

[Full-Disclosure] Disclosure Debate FW: [ISN] When to Shed Light

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2003-06/0638.html>

From: Jason Coombs (jasonc_at_science.org)

Date: 06/19/03

To: <full-disclosure@lists.netsys.com>, "Isn@Attrition. Org" <isn@attrition.org>

Date: Thu, 19 Jun 2003 08:07:28 -1000

Aloha, Pete and Bill.

I appreciate both of your viewpoints on this subject and find the debate valuable.

Neither of you seem to have made the most important point, so let me add it to the fray:

THERE IS NO SUCH THING AS SECURITY.

Information security, in particular, cannot exist. But all forms of security are figments of the imagination; they are temporary conditions perceived to be "safe enough" in which "bad things" tend not to happen, resulting in a psychological perception of security or "safety". With infosec what we have when we believe we have "security" is a process that never achieves its objective. The moment we stop the process, we stop our security. The fact that there are more black-, white-, and gray-hat hackers (and aspiring script kiddies) banging on more pieces of code is a sign that there are more hands stirring the pot, keeping the process going. Anything other than support for full disclosure results in FEWER hands at work in this process, and therefore LESS security.

There cannot be a technological solution that "cures" the security problem. Both of you seem to imply that you believe there might be, or at least that there *should* be, since we're all really smart and if somebody would just give us venture capital funding surely we could find and build *the cure* as a technology over which our investors could own patent and other intellectual property rights.

Only behavioral change and awareness will cure the disease, and anything other than full disclosure fosters political self-interest that institutionalizes systems that slow down the process of spreading the awareness and knowledge of safe behavior (and safe technology that can be reasonably trustworthy) that are the only defense against the various infosec threats and adversaries.

Full-Disclosure: [Full-Disclosure] Disclosure Debate FW: [ISN] When to Shed Light

You may both be interested to know that I've personally been unable to find a publisher willing to publish my recent book about the challenge of security for administrators and programmers working with IIS/Windows due to the fact that my book is critical of Microsoft's behavior and security-related decisions. Apparently, publishers are unable to publish works that criticize Microsoft because of how dependent publishers are on access to beta software and such for their other authors (and future authors) who write about Microsoft products. Since books about Microsoft products sell better than most technical how-to books, publishers can't risk harming their relationship with Microsoft. In addition, the DMCA has caused publishers including John Wiley & Sons to cancel books that might run afoul of the DMCA and thus create civil or criminal liability for those responsible.

If you want anything other than full disclosure then what you are saying is that you want somebody else to tell you when you are "safe". Good luck, you'll need it.

Sincerely,

Jason Coombs

jasonc@science.org

"IIS Security and Programming Countermeasures"

http://www.forensics.org/IIS_Security_and_Programming_Countermeasures.pdf

-----Original Message-----

From: owner-isn@attrition.org [mailto:owner-isn@attrition.org] On Behalf Of InfoSec News
Sent: Thursday, June 19, 2003 12:05 AM
To: isn@attrition.org
Subject: RE: [ISN] When to Shed Light

Forwarded from: "Bill Scherr IV, GSEC, GCIA" <bschnzl@bigfoot.com>

I couldn't let this pass...

On 18 Jun 2003 at 2:57, InfoSec News wrote:

- > Forwarded from: Pete Lindstrom <petelind@comcast.net>
- >
- > To further my comments in the article:
- >
- > I think actively seeking vulnerabilities is just plain destructive.
- > Sure, if the vulnerability is known we should disclose it, but it
- > never should have gotten to that. I believe there is a lot of faulty
- > logic behind the disclosure phenomenon. For example:
- >
- > 1. We claim that disclosure actually makes our systems stronger/more
- > secure. Of course, if that is the case then Microsoft has the
- > strongest software on the planet and we should be happy to deploy it
- > in our enterprise. Any takers? (By the way, I happen to believe
- > Microsoft gets a bum rap, but use this as a common example of what

- > goes on in the security space.) The whole concept of counting
- > vulnerabilities as a measure of security is bogus – it is an
- > unpopularity contest, nothing more, and doesn't say anything about
- > the software itself. By the way, enterprises have shown time and
- > again that they don't patch their systems anyway, so we can't get
- > more secure this way.

