SecurityFocus HOME Guest Feature: The Realities of Disclosure

The Realities of Disclosure
by Michael Morgenstern, Tom Parker (info@globalintersec.com)
Jul 12 2002 3:03PM GMT

Four months ago, we published a SecurityFocus guest feature entitled It's Time to be Responsible (March 1, 2002) calling for greater consensus in the computer security arena on policies of vulnerability disclosure. Since that time little positive movement has occurred, to the detriment of all involved parties. Microsoft's consortium remains a black hole; vulnerabilities (and exploits) continue to be released without control; and everyone suffers - vendors and users included. Thankfully, not all movement has been entirely negative. Unfortunately, Steve Christey and Chris Wysopol's RFC of February 2002 was only tepidly received, despite calling for positive and proactive measures. We surmise that no concrete movement has occurred due mostly to the segregated computer communities and the lack of any consensus on these matters. It is high time the computer cognoscenti finally comes together and advocates responsible disclosure practices.

One of the largest problems confronting such a union remains a lack of understanding regarding the process of vulnerability information release. Prior to Scott Culp's October 2001 essay entitled It's Time to End Information Anarchy, and Microsoft's January 2002 consortium, there were two main models of behavior - that of the security community, and that of the computer underground. Post January there are three models: the BlackHat "Exploitation Model", the Corporate "Limited Disclosure Model", and the GrayHat/White Hat "Responsible Disclosure Model". All three contain components from the following matrix:

Generation 0: Researcher discovers vulnerability
Generation 1: Knowledge passed to the small, tight knit community surrounding the researcher. This could include colleagues, employers, members of any security groups, etc.
Generation 2: Information passes to associates of the Generation 1 community. This stage occurs at a rate determined by the individual characteristics and goals of those who obtain the relevant information
Generation 3: Vulnerability enters the public sphere
Wildcard A: Exploit developed
Wildcard B: Patches and/or work-arounds released

There are several important features of this paradigm. First, not all generations occur in every vulnerability discovery and release. Second, the two wild cards can occur at any stage (in any order) after Generation 0, but do not have to occur at all. There are still many vulnerabilities with no known exploits and conversely, others with no known fixes. Most importantly, growth curves are each unique. Sometimes they can be exponential to a certain degree, but vulnerabilities each have their own rate of propagation, depending on a multitude of factors. All three major models fit into a pyramid shaped metric, with more people having knowledge of a particular vulnerability as time passes.

Exploitation Model

Although Black Hat motivations vary, there are some constants within the computer underground. They value information. And they value "secret" or "private" information above other forms. Such beliefs hold true in the vulnerability/exploit discussion. These motivations lead to faster exploit development and privately held code. They guard their private resources and tend not to divulge the information to untrusted parties. The pyramid structure is very narrow until this stage. Then someone leaks information and/or exploit code to those not seeking to hack and/or those seeking the esteem of going public with the new found knowledge. An individual or firm presents the information to the public. The security community learns about it and the vendors play catch up. Meanwhile, script kiddies go wild with the public exploits and computer users suffer break-ins until patches are available.

The spread metric for the exploitation model generally occurs in the following order: Generation 0, Generation 1, Wildcard A, Generation 2, Generation 3, Wildcard B. When exactly Wildcard A occurs remains fluid; however it almost always materializes before Generation 3 and before Wildcard B. Indeed, the main goal of vulnerability research within the BlackHat community is to develop an exploit before knowledge of the vulnerability becomes public. This allows continued (and many times undetected) roots.

Limited Disclosure Model

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. Microsoft, for example, tends not to follow this track instead purporting to update the issues in their next service pack, or in their next OS. Their agreement carries a 30 day decision period during which the discovering companies are under an information moratorium (disallowing them from even discussing their find). On paper, the agreement looks very similar to the true Responsible Disclosure model. In reality, what truly occurs is a gaping black hole of information, with no market oversight. Indeed, as many of the great free market economists claim, abundant and available information is necessary for market equilibrium. Microsoft solidifies its monopolistic market-share by denying such information to the public. Scott Culp stated plainly: "regardless of whether the remediation takes the form of a patch or a workaround, an administrator doesn't need to know how a vulnerability works in order to understand how to protect against it". In a world of finite development, this might be true. But in our world of continuous vulnerability research and exploit release, administrators do need to understand what they are protecting against so that they do not open themselves up to other forms of attacks by patching against the newest form.

