Law of Vulnerabilities

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

My friend and colleague Jim Reavis contributes the following report on his recent visit to the Black Hat Briefings. Everything below is entirely Jim’s work:

***

The Black Hat Briefings in Las Vegas is one of those security conferences where the piercings and tattoos coexist freely with the suits. This coexistence does not imply unanimity, and this was evident at the most lively session I attended, entitled the Law of Vulnerabilities. However, the contentious debate over software bugs was very educational in illuminating the differences of opinion over software quality and the responsibilities of those who build it.

The Law of Vulnerabilities is the result of a research project conducted by Qualys, a provider of managed vulnerability assessment solutions. It is an attempt to identify statistically significant patterns in real world security vulnerabilities and their corresponding exploits. In theory, identifying these trends can help us understand the window of exposure that is created by vulnerabilities and quantify the associated risk encumbered by our computer networks. The data used for this study came from vulnerability scans conducted by Qualys and was presented by their CTO, Gerhard Eschelbeck. The findings were mined from 1.5 million scans, 1.2 million critical vulnerabilities and 2,041 unique vulnerabilities. Among the “laws” pertaining to vulnerabilities extrapolated from this data were their half-life and lifespan, as well as the availability of exploits. According to Eschelbeck, the half-life of a critical vulnerability is 30 days, meaning that from the time a major bug is announced, it takes a month for half of the systems with that vulnerability to get patched. Another finding stated that when a vulnerability is released, exploits are “in the wild” within 60 days of the release date. In terms of prevalence, 50% of the most popular vulnerabilities change on an annual basis, and some vulnerabilities have been shown to have an unlimited lifespan at this point.

Are these laws immutable? Probably not. Caleb Sima, CTO of SPI Dynamics, an application security software company, attended the session and found the findings interesting. However, the scope of the research probably skewed the results. “This is a fairly small set of vulnerability scan data and by limiting the data to Qualys customers you have a bias in favor of security conscious organizations. My feeling is that a larger and more randomized set of data would show that the real situation is even worse. Most companies will patch vulnerabilities more slowly, increasing the vulnerability half-life”, said Sima, adding, “We also don’t know the breakdown between internal and external IP addresses scanned, which is important because most people have a different standard for how quickly they fix problems. I would also like to see how the results compare between large enterprises and small companies, as well as a breakdown between different system types.” I have to agree with these points, but I like the concept of these laws. While I am certain that more research would change the findings, I hope that this work continues and we get a better idea of what a vulnerability half-life really is.
One thing the session proved was that it is much easier to present research than it is to act upon it. A panel discussion of the findings by security experts was highly contentious. A hacker named Simple Nomad used some colorful language to place the blame for software vulnerabilities squarely upon the software companies themselves. To paraphrase Mr. Nomad, the profit motive causes software companies to continually release software with the qualities of excrement – wrapped in an attractive package to conceal its poor quality. At one point Mr. Nomad mocked Oracle’s “unbreakable” marketing claim after their Chief Security Officer Mary Ann Davidson explained how security is built into Oracle’s software release process. Sima said, “The problem with these hackers is that they are only looking at this from a technical perspective and they tend not to have experience in the business of releasing software. You will never make perfect software - even if you could, you would still have vulnerabilities introduced during installation and configuration. I was impressed by Davidson’s explanation of Oracle’s QA procedures and I think Microsoft has done a decent job at improving the security of their code since they announced the Trustworthy Computing Initiative. It’s a huge job.”

Maybe that is a cultural shift that needs to take place in the security industry. A software vulnerability is not the byproduct of evil software executives, but is in fact a difficult technical and educational problem. I’ll give the last word to Davidson, who got stunned silence with the following call to the hackers in the audience, “Take the energy you have for developing exploits for software and put your creative energies into creating better capabilities for automating secure software development.” Now that’s a law I would like to see.

Jim Reavis <mailto:jim@reavis.org> is the editor of the CSOinformer <http://reavis.org/informer.shtml>, a monthly e-publication with news and interviews about information security. Jim has been instrumental in the launch of several security companies in addition to being the founder of SecurityPortal. Servicing hundreds of thousands of Web visitors monthly in addition to performing over 700 corporate consulting engagements has provided Reavis Consulting Group with insight into the dynamics of the information security marketplace. Their strengths are in understanding of a wide variety of technical, business and social issues, and being able to identify future trends in the information security industry.

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.