Global Information Assurance Certification Paper

Vulnerability Disclosure, The Double Edged Sword

By Mike Palella

GSEC Assignment 1.4b

Abstract

During the past couple of years, the area of vulnerability disclosure in the information security community has been a hot topic for debate. Vulnerability disclosure, in essence, is the communication of information related to security vulnerabilities discovered in operating systems and applications, some of which are connected to the Internet and thus publicly accessible. One of the first organizations created to coordinate the dissemination of such information was the CERT® Coordination Center, founded in 1988 after the "Morris Worm" attack on the Internet. Since then, several other volunteer and commercial organizations and public forums have also been established to provide similar information. Unfortunately, releasing vulnerability information has been far from trivial. As the information security industry continues to mature, vulnerability disclosure has become a thorn in the industry's side. Many have made attempts to standardize this process, however, it has been difficult to find common ground.

The purpose of this document is to introduce and elaborate on the different methods of vulnerability disclosure, explain the advantages and disadvantages of each, discuss the government's role, and consider the legal ramifications.

Introduction

Some experts claim that software companies have had little motivation, from a legal standpoint, to release solid products to market due to the absence of product liability laws holding them accountable. Others feel that flaws in applications are inherent because software development is an arduous process. The development process is complicated further because customers want feature rich, and easy to use software. Regardless of the cause, the end result is that these shortcomings are inevitable. Many of these defects create security voids that must be fixed as quickly as possible when discovered. Marry this with the ever-increasing pressures to secure information resources, and you now have a hot bed for vulnerability disclosure.

On one side, you have those in favor of full disclosure, which is primarily made up of end users, and security professionals that are responsible for securing information infrastructures. On the other side, you have those who believe that limited disclosure is the best approach. This group consists mostly of vendors responsible for patching holes discovered in their products, or systems. Somewhere in the middle you have those trying to find common ground in order

to make vulnerability disclosure work as effectively as possible. These folks have introduced a method commonly referred to as responsible disclosure. Unfortunately, unilateral acceptance of any one method has been slow in coming; however, lately responsible disclosure appears to be gaining momentum.

To complicate matters further, laws such as the Digital Millennium Copyright Act, (DMCA) signed into law by President Clinton on October 28, 1998, give software vendors an avenue to threaten security experts, or anyone else for that matter, with legal action if information about their product is leaked out to the public. The law does have provisions to allow for security research, but many security experts fear paying exorbitant legal fees simply to prove that they did not do anything illegal.

The United States Government also realizes the sensitivity of this overall situation and has become increasingly involved. DHS, the U.S. governments newly created Department of Homeland Security, is currently developing a private network, isolated from the Internet, to securely channel vulnerability and other security related information amongst federal agencies and private sector experts. This move could be an indication that the U.S. government is planning to play a bigger role in the private sector vulnerability disclosure business.

Full Disclosure

In 1993, Jeremy Rauch and fellow co-founders of SecurityFocus.com, created BugTraq, a very popular vulnerability full disclosure mailing list. Open forums, such as BugTraq, have since fueled the full disclosure revolution. In fact, in an attempt to better its footing as an information security company, Symantec Corporation acquired SecurityFocus on August 6, 2002, which included the BugTraq mailing list.

The argument for full disclosure is that it offers a means to share detailed information about specific vulnerabilities with others, so that responsible decisions can be made to protect against them. To quote Mr. Rauch on full disclosure, “Its sole purpose is to arm the security-conscious with the knowledge necessary to evaluate risks and take applicable action.” (Rauch, p.1). It is not wise to make a decision on protecting your systems without a complete understanding of what you are up against. Anyone can use this insight to evaluate how it affects their systems, and then make educated decisions to protect these systems when necessary.

Often times, full disclosure forums offer intimate details on bugs, worms, viruses and other security exploits discovered by security professionals and the like. Postings offer temporary countermeasures, or information regarding available patches. In some cases, the actual exploit code is even included so those

capable individuals can determine how to counter it. When vulnerabilities are made public, vendors are immediately pressured to produce fixes. Everything about it sounds good, so what is wrong with full disclosure?

"Knowledge is power!"

The down side to having all of this knowledge readily available to anyone is that there are individuals that will use it with malicious intent. Of course, this would be a moot point if the disclosures were made after the software companies had an opportunity to develop and distribute patches for these vulnerabilities, and 100% of their user base actually deployed them. Nimda, a mass-mailing worm discovered on September 18, 2001, was downgraded by Symantec's security response from a threat level 4 to a level 2 on January 15, 2003. Although on the decline, this worm is still alive and propagating the Internet more than a year and a half later. Patches are even more unlikely to be applied expeditiously if they are complicated to install, as in the case of the recent SQL Slammer worm. As we have seen, since we live in an imperfect world, timely patching does not always happen.

