

Vulnerability Disclosure

Jonathan Arbaugh

Computer Science 116: Introduction to Computer Security

Professor Ming Chow

December 14, 2016

Abstract

Vulnerabilities are found constantly, both in high profile platforms as well as everyday devices. As vulnerabilities are discovered by malicious, benign and hobbyist hackers, corporations, organizations and individuals attempt to defend against them. But, the world is increasingly dependent on software for everyday tasks and procedures with mortal consequences. This reality begs the question - is there a way for the hackers and organizations to work together for the benefit of everyone? There are a number of different opinions as to how vulnerabilities should be disclosed., Some argue for full and immediate disclosure of bugs, others for non disclosure, and others for a “responsible” middle ground approach. This paper discusses the moral and legal justifications of vulnerability disclosure and explores potential policy changes that could encourage a safer software-reliant world.

To The Community

I chose to research the topic of vulnerability disclosure for two reasons. First, I have a genuine curiosity about how the vulnerability ecosystem works. As a user of proprietary products in daily life, an avid consumer of open source projects and a writer of proprietary software, I feel it is important to understand how vulnerabilities are managed currently and possible improvements to improve the vulnerability management system. Second, there have been a number of high profile vulnerability disclosure cases lately that have exposed the moral and legal background for a discussion of vulnerability disclosure. It seems if there was ever a time to study disclosure, now seems apt.. For example, MedSec’s recent disclosure of vulnerabilities in St. Jude Medical’s Cardiac Defibrillator Implant piqued my interest because the case involves several legal and moral complexities of vulnerability disclosure, the likes of which will be explored in this paper.

Terms

In this paper many common terms are used to refer to specific parties, events and items. The following are definitions of the terms used in this paper.

Vulnerability: A flaw or unintended behavior in software or hardware product that can be exploited by someone to gain information or privileges that they are not intended to have.

Researcher: A person conducting research or investigation for themselves or an organization. In this paper, we will consider both funded and unfunded researchers. We will also not assume that a researcher is benevolent. They can most certainly be a malicious party.

Hacker: A person who searches for vulnerabilities in systems for personal satisfaction, to build a reputation or for economic gain. This paper will not focus much on malicious hackers. Instead it will focus primarily on hackers and researchers that want to disclose their discoveries.

Vendor: Any entity that builds and maintains a product used by the public.

Introduction

Vulnerability disclosure describes the act of releasing information about a security vulnerability in a product to the vendor and/or to the general public. Digital products now play a major role in society, handling sensitive data including financial information or personal conversations. Digital products are also used in healthcare, transportation, infrastructure and much more. It is impractically difficult, if not impossible, for people to build perfectly secure software and given the prevalence of all of these products there are, expectedly, many

opportunities to discover vulnerabilities. When researchers discover these vulnerabilities, however, there is no consistent system for reporting vulnerabilities. Even for individual companies it can be confusing, dangerous or frustrating for researchers to report bugs.

There are a number of incentives at play when it comes to vulnerability disclosure. Researchers are often the parties that discover vulnerabilities, but if they do not have an intent to exploit the vulnerability, they will either want credit for finding it or want the general public to know so that the public can make informed decisions about what they do. Vendors, on the other hand, have a different perspective. Vendors value the reputation of their brand and the way their brand is perceived. Since brand perception is important, vendors do not want their customer base to discover that the vendors are building vulnerable products. Vendors also have a fiduciary responsibility to their investors to protect the value of their stock.

Methods of Vulnerability Disclosure

After discovering a vulnerability, researchers are confronted with the problem of what to do next. Depending on the case, the researcher could have knowledge about a vulnerability that could negatively impact millions of users personally or financially. At this point, we will assume that the researcher is benevolent. Later, we will address the malicious researchers. A benevolent researcher, if they do in fact know about a dangerous vulnerability, will want the vendor to patch it as soon as possible to protect the general public. As discussed earlier, we know that vendors may not share the exact same interests. They have budgets that they must adhere to and reputations that they need to protect. So, how do benevolent researchers achieve their goal of disseminating vulnerability information for the betterment of the public's safety? Their strategies can be sorted into three categories: Non-Disclosure, "Responsible" disclosure and Full Disclosure.