This assumes that the software vendors are the target of disclosure. They are NOT! The folks running their vulnerable systems are the intended audience. The patches / workarounds are meant for them. Yes, OK, the vendors created, and are responsible for fixing the issue, but the admins put it up!

- > 2. The more vulnerabilities we find, the closer we are to "the
- > cure," i.e. some sort of security nirvana where no more
- > vulnerabilities exist in the world. Hmmm, this is a good one. So,
- > count the number of lines of code in existence, then come up with
- > some metric for the number of vulnerabilities in that code (I
- > suspect you could use a very, very low number to be conservative).
- > Now add in the number of lines of code being added to the world's
- > code base every day. Finally, we factor in the number of
- > vulnerabilities found. Are we getting any closer to finding all
- > vulnerabilities in the world? Not a chance. More likely, we are
- > getting further away. That shouldn't further our resolve to try
- > harder, it should make us look at alternatives.

Each vulnerability blasted to every corner of human extent is one less that folks have not been warned about. "Security nirvana" is a journey, not a destination. Which is to say, show me a path where I can customize the machine to my requirements, which includes info-security.

- > 3. If we don't find it, then the bad guys will. This is another one
- > that doesn't work in the "macroeconomics" of the world's code base.
- > Though I can't prove this, I suspect that, given the amount of code
- > in the world, the likelihood of a good guy finding the same hole as
- > a bad guy is probably the same as the likelihood of a collision in a
- > crypto hash – nearing impossible. The most recent WebDAV
- > vulnerability is the only case I am aware of where the vulnerability
- > wasn't known beforehand. So the real question is, how many new
- > exploits would there be if there weren't such a large pool of
- > vulnerabilities to choose from? At the very least, it would reduce a
- > lot of noise out there... (I would love to know about other exploits
- > that occurred with unknown vulnerabilities, and am glad to keep them
- > anonymous).

That would work if the criteria of universal applicability as well as application positioning on public networks was not considered, or considered equal across all lines of code. For instance, IIS vulnerabilities SHOULD be more easily accessible than SQL or NetBIOS vulnerabilities. Again, a little smarts applied to the network

equipment goes a long way. This is particularly why we need to spray vulnerability data everywhere. People need to know what vectors are being attacked.

(Most folks watch their wires with signature based IDSs. These only show known attacks. The good attackers use IDS avoidance techniques and efficient and effective methods. That is one reason why the attacks are still unknown.)

> *I guess what really bothers me are the pretenses under which we
> operate. Those engaged in seeking out new vulnerabilities should
> just go ahead and say that they think it proves they are smarter
> than their competition. Period. It has nothing to do with the common
> good, it has to do with boosting egos and generating revenue.*

Actually it is division of labor. But I suppose I would pay more for a guy who worked side by side with one who finds issues on his own.

> *If consultants really want to spend time on this (honestly, I don't
> understand how companies can absorb the simple cost of it) they
> should be setting up honeypots. I don't advocate honeypots for most
> enterprises, but this would be the perfect fishbowl to really
> determine what was going on 'in the wild.' Setting up a honeypot
> would truly further our understanding of things like likelihood of
> attack, prevalence of attacks, the nature of security on the
> Internet, etc... All great stuff we really have limited information
> on, but what we do have is valuable (thanks, Lance).*

That would be great if there was one organization with a) a view of every network, b) the machines and resources to process it all, and c) a way of synergizing human consciousness to grok and conglomerate the big picture. Right now, none of those exist (and the implications of such are not to be discussed here).

> *There is one other reason that is a bit more difficult to dispense
> with – That we really do this just to 'stick it to the vendor' and
> make them pay the price for having written poor software. In my
> opinion, this seems a bit spiteful and amounts to a pyrrhic victory
> – sure we sock it to 'em, but at what cost? The real loser ends up
> being enterprises.*

>
> *My solution for this one is still a bit sketchy, but let me try. I
> don't advocate software liability because it is too likely to be
> wrong – the old "it's not a bug, it's a feature" cliché would create
> lots of problems, and we only think about Microsoft and not the
> little guys in our argument. I also don't believe we will ever
> completely eradicate vulnerabilities and must therefore come up with
> a new metric to measure 'software risk' (how about person hours per
> vulnerability found?).*

Full-Disclosure: [Full-Disclosure] Disclosure Debate FW: [ISN] When to Shed Light

Caveat Emptor! The Enterprises are responsible for running what they run. Personally , I like netcat for transferring files. Its small, tight, and efficient. Others have this unexplainable attachment to Outlook. It's like parents who put their kids on Ritalin. BUT, I never wished for nor claimed omniscience.

