful; after all, information has a natural tendency to flow. Perhaps it is true that strategies enforcing secrecy are just doomed[82]. Full disclosure is reported as akin, in many ways, to the open-source movement; like open-source, full disclosure allows for peer review, learning and collaboration that leads to making better software[83].

The answer to the question 'to tell or not to tell' is not an easy one and the parties to this conflict are not two; very diverse interests, too many different representatives of different communities interplay in this discussion. But when companies, not bearing liability for their products, urge for silence and when this silence has to do with concealing their deficiencies, one ought to be very careful before siding with them. Physicians have for centuries argued for silence, only to cover up for their sometimes fatal mistakes[84]; scientific research too, has its own very dark pages of immense harms covered by silence[85]. It is history itself, which gives us a perspective of suspicion before a mandate for concealment.

1985, the 9th Circuit stated that, if the intent of the actor and the objective meaning of the words used are so close in time and purpose to a substantive evil as to become part of the ultimate crime itself, *the actor's intent is irrelevant* (italics mine) and she is liable (this was a case about tax evasion counseling at seminars held in protest of tax laws). There are many other relevant, but not on-the-point cases (see in detail *Preston,* id). A researcher who publishes details of a system's vulnerability may really want to press the vendor to issue a patch; she may also know, though, that the publication may be used by 'the bad' guys, hackers who will immediately take advantage of the new knowledge. In this case, the question of liability remains mainly open ('..if *Rice* is correct, the intent to inform legitimate users as well as computer criminals is no barrier to liability…', *Preston*, id., p. 109). Until the lawmaker or the common law deal explicitly with a case like this one, there is no absolutely safe answer to the question of liability, and this vagueness reasonably leads to fewer publications and fewer publications have been reported as a factor for *less* security (not more).

[80] 273 F. 3d 429 (2d Cir. 2001).

[81] 111 F. Supp. 2d 294 (SDNY 2000).

[82] *Schneier B*., (2000) Full Disclosure and the Window of Exposure, available at www.schneier.com/crypto-gram-0009.html#1, id, last visit June 28, 2006.

[83] *Rauch J*., The Future of Vulnerability Disclosure? date of publication unavailable, text available at http://www.usenix.org/publications/login/1999-11/features/disclosure.html, last visit June 28, 2006.

[84] *Katz J*., id, note 2.

[85] See among others *Jordan M*., HUSH HUSH, The Dark Secrets of Scientific Research, Quintet, 2003.