The fundamental problem with the true form of full disclosure is control. It is important to stay informed so that educated decisions can be made. However, in many cases the end user relies on the vendor's patches to fix the vulnerabilities that are discovered in their applications or systems. So if exploit code is posted (to sites such as BugTraq) as soon as it is discovered, without giving the vendors the opportunity to develop patches, we are simply creating an opportunity for the "bad guys" to take advantage of. Keep in mind; complete control over vulnerability information is impossible. "Bad guys" will always find a means to share this type of information via their underground network. We do not help matters by irresponsibly posting exploit code to the general public. If the real intent is to share vital information so that system administrators and users worldwide can educate themselves in order to maintain an acceptable level of information security, then this form of full disclosure does not work effectively.

Limited Disclosure

Let us take a look at the disclosure dilemma from another viewpoint. Large software vendors spend millions of dollars developing and marketing their applications. When vulnerability information is released about one of their products, it makes them look bad, especially if no fixes are immediately available. When you are made to look bad too many times, it will mar your reputation, and as we all know, a bad reputation is bad for business. Many events of the past few years have brought newfound awareness to security in general, so vendors have to be sensitive to their customer's increasing demands for secure products. In order to protect their reputations, these companies are strong advocates of the limited disclosure model.

What is limited disclosure?

Limited disclosure is quite the opposite of full disclosure. Software vendors feel that when vulnerabilities are discovered in their products, they should be the first, and only ones to know about them. Those who disclose the information to the vendor would be sworn to secrecy, or suffer the wrath that the vendor would impose on them. The vendors could then address the vulnerabilities at their leisure. If they felt that it was necessary, patches would be developed and released with whatever descriptive information they felt was appropriate.

The vendors essentially want complete control over any vulnerability information related to their products. In addition, the software giants have been marketing this approach as the responsible method of disclosure. Bryan Davies, a practicing attorney of 19 years who has been following the disclosure debate closely, made the following quote “It is important to note at the outset that corporate PR does not title this model the "limited" disclosure model, but rather a "responsible" disclosure model. Thus they seek to mislead the casual observer into believing that the software giants are doing what's best for the consumer by being responsible.” (Davies, p.1). It is fairly obvious that vendors are simply trying to advocate a method of disclosure that allows them to control the information released to the public in order to protect their self-interests.

For the most part, limited disclosure is a Gestapo approach to vulnerability disclosure. With this approach, the information you receive is always going to be biased, and incomplete. The end user will almost always be at the mercy of the software vendor.

Another problem with limited disclosure is that it assumes no one else, besides the responsible party that reported the vulnerability and the vendor, knows about the vulnerability. Malicious individuals may have discovered the vulnerability, days, months, or years prior to the responsible party’s discovery. Imagine if the vendor decides to take their time developing a patch, or worse, they decide not to develop a patch at all. Your options, and ability to protect your systems, become limited.

Here is an example of why limited disclosure does not work. A large software vendor releases a new version of an extremely popular application to market. Immediately after releasing it, a vulnerability with massive security implications is discovered and reported to them. If they do the right thing by developing a patch and releasing it to the public with details, they will probably hamper the initial acceptance of the product and waste millions of dollars spent on the product’s marketing campaign. Their other option would be to delay the release of any information for an indefinite period of time in order to minimize the impact this negative information would have on its initial acceptance. Since companies are in business to make money, most would have to presume that in a limited

disclosure world, more companies, then not, are going to delay the release of the information.

There is one positive thing to note about limited disclosure. The product developer should be notified first after the vulnerability is discovered so that they can begin working on a fix immediately. All other aspects of this method are one sided and the general public would be at the mercy of a vulnerability information Gestapo.

Responsible Disclosure

Essentially, responsible disclosure is a hybrid of full and limited disclosure. It attempts to utilize the best features of both in order to appease the interests of the software vendors and the security conscious end users. "In the responsible disclosure model, parties present newly discovered vulnerability information to the vendors first, and allow them the opportunity to correct the issue. If vendors ignore the warnings, then releasing a public advisory to a proper forum (such as Bugtraq) is warranted." (Morgenstern and Parker, p. 2). Responsible disclosure is essentially full disclosure with a twist. It adds the missing piece of control, or responsible management of the vulnerability information. It is a democratic approach to disclosure.