Let the Market decide. It is the best system we (the human race) have devised so far to deal with shoddy products. Yes some folks get hurt in the process. Anyone wanna buy an Edsel?

- > *Instead of software liability, I advocate Material Safety Data*
- > *Sheets for software. In the same way chemical/pharmaceutical*
- > *manufacturers must document the interactions of their chemicals with*
- > *"the world around them," we should have software vendors document*
- > *software interactions with the rest of the operating environment.*
- > *This will ensure that they have completely tested their software and*
- > *provide us with a blueprint to create security profiles in host*
- > *intrusion prevention software. At least then we have a set of*
- > *assertions from the vendor about how their software works. Heck, it*
- > *also sets the stage for demonstrable negligence and fraud in the*
- > *future.*

Hey right! How 'bout putting an evil bit in the IP header!!! Oh wait...
<ftp://ftp.rfc-editor.org/in-notes/rfc3514.txt>

- > *Just some ideas.*
- >
- > *Regards,*
- >
- > *Pete*
- >
- >
- > *Pete Lindstrom, CISSP*
- > *Research Director*
- > *Spire Security, LLC*

My \$0.02... And NOT my employers...

Bill ...

- > -----Original Message-----
- > *From: owner-isn@attrition.org [mailto:owner-isn@attrition.org]*
- > *On Behalf Of InfoSec News*
- > *Sent: Tuesday, June 17, 2003 3:14 AM*
- > *To: isn@attrition.org*
- > *Subject: [ISN] When to Shed Light*
- >
- >
- > <http://www.eweek.com/article2/0,3959,1128749,00.asp>
- >
- > *By Dennis Fisher*

- > June 16, 2003
- >
- > *Until recently, software security vulnerabilities were discovered*
- > *mostly by chance and by developers, security specialists or other*
- > *professionals. Once the flaw was discovered, news about it spread*
- > *slowly and typically by word of mouth on bulletin boards or perhaps*
- > *the occasional security lecture.*
- >
- > *The huge network of security researchers – independent or otherwise*
- > *– who race to find the next big vulnerability in Windows or Apache,*
- > *for example, is a recent phenomenon.*
- >
- > *So, too, are the overlapping and interconnected mailing lists on*
- > *which the researchers publish their vulnerability bulletins. Lists*
- > *such as BugTraq and Full Disclosure were founded to give*
- > *administrators and other IT professionals a place to get early*
- > *information on developing software problems.*
- >
- > *But the amount of publicity and attention security has commanded in*
- > *recent years has brought new, less experienced and less disciplined*
- > *people into the security community. This, in turn, has led to*
- > *vulnerability reports being published before patches are available,*
- > *bulletins being stolen from researchers' computers and posted*
- > *without their knowledge, and a litany of other problems.*
- >
- > *This chaos has led some in the community to question whether*
- > *vulnerability research and disclosure, in its current form, does*
- > *more harm than good. One side of the debate argues that because*
- > *there is essentially an infinite number of potential vulnerabilities*
- > *in software, finding and fixing a handful every year has no effect*
- > *on the overall security landscape. On the other hand, since*
- > *disclosing a vulnerability to the public means that good guys and*
- > *bad guys alike get the information, disclosure can actually cause a*
- > *great deal of damage.*
- >
- > *"The point is not to say that these folks don't have the right to*
- > *disclose anything they want – of course, they do. In fact, we must*
- > *assume that, in general, people are finding vulnerabilities and not*
- > *disclosing them and [that] they can be used against us," said Pete*
- > *Lindstrom, research director at Spire Security LLC, in Malvern, Pa.*
- > *"The point is to demonstrate that those folks that say full*
- > *disclosure is in some way good for us are actually doing more harm*
- > *than good. Just think how much better our security might be if the*
- > *highly skilled people who spend all day, every day, searching for*
- > *vulnerabilities in software would try to design a security*
- > *solution."*
- >
- > [...]

Full-Disclosure – We believe in it.

Full-Disclosure: [Full-Disclosure] Disclosure Debate FW: [ISN] When to Shed Light

Charter: <http://lists.netsys.com/full-disclosure-charter.html>