Non-Disclosure, as a method for vulnerability disclosure, is aptly named. It involves the researcher choosing to, in essence, keep the vulnerability a secret from both the public and the vendor that maintains the affected product. This can happen for several reasons. First, in this case, the researcher may not be benevolent. By discovering and not disclosing a vulnerability, an individual or organization has the privilege of exploiting a system or product with little time pressure because the vulnerability is unknown to the vendor. The researcher also has the opportunity to sell the knowledge of the exploit to another actor. For this reason, Non-Disclosure is very popular among black-hat hackers - it is essentially the essence of black-hat hacking. Non-Disclosure can happen in non-malicious situations as well, however. For example, a user or researcher may discover a vulnerability and not report it because either they do not realise the severity of it the vulnerability, do not feel it is their responsibility to report it or do not feel that reporting the discovered vulnerability will not lead to any improvement in the product. Unfortunately, due to the nature of Non-Disclosure it is very difficult to measure how often and why it occurs. (Cencini)

In Full Disclosure, researchers will fully disclose the vulnerability to the vendor. They fully disclose the information about the vulnerability they have discovered. In a Full Disclosure scenario, the general public gets access to that information at the same time as the vendor. Researchers also often release proof-of-concept code or more fleshed out pieces of code, "tools", to demonstrate how to find and exploit the vulnerability in question.

Full Disclosure is a controversial approach to vulnerability disclosure with researchers that will argue very passionately on both ends of the spectrum, though vendors are rarely in support of it. Researchers that advocate for Full Disclosure do so to respond to their experiences reporting vulnerabilities to vendors secretly only to see them go unfixed for extended periods of time. By releasing vulnerabilities publicly and immediately, the researchers

afford the vendor no time to distribute patched versions of the software. Researchers do this for three reasons. First, to create public relations nightmare for the vendor. Depending on the product, word of the lack of security can spread across the internet causing concern among users. Second, if the vulnerability info is publicly available, potentially along with proof-of-concept code, then the likelihood of someone exploiting it is much higher as the exploit has become available to people who could not have found it otherwise. Third, some researchers argue that it is of the utmost important for users to know about discovered vulnerabilities immediately so that they can make informed decisions with respect to their online behavior. All three of these reasons, it is claimed by Full Disclosure advocates, encourage or force the vendors to patch the vulnerabilities as quickly as possible, thus improving the security of the product (Schneier) (Peterson).

The most notable drawback to Full Disclosure of vulnerabilities is that it dramatically heightens the risk of a vulnerability being exploited without providing the vendor any time to mitigate the problem. Some vulnerabilities can take weeks or months to release a patch for and depending on the vulnerable system, the patches can take even longer to deploy, which means the systems could be vulnerable to a publicly known exploit for months before being fixed. For this reason, vendors and many researchers strongly oppose this approach.

Because neither one of these approaches arguably solves the problem of vulnerability disclosure, a third form of vulnerability disclosure exists that can be considered a middle ground between Full and Non Disclosure, "Responsible" Disclosure. The goal of Responsible Disclosure is to provide the vendor reasonable time to patch a product before the vulnerability is released publicly, while still preserving some of the urgency of Full Disclosure by attaching a "release date" to the vulnerability information. If a researcher is exercising Responsible Disclosure, then after discovering a vulnerability they will establish contact with the vendor,

provide information about the vulnerability and agree on a deadline for the information to be released. The researcher, or a third party, will then release the vulnerability information on the agreed upon date regardless of whether the vendor has successfully patched the product. Of course, this approach requires the willing cooperation of both parties.

Responsible Disclosure is embraced by vendors such as Google because it allows them to encourage vulnerability research and embrace the attitude of holding vendors accountable for the security of their software, while simultaneously providing them with advanced notice about disclosures so that they can properly protect their systems and products (Application Security – Google). Organizations such as CERT also provide Responsible Disclosure programs for software products in general (Vulnerability Disclosure Policy). There are, however, a few problems with Responsible Disclosure. First, it requires the cooperation of the vendor. In order to engage in Responsible Disclosure, vendors need to have the policies in place, which requires forethought and a commitment on their end. Second, many vendors would prefer that their vulnerabilities are never released, putting researchers that contact them with information into a hard moral situation. Vendors that do not have Responsible Disclosure programs may react poorly to researchers approaching them with the prospect and may threaten to take legal action if the researcher releases the vulnerability.

The Law

The matter of disclosing vulnerabilities is further complicated by ambiguous legal precedents and spotty legislation. According to the Electronic Frontier Foundation (EFF), there are several laws that must be taken into account when disclosing vulnerabilities, regardless of which strategy is used. Those laws (inside the United States) include: The First Amendment of the United States Constitution, Copyright Law, Trade Secret Law, Patent Law, The

Anti-Circumvention Provisions of the DMCA, Contract Law and Criminal Laws including Conspiracy and Aiding and Abetting (Coders' Rights Project Vulnerability Reporting FAQ). Source code and byte code are protected forms of expression under the First Amendment, but those freedoms can be limited when the released proof-of-concept code violates one of the other listed laws. When a researcher releases their findings, especially without consulting the vendor first, these laws and often the ambiguity of these laws, can be used by the vendors in legal action against the researcher. The lack of law that specifically addresses vulnerability disclosure also leaves an enormous amount of ambiguity about what is appropriate on the part of both the researchers and the vendors.