Conceptually speaking, responsible disclosure consists of the following key steps (many details have been intentionally left out for the sake of highlighting the key concepts):

1. Responsible party discovers vulnerability.
2. The responsible party contacts the software vendor to inform them of the vulnerability.
3. The vendor would confirm or deny the discoverer's claim.
4. If the report were confirmed, the vendor would develop a patch.
5. Once the patch was completed, the vendor would coordinate testing with the discoverer.
6. Once the patch has been verified, either the vendor would release limited information including the patch, while the discoverer delays releasing more detailed information, or they would both release their information simultaneously.

The key feature that sets responsible disclosure apart from the rest is control of the information, until a patch has been developed and released to the public. In order to work, it requires open communication, and due diligence on the part of the discoverer and the vendor. If either party drops the ball, it becomes nothing more than full disclosure.

Agreement on the details, and the hard-core advocates of full and limited disclosure have stalled widespread acceptance of a "standard policy" for responsible disclosure. Albeit, attempts have been made to create a "standard policy." For example, in February 2002, Steve Christey of MITRE Corporation, and Chris Wysopal of @stake, Inc. jointly submitted an Internet-Draft to the Internet Engineering Task Force (IETF) titled "Responsible Vulnerability Disclosure Process." Unfortunately, the authors withdrew the draft before it could make it to RFC status. According Steve Christey, in an IETF posting, the reason the Internet-Draft was withdrawn was "because many people in the Security Area Advisory Group (SAAG) questioned whether or not the IETF should work to adopt "human practices" instead of technical protocols." (Christey, p. 1). Another example is the effort that some software and security vendors have put into the "Organization for Internet Safety," which is also working on a "standard" responsible disclosure policy.

Even if the security community, vendors and end users can come to terms on a "standard" responsible disclosure policy, without a governing body to enforce it and act as a coordinator/mediator between the vendor and vulnerability discoverer, it is merely a process based on the honor system. As we saw by the end result of the Christey-Wysopal Internet-Draft, the Internet Engineering Task Force will not be that governing body.

Several popular private sector organizations involved with the coordination of vulnerability information, namely CERT and SecurityFocus, have recently been on the hot seat for pre-releasing vulnerability information to paying customers of their products or services. Some debate that this violates the concept of responsible disclosure. In fact, some security professionals regularly involved with discovering vulnerabilities, are protesting these organizations, by not disclosing information to them until the last minute. There is a general feeling that, not only is this an unethical practice, but also unsafe by potentially putting other systems at risk, if information is leaked out during the pre-release stages. The information security community has made it loud and clear to these organizations that they will not tolerate their attempt to use such information to promote their own self-interests.

Despite responsible disclosure's immaturity, its best of both worlds approach offers the most effective means for the dissemination of vulnerability information so that the public can protect its information resources in a timely manner.

Government's Role

Because of the lack of control over newly discovered vulnerability information, the United States Government has been considering playing a greater role in the area of vulnerability disclosure. The recently created Department of Homeland Security (DHS), led by Tom Ridge, has been given the responsibility to protect

the nations critical networks. This is an extremely complex responsibility given the vastness of the Internet, and the fact that many, if not all, of the nations critical networks are directly or indirectly connected to it. To make this task more perplexing, "more than 85% of critical infrastructures in the United States are owned and operated by the private sector." (William and Dingle, p.1). This means that the DHS is responsible for securing networks, of which, it directly controls less than 15%. With so much of the nations critical infrastructures in the hands of the private sector, it seems to be in the DHS's best interest to ensure consistently responsible vulnerability disclosure across as much of the Internet as possible.

One of the first goals of the DHS is to build a private network, called the "Cyber Warning Information Network," consisting of the National Infrastructure Protection Center (NIPC), the Critical Infrastructure Assurance Office (CIAO) and other government entities created to protect federal systems. Prior to the creation of the DHS, all of these entities were either independent, or the responsibility of another department within the government. The DHS also plans to include the private sector Information Sharing and Analysis Centers (ISAC) at some point in the future. This isolated network will allow government agencies and private sector security experts to communicate during wide spread Internet outages, caused by large-scale attacks.

Recently, the DHS played its first major mediation role in coordinating the serious and widespread, Sendmail vulnerability, although, this is not the first time that the government has been involved with coordinating vulnerability information. Prior to being moved to the DHS, the National Infrastructure Protection Center, which was part of the Federal Bureau of Investigation (FBI), played the part of coordinator several times.

