Moore's law is a double-edged sword

Lori MacVittie, 2008-07-10

In the good old days when I was in college I had a generic PC. That's the way we did it back then - we built our PCs out of parts (obligatory "you kids don't know how good you have it these days" look). On that PC is something you don't often see today; a small toggle switch that changed the processor clock rate from 4 to 7 MHz. That's right, I said MHz. Not GHz.

That was not *that* long ago in real years, but in technological years it's been a lifetime. As Moore's law correctly predicts, processing power has exponentially doubled every couple of years since then, offering desktop PCs and servers unprecedented power.

What is Moore's law?

Excerpt from Wikipedia:

Moore's law describes an important trend in the history of computer hardware. Since the invention of the integrated circuit in 1958, the number of transistors that can be placed inexpensively on an integrated circuit has increased exponentially, doubling approximately every two years.[1]

In practical terms, this means that the compute resources available on desktops and servers increases with nearly every release of a new processor. These increases mean high capacity servers and faster desktop applications with better performance and more efficient processing overall.

John Emerich Edward Dalberg Acton was the first to observe that absolute power corrupts absolutely and we have come to view this as a nearly philosophical truth. We can easily adapt that truth slightly to reflect the abuse of processing power that has continued to increase over the past few decades. Increasing processor power corrupts increasingly. Or something like that.

While most of us consider the increases in processing power as a mechanism for improving the efficiency of our data centers and allowing us to better serve applications to our customers and other end-users, some folks out there view the increase in processing power as a means to a very bad end.

In the past a DoS (Denial of Service) attack against a web site or application architected for high-volume and stellar performance required the combined processing power of hundreds of PCs. But because Moore's law has held true, today it requires only a handful of PCs in order to take down some of the the most resilient sites on the web.

Attacks coming from even a single machine today can threaten to interrupt service due to the increased processing power available and the admittedly brilliant manipulation of the protocols that make the web work.

Moore's law means that even the simplest of scripts designed to brute force their way into a site or application can be run in hours instead of days, making the likelihood of an attack eventually succeeding increasingly real.

So even while we laud the advances in technology and marvel at our ability to continually improve the processing power available at our fingertips, we need to be ever vigilant and aware of the impact of those improvements on the ability of "the bad guys" to successfully exploit vulnerabilities and the inherent nature of the protocols that make the web work.

Our desire for applications and sites to be as fast as possible is not a bad thing, but it can get in the way of ensuring that those applications and sites are as secure as possible. Moore's law can work to our advantage in that we can increase the security measures we use to thwart such attacks without severely impacting performance. By leveraging the increases in processing power we can apply greater security if we are willing to forego a bit of a performance boost now.

This is the balancing act every CSO and CIO must perform on nearly a daily basis: balancing the need to be secure with the equally important need to be fast and flexible. Moore's law promises that we'll continue to be able to get faster often. But at some point we have to take into consideration that this law is a double-edged sword and just as we're able to do things faster so are "the bad guys". So perhaps applying some of that increase in processing power toward better security would be a much better application of the benefits of Moore's law than simply removing a few microseconds from the response time of an application.

Those few microseconds are not likely to be noticed by an end-user. But a breach in security? Now *that* will get you noticed.

So don't let the double-edge of Moore's law cut you too deeply. Consider how best to leverage the improvements in processing power and think seriously about applying it toward a more secure application infrastructure. Fast is good, but fast *and secure* is better.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com