There are many problems with this paradigm. Foremost, it only applies to information discovered by companies signed into the agreement. Other information will continue to be released to the public in an uncontrolled manner - just as it has been for years. Importantly, this still leaves systems vulnerable and open to attack by other's who receive or develop similar vulnerability and exploit code. The spread metric for the limited disclosure model generally occurs in the following order: Generation 0, Generation 1, Wildcard B. Corporate executives hope that Generation 2 is curtailed so that Generation 3 and Wildcard A do not ever occur. This ignores the reality that elsewhere some of the other models may be occurring simultaneously. The bottom line shows that consumers lose. They suffer a lack of control of their computers, a need for continued financial investment in their software (for costly update packages), and a general lack of security in their existing infrastructure.

Responsible Disclosure Model

As is often the case, the middle ground offers benefits to everyone, from the vendors to the end-users. Such a course must enable software companies to create patches by giving them sufficient information about the problem, while also ensuring that the information does not fall into the wrong hands. (See our March 1 article.) 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. Follow the principles of Christey and Wysopol's RFC whether or not you agree with the specifics. When researchers or hackers discover a vulnerability, go to the vendors immediately, before spreading the information around to colleagues. Such action will cause the dissemination pyramid to flatten, shrinking Generations 1 and 2 and protecting the public. Concurrently, the market must hold vendors accountable for their products and boycott insecure software. This will force software companies to focus on security issues.

The spread metric for the responsible disclosure model presents the safest possible path. Immediately after discovery (Generation 0) vendors are notified, allowing for development of Wildcard B. Generations 1, 2, and 3 follow. Whether or not the underground develops an exploit (Wildcard A) remains immaterial provided that users patch their systems promptly. Granted, this is an ideal situation requiring fluid communication and attention to security - an environment that does not currently exist. Pursuit of this model will, however, cause such a structure to begin materializing, as attested by some of the less impacting vulnerabilities that were responsibly released (see Global InterSec's April 25, 2002 advisory regarding a vulnerability in sudo).

We accept that the Responsible Disclosure model is not foolproof. Indeed, opponents argue that often the discovering parties do not give the vendors enough time. Other opponents contend that offering vulnerability information to the public is irresponsible because it fosters the rampant activities of script kiddies. Both of these oppositions are incorrect. If the vendors respond in a positive manner and keep the discoverer informed (perhaps in the future even pay for such information) they will find themselves mainly working with reasonable individuals. Additionally, vulnerabilities do not aid script kiddies. Such individuals require an actual exploit (often with "auto-root" capabilities or a front-end). If Wildcard B precedes all stages after Generation 0, then even when an enterprising hacker creates an exploit, individuals and corporations with up-to-date security programs will be safe - at least from that particular exploit. The most accurate concern is that such a call for responsibility only works if everyone is on board. We contend that bringing everyone together is a step-by-step process. After more computer-using communities have embraced this course (to the detriment of BlackHats and script kiddies) we can all move forward into a relatively more secure and responsible computing age.

Michael Morgenstern and Tom Parker are Principals of Global InterSec LLC and may be reached at info@globalintersec.com.

Works Cited

Christey S., and Wysopal, C. "Responsible Vulnerability Disclosure Practices". Internet Engineering Task Force. February 2002.

Culp, S. "It's Time to End Information Anarchy". Microsoft. October 2001.

Global InterSec Research Team. "Sudo Heap Vulnerability (Password Prompt)". Global InterSec LLC. April 25, 2001.

Morgenstern, M., Parker T., and Hardy, H. "It's Time to be Responsible". SecurityFocusOnline. Guest Editorial. March 1, 2002.