Current Events

One vulnerability disclosure that attracted a lot of attention recently was MedSec's disclosure of vulnerabilities in St. Jude Medical's Cardiac Defibrillator Implant (Gallagher). MedSec, a security firm that specializes in medical devices, released a report detailing that they had found several vulnerabilities in the implant including ways to rapidly drain the battery of the implant, risking the life of the patient. This disclosure was unique for several reasons. First, it highlighted vulnerabilities in a product that people's lives rely on. Second, it was marred with controversy. Before releasing the vulnerability, MedSec partnered with an investment firm, Muddy Waters Capital, to short St. Jude's stock with the expectation that the disclosure would drive down the stock price. It did, and both MedSec and Muddy Waters Capital benefitted greatly. Despite the obvious malice with which this disclosure was done, there are still several important takeaways that can be made. The event was a Full Disclosure, because St. Jude was given no advanced warning and exhibits several problems with Full Disclosure. First, because St. Jude was given no time to evaluate the claims, they were unable to have a statement

prepared or take action in advance. This lack of warning is especially relevant in this case because the claims made by MedSec, while true, are greatly exaggerated, according to St. Jude. This has lead St. Jude to take begin taking legal action against MedSec. St. Jude also expects to lose revenue for several years due to the incident. MedSec's CEO, Justine Bone, has responded to criticism with the arguments often used in favor of Full Disclosure. She has said that fully disclosing the information and shorting the stock was "the only way to spur St. Jude Medical into action", and that "potential and existing patients have a right to know about their risks" (St. Jude Sues MedSec Over Device Security Allegations | SecurityWeek.Com).

Action Items

The debate about what form of vulnerability disclosure is best for society continues, but Responsible Disclosure has both vendor and researchers supporting it and is the only approach that attempts to minimize risk to users and vendors while simultaneously providing vendors with advanced warning and reasonable time to patch systems. It caters to the desire of the researchers to receive credit for their work and allows vendors to encourage disclosure, while still allowing them to stay ahead of the curve. An actionable step that software vendors could take to improve vulnerability disclosure for all is to take the time to implement their own Responsible Disclosure system if they have not already.

The government could also help improve the safety and reliability of consumer products by clarifying ambiguities in laws like Trade Secret law that companies use to intimidate researchers. Additionally, the government could work to pass a law that gives a clear legal structure to Responsible Disclosure. Such a move could give both researchers and vendors more confidence in the process.

Conclusion

Software products are now an essential part of society. Users in the general public entrust them with financial, health and personal information and the vendors that build these products cannot reasonably be expected to build products that have zero vulnerabilities. For the betterment of the general public, there needs to be a more common way for vulnerabilities to be reported and fixed that balances the interests of both researchers and vendors. At this time, Responsible Disclosure is the procedure that can fulfill those requirements. All software companies would do well to implement a Responsible Disclosure program and Responsible Disclosure legislation on the part of the US government would help give confidence to all involved parties.

References

Schneier, Bruce. "Schneier on Security." Blog. N.p., 2007. Web. 14 Dec. 2016.

"Vulnerability Disclosure Policy." Vulnerability Disclosure Policy | Vulnerability Analysis | The CERT Division. N.p., n.d. Web. 14 Dec. 2016.

Andrew Cencini, Kevin Yu, Tony Chan. "Software Vulnerabilities: Full-, Responsible-, and Non-Disclosure." Web. 14 Dec. 2016.

Peterson, Dale G., Jack.t.pierce Says, David_maier Says, Bryan Says, Peck Says, Reid W, and Dale Peterson. "Home." Digital Bonds ICS Security. N.p., 2008. Web. 14 Dec. 2016.

"Coders' Rights Project Vulnerability Reporting FAQ." Electronic Frontier Foundation. N.p., 2015. Web. 14 Dec. 2016.

Gallagher, Sean. "Trading in Stock of Medical Device Paused after Hackers Team with Short Seller." Ars Technica. N.p., 2016. Web. 14 Dec. 2016.

"St. Jude Sues MedSec Over Device Security Allegations | SecurityWeek.Com." St. Jude Sues MedSec Over Device Security Allegations | SecurityWeek.Com. N.p., n.d. Web. 14 Dec. 2016.

"Application Security – Google." Application Security – Google. N.p., n.d. Web. 14 Dec. 2016.