Many feel that the government could add little more than bureaucracy to the problem of vulnerability disclosure. In addition, they feel this bureaucracy would lead to inadvertent and premature release of critical vulnerability information, leaving many systems exposed until a patch, or workaround, could be developed. According to Richard Clarke, former chairman of the President's Critical Infrastructure Protection Board, "The federal government can't effectively mandate cyber-security or legislate cyber-security. At the end of the day, market pressure is probably what will work." (Fisher, p.1). So there you have it, even members of the government advocate keeping the responsibility of governing vulnerability disclosure in the hands of the private sector.

Contrary to the belief of many naysayers, the DHS's coordination of the Sendmail vulnerability occurred, for the most part, without a hitch. However, long-term performance is difficult to judge based on a single incident. There are those that feel that the U.S. government is the best suited to be the governing body for responsible disclosure. They also feel that the government needs to get more involved by holding software vendors liable for the security of their products.

Whatever the case, there is no doubt that the government will be involved, the only question that remains is, to what extent? In the past, the government has primarily followed a "hands off" approach with private sector vulnerability disclosures, unless the vulnerabilities were serious with widespread implications. With the escalated sensitivity toward national security in the past couple of years and increased pressure to protect our nation's critical infrastructures, market pressure alone is probably not going to cut it in the government's eyes. One has to presume that the government plans to become more involved, but only time will tell what future role they will play.

Legal Ramifications

With identity theft on the rise, several industries are being forced to provide stringent levels of security in order to protect their customer's personal information. Statutes such as the Health Insurance Portability and Accountability Act (HIPPA) enacted to protect patient information, Gramm-Leach-Bliley Act enacted to protect customer's financial information, Sarbanes-Oxley Act enacted to protect investors by improving the accuracy and reliability of corporate disclosures, and California's new disclosure law forcing companies to notify their customers when personal information has been compromised. U.S. Senator. Diane Feinstein (D-Calif.) has been contemplating the proposal of the Database Security Breach Notification Act, based on California's new disclosure law, which would extend to businesses throughout the rest of the nation the requirement to notify customers when their personal information has been stolen. Many experts fear that the implementation of such laws will spark a frenzy of class-action lawsuits in cases of product liability.

From a software vendor's standpoint, the Digital Millennium Copyright Act (DMCA) was enacted to protect intellectual property. DMCA contains provisions for security research, however, its lack of clarity gives large software vendors a means to threaten, and possibly pursue legal action. Vendors trying to intimidate others for disclosing vulnerability information about their products have regularly cited this vague law when doing so. For example, during the middle of last year, Hewlett-Packard (HP) threatened legal action against Secure Network Operations, Inc. for disclosing vulnerability information regarding HP's Tru64 UNIX Operating System. HP claimed that they violated the DMCA. Many in the security industry do not have the financial wherewithal to fight such vendors with bottomless pockets. Fearing the financial burden, many security experts have developed cold feet when it comes to disclosing vulnerability information. Until such statutes are more clearly defined, they do very little to help in the fight to maintain secure systems, in fact they appear to be hampering the effort instead.

The relevance of information security is obvious by the creation of such aforementioned statutes. Unfortunately, because of lack of clarity, some of them appear to be having adverse affects on vulnerability disclosure, including

responsible disclosure. The foundation of the information security legal landscape is set; it is now time to put its integrity to the test.

Summary

In conclusion, the split in the industry over vulnerability disclosure is apparent in the aim of both full disclosure and limited disclosure. This divide can only be overcome if both sides are willing to iron out their differences to discover common ground; that common ground is the best of both worlds approach called responsible vulnerability disclosure. The government's ultimate role is still unclear, but with the added pressures to protect the nations critical infrastructures, there involvement is inevitable. With identity theft slated as one of the fastest growing crimes, statutes to protect information are becoming prevalent. Unfortunately, lack of clarity in some statutes has hindered the forward progress of responsible disclosure. All in all, there is no doubt that responsible disclosure is the best choice when it comes to maintaining an acceptable level of information security, but in order to work effectively, it will require open communications and due diligence on the part of both the software vendors and the vulnerability discoverers.

Citations

Chien, Eric W32.Nimda.A@mm. 7 Feb 2003
URL:
http://securityresponse.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html (1 May 2003)

Christey, Steven M.. "Re: Status of draft-christey-wysopal-vuln-disclosure-00.txt" 27 Dec. 2002
URL: http://www1.ietf.org/mail-archive/ietf/Current/msg18630.html
(27 Apr. 2003)

Christey, Steven M. & Wysopal, Chris "Responsible Vulnerability Disclosure Process." Feb. 2002
URL:
http://www.globecom.net/ietf/draft/draft-christey-wysopal-vuln-disclosure-00.html
(19 Apr. 2003)

Davies, Bryan. "Information Anarchy? One Simple Solution." 27 Feb. 2002
URL: http://www.infosecnews.com/opinion/2002/02/27_02.htm (23 Apr. 2003)

Delio, Michelle "How Much Hack Info Is Too Much?" 19 Nov. 2002
URL: http://www.wired.com/news/infostructure/0,1377,56463,00.html
(16 Apr. 2003)

Fisher, Dennis. "Availability of Patches Stirs Controversy." 25 Nov 2002.
URL: http://www.eweek.com/article2/0,3959,732490,00.asp (23 Apr. 2003)

Fisher, Dennis. "Feds Consider New Security Reporting Role." 11 Nov. 2002
URL: http://www.eweek.com/article2/0,3959,685579,00.asp (23 Apr. 2003)

Fisher, Dennis. "Feds Move to Secure Net." 10 Mar. 2003
URL: http://www.eweek.com/article2/0,3959,922583,00.asp (23 Apr. 2003)

Fisher, Dennis. "Feds Warming to Idea of Regulating Security." 21 Oct. 2002
URL: http://www.eweek.com/article2/0,3959,685622,00.asp (23 Apr. 2003)

Fisher, Dennis "Symantec Defends BugTraq." 7 Apr. 2003
URL: http://www.eweek.com/article2/0,3959,1007560,00.asp (24 Apr. 2003)

Frank, Diane "White House Casting Cyber Nets." 19 Nov. 2001
URL: http://www.fcw.com/fcw/articles/2001/1119/web-board-11-19-01.asp
(3 May 2003)

Gray, Patrick "Security Firm Regrets Samba Disclosure." 8 Apr. 2003
URL: http://news.com.com/2100-1002-995939.html (24 Apr. 2003)

Hulme, George V. "HP Threatens Legal Action Against Security Group."
5 Aug. 2002
URL: http://www.informationweek.com/story/IWK20020802S0033 (4 May 2003)

Jackson, William. "Vendors Battle Over Airing Software Flaws." 16 Dec. 2002
URL: http://www.gcn.com/21_34/security/20634-1.html (23 Apr. 2003)

Lasser, Jon. "Development of Exploits for CVE-2000-0666." 26 Feb. 2001
URL: http://www.sans.org/rr/threats/development.php (14 Apr. 2003)

Lemos, Robert. "CERT's 'Favoritism' Draws Fire." 30 Jan. 2003
URL: http://zdnet.com.com/2100-1105-982663.html (23 Apr. 2003)

Lemos, Robert. "Security Experts Protest Copyright Act." 7 Sep. 2001.
URL: http://in.tech.yahoo.com/010907/22/149vb.html (27 Apr. 2003)

Leyden, John "Show us the bugs - users want full disclosure." 7 Aug. 2002
URL: http://www.theregister.co.uk/content/55/26090.html (23 Apr. 2003)

McWilliams, Brian "Leaked Bug Alerts Cause a Stir." 19 Mar. 2003
URL: http://www.wired.com/news/infostructure/0,1377,58106,00.html
(23 Apr. 2003)

Morgenstern, Michael; Parker, Tom; and Hardy, Scott; "It's Time to be Responsible." 1 Mar. 2002
URL: http://www.securityfocus.com/guest/10711 (23 Apr. 2003)

Morgenstern, Michael; Parker, Tom "The Realities of Disclosure." 12 Jul. 2002
URL: http://www.securityfocus.com/guest/14155 (23 Apr. 2003)

Rauch, Jeremy "The Future of Vulnerability Disclosure?" 8 Dec 1999
URL: http://www.usenix.org/publications/login/1999-11/features/disclosure.html
(23 Apr. 2003)

Roberts, Paul "In Sendmail threat, beginnings of a cyber plan." 4 Mar. 2003
URL: http://www.infoworld.com/article/03/03/04/HNcybersecurity_1.html
(23 Apr. 2003)

Rosencrance, Linda. "Bug-reporting standards proposed to IETF." 22 Feb. 2002
URL:
http://www.computerworld.com/securitytopics/security/story/0,10801,68558,00.html (23 Apr. 2003)

Tauzin, William J. and Dingell, John D. "Evaluation of Critical Infrastructure Protection Information Sharing and Analysis Centers." 7 Mar 2002
URL: http://energycommerce.house.gov/107/letters/03072002_530.htm
(3 May 2003)

Thibodeau, Patrick. "Bill Would Force Companies to Disclose Thefts of Personal Data." 16 Dec. 2002
URL:
http://www.computerworld.com/securitytopics/security/story/0,10801,76768,00.html (4 